Analysis of SMS Spam in Mobility Networks
Ilona Murynets, Roger Piqueras Jover

Abstract—The Short Messaging Service (SMS), one of the most successful cellular services, generating millions of dollars in revenue for mobile operators yearly. Current estimations indicate that billions of SMSs are sent every day. Nevertheless, text messaging is becoming a source of customer dissatisfaction due to the rapid surge of messaging abuse activities. Although spam is a well-tackled problem in the email world, SMS spam experiences a yearly growth larger than 500%. In this paper we expand our previous analysis on SMS spam traffic from a tier-1 cellular operator presented in [1], aiming to highlight the main characteristics of such messaging fraud activity. Communication patterns of spammers are compared to those of legitimate cell-phone users and Machine to Machine (M2M) connected appliances. The results indicate that M2M systems exhibit communication profiles similar to spammers, which could mislead spam filters. We find the main geographical sources of messaging abuse in the US. We also find evidence of spammer mobility, voice and data traffic resembling the behavior of legitimate customers. Finally, we include new findings on the invariance of the main characteristics of spam messages and spammers over time. Also, we present results that indicate a clear device reuse strategy in SMS spam activities.

1. Introduction

For the past two decades, the Short Messaging Service (SMS) has gained tremendous popularity throughout the world. Reports estimate billions of text messages handled daily by cellular providers’ messaging infrastructures [20], generating millions of dollars of yearly revenue [8]. Being unquestionably successful, text messaging is steadily becoming an annoyance due to the surge of SMS fraudulent activities [17], such as spam and the spreading of malware two of the main examples.

Spam is the widely adopted name to refer to unwanted messages that are massively sent to a large number of recipients. This kind of messaging abuse is a well-known and tackled problem in the context of electronic mail (e-mail). Numerous applications detect and block spam e-mails daily resulting in a small amount of spam reaching customer’s inboxes and it is common nowadays to have anti-spam engines integrated into e-mail services. These anti-e-mail spam services are very effective, especially given the estimates indicating that 90% of the daily electronic mail traversing the Internet is spam [4].

In the context of text messaging abuse, the trend has rapidly increased with the introduction of unlimited messaging plans, which provide a new cost-effective platform to fraudsters. Current studies estimate mobile SMS spam to be experiencing a steady yearly growth larger than 500% [9]. Effective anti-abuse messaging filters are being deployed, sparing networks from spam text messages injected into cellular networks from the Internet. However, content-based algorithms used to detect e-mail spam, are less efficient in the case of SMS spam [11]. The length of an SMS is limited to only 160 characters [24] and customers often use acronyms, pruned spellings and emoticons which mislead detection algorithms. Thus, mobile originated SMS spam still remains a problem for cellular networks.

Spammers connect USB cellular modems and cell-phones to personal computers (PCs). These simple low-cost set-ups allow them to send thousands of spam messages every day, mostly using pre-paid SIM (Subscriber Identity Module) cards combined with unlimited messaging plans.

The defense against message abuse often relies on SIM shutdowns and subsequent account cancellations. However, as our results support, this does not stop most spammers, though, who purchase multiple cards and swap them to limit the daily per-SIM volume [9]. Message abusers also rapidly replace canceled SIM cards to continue their spam campaigns.

Millions of illegitimate text messages are transmitted via cellular networks daily [17]. These messages consume network resources that could be allocated to legitimate services otherwise. SMS spam results also in a major inconvenience for cellular customers because, without an unlimited plan, the end user is paying at a per received message basis. Therefore, SMS spam potentially generates unwanted bill charges for some users leading to negative messaging experience and customer dissatisfaction. Spam also exposes smartphone users to attacks. Often multiple fraudulent messaging activities such as phishing, identity theft and fraud [26] are related to SMS spam. SMS is also known as an entry vector for malware propagation [16].

In this paper we expand our analysis in [1] on the characteristics and communication patterns of SMS
spammers. The analysis is based on mining SMS, Voice and IP network traffic from a tier-1 network operator in the United States. The behavior of over 9000 positively identified and known spammers is analyzed and compared to legitimate cell-phone users and embedded Machine to Machine (M2M) appliances. An extra set of positively identified and canceled spamming accounts is included in the analysis to investigate potential changes in spamming behavior over time. Some M2M communication systems exhibit a behavior that closely resembles in some aspects that of an SMS spammer, which could potentially mislead spam detection algorithms.

The results of this investigation have been used to develop an advanced SMS spam detection engine, the details of which are out of the scope of this paper.

The analysis herein presented highlights expected features from message abusers, such as large loads of sent text messages to long target lists. Nevertheless, some other unexpected and very interested findings are made, being expanded from the analysis in [1]. For example, the vast majority of spammers utilize just five different models of hardware to send the messages and this list has barely changed since the publication of the first results in [1]. Some of these devices are very popular feature phones that are re-flashed to be used as cellular modem. Moreover, we identify a clear device reuse of message abusers who, upon an account shutdown event, simply swap the canceled SIM for a new one and continue spamming using the same piece of hardware.

In terms of traffic, spammers appear to make a large number of phone calls, of very short duration, perhaps to mislead detection schemes that might discard accounts with a near-human voice communication profile. We also find the main geographical hot-spots (sources) of messaging abuse activities in the US, which have been constant over the last year, and that some spammers launch very geographically targeted campaigns.

Beyond the results presented in [1], this paper expands our dive into SMS spam with the following contributions:

- analyze certain behavior and strategy change of spammers over six months.
- analyze the content of the spam messages and identify certain common spamming campaigns.
- identify the device reuse of spamming tools after account cancelation.

The rest of the paper is organized as follows. Section 2 describes the three data sets under analysis (SMS spammers, legitimate users and M2M systems) and how they are labeled. Section 3 presents the data analysis of the spam network traffic and message content. Section 4 introduces the analysis on the changes in spamming characteristics over long periods of time and Section 5 overviews and new technique of messaging abuse. In Section 6 we give some introductory comments on an SMS spam detection engine that has been designed based on the data analysis in this paper. Section 7 discusses the related work. Finally, the study is concluded with the closing remarks in Section 8.

2. Data Set

The analysis presented in this paper is based on traffic data provided by a tier-1 cellular operator in the United States. The data sample contains Call Detail Records (CDR) of 9000 spammer accounts and almost 17000 legitimate accounts. This last set includes about 7000 Machine to Machine devices and 10000 post-paid family plans, from the one year period between March 2011 and February 2012. Finally, we add an extra sample of spammer accounts from August 2012. This new sample allows exploring the potential changes in spamming behavior of message abusers that might have occurred over six months.

CDRs are records logging each phone call, text message and data exchange in the network. If two communicating ends belong to the same provider, a duple of records is stored. The Mobile Originated (MO) record logs data of the transmitting party, while the Mobile Terminated (MT) one stores information of the receiver. Note that the MO and the MT records for the same transaction contain duplicated data, such as the originating number and the terminating number. IP (Internet Protocol) data traffic generates only MO logs.

Table 1 summarizes the CDR fields used in our analysis. The originating and terminating phone numbers are fully anonymized and only the first 8 digits of the International Mobile Equipment Identity (IMEI) are parsed, discarding individual serial numbers. This first portion of the device identifier, known as the Type Allocation Code (TAC), determines the manufacturer and model of the wireless device. In the case of a phone, the TAC indicates the manufacturer and model of the phone itself (e.g. Nokia Lumia 900) and, in the case of an M2M connected device, the TAC identifies the embedded cellular modem (e.g. Sierra Wireless Q2687).

The spammer data set is obtained as follows. A list of...
positively identified spamming accounts and their cancelation dates were provided by the Fraud Department of the cellular operator. The Fraud Department maintains a constantly updated white-list of known legitimate sources of large loads of text messages (i.e. Twitter, American Idol alerts, etc) so they are never confused with spam. Therefore, this data set contains exclusively spammer accounts that were positively identified and disconnected from the network.

The legitimate account data set is obtained in two steps. First legitimate user accounts are selected and then legitimate M2M appliances are classified and included to the set. Our analysis of spammer accounts revealed that 99.64% of spammers have prepaid plans.

Therefore, the set of legitimate customers is drawn from a random and geographically uniform sample of post-paid family plan accounts, which are highly unlikely to be used by a spammer. This way we minimize the probability of having an unknown spammer mislabeled as legitimate. In parallel, M2M connected appliances are identified by the TAC and extracted from the operator's list of M2M approved devices. This is a database of the M2M devices that have been selected, tested and approved to operate on the provider's cellular network.

The M2M devices include connected appliances running all kinds of services. Some applications found in our data set are asset tracking, remote medical monitoring, security monitoring, Automatic Teller Machines and smart grid power meters. We discard, though, approved M2M systems with a Universal Serial Bus (USB) port because these could be used to send illegitimate messages if plugged to a spammer's computer.

Message abusing accounts stay alive for a short period of time (see Section 3.A), therefore we collected CDR records for spammer accounts for one week prior to cancelation. For each legitimate account we collected data for a random week between March 2011 and February 2012.

From the CDR data fields we extract multiple features that characterize customer communication patterns. For example, based on the time stamp of each MO SMS (and MO call) we calculate the intervals between two consecutive outgoing messages (and phone calls) and the number of outgoing messages (calls) per day. Based on the time stamps of MT SMSs (MT calls) we calculate the average number of MT messages (calls) per day. The response ratio is computed combining the average number of MO and MT messages (calls) per day. The terminating number field for SMS and voice traffic, also anonymized, is used to calculate the number of individual recipients and the
number of different terminating area codes per day. From uplink and downlink byte counts we compute aggregated data usage per week.

Geo-location data is extracted from the CDR records. The coordinates of the serving base station are recorded each time an SMS is transmitted. MO records contain the coordinates of the tower receiving the message in the uplink, whereas the MT record lists the base station delivering the SMS in the downlink. Based on this data fields, the location of a device can be estimated with an accuracy equivalent to the size of a cell or sector. If two communicating devices are connected to the same operator, we know approximate locations of both the sender and the receiver.

Finally, we extract samples of spam message content from the Cloudmark SMS spam reporting platform [2].

3. SMS spam analysis

This section describes the analysis of confirmed SMS spammer accounts that were canceled due to messaging abuse activities. The study compares communication patterns of spammers to those of legitimate customers, both cell-phone users and M2M devices.

In all the figures throughout the paper, legitimate cell-phone users, M2M systems and spammers are represented in green, blue and red, respectively. All results are normalized, including only aggregated results.

The analysis is organized in five subsections. We start with Subsection 3.A, which briefly describes the characteristics of the accounts of message abusers. Subsection 3.B investigates the SMS spam traffic in general and Subsection 3.C studies the location information of both spammers and their targets. In Subsection 3.D we investigate the mobility of spammers. Subsection 3.E discusses tools used in messaging abuse and Subsection 3.F investigates the reuse of these tools by spammers. Voice and data traffic are investigated in Subsection 3.G. Finally, in Section 3.H we introduce results on the analysis of the content of SMS spam messages reported to the 7726 service.

A. Spammer account information

Detailed analysis of Call Detail Records indicates that the great majority of spammers (99.64%) are using pre-paid accounts. As the GSMA Messaging Anti-Abuse Working Group investigated [9], spammers purchase bulk SIM cards with unlimited messaging plans. These SIM cards are constantly switched to circumvent detection schemes and reduce the number of messages sent per day. Also they discard them once an account is canceled and continue spamming with a new one.

The average age of an illegitimate account is 7 to 11 days. This indicates that message abuse accounts are canceled rapidly on average. The account age of a legitimate user is often several months to a couple years.

B. SMS messaging patterns

Figure 1-a and b compare the empirical histograms for the number of text messages sent and received by legitimate accounts, M2M and spammers. Intuitively, spammers generate a large load of messages. The number of spam SMSSs is two orders of magnitude higher than that of legitimate user text messages and one order of magnitude above the number of messages from networked appliances.

Spammers not only send but also receive two orders of magnitude more messages than legitimate customers do. Although this behavior is, at first, unexpected, it can be explained by the nature of SMS spam messages. Upon reception of an unrequested text message, users sometimes attempt to reply to opt-out from the advertised service. Furthermore, actual spam messages often attempt to trick the recipient into replying to the message (Figure 1). Despite a small percentage of users will reply, the large amount of accounts targeted in a spam campaign results in many responses.

Figure 1-c, which plots the distribution of the number of destinations, shows that legitimate accounts have a small set of recipients. Cell-phone users text on average to 7 contacts per day, while spammers hit a couple of thousand victims each day.

The ratio of the number of recipients to the number of messages, shown in Figure 1-d, provides an additional insight. On average, spammers send one message to each victim. Legitimate users send multiple messages to a small set of destinations. For this specific feature, M2M appliances display a mixed distribution. Some devices send many messages to a small set of destinations while others transmit one single message to each destination. It is important to note that such M2M systems could be miss-labeled as message abusers by simple spam filters.

1) Response ratio: In this subsection we investigate the ratio between the number of received and transmitted messages (response ratio). Although spammers receive a lot of messages, the response ratio is very different to that of a legitimate user. Figure 3 plots an example for a randomly
selected spammer and legitimate user (with a post-paid family plan). The number of messages is equally normalized in both cases.

In the case of legitimate users, generally messages are sent in response to a previous message in a sequential way. Therefore, the response ratio is close to 1. For spammers the amount of MT SMSs is proportionally very small to the number of transmitted messages. Therefore, the response ratio is close to 0.

2) SMS spam message timing: This sub-section investigates timing characteristics of spam messages. Due to the large load of SMSs, the intervals between two consecutive messages are short. On the other hand, legitimate users and M2M message less frequently. This can be observed in Figure 4-a, which shows the distribution of the intervals between two sequential messages.

Figure 4 b plots the distribution of the inter-message time entropy. Usually, spammers send messages at a constant rate using a computer. Legitimate users are less predictable. One cannot accurately estimate when the next text message will be sent given the time of the previous one. Inter-SMS intervals for spammers are less random resulting in low entropy values. On the other hand, intervals between two legitimate messages are random, with higher entropy.

Messaging activities of certain M2M devices have a pre-scheduled nature. For example, smart grid meters report measurements periodically. Other applications, such as parking meters and ATMs, have communications initiated by humans. A message is sent each time a parking receipt is issued. Therefore, we observe a large number of M2M connected devices with a low value of the entropy, overlapping with spammers, and some with a higher value of the entropy, overlapping with legitimate users.

C. Geographic originations and destinations of spam

The next step of our analysis is to determine the geographical distribution of messaging abuse. We aim to find out where spammers base their activities and where the
targets of such SMS traffic are located.

Figure 5 shows the locations of accounts identified for messaging abuse activities during the one year period under analysis. Location data is displayed on a map of the counties of the United States. Yellow, orange and red counties indicate the presence of a message abuser, with red indicating the most intense spamming hot-spots.

Our data indicates that spammers are mainly located in California, specifically in the counties of Sacramento and Orange and in the surroundings of Los Angeles. Other notable sources of spam are observed in the New York/New Jersey/Long Island areas and in Miami Beach. Smaller sources of messaging abuse are found in Illinois, Michigan, North Carolina and Texas. Note that this does not imply that spam will always come from only these areas, but gives an indication of the non-uniform origin of SMS spam messages. Messaging abuse in the SMS world appears to originate from a few locations over the US.

In Section 4 we expand the spamming hot-spots analysis by identifying the constant and new main areas of message abuse originations after 6 months.

Figure 6-a and Figure 6-b show the recipients of SMS messages sent out in one day by a randomly selected spammer and legitimate customer respectively. Each map plots the source (spammer or legitimate user) with a pin and individual recipients with a diamond. Note that we only have location information for customers (recipients) subscribed to the cellular operator under analysis. The legitimate customer communicates only with a small number of contacts. Most of the recipients for the given user belong to the local area (i.e. the area around the subscriber's home) as well as several other locations (e.g. areas where the subscriber works, used to live or where friends and relatives reside). In contrast, the recipients of spam text messages appear to be distributed uniformly over the US population (the spammer sends messages to most area codes).

Figure 8-a plots the distribution of the number of unique area codes contacted in one day by spammers, legitimate customers and M2M systems. Spammers are characterized by messaging a large number of area codes, always greater than those of cell-phone users and M2M. We observe, though, a small amount of spammers contacting a reduced number of area codes. Most M2M devices contact numbers just within one area code.

Independent of the number of unique area codes, it is interesting to know how often these area codes are contacted. Figure 8-b plots the entropy of these area codes. In this context, entropy stands for the randomness of the connections in one day. A low value of the entropy implies that this specific user contacts repeatedly the same area codes. On the other hand, a high value of the entropy indicates a user that sends messages to a more random set of area codes.

Network enabled appliances report to specific servers and data collectors or, in the case of user applications (i.e. home monitoring), to a predefined set of cell-phones. Therefore, the entropy is the lowest. Spammers show a
much more random set of SMS abuse targets with high entropy. Further analysis of the spam data identifies a messaging strategy that consists of messaging numbers in ascendent order. Thus, sending bulk SMSs to each area code sequentially.

The aforementioned results are summarized in Figure 8-c, which plots the correlation between the number of sent messages and the number of recipients. The linear relation in the case of SMS spammers is obvious. Both M2M systems and cell-phone users cluster around the bottom-left area of the graph. One can notice in the figure some M2M appliances sending up to 20000 messages to 1 single destination. This is a common situation in, for example, security or monitoring M2M applications in which reports are timely sent to a controlling server. Shipping couriers implement similar services that gather messages around one specific destination in order to, for example, track a fleet of delivery trucks.

The relation between the ratio (number of message recipients)/(number of messages sent) and the average number of area codes reached by day is plotted in Figure 8-d. Cell-phone users congregate at the bottom left of the Figure, with low destinations-to-messages ratio and a small set of contacted area codes. A great majority of spammers exhibit the opposite behavior, clustering on the top-right corner of the figure. Nevertheless, a substantial number of spammers with a different behavior is identified.

The spammers aggregated on the bottom-right corner of Figure 8-d are message abusers that target very specific geographical regions. These accounts still send thousands of messages per day with a ratio close to one destination per message. However, the number of targeted area codes is in the range of the number of recipients from legitimate cell-phone users.

D. Mobility of spammers

In this subsection we attempt to determine whether spammers are mobile or not. In terms of mobility, one expects spammers to not move. Therefore, all messages should be handled by one single base station. Figure 7 plots the distribution of the number of base stations (Location Area Code - Cell ID, LACCI) a device is connected to in one day. Legitimate customers display a highly mobile behavior, with most of the users visiting at most 30 cells sectors. This number depends on many factors, such as the length of the daily commute. The distribution exhibits a long tail with a minority of highly mobile cell-phone users.

Spammers, as expected, are much less mobile. They still appear to traverse an average of about 4 cells or sectors. This might be due to the following reasons. On one hand, spammers might mount their equipment on a vehicle and drive around the area in an attempt to misguide detection schemes looking at device mobility. On the other hand, especially in the case of aircards, the hardware often connects to the network by means of a Third Generation (3G) technology. 3G wireless networks in the operator under study are based on Wideband Code Multiple Division Access (WCDMA). In such technology, the receiver can be physically connected to up to 6 sectors at the same time, combining the signal at the RAKE receiver [23]. Depending on the channel conditions and fading, the serving base station might fluctuate throughout this list of 6 LACCs. This would result in CDR records from the same static device appearing to come from up to 6 different sectors.

Note that, though, based on the IMEI, we are able to determine the actual hardware used by the spammer to send messages. In the case of GSM devices, a cell-phone or cellular modem is at all time connected to, at most, one cell tower [7]. Camping on base stations miles away from each other definitively indicates movement.

The distribution of recipients' area codes for M2M is mixed. The majority of appliances are quasi-static, with most of their messaging load being handled by a couple of sectors. This corresponds to non-mobility M2M applications such as alarms and smart grid readers. Another large set of devices are highly mobile, with an average of 28 sectors visited per day. In this case, these are mobile applications such as fleet control/monitoring and asset tracking.

The final answer to the question is found in Figure 9, which plots the observed locations of a randomly chosen spammer on the map of an undisclosed area. The legend indicates the length on the map that corresponds to 1 mile and 2km. Based on this information, it seems that certain spammers move while sending illegitimate SMSs. In the case of the example, this spammer is observed in the
vicinity of cell sites as far as 4 miles apart. Computing the longest distance between the cell sites on which every spammer in our database camps on indicates a maximum displacement of 15 miles in the case of the most mobile message abusers.

83% of the spammers identified in one year use one of the top five identified devices. About 65% of the spammers in the US send messages with the top device.

Devices used by spammers are anonymized and ranked based on their usage. The top 5 cellular USB modems and feature phones most frequently used by spammers are listed as follows.

- USB Modem/Aircard A1
- USB Modem/Aircard A2
- Feature mobile-phone M1
- USB Modem/Aircard A3
- Feature mobile-phone M2

Thus spammers often rely on modems and aircards connected to a PC via USB interface. A1, A2 and A3 belong to this category. In parallel, spammers also use common feature phones as cellular modem. This might be done in order to mislead detection schemes by making messages appear to be originated at a legitimate cell-phone. Several resources can be found online with detailed instructions on how to re-flash typical feature phones from most manufacturers with custom firmware [3], [6], [5].

Note that these devices are legitimate hardware that spammers use for SMS abuse. All of them are used in

E. SMS transmission tools used by spammers

Observing of the IMEI from the CDRs gives us an insight on the kind of device used to connect to the cellular network. Analyzing the TAC data from known and already canceled spamming accounts, we observe that an impressive
Ilona Murynets et al.: Analysis of SMS Spam on Mobility Networks.

It is interesting to note that the spam traffic analysis indicates that at least 16% of the SMS traffic originated by all the A1 modems in the network is spam. This shows a clear preference of spammers for this particular cellular modem.

F. Device reuse

Further analysis of the anonymized IMEI data indicates devise usage characteristics that are common to spammers. As already discussed in Section 1, spammers get a hold of numerous SIM cards and swap them once they are detected and their account is canceled due to messaging abuse. This results in a generalized pattern of numerous SIM cards being sequentially used on the same hardware.

This behavior can be observed in Figure 10, which plots the normalized number of spam messages sent from one single spamming IMEI during a period of two months. In this specific example, 5 different SIM cards are observed, which are used in sequence. The number of messages sent by the IMEI in the figure is normalized by the same value as Figure 3. This is done to avoid displaying the load of messages sent by individual spammers.

It is interesting to note that the total number of positively identified and cancelled spamming accounts from our data set maps to a much smaller set of individual IMEIs. We observe a ratio of 10 different SIM cards per IMEI.

Moreover, a query of anonymized network data from the list of spamming IMEIs between March 2011 and February 2012 indicates that a majority of these cellular modems and feature phones were still being used for spamming purposes during the summer of 2012. A large number of SIM cards were active in August of 2012 on some of those devices generating large loads of messages.

G. Voice and IP traffic analysis

As observed in the previous sections, SMS spammers attempt to reach as many targets as possible by flooding large amounts of messages. This paper focuses on SMS spam analysis. Nevertheless, we include voice and IP traffic data in our study and the results are rather interesting. Spammers do generate both data and voice traffic, perhaps to increase the chances to go undetected through spam filters that search for non human-like communication traffic or perhaps other forms of fraud.

1) Voice calls: Figure 11-a and Figure 11-b plot the empirical histograms of the number of phone calls and their recipients. Figure 11-c corresponds to the empirical histogram of the duration of voice calls. On average, spammers make many more phone calls than legitimate users, however the average number of phone call destinations is much lower (Figure 11-a and Figure 11-b). This number of phone calls could perhaps indicate that they are trying to mimic legitimate users. In terms of voice traffic duration, phone calls placed by spammers are much shorter than those of legitimate users, as it can be observed on Figure 11-c. This is because, despite they seem to attempt to match the calling profile of a legitimate user, these calls cannot be sustained for a long time since the recipient will hang up. The short call duration could also indicate that these calls might be spam as well. Most of the times, the recipient of a spam call will hang up immediately.

Unlike in SMS traffic, spammers do not flood with calls a large number of recipients. They might be communicating with a small set of numbers that they know will pick up the call even though they might hang up quickly.

The results are further detailed in Figure 12. The difference in behavior of spammers is highly accentuated in this figure, which plots the average number of SMS destinations (x-axis) against the number of voice call destinations (y-axis). Spammers appear to be placing phone calls to a set of recipients that is much smaller than the set of targets for the text message abuse. This figure also hints that legitimate users, on average, tend to communicate to a larger set of contacts by phone than by text message. This could be explained based on the fact that cell-phone users

Figure 9: Example of observed locations for one spammer

Figure 10: Normalized number of messages sent by a spamming IMEI
rely on the extremely popular SMS service to communicate with friends and relatives. However, phone calls are made to this same set of users plus other contacts such as restaurants to make a reservation, the doctor’s office to make an appointment, etc. Therefore, the set of call recipients will be larger than for SMSs.

more bandwidth in the downlink, by browsing videos, media and other kinds of content. Their uplink traffic is generally lower. M2M appliances have the opposite behavior. Used mostly as reporting tools for applications such as remote alarm and fleet control, they often generate a larger load in the uplink.

2) IP traffic: Finally, we examine IP traffic. Figure 13 plots the distribution of the up-link (a) and down-link (b) byte counts related to the three account categories under analysis. Spammers generate a small amount of data, consisting of several small transactions.

Cell-phone users and M2M systems generate asymmetric IP data traffic. Regular users often consume

It is not clear why spammers generate IP traffic. One possibility would be that the fraudsters are attempting to mislead spam filters by generating network behavior close to that of a legitimate user.

H. SMS spam message content
An analysis of the content of SMS spam messages is performed over data extracted from the Cloudmark 7726 service [2].

The main observation extracted is that message abusers launch very specific spam campaigns that originate from a set of spamming hot spots. In other words, spam messages coming from one given location, and hence most likely from the same fraudster ring, belong to a specific campaign.

<table>
<thead>
<tr>
<th>Origin</th>
<th>Message content example</th>
</tr>
</thead>
<tbody>
<tr>
<td>West Coast</td>
<td>Are you having a hard time paying your mortgage? Do you need help restructuring the mortgage to get a lower payment? If so reply HELP. To cancel reply STOP.</td>
</tr>
<tr>
<td></td>
<td>Having a hard time paying your Mortgage? Need help lowering your mortgage payment? Get an Interest Rate as low as 2% Fixed. If so reply HELP. To cancel reply STOP.</td>
</tr>
<tr>
<td></td>
<td>$200 to $1500 in just one hour is now available for you at <a href="http://WWW.XXXXXXXXXXX.COM">WWW.XXXXXXXXXXX.COM</a> - If you wish no further contact please txt back QUIT.</td>
</tr>
<tr>
<td>South East</td>
<td>Hiring in your Area! Secret Shoppers Needed Make up to $50/hr Call 8xxxxxxxxx Now. Reply STOP for DNC.</td>
</tr>
<tr>
<td></td>
<td>Hiring in your Area! Secret Shoppers Needed Make up to $50/hr Call 8xxxxxxxxx Now. Reply stop4optout.</td>
</tr>
<tr>
<td></td>
<td>Apple is looking for Iphone 5 testers! The first 1000 users that go to <a href="http://xxxxxxxxxx.com">http://xxxxxxxxxx.com</a> and enter code: 1459 will get to test &amp; keep the Iphone 5</td>
</tr>
</tbody>
</table>

For example, most of the spammers on the West Coast send messages with content mainly related to mortgage and loan fraud. On the other hand, spam messages originating in the South East belong to hiring fraud campaigns and also often contain links to websites claiming to give away Apple products for free. Note that this last case is probably an
Ilona Murynets et al.: Analysis of SMS Spam on Mobility Networks.

International Journal Publishers Group (IJPG) ©

attempt to lure victims into malicious web site to download infected applications or unwillingly sign up for premium rate services.

Table 2 shows an example of message content coming from hot-spots in the West Coast and the South East. Note that URLs and phone numbers have been omitted in purpose.

4. Spammer behavioral long term change

In this section we aim to investigate whether spammers vary their message abuse activity substantially over long periods of time.

Re-generating certain features from our analysis indicates that spammers are generally following the same patterns investigated in Section 3. However, there is a new player in the SMS spamming ecosystem, which is briefly described in Section 5.

New hot-spots are observed appearing in Ohio, Wisconsin and Texas.

As introduced in Section 3.F, message abusers reuse the hardware to inject messages into the cellular network. Moreover, as discussed in Section 3.E, message abusers exhibit a clear preference for a small set of cellular modems and feature phones. Figure 14 plots the top 5 devices used by spammers in the period under analysis (March 2011 to February 2012) and for the months of July and August of 2012. One can observe the sustained preference of spammers for the first two devices (USB Modem/Aircard A1 and A2) and a series of common feature phones and cellular modems being used less consistently.

As stated in Section 3.F, we observed an average of 10 SIM cards per device (IMEI) over one year. The same analysis indicates that the frequency of device reuse has substantially increased. During August 2012, each spamming device utilized an average of 5 SIM cards. These results seem to suggest two things. On one hand, SMS spam detection and mitigation techniques have improved, reducing the reaction time to cancel an abusing account. On the other hand, device reuse is clearly a widespread technique among SMS spammers.

5. New spamming techniques

The majority of SMS spam that originates in the mobility network is injected by cellular devices owned and controlled by the message abusers. However, new spamming techniques are starting to gain momentum in the message abuse ecosystem.

A recent report from Lookout identified a new mobile threat (SpamSoldier) that turns legitimate smart phones into members of a large spamming bot-net [28]. A malicious application infects phones and connects them to a command and control server, which instructs the malicious payload on what spam message to send and to what destinations.

Figure 15 plots an example of the messaging behaviour of legitimate customers who, unknowingly, were part of this spamming botnet. The amount of messages sent by each victim in the example is normalized by the same value as in Figure 4 and Figure 10.

Each legitimate user in the example transmits a few messages per day, which is standard messaging behaviour.
for legitimate users. However, one can clearly observe the instant of time when the smart phone was infected, which generated an increase in order of magnitudes of the MO load of text messages. Note that this kind of infection could result in customer dissatisfaction, especially in the case of legitimate users with no unlimited messaging plan and those victims receiving replies to the spam messages.

The new message spamming technique described in Section 5 is very challenging for spam detection and mitigation engines. In this case, the spam messages originate at a device that, in parallel, behaves as a legitimate user. Also, upon a theoretical detection, the cellular provider cannot proceed normally and shutdown the SIM card. However, there are certain features that would allow distinguishing a spammer from a legitimate customer infected by SpamSoldier, such as the account age.

In this context, the authors of [29] introduce an algorithm for anomaly detection in M2M systems over cellular networks that could potentially detect such changes in network behaviour from devices belonging to the spamming bot-net. The mitigation side, though very complex, could be approached by remotely detecting and blocking the malicious app responsible for generating the spam traffic. Such effort could be achieved by the malware mitigation scheme presented in [30].

7. Related work

SMS spam had not been widely discussed in the literature but is gaining some momentum as new advanced detection techniques and analyses are introduced. To the best of our knowledge, the first specific and detailed analysis of SMS spam was introduced in [1], the results of which are expanded in this paper.

In parallel, there is some work introducing different detection schemes. For example, the authors of [25] propose a detection engine based on analysing the social network of connections of spammers. Other approaches are based on investigating the content of SMS spam messages [13].

There is plenty of literature on spam messaging analysis on other communication systems. The most widespread type of spam is electronic mail (email) spam. In this context, [18] presents interesting findings on how message abusers harvest large lists of email addresses to use as targets for their spam campaigns. The authors of [19] study the network-level behaviour of spammers in the email world. Email messaging abuse is found to originate from a very few regions of the IP address space. These messages are generated from an immense swarm of bots, each one of them sending only a few pieces of mail over very short periods of time. It is interesting to note that this somehow correlates with the SMS spam world where, based on our data analysis in Section 3, messages are originated from a few geographic hot-spots and by accounts with a very short tenure. Based on the findings in [19], the authors of [27] proposed an algorithm to detect and track bot-nets based on email spam records.

Email spam has been a known problem for many years and there is already plenty of work proposing advanced detection schemes. For example, the authors of [14] study the effectiveness of DNS blacklisting and [11] presents a survey of known spam filtering techniques with particular emphasis on how well they work.

There is also some work analysing other kinds of spam and messaging abuse. For example, [15] studies the traffic characteristics of tweet spam and propaganda.
(tweet) abuse is generated by a small amount of players that generate large amounts of messages, most of which appear to be retweets, in short periods of time. Other interesting works analyse messaging abuse and spam in the context of YouTube comments [21] and the blogosphere [22]. Finally, the authors of [10] study the risk of sophisticated context-aware spam that could result from information sharing on social networks.

8. Conclusions

In this paper we expand our analysis on SMS spam data presented in [1]. We investigate the characteristics and traffic patterns of SMS spam accounts based on real cellular network from a tier-1 provider in the United States. The results are compared against a sample of real traffic from legitimate cell-phone users and M2M devices.

Our analysis confirmed certain common intuitions about spammers, such as the large number of text messages sent per day to a wide target list. Spammers generate two orders of magnitude more messages than cell-phone users and one order of magnitude greater than most M2M systems. Data analysis indicates that spammers also receive a large number of messages, which is still very low with respect to the number of transmitted spam texts. Spammers often trick recipients into replying as a useful way to check whether a number in the hit-list is a valid spam recipient.

Our traffic analysis indicates that certain networked appliances have messaging behaviour close to that of a spammer. A small number of M2M systems transmit a large number of SMSs per day. Based on the investigation in this paper, we identify Machine to Machine communications as an important player in SMS networks. Such systems should be taken into consideration when designing SMS spam detection and filtering schemes. Systems designed otherwise could incur the risk of blocking or erroneously labelling legitimate text messages as message abuse.

The expanded analysis indicates that spammers have sustained preference for a very small set of hardware devices. Spam traffic analysis reveals that 84% of the spammers use one of the top 5 spamming tools in the US. In particular, 65% of the spammers choose to connect to the network with the top device. The top used spamming devices remain very similar over long periods of time, confirming the clear preference of message abusers specially for the top two cellular devices.

The study of geo-location data identified the areas of Sacramento, Los Angeles-Orange County and Miami Beach as the major spamming hot-spots in the US. Over long periods of time, these appear to still be among the main originating areas of spam, with the appearance of some new hot-spots in Florida, Wisconsin and Texas. In terms of mobility, our analysis indicates that spammers are often mobile around their local area.

The results presented in this paper are being used to design an advanced SMS spam detection system.

Acknowledgment

The authors would like to thank Cheri Kerstetter, Rick Becker, Joel Casey, Jeff Bickford and Alex Bobotek for their help, comments and valuable suggestions.

References


Ilona Murynets is a scientist at the Chief Security Office at AT&T. She obtained her Ph.D. in Systems Engineering at School of Systems and Enterprises, Stevens Institute of Technology. Her dissertation received an Outstanding Dissertation Award. Ilona holds B.Sc. degree in Mathematics and M.S. degree in Statistics and Financial & Actuarial Mathematics from Kiev National Taras Shevchenko University, Ukraine. Ilona’s research is in the area of data mining, optimization and statistical analysis in application to malware propagation, spam detection, mobile and network security.

Roger Piqueras Jover is a Member of Technical Staff at the AT&T Security Research Center. He graduated from the Escola Tècnica Superior d’Enginyeria de Telecomunicacions de Barcelona (ETSETB) in 2006 with the degree of Telecommunications Engineer. That same year he was awarded a Balsells Fellowship to pursue graduate studies in Electrical Engineering at the University of California in Irvine, where he graduated in 2008 with an MSc in Electrical and Computer Engineering. In 2010 he graduated with an MPhil/MSc in Electrical Engineering from Columbia University. His research interests are in the area of mobile and wireless communications, radio resource allocation, new network architectures and security for wireless networks.