Understanding the Time-series Behavioral Characteristics of Evolutionally Advanced Email Spammers

Yukiko Sawaya
KDDI R&D Laboratories, Inc.
2-1-15 Ohara Fujimino-Shi
Saitama 356-8502, Japan
+81-49-278-7560
yu-sawaya@kddilabs.jp

Ayumu Kubota
KDDI R&D Laboratories, Inc.
2-1-15 Ohara Fujimino-Shi
Saitama 356-8502, Japan
+81-49-278-7898
kubota@kddilabs.jp

Akira Yamada
KDDI Corporation
3-10-10 Iidabashi Chiyoda-ku
Tokyo 102-8460, Japan
+81-80-5944-9980
ai-yamada@kddi.com

ABSTRACT
There are many anti-spam techniques available today. However, spammers evolve mass mailing techniques in order to circumvent these countermeasures. One example of such evolutionally advanced spammers is observed in email services offered by Japanese mobile phone service providers. Because they have been enforcing very strict anti-spam filters, commonly used mass mailing techniques such as spam botnets are becoming less effective, and spammers thus have to evolve their technologies. In order to understand such evolutionally advanced spam-sending hosts' behaviors, we collected and analyzed their traffic flow data retrieved at a backbone network in the real commercial network of one of the largest mobile phone service providers in Japan, which has over 30 million customers. In this paper, we first show that many of the existing anti-spam techniques are not effective against advanced spammers, and then reveal that such advanced spammers have distinctive time-series behavioral characteristics that have the potential to be exploited in developing new mitigation techniques and predicting their behavior in the future.

Categories and Subject Descriptors
D.4.6 [Security and Protection]: Invasive software (e.g., viruses, worms, Trojan horses); G.3 [Probability and Statistics]: Statistical computing

General Terms
Algorithms, Security

Keywords
Spammer, Mobile Email Services, Time-series Behavior, Clustering, X-means Algorithm

1. INTRODUCTION
Email service is widely used by Internet users. Typically in Japan, mobile phone service providers offer email services and people usually use mobile phone email (which we call "MPE") services on their feature phones or smart phones rather than email services offered by third-party providers such as Gmail [1] or Hotmail [2]. MPE service providers offer spam filters similarly to third-party email services. A difference between them is that spam filters offered by MPE services have the strict option of dropping such email messages whose email addresses are spoofed, listed in blacklists defined by users, and so on. Moreover, the Japanese government has suggested that Internet service providers (ISPs) should apply Outbound Port 25 Blocking (OP25B) [3], which blocks access to port 25 from dynamic IP addresses on their own networks. As a result, commonly used mass mailing techniques such as spam botnets become less effective, and spammers have thus been evolving techniques in order to pass such filters.

In order to understand such evolutionally advanced spam-sending hosts' behaviors, we collected and analyzed their traffic flow data retrieved at a backbone network in the real commercial network of one of the largest mobile phone service providers in Japan, which has over 30 million customers. In this paper, we first show that many existing anti-spam techniques are not effective against evolutionally advanced spammers, and then reveal that such advanced spammers have distinctive time-series behavioral characteristics that have the potential to be exploited in developing new mitigation techniques and predicting their behavior in the future. To the best of our knowledge, neither analysis of such evolutionally advanced spammers nor a time series of their behaviors has been studied before.

In order to perform time-series behavioral analysis, we first collect spam messages received by accounts that never receive legitimate messages. We then collect a time series of the sending patterns of each spam-sending host from the backbone routers for one week to extract their entire spamming activities at MPE service and to categorize these patterns into arbitrary clusters by an unsupervised machine-learning algorithm, i.e., X-means [4].

According to our analysis, we observed typical behaviors of evolutionally advanced spammers: (1) sending spam at a specific time period and then stopping sending, (2) periodically repeatedly sending spam messages and then stopping spamming at some specific time in a day, and (3) sending spam messages continuously. We also found that some spammers used different organizations to send spam messages and that some organizations played the role of spam-sending agent. Moreover, we revealed that many spam-sending hosts do not change their behavior even in the future. From these results, analyzing the time-series behaviors of spam-sending hosts can be an important part of predicting the future behaviors of spammers as well as the relationships among them.

This approach will be a countermeasure detecting not only MPE spam-sending hosts but also spam messages if spammers targeting non-MPE services change their strategies when the current detection techniques are widely and strictly used in the future.

AISec'12, October 19, 2012, Raleigh, North Carolina, USA.

2. RELATED WORKS

2.1 Spam Mitigation Techniques

A huge number of spam detection and mitigation techniques have been proposed. Among them, the following spam detection and mitigation techniques are widely used at enterprise networks or ISP networks.

2.1.1 OP25B

OP25B is an anti-spam ISP measure by which the ISP checks the IP address and the port number of all accesses through its routers and blocks access to port 25 from dynamic IP addresses on its network. Access to port 25 on an ISP's mail server from the static IP address of their customers is allowed, while access to port 25 from the dynamic IP address of their customers is blocked. By using this method, spam messages sent from the customers of the ISP controlled by botnet is blocked and as a result, the outgoing spam mail from the ISP is blocked. This method is quite efficient if all the ISPs apply it, but incoming spam mails cannot be blocked.

Typically in Japan, the government suggested that ISPs use this technique and as a result, the spam mails sent from botnet-controlled hosts in Japan have decreased, but spam messages from ISPs that do not apply this technique or spam messages sent from Japanese static IP addresses are still transmitted.

2.1.2 Content filters

Content filters are widely used at enterprise email servers. One of these techniques, SpamAssassin [5], is a program released under the Apache License 2.0 used for email spam filtering based on content-matching rules. SpamAssassin also uses a variety of spam detection techniques, which includes DNS-based and fuzzy-checksum-based spam detection, Bayesian filtering, external programs, blacklists, and online databases. It is used widely in personal usage as well as enterprise usage.

2.1.3 SPF/Sender-ID

Spammers often spoof their own mail addresses to hide their real identities. The Sender Policy Framework (SPF) [6] is an email validation system designed to prevent email spam by detecting email address spoofing, a common vulnerability, by verifying sender IP addresses. SPF allows administrators to specify which hosts are allowed to send mail from a given domain by creating a specific SPF record (or text record) in DNS. Mail exchangers use the DNS to check that mail from a given domain is being sent by a host sanctioned by that domain's administrators. Sender-ID [7] is a technique similar to SPF. SPF verifies the email addresses of the mail-from header in the SMTP envelope, while Sender-ID verifies the email address in the email header instead.

2.1.4 DNSBL

DNSBL such as [8, 9] is a common approach to detect spam mail by determining spam-sending hosts. DNSBLs, which are provided by international nonprofit organizations or security product companies, operate a list of spam senders' IP addresses, and SMTP servers block mail according to this list. DNSBL is often used as indicator of spam messages by content filters such as SpamAssassin. Although this method is efficient for well-known spam-sending hosts, it is not efficient for unknown or new spam-sending hosts.

2.1.5 S25R

S25R [10] is a method whereby SMTP servers determine whether the SMTP client seems to be an end-user of the ISP network. This method is based on the fact that spammers send spam mail directly from end-users' computers, which are infected by bots, while legitimate mail senders use the mail servers that are operated by the ISPs. They use the character string features of the hostname obtained by querying the DNS reverse lookup of IP addresses. For example, if the hostnames of SMTP clients include "dhcp," "dialup," or "ppp," or have a lot of numbers, which are often seen in end-host names, they are determined to be spam-sending clients. It also determines clients that have no hostname to be spam senders.

As many false positives occur by using this method, it is usually used with the other techniques.

2.2 Spammer Analysis

There are several reports on spammer behavior analysis. Husna et al. showed that the relationship among spammers demonstrates highly clustering structures based on features such as content length, time of arrival, frequency of email, active time, inter-arrival time, and content type [11]. They performed Principal Component Analysis (PCA) on a feature set to identify the features that account for the maximum variance in spamming patterns. Further, they calculated the proximity between different spammers and classified them into various groups and showed that each group represented similar proximity. For classification into botnet groups, they used clustering algorithms such as Hierarchical and K-means. They identify botnet spammers into a particular group with a precision of 90%.

Tang et al. built such systems that extracted email senders' behavior data based on global sending distribution, analyzed them, and assigned a value of trust to each IP address sending email messages [12]. They analyzed the performance of two commonly used data-mining techniques: Support Vector Machines (SVM) and Random Forests (RF). Inputs to both models are sending behavior collected from sensors in real time. These systems returned IP addresses' reputation scores as outputs, and the effectiveness and efficiency of classification modeling were then empirically analyzed.

Revealing spam-sending patterns by using features such as the traffic volume, frequency, and time is reported as described above and some studies are detecting automated activities in other areas (e.g., [13]). But neither analysis of time-series sending patterns of spam nor analysis of such evolutionally advanced spam-sending hosts has yet been reported.

3. ANALYSIS OF MPE SPAM

In this section, we describe the differences between MPE messages and other non-MPE email messages, i.e., spam messages targeting non-mobile ISPs. We then apply the previous spam detection techniques to evaluate whether they are effective in detecting MPE spam messages.

3.1 Country Statistics of MPE Spam

We describe the difference in country distribution of spam messages between MPE spam and non-MPE spam. A total of 30,839 spam messages were retrieved at 18 Japanese MPE accounts from March 1, 2011 to March 31, 2012.

Figure 1 shows the country distribution of hosts sending spam to MPE services. We used the mapping table of IP addresses and countries provided by [14]. According to reference [15], the top three countries sending spam messages to both MPE and non-MPE accounts in Japan are China, the United States, and Japan, while Japan, the United States, and the Philippines are listed as

the top three countries sending spam messages to MPE accounts. This difference indicates that Filipino providers are used quite frequently for sending spam messages to MPE accounts. Over 50% of spam messages were sent from Japanese hosts, i.e., almost all of them were not bot-controlled hosts (see Section 2.1.1).

3.2 Evaluation of Existing Methods

We evaluated whether the previous techniques are efficient in detecting MPE spams as well as non-MPE spams. We tested four techniques: content filter, SPF, DNSBL, and S25R.

3.2.1 Content filter

We evaluated customized SpamAssassin, which detects spam messages written in Japanese as well as in English. This filter detected all of the spam messages received at one non-MPE account (zero false negatives) with a few false positives (0.4%) during the period from August 1, 2011 to June 6, 2012. We applied this filter to 1,417 spam messages received at one MPE account from May 17 to May 21, 2012. The results showed that 836 false negative spam messages were observed. We found that almost all of these messages were about online social networking services including friendly terms to mimic acquaintances. Although these MPE spam messages were written in Japanese as were the non-MPE spam messages, this filter did not work well. Therefore, the contents of MPE spam messages are quite different from those received at non-MPE accounts and are rarely identified as spam by content filters.

3.2.2 SPF

We applied SPF to 35,383 spam messages retrieved at 18 MPE accounts from March 1, 2011 to March 31, 2012. Figure 2 shows the distribution of SPF authentication results. Over 50% were determined as "Pass." This means that they did not spoof their source email addresses and registered SPF records to mimic a legitimate sender. On the other hand, the non-MPE spam messages discussed in Section 3.2.1 did not contain such "Pass" messages. From these results, SPF is less useful for MPE spam messages.

3.2.3 DNSBL

We evaluated two DNSBLs of IP addresses in the 35,383 messages retrieved at 18 MPE accounts from March 1, 2011 to March 31, 2012. Spamhaus Zen [8] DNSBL detected 50.0% of spam messages, whereas Barracuda Central [9] detected only 17.8% of them. The result of Zen DNSBL was lower than 85.0%, which is the rate reported in the whitepaper of Spamhaus [16] for non-MPE messages. This result shows that MPE spammers are either using clean IP addresses that have never been used for sending spam before or narrowing down their target to specific email accounts. For these reasons, DNSBL does not show high performance for MPE spam messages.

3.2.4 S25R

We performed S25R techniques for 35,383 spam messages retrieved at 18 MPE accounts from March 1, 2011 to March 31, 2012.

S25R detected only 71.4% of all spam-sending hosts. From a report of S25R sites, it detected 98.5% of non-MPE spam messages with many false positives [10]. As we mentioned before, many MPE spam messages do not come from botnet-controlled hosts, so it is difficult to identify MPE spam messages by S25R, which focuses on detecting botnet-controlled hosts.

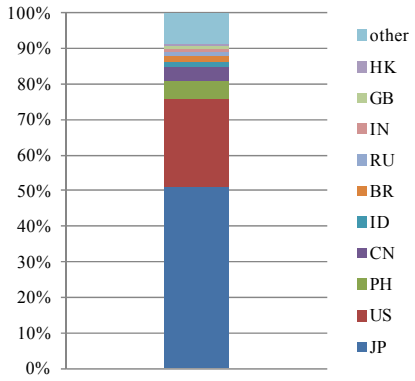


Figure 1. Country distribution of MPE spam messages.

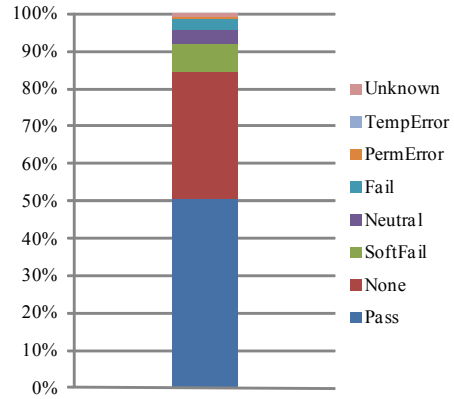


Figure 2. SPF query result of MPE spam messages.

4. BEHAVIORAL ANALYSIS OF MPE SPAM

According to our preliminary evaluation, we found that different spam-sending hosts showed similar time-series behavior, even if previous techniques such as DNSBL and content filters find such behavior difficult to handle. Therefore, we focused on the time-series spam-sending behaviors of MPE spam-sending hosts.

4.1 Experimental Environments

We describe the experimental conditions. Figure 3 shows our experimental environment. Two types of logs are collected: MPE spam messages and traffic flow data.

MPE spam messages are collected at 18 MPE accounts that receive only spam messages, called decoy accounts. These accounts receive approximately 1,000 spam messages per day on average.

The traffic flow data is collected with NetFlow [17] and sFlow [18] at the core routers in a mobile phone service provider's network in which MPE traffic is observed. The traffic data contains the following information:

- Source IP addresses
- Data sizes (packets, bytes)
- Timestamps

Technically, we can collect raw traffic flow data at a flow collector and analyze it directly. However, according to the law of the secrecy of communication in Japan [19], hosts related to the traffic data should be anonymized before we evaluate the data.

4.2 Sending Pattern of Spammers

We analyzed the time-series sending patterns in a specific time period. The following subsections describe the analysis process in detail.

4.2.1 Extracting behaviors

For extracting behaviors of spam-sending hosts, we applied the process as shown in Figure 4. Each behavior is extracted by the following four steps.

(1) First, unique IP addresses during specific time period D from time T, i.e., between the time T and $T+D$, are extracted from messages received at decoy accounts and identified as known spam-sending hosts.

(2) Next, all the traffic flow data sent from the known spam-sending hosts retrieved between time T and $T+D$ are extracted. Not only the traffic destined for decoy accounts but also for other MPE accounts from known spammers is extracted. The hourly behaviors of each host h, x_{hk}, are then extracted from the traffic flow data by the following equation as shown in Figure 5.

$$x_{hk} = \begin{cases} 1 & \text{if host } h \text{ was sending messages during the period between } k \text{ and } k+1 \\ 0 & \text{otherwise} \end{cases} \quad (1),$$

where k is the hours elapsed from time T ($0 \le k < D$).

The behavior vector of each host h during period D, $\boldsymbol{X_h}$, is defined as:

$$\boldsymbol{X_h} = \langle x_{h0}, x_{h1}, \ldots, x_{hD-1} \rangle \quad (2).$$

(3) Then, the MPE spam-sending hosts' properties are retrieved before anonymization. DNSBL query results, S25R results verified by DNS reverse lookup, and the organization names for the corporation of each host from Whois query are collected.

(4) Finally, the IP addresses and Whois information of known spam-sending hosts are anonymized while keeping their correspondences. The one-way hash function is applied.

4.2.2 Clustering behaviors

As hosts have various kinds of behaviors, we categorized the MPE spam-sending hosts into multiple clusters using the clustering technique to understand the behavioral proximities and relationships among the spam-sending hosts. We used the X-means algorithm for clustering spam behavior vectors $\boldsymbol{X_h}$. X-means is extended K-means for estimating the number of clusters, and the number of clusters is not necessary.

4.2.3 Result of clustering

We collected the spam-sending hosts from decoy accounts and their traffic flow data. T and D were March 15, 2012 19:00 and one week, respectively. We collected 2,695 spam-sending hosts' behaviors. Then these spam-sending hosts were clustered into multiple clusters.

The number of clusters was 31. The entire behaviors are described in Appendix 1, and Figure 6 shows a typical example of the

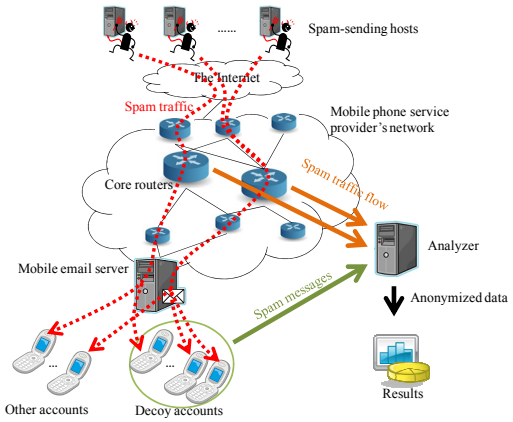


Figure 3. Experimental environment.

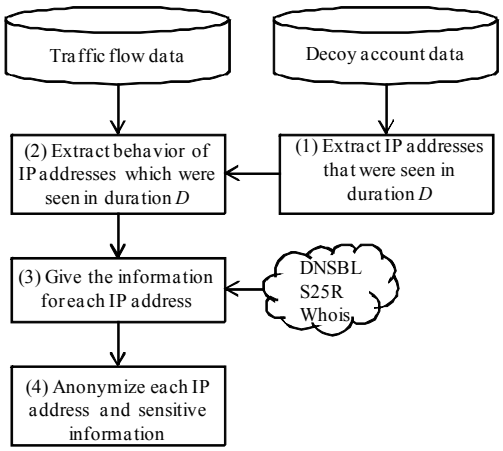


Figure 4. Process overview.

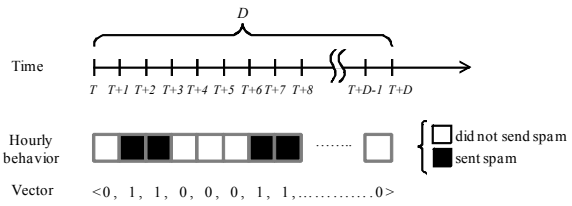


Figure 5. Behavior extraction for each host.

characteristic patterns of spam-sending hosts. The clustering technique worked effectively since hosts in each cluster start sending spam and stop sending at similar timings and seem to exhibit similar behaviors, and when we re-run this algorithm for the same dataset, we could obtain similar clusters as described in Appendix A.1. We found three typical patterns. The spam-sending hosts in Cluster 17, 19, 20, 21, 22, and 23 were sending spam at a specific time period and then stopped sending, which we call **burst behavior**. Cluster 11 and 28 periodically repeated sending spam messages and stopped at some specific time in each day, which we call **cyclic behavior**. The hosts clustered into Cluster 1, 2, 3, 5, and 6 were sending spam messages

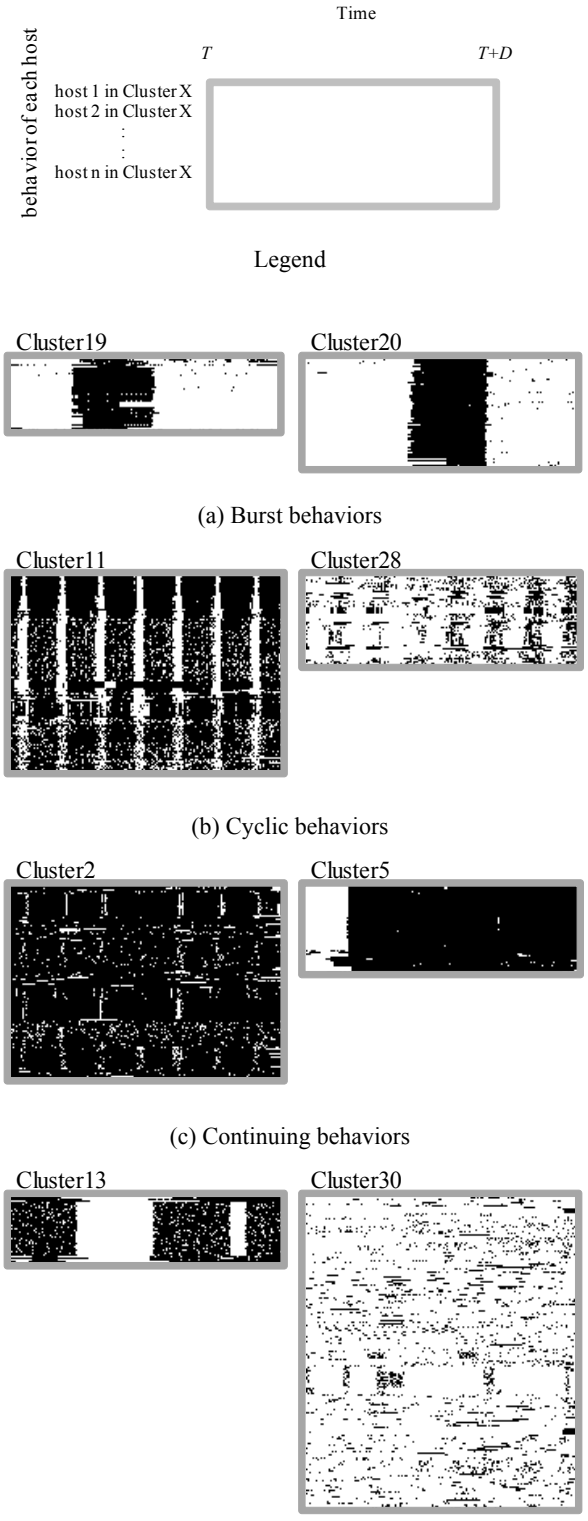


Figure 6. Behaviors of spam-sending hosts (excerpt).

continuously, which we call **continuing behavior**. The other behaviors do not seem to have specific characteristics and were sending randomly or sending at specific intervals in a week. From these results, there is a potentiality that the hosts clustered into the same cluster use a similar spam-sending program.

4.2.4 Properties of clusters

Figure 7 shows the percentage of hosts listed in DNSBL for each cluster. On the x-axis, clusters whose behaviors were "burst," "cyclic," and "continuing" are denoted as prefixes (α), (β), and (γ) respectively. A relatively small number of hosts in Cluster 3, 5, 6, 8, 9, 17, 20, 21, 22, and 25 were listed in DNSBL. These clusters have burst, continuing, and other behaviors, and no cyclic behaviors. On the other hand, many hosts that had cyclic behaviors (Cluster 11 and 28) were listed in DNSBL at a high rate. This result seems to show that the hosts whose behaviors were cyclic frequently appeared and as a result, they were listed in DNSBL. Hosts in some clusters of continuing behaviors such as Cluster 5 and 6 were scarcely sending spam messages at time *T*, but started sending spam messages in duration *D*. Since a relatively small number of them were listed in DNSBL, this result indicates that they were new spam-sending hosts that had not sent spam messages before the time we observed.

Figure 8 shows the distributions of the top five organizations that frequently appeared in 2,695 hosts for each cluster. Over half of the hosts in Cluster 5, 9, and 13 were single organizations of the top five. On the other hand, the top five spam-sending organizations seldom appeared in the other clusters. We examined all the distributions of organizations in these clusters. The hosts in the other clusters diverged into multiple organizations. This result indicates that many spam-sending hosts in different organizations or countries have the same sending patterns and that some spammers in the background use different organizations to send spam messages and some organizations play the role of spam-sending agent.

Organization A was observed the most in Cluster 13. Almost all the hosts in Cluster 13 sent and stopped sending spam simultaneously. However, this organization was observed at many other clusters whose patterns were different. From this result, this organization has many different types of spammers or one spammer changes their behavior. Organization C was observed in Cluster 5 at a high rate. Cluster 5 has continuing behavior and a small number of the hosts were listed in DNSBL. For these reasons, Organization C is suspected of being an organization whose IP addresses are not often used for spam-sending activities and at this moment, they have started to send many spam messages.

Figure 9 shows the distributions of the top 10 countries that frequently appeared in 2,695 hosts for each cluster. The small number of hosts in Cluster 10 came from the top 10 countries. We looked deeply at the countries of these hosts in this cluster and found that 21 countries were observed. Since they send and stop sending spam messages at same time, and the organizations in Cluster 10 were multiple as mentioned before, we observed that spammers in the background are sending spam messages using multiple organizations in different countries.

4.2.5 Behaviors of the next one week

We tracked the next one-week behavior for each cluster by Step (2), Section 4.2.1. The entire behaviors are described in Appendix A.2, and Figure 10 shows a typical example of the results. A total of 16 of 31 clusters (Cluster 1, 2, 3, 5, 6, 9, 10, 11, 14, 18, 19, 20, 22, 28, 30, and 31) did not change their behavior. Cluster 5 and 6, i.e., continuing behavior, also kept sending spam messages. Neither did the cyclic behavior change even in the next week.

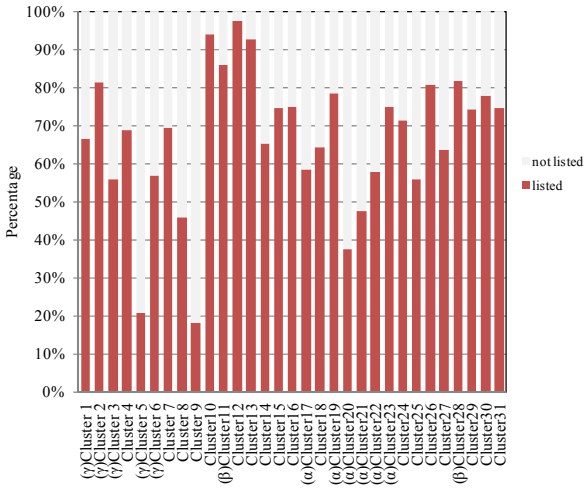


Figure 7. Ratio of DNSBL-listed hosts of each cluster.

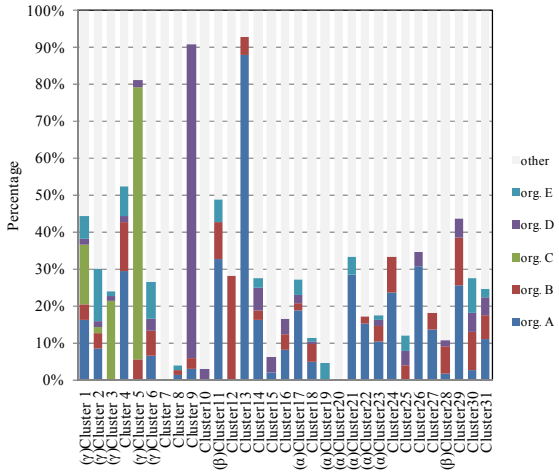


Figure 8. Ratio of spammers' organizations of each cluster.

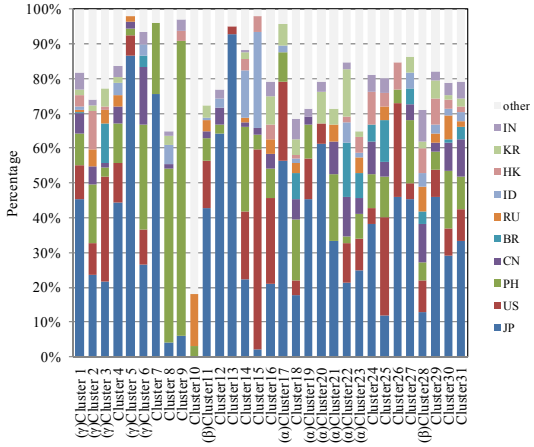


Figure 9. Ratio of spammers' locations of each cluster.

Cluster 19, 20, and 22, and a portion of Cluster 17, 21, and 23 did not change their burst behaviors even in the next week. Cluster 1, 30, and 31 were the biggest three clusters and also continued similar behaviors as in the previous one week.

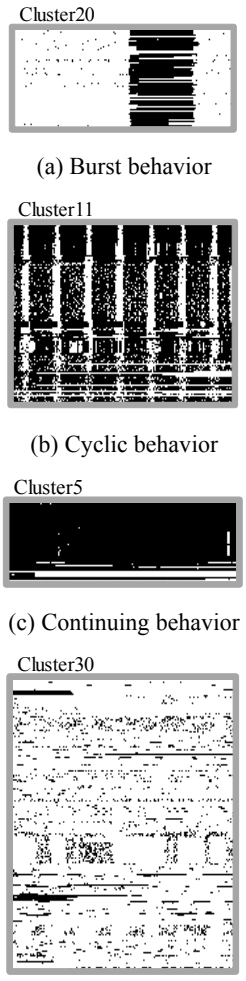


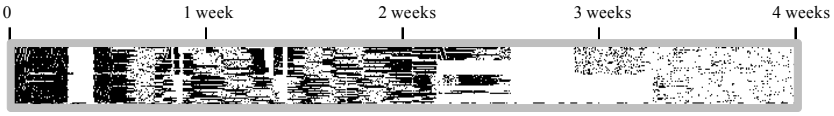
Figure 10. Behaviors of spam-sending hosts of the next 1 week (excerpt).

5. DISCUSSION

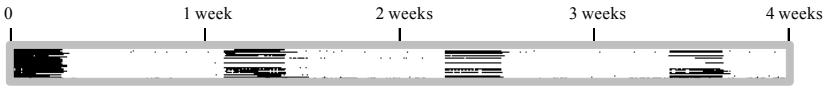
According to the result of Section 3, we showed that MPE spam messages are quite different from non-MPE spam messages and that the previous techniques are not effective. However, in Section 4, we found three typical spam-sending activities and discovered that they maintained similar behaviors into the future.

5.1 Behaviors over a Longer Duration

We analyzed the clusters that did not have these three behaviors in detail. Cluster 16, whose behavior did not fit into our three categories, was stopping sending messages gradually. We examined these behaviors in the next week and found that they scarcely sent spam messages in the next week. From this result, though we did not see any clear patterns of the spam-sending hosts, we can predict their future behaviors by observing the tendencies of the past. We also analyzed the behaviors of Cluster 7 and 26 for the next four weeks in order to see whether they have periodicity or a clear tendency over a longer duration. Figure 11 shows their behaviors. In four weeks, the hosts in Cluster 7 sent messages and stopped concurrently after the first week and gradually stopped during the next week, and finally, they sent



(a) Cluster 7



(b) Cluster 26

Figure 11. Four-week behavior of Cluster 7 and Cluster 26.

messages randomly. The hosts in Cluster 26 repeated burst behavior multiple times, which shows that they behave cyclically with an eight-day cycle. From these results, if we employ our clustering technique for the longer term, we will be able to discover the tendency and periodicity of hosts that cannot be observed in a shorter period of time.

5.2 Behavior Comparison with other Messages

In order to evaluate whether the three behaviors shown in Section 4 are unique to evolutionally advanced spam-sending hosts or not, we applied our clustering technique to 13,221 spam-sending hosts targeting non-MPE accounts retrieved at our enterprise network from May 17, 2012 19:00 to May 24, 2012 18:59. Only two clusters were created: one was a cluster of continuing behavior (similar to Cluster 1 in Appendix A.1) and the other was random sending hosts cluster (similar to Cluster 30 and 31 in Appendix A.1). We also evaluated it for 1,186 legitimate hosts for non-MPE accounts. Three clusters were created and all of them were random behaviors similar to Cluster 30 in Appendix A.1. These results indicate that the three behaviors were unique to MPE spam-sending hosts. This seems to result from the fact that evolutionally advanced spam-sending hosts deliberate their sending methods so as to send spam messages efficiently using a spam-sending program. For this reason, since these three sending patterns are unique to spam-sending hosts, we will be able to detect such evolutionally advanced spam-sending hosts by their behaviors. Although we dealt with the behaviors of MPE spam-sending hosts in Japan in this paper, such behavioral differences could be observed even if we are dealing with evolutionally advanced non-MPE hosts.

5.3 Other Usage of Decoy Accounts

We discuss another usage of the data collected in decoy accounts. Half the spam messages received at decoy accounts were not listed in DNSBLs. This indicates that there is a possibility of creating an efficient blacklist of spam-sending hosts using decoy accounts. We calculated the traffic volume of 2,695 hosts from decoy accounts during the period from March 15, 2012 to March 22, 2012. The traffic volume was 3.7 TB/week, i.e., 6.1 MB/sec. According to a mobile phone service provider [20], the size of one email message is approximately 11.3 KB including the header and message body. Therefore, our technique detected spam messages corresponding to 47 million email messages per day by collecting the hosts sending spam messages to decoy accounts.

6. CONCLUSION AND FUTURE WORK

In this paper, we revealed the spam-sending patterns of evolutionally advanced spammers such as Japanese MPE spammers by using the traffic flow data retrieved at a backbone network in a real commercial network.

We showed that our technique can estimate typical evolutionally advanced spam-sending hosts because some of their behaviors are unique to MPE spam-sending hosts. Also, we can predict the behavior of the spam-sending hosts by checking their past behaviors. By using this technique, if we see a host that is likely to send spam messages at some point in time, we can predict the timing of spam-sending activities in the future.

We believe that this is an important step towards understanding what MPE spam messages are and towards designing a strong weapon against today's evolutionally advanced spammers.

Currently, we are planning to develop a method to predict spam-sending hosts based on the study in this paper and to conduct further evaluation in order to discover optimum parameter T and D using more data collected over the longer term.

7. ACKNOWLEDGMENTS

A part of this work was supported by the Ministry of Internal Affairs and Communications (MIC), Japan.

8. REFERENCES

[1] Google Inc. Google Gmail - Top 10 reasons to use Gmail – About Gmail –Google. http://mail.google.com/mail/help/intl/en/about.html.

[2] Microsoft Corporation. Get started with Hotmail - All your email and contacts in one place. http://windows.microsoft.com/en-us/Hotmail/get-started

[3] Telecommunications Consumer Policy Division, Telecommunications Bureau, Ministry of Internal Affairs and Communications. Important Legal Matters concerning the Introduction of Outbound Port 25 Blocking by an ISP.

http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/op25b-e.pdf.

[4] Pelleg, D. and Moore, A.W. 2000. X-means: Extending K-means with Efficient Estimation of the Number of Clusters. *Seventeenth International Conference on Machine Learning*, 727-734. 2000

[5] SpamAssassin. The Apache SpamAssassin Project. http://spamassassin.apache.org/index.html.

[6] Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1. http://www.ietf.org/rfc/rfc4408.txt.

[7] Sender ID: Authenticating E-Mail. http://www.ietf.org/rfc/rfc4406.txt.

[8] The Spamhaus Project Ltd. The Spamhaus Project. http://www.spamhaus.org/dnsbl_function.html.

[9] Barracuda Networks Inc. BarracudaCentral.org – Technical Insight for Security Pros. http://www.barracudacentral.org/.

[10] Asami, H. Study Report of an Anti-spam System with a 99% Block Rate − The Selective SMTP Rejection (S25R) System −. http://www.gabacho-net.jp/en/anti-spam/paper.html.

[11] Husna, H., Phithakkitnukoon, S., Palla, S., and Dantu, R. 2008. Behavior Analysis of Spam Botnets. *3rd International Conference on Communication Systems Software and Middleware and Workshops. COMSWARE 2008,* pp. 246-253, Jan. 6-10, 2008.

[12] Tang, Y., Krasser, S., He, Y., Yang. W., and Alperovitch, D. 2008. Support Vector Machines and Random Forests. Modeling for Spam Senders Behavior Analysis. *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE,* pp.1-5, Nov. 30, 2008-Dec. 4, 2008.

[13] Zhang, C.M. and Paxson, V. 2012. Detecting and Analyzing Automated Activity on Twitter. *Proceedings of the 12th International Conference on Passive and Active Measurement*, pp. 102-111, March 20-22, 2011.

[14] MaxMind, Inc. IP Geolocation and Online Fraud Prevention | MaxMind. http://www.maxmind.com/

[15] Internet Initiative Japan Inc. Statistics of Spam Messages. http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol15_EN.pdf.

[16] The Spamhaus Project Ltd. The Spamhaus Project − Effective Spam Filtering. http://www.spamhaus.org/whitepapers/effective_filtering/.

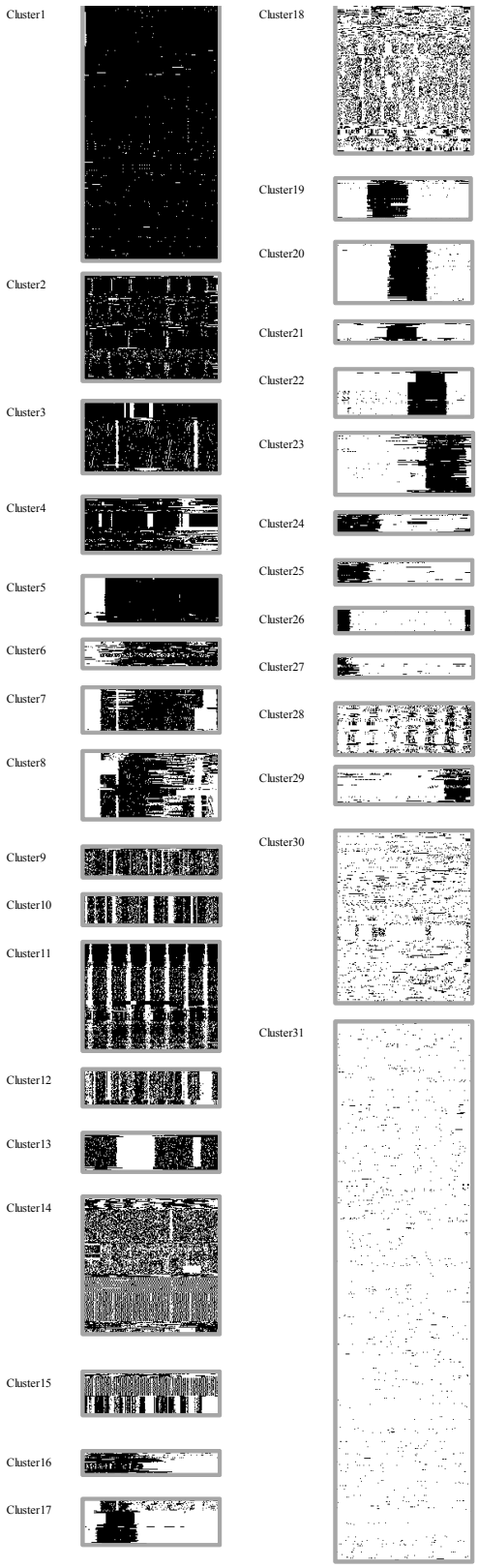
[17] RFC3954: Cisco Systems NetFlow Services Export Version 9. http://tools.ietf.org/html/rfc3954.

[18] RFC3176: InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks. http://tools.ietf.org/html/rfc3176.

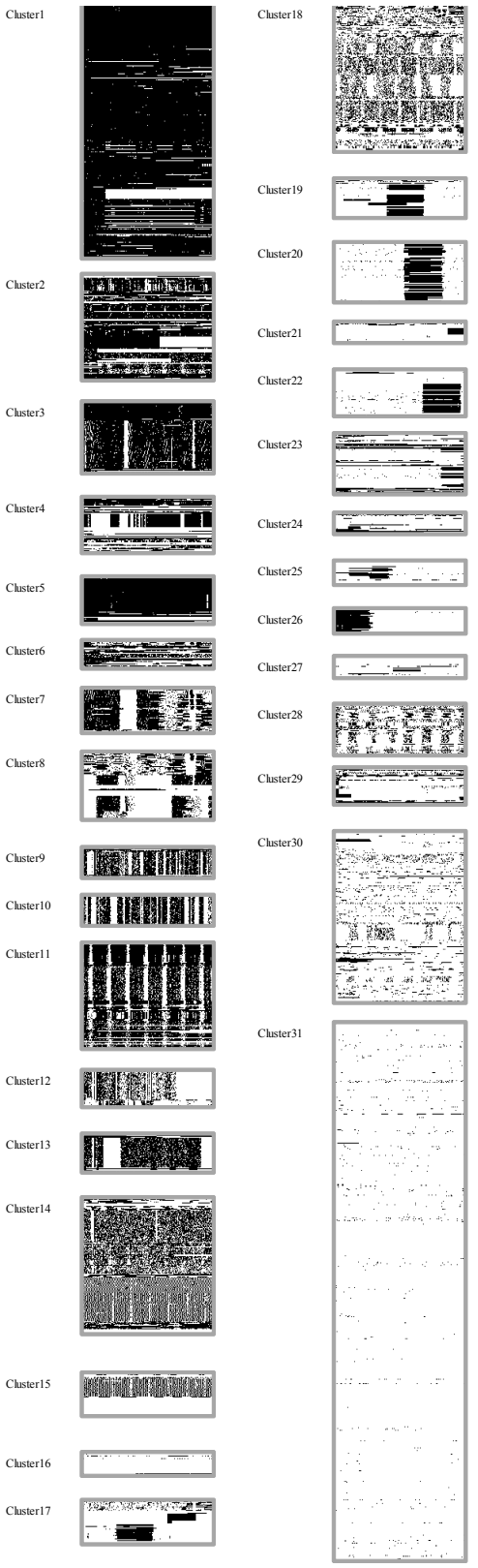
[19] Yamada, Y., Yamagishi, A., and Katsumi, T. B. A Comparative Study of the Information Security Policies of Japan and the United States. http://infosecmgmt.pro/sites/default/files/us-japan_information_security_comparison_4_yamada.pdf.

[20] KDDI Corporation. au. http://www.au.kddi.com.

APPENDIX



A.1. Behaviors of spam-sending hosts (past 1 week).



A.2. Behaviors of spam-sending hosts (next 1 week).