How Do We Discourage Asia from Continuing to be a Source of Spam?

In this report, we will offer our analysis of trends in the ratio of spam and regional sources of spam detected over the period between weeks 27 and 39 of 2009. At the same time, we will also comment on the results of international activities designed to reduce or prevent spam, as well as the adoption rates of sender-authentication technologies.

2.1 Introduction

In this report, we have summarized the latest developments with respect to spam, information about anti-spam technologies, and other activities in which IIJ is deeply engaged. To analyze spam trends, we conducted an analysis of spam from a number of different angles, based on information obtained through the spam Filter Feature of the IIJ email services. The volume of email varies depending on the day of the week according to the service under consideration. Accordingly, we have consolidated data on a weekly basis to better understand the trends revealed in our analysis. Our survey covered the 13 weeks between week 27 (June 29 through July 5, 2009) and week 39 (September 21 through September 27, 2009)—a total of 91 days. Our prior report (Vol. 4) marked the first year since we began publishing the IIR. We will thus also provide a summary of certain data collected over that span of time.

We will also cover international activities related to the adoption of anti-spam measures. The IIJ has been active in international discussions regarding spam, mainly through the Messaging Anti-Abuse Working Group (MAAWG). We will provide an overview of other organizations and activities herein. We will also take another look at sender-authentication technologies, discussing to what extent this and other anti-spam technologies have actually been adopted.

2.2 Spam Trends

In this section, we will report on historical ratios of spam and the results of our analysis concerning spam sources based on trends detected through IIJ spam filters. Figure 1 shows the last year of data (69 weeks), including the weeks that are the focus of our survey—weeks 27 through 39, 2009.
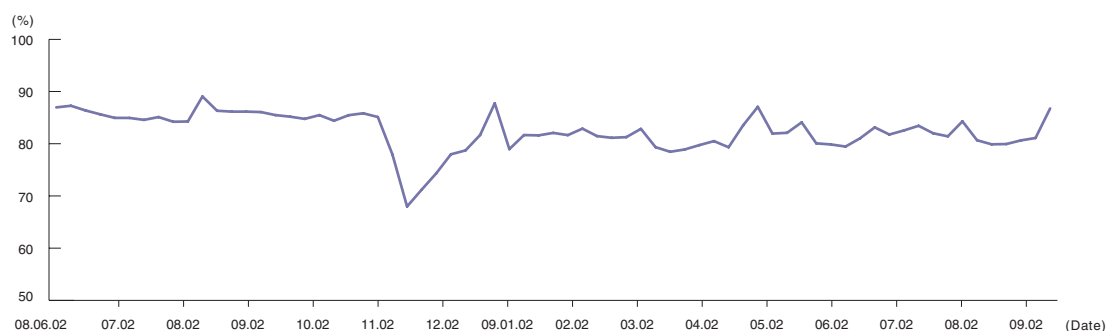

Figure 1: Spam Ratio Trends

IIJ Internet Initiative Japan

2.2.1 Spam Ratio Trends

The ratio of spam averaged 82.2% of all incoming emails over the 91-day period from week 27 to week 39, 2009. This compares to an 81.6% average in our last survey (weeks 14 through 26, 2009), indicating a slight comparative increase. Week 39 (September 21 through September 27, 2009) had the highest ratio of spam at 86.7%. This week happened to include an extended national holiday, and the associated lower levels of overall email activity likely contributed to this bump in spam ratios. Given our experience to date, we expect spam to increase during autumn. Accordingly, we will be keeping a close watch on spam during the upcoming months.

We have noted a recent increase in spam that sends malicious programs as attachments. New variants of these programs are released at a very high rate. In some instances, anti-virus software has not been able to keep up with the changes. Users must take greater care before uncompressing or executing file attachments.

2.2.2 Sources of Spam

Figure 2 shows our analysis of regional sources of spam over the period studied.

Brazil (BR) remained at the top of the list as the number one source of spam, accounting for 12.1% of the total. Brazil actually increased its overall share of this dubious honor by 0.3%. In our opinion, there is a need to investigate the underlying causes that have made this region a major source of spam, as well as what measures can be introduced to reduce spam originating there. We noted a slight variance in the ranking of other top regions during the period investigated. The United States (US) continues to remain near the top, but fell in rank to No. 4 at 7.1%, down 4.3% since our last survey. As we reported earlier, the activities of the U.S. Federal Trade Commission (FTC) and other consumer protection agencies engaged in enforcement may be responsible for this positive trend.

Both China (CN) at 9.8% and Korea (KR) at 7.2% remain near the top of the list at No. 2 and No. 3, respectively. Combined with Vietnam (VN) at No. 6 (5.6%), these countries are the main reason that Asia has experienced growth as a source of spam. Vietnam rose rapidly up the ranks from No. 14 in our previous survey, calling for continued close monitoring. Both Vietnam and Brazil are representative of a global trend—a stronger network infrastructure due to economic growth also sets the stage to become a growing source of spam. India (IN) has also demonstrated this trend, ranking No. 5 in our survey at 6.0%, nearly unchanged since our last survey.

Japan ranked No. 9 in this survey at 3.1%, but increased in ranking and percentage as a source of spam over the previous survey. We can think of several reasons for this. One factor that stood out was the volume of so-called error emails. Among those emails originating in Japan determined to be spam, many originated from major Japanese Internet Service Providers. Looking at the transmission source (envelope From) information and transmission period of these emails, we see that the majority were error notifications in connection with mail sent to an unknown recipient. In other words, the majority of emails identified as spam coming from Japan were bounces.
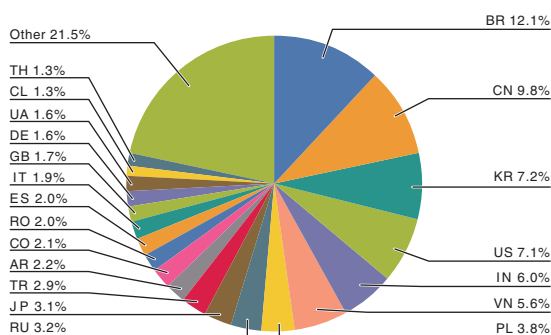

Other 21.5%
TH 1.3%
CL 1.3%
UA 1.6%
DE 1.6%
GB 1.7%
IT 1.9%
ES 2.0%
RO 2.0%
CO 2.1%
AR 2.2%
TR 2.9%
JP 3.1%
RU 3.2%

BR 12.1%
CN 9.8%
KR 7.2%
US 7.1%
IN 6.0%
VN 5.6%
PL 3.8%

Figure 2: Regional Sources of Spam

This phenomenon occurs when IIJ customer domain names are appropriated illegally as source information for spam. In general, this type of malicious usage is difficult to prevent on the part of the domain administrator. One countermeasure is the adoption of sender- authentication technologies on the part of the sender, as offered by IIJ. Performing sender authentication on the part of the receiver as well is necessary to determine whether the domain indicated in the sender information represents the true gateway for the email being sent. In other words, this type of spam can be eliminated by introducing technology that does not return a bounce message in connection with email that uses an unauthorized domain name in the sender information.

Figure 3 shows trends in the ratio of spam from the top six countries (Brazil, United States, China, Korea, Vietnam, India) and Japan.

At the outset of the period surveyed, Vietnam was ranked lower than Japan as a source of spam. However, the Asian nation rose quickly through the ranks, reaching as high as No. 4 and No. 5 at certain points since August. These bumps pushed Vietnam higher overall, ranking No. 6 out of the countries surveyed at the end of the period studied.

From Figure 3, we see the seasonal differences in spam volume over time for each regional source. However, the variances are not necessarily consistent in each country. For example, Korea (KR) was the greatest source of spam in week 34 (the week beginning August 17, 2009), exceeding 10%. The increase in total spam volume during this week was due to a large volume of mail sent from the same source (IP address). While Brazil (BR) experienced some fluctuations in volume weekly, looking solely at the spam coming from that country, we do not see a great variance in the ratio of large-volume spammers or in those who send just one spam email in a week. Based on the patterns identified here, we see that a single source of a large volume of spam had a significant impact on the overall volume of spam sent from Korea to Japan. Brazil and other regions have a small number of high-volume spam sources, leading us to conclude that much of the spam volume is attributable to computers infected with bots or similar malicious programs.

While we can expect legal measures in different regions to have some positive effect on large-volume spam sources, there are limits to what can be accomplished legally where there are significant numbers of small-volume sources. We see here that each region and source of spam must be treated according to the individual nature of the region and source.
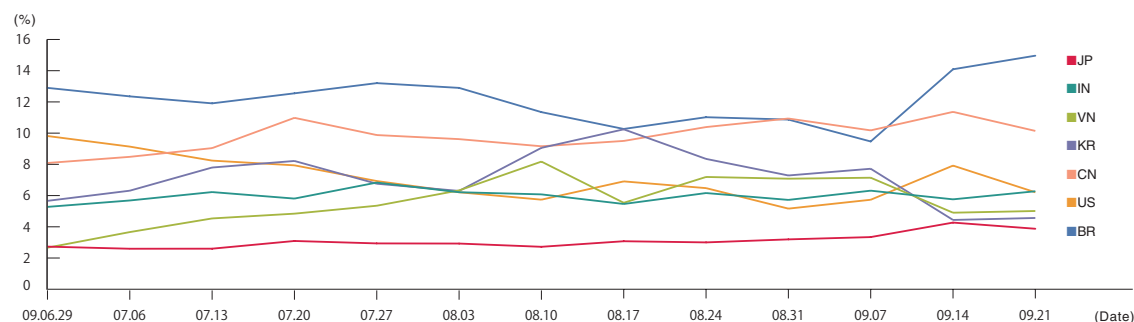

Figure 3: Trends in Sources of Spam

2.2.3 International Anti-Spam Activities

As we have clearly demonstrated in our analysis, the majority of spam sent to Japan originates outside the country. Asia, in particular, has the dishonor of being identified by security vendors as being a source of global spam.[1]

The Asia Pacific Coalition against Unsolicited Commercial Email (APCAUCE) is a private organization that addresses spam in Asia. The APCAUCE is the Asian arm of the Coalition against Unsolicited Commercial Email (CAUCE), which is based in North America. This author participated in the 2006 and 2007 APCAUCE meetings, presenting anti-spam initiatives conducted in Japan. Unfortunately, the APCAUCE has not met since the 2007 symposium in India. Accordingly, several Asia-based organizations featuring the "Asia Pacific" moniker in their names have come together to sponsor the AP*Retreat[2] (an information exchange symposium), held at the same time as the APNIC 28 meeting in Beijing. The APCAUCE, however, did not participate. The issue of spam is an important topic, and the cooperation of the co-chair of the AP*Retreat allowed the opportunity for presentations regarding the state of anti-spam initiatives in Japan and China.

These types of volunteer-based organizations tend to rely heavily on the efforts of a single organizer, which is perhaps why such meetings occur only irregularly. With anti-spam measures in Asia representing such an important issue, the Internet Association Japan has stepped forward to take the lead as the Japanese representative, moving forward with plans to hold a meeting some time next year.

MAAWG is a private global organization that we have discussed in the Internet Topics section of our prior issue (Vol. 4). Presently, participants mainly come from Europe, the United States, and the author's home country of Japan. Asia does not provide many participants. With MAAWG meetings generally held in North America or Europe, it is difficult for professionals in other regions to participate. Accordingly, IIJ believes in the growing need to hold MAAWG meetings in Asia.

The London Action Plan (LAP)[3] is an example of a global organization that works in cooperation with government agencies. LAP sponsors annual meetings according to an action plan ratified in 2004 for the purpose of promoting the sharing of information, organizational coordination, and public-private interaction among enforcement authorities. LAP, MAAWG and the Contact Network of Spam Enforcement Authorities (CNSA) held a joint meeting in 2007. The fifth joint CNSA-LAP Workshop was held in Lisbon, Portugal from October 7 to October 10, 2009. The Japanese Ministry of Internal Affairs and Communications is a member of this organization, and participated in the October meeting, along with this author and the Japan Data Communications Association, presenting Japanese initiatives.[4]

The LAP symposium included discussions of anti-spam laws and enforcement in different countries, as well as other anti-spam activities. Representatives from private organizations (including this author) shared information, as did the German "eco" ISP group and representatives from MAAWG, who discussed their activities in this field. Other presentations discussed how best to engage in cooperative activities with law enforcement agencies in the future. The FTC of the United States made a presentation about the circumstances surrounding the Pricewert shutdown, which we discussed in a previous issue of this report.

*1 For example, Asia is responsible for one-third of all spam according to a continent-by-continent survey conducted by Sophos. (http://www.sophos.com/pressoffice/news/articles/2009/07/dirtydozenq209.html)
*2 See http://www.apstar.org for an overview of the AP*Retreat symposium.
*3 LAP: London Action Plan (http://www.londonactionplan.org)
*4 Workshop CNSA-LAP "Spam-Fighting" (http://www.anacom.pt/render.jsp?contentId=962326)

Australia, New Zealand and several other countries in the Asia Pacific region actively participate in the LAP. Participation by government agencies throughout Asia is relatively high, with participation with from Hong Kong, Taiwan and Malaysia this year. The Seoul - Melbourne Multilateral Memorandum of Understanding on Cooperation in Countering Spam*5 was signed in 2005, representing a collection of government agencies in the Asia Pacific region. Symposia have been held in different member countries. The Ministry of Internal Affairs and Communications represents Japan, with a symposium held in Tokyo in March 2008.

These types of organizations offer government agencies opportunities to share information. While consistent enforcement of the law is of course important, technological measures to fight highly advanced spam technologies, such as botnets, are also important. The public and private sectors must work effectively in concert, cooperating in both technological and legal enforcement in the pursuit of new anti-spam measures. Sending spam from Japan has become more difficult with the introduction of technological tools, such as OP25B (Outbound Port 25 Blocking). This means that spammers are more likely to set up bases overseas, particularly farther east in Asia. Cooperation among and between government agencies in Asia is an important step in doing away with large-scale spam.

2.3 Trends in Email Technologies

2.3.1 Adoption of Sender-Authentication Technologies

We have discussed sender-authentication technologies such as DKIM which uses digital signature technology and network-based SPF/SenderID. We have also offered the results of a WIDE project survey*6 regarding adoption of such technologies, particularly the adoption of SPF on the part of the sender.

Here, we will discuss the results of our survey regarding the degree of sender-authentication technologies for emails actually released. IIJ adopted sender authentication technology*7 in 2005, additionally introducing SPF and DKIM in our continuing pursuit of email safety and security.

Figure 4 shows the ratio of authentication results when email is received in connection with some of the IIJ emails services.

The period subject to this survey was the entire month of September 2009. Of the emails received during this period, 56.2% indicated "none" as the result of SPF authentication for the domain name indicated in the sender information. This means that the domain for 43.8% of email received declared an SPF record. According to a WIDE survey, the declaration rate for "jp" domains in October 2009 was 36.8%. Our results showed a greater result under a basis of actual volume. Of course, sender
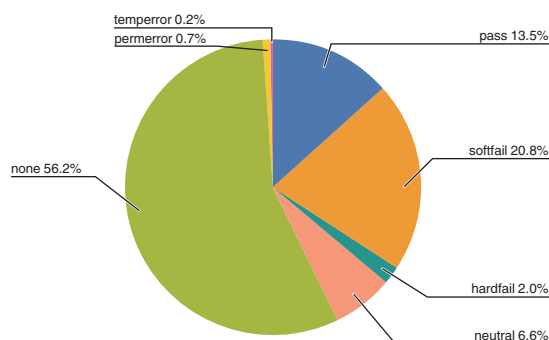

Figure 4: Authentication Results (SPF) for Email Received

---

*5   Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Countering Spam (http://www.sm-mou.org/

*6   Survey Results of the Deployment Ratio of Sender Authentication Technologies published by WIDE (http://member.wide.ad.jp/wg/antispam/stats/index.html.ja)

*7   IIJ Introduces Sender Authentication Technology (http://www.iij.ad.jp/news/pressrelease/2005/0317.html)

IIJ Internet Initiative Japan

domains for email received include other top level domains (TLD) such as "com" and "net" in addition to "jp." We believe that the results from analyzing emails received in Japan indicate a comparatively advanced usage of SPF.

The ratio of email receiving a "pass" as the result of SPF authentication was 13.5%, while the ratio of authentication failure ("softfail" and "hardfail") was 29.4%. From this result, we can conclude that the volume of email that falsely represents sender information was greater than the volume of email sent from a legitimate mail server. Where the volume of spam exceeds 80% of all email received, this is a result with which we can be relatively satisfied. SPF requires care in management, as it is susceptible to forwarding problems and other issues related to false positives. But considering the declaration rates and usage of SPF, a certain level of screening through SPF authentication is one method that can be very effective.

Next, let's look at Figure 5, which addresses DKIM authentication results.

As with our SPF survey, the period studied was the entire month of September 2009. Of all emails received, 0.8% were from senders using some type of DKIM. Given the comparative expense of DKIM for the sender compared to SPF, we see that DKIM has not been embraced on a large scale. However, DKIM offers comparatively fewer false positives than network-based SPF/SenderID, which is why we expect usage to increase in the future for important email messages. Where both SPF and DKIM require the incorporation of additional functions, the cost of authentication on the part of the receiver is the same. Accordingly, we believe that it is important to promote DKIM incorporation in parallel with SPF for authenticating incoming messages.

2.4 Conclusion

Here, we have reported on the ratio of email determined to be spam and the regional distribution of sources of spam under the heading of messaging technology. We have also discussed significant global and Asia Pacific (including Japan) international cooperatives. These activities serve as an important anti-spam measure, as private and government agencies share information through various symposia and engage in cooperative initiatives.

IIJ has presented the data and technologies published through the IIR at international conferences, promoting the adoption of activities and measures in different locales. We will continue to be active in the promotion of anti-spam measures in a variety of different settings.
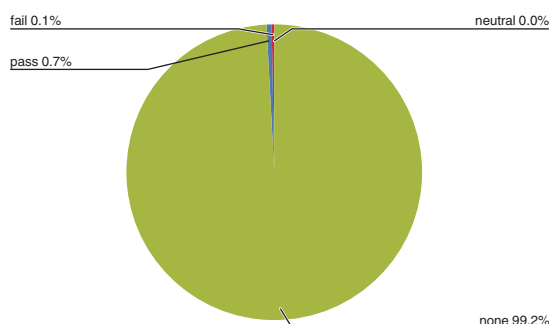

fail 0.1%   neutral 0.0%
pass 0.7%

none 99.2%

Figure 5: Authentication Results (DKIM) for Email Received

Author:
Shuji Sakuraba
Shuji Sakuraba is a Senior Program Manager in the Service Promotion Section of the Messaging Service Division in IIJ Network Service Department. He is engaged in the research and development of messaging systems. He is involved in various activities in collaboration with external related organizations for securing a comfortable messaging environment. He is a MAAWG member and JEAG board member. He is a member of the Council for Promotion of Anti-Spam Measures and administrative group. He is also a member of Internet Association Japan's Anti-Spam Measures Committee.