The DMARC Internet-Draft

In this report we will present an overview of spam trends for week 1 through week 13 of 2013.
Spam from regions neighboring Japan and Asian countries accounted for a large portion of the total, at 64.8%.
It is still crucial to implement measures for dealing with spam sent from neighboring countries.
We also discuss the DMARC Internet-Draft submitted to the IETF on March 31, 2013.

2.1 Introduction

In this report we discuss the latest trends in spam and email-related technologies, and summarize various activities in which IIJ is engaged. In this volume we report the results of our analysis of survey data for the period of 13 weeks from week 1 of 2013 (December 31, 2012 to January 6, 2013) to week 13 (March 25 to March 31, 2013), which corresponds to the 4th quarter for many Japanese companies.

We look at spam trends, including our analysis of changes in spam ratios and the regional sources of spam. Regarding trends in technology, we once again examine the adoption of sender authentication technology. We also discuss the Internet-Draft for DMARC, a new technological framework using sender authentication technology that we have covered on a number of occasions.

2.2 Spam Trends

In this section, we will report on spam trends, focusing on historical ratios of spam detected by the Spam Filter provided through IIJ's email services and the results of our analysis concerning spam sources.

2.2.1 An Upward Trend in Spam Ratios

The average spam ratio for the current survey period (December 31, 2012 to March 31, 2013) was 45.5%. This is an increase of 5.0% over the previous report (Vol.18). Compared to our report for the same period the previous year (Vol.15), the ratio has fallen 1.7%, so spam ratios are returning to previous levels after the decline seen in the previous report. Figure 1 shows changes in the spam ratio between the same period the previous year (Vol.15) and the current survey period.

During this period, the ratio was highest in week 1 of 2013, at 62.1%. This was the year-end and New Year holiday period when the volume of regular mail was low, so the spam ratio increased relatively. The ratios subsequently returned to previous levels, but from March 2013 spam ratios began to climb again. The actual volume of spam is also increasing, so an eye must be kept on this in the future.

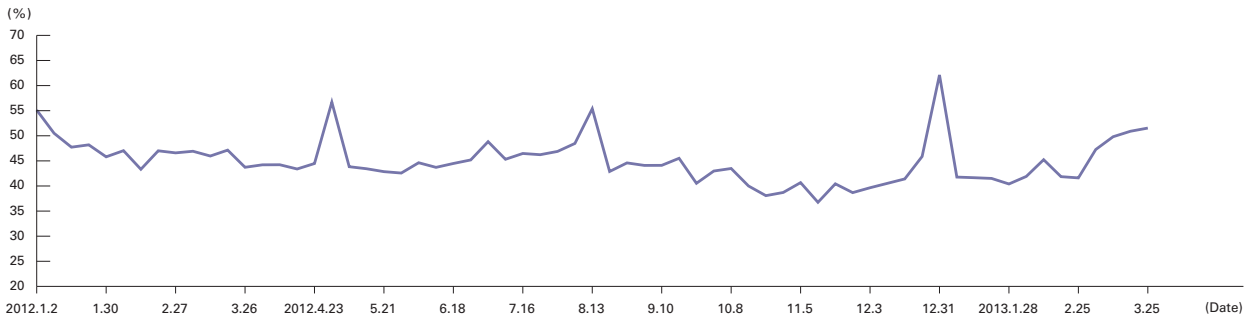

Figure 1: Spam Ratio Trends

2.2.2 Trends in the Regional Sources of Spam

Figure 2 shows our analysis of regional sources of spam over the period studied. China was once again the number one source of spam in this survey, accounting for 21.7% of total spam. This is a drop of 4.9% from the previous survey. Japan (JP) was 2nd as in the previous report, with its ratio also declining 3.2% at 15.4%. South Korea (KR, 8.7%) was 3rd, climbing from 4th place in the previous report due to its higher ratio. Hong Kong (HK, 8.5%) was 4th, Bangladesh (BD, 6.7%) was 5th, and Russia (RU, 3.8%) was 6th.

Bangladesh climbed from 6th place in the previous period to 5th, and its ratio almost doubled to 3.5%. We noted with concern in the previous report that its ratio was rising, and in the current survey results we can see that it continues to grow. In the future it may be necessary to take some kind of action in this region, such as supporting countermeasures through international cooperation. Meanwhile, the United States (US), which had previously been a major regional source of spam, fell to 7th place in the current survey with a significantly lower ratio of 3.6%. To date there have been various reports on initiatives implemented in the United States, such as efforts to take down botnets, and the implementation of port 25 blocking by major telecommunications carriers, so it may be that these are starting to take effect.

At the same time, each of the top six regions now neighbor Japan, so measures to combat spam in Russia and Asian countries may not be sufficient. The ratios for the top six regions total 64.8%, indicating that the majority of spam received in Japan is sent from neighboring regions. Figure 3 shows trends in the ratio of spam sent from these top six regions (CN, JP, KR, HK, BD, RU) for the period of a year (April 2, 2012 to March 31, 2013).

China (CN), which had held the top place for quite a while, fell to 2nd place between week 9 and 10 of 2013 (February 25 to March 10, 2013), with Japan (JP) taking over the top position. There were a number of other fluctuations during the current survey period, such as Hong Kong (HK) taking 2nd place in week 5 of 2013.

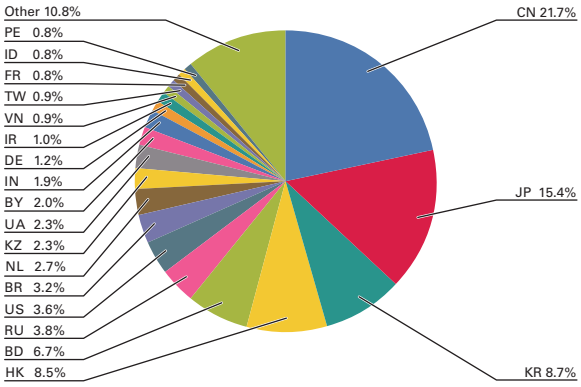

Figure 2: Regional Sources of Spam

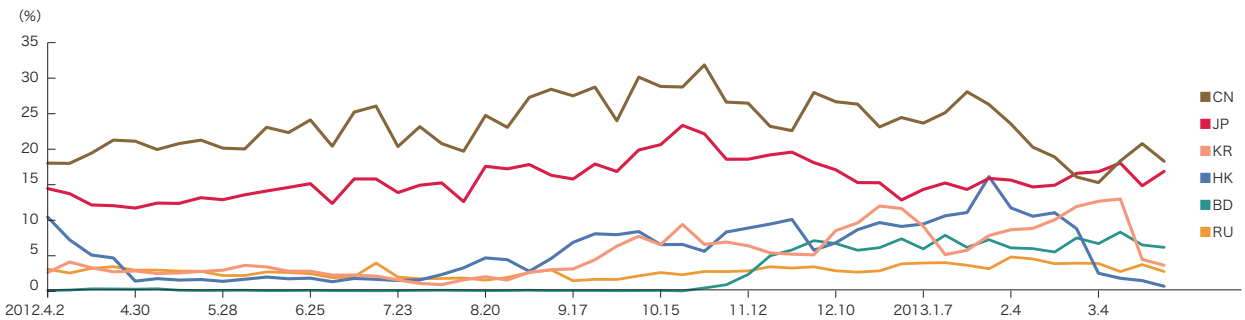

Figure 3: Trends in Ratios for the Main Regional Sources of Spam

2.3 Trends in Email Technologies

Here we will examine a variety of technological trends relating to email. In this report we look at the deployment status of sender authentication technology from the perspective of mail recipients, and discuss the status of the DMARC*1 Internet-Draft submitted to the IETF*2.

2.3.1 Deployment Status of Sender Authentication Technology on IIJ Services

Figure 4 shows SPF authentication result ratios for email received during the current survey period (January to March 2013). The ratio of authentication results showing "none," indicating that the sender domain has not implemented SPF (no SPF record declared), was 25.8%. This is a 2.2% drop from the previous survey period (Vol.18), indicating that the ratio of mail for which authentication was possible increased 2.2%, conversely. In other words, the sender SPF deployment ratio for mail received increased to approximately 74.2% in the current survey period.

This sender SPF deployment ratio is a 10.7% increase over the same period the previous year (2012, period covered by Vol.15), and a 24.4% increase over the same period the year before last (2011, period covered by Vol.11). This demonstrates that the mail sender SPF deployment ratio is rising steadily.

Next, Figure 5 shows DKIM authentication result ratios. The ratio of mail received that had no "DKIM-Signature" header and showed "none," meaning that DKIM authentication could not be carried out, was 88.5%.
This is an increase of 0.1% from the previous survey period (Vol.18), and a decrease of 1.8% from the survey period before that (Vol.17). In other words, DKIM authentication could be carried out for 11.5% of mail in the current survey period, which is a drop of 1% compared to the previous report, and an increase of 1.8% over the report before that. Comparing deployment ratios for DKIM by year, this is a 3.3% increase from the same period last year (2012, period covered by Vol.15), and an 8.6% increase from the year before last (2011, period covered by Vol.11). The deployment ratio for DKIM is not growing very rapidly, perhaps in part due to the cost of implementation on the sender side. As our previous analysis showed (Vol.17), specific domains account for the majority of volume for senders implementing DKIM. This further reinforces the fact that adoption has not progressed much when looking at mail users as a whole. DKIM has many advantages over SPF, so it will continue to be crucial to foster correct understanding of the technology, and promote the goal of having DKIM signatures attached to all important mail in the future.

2.3.2 The DMARC Internet-Draft

We discussed DMARC in Vol.15 and Vol.16. DMARC is already used by Gmail and Yahoo! (yahoo.com), among others, but the specifications were only made available on the dmarc.org website. This was based on dmarc.org's policy of putting the technology into operation, and evaluating issues that arise before considering specifications, rather than spending time evaluating specifications from the outset. The DMARC specifications were finally submitted to the IETF as an Internet-Draft*3 on March 31, 2013. This will likely lead to the specifications being considered by the IETF in the months ahead.

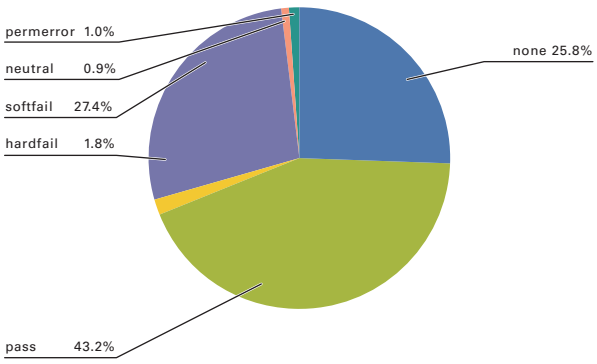

Figure 4: SPF Authentication Result Ratios

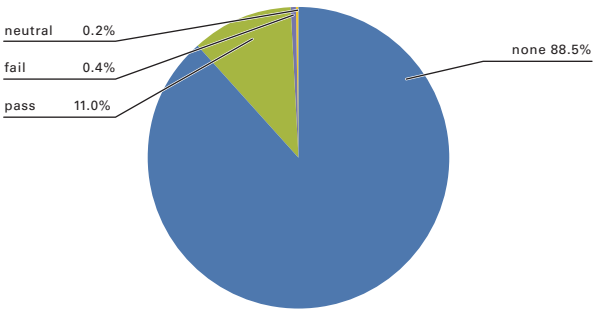

Figure 5: DKIM Authentication Result Ratios

*1 DMARC: Domain-based Message Authentication, Reporting and Conformance.
*2 IETF: The Internet Engineering Task Force.
*3 draft-kucherawy-dmarc-base-00 (http://www.ietf.org/id/draft-kucherawy-dmarc-base-00.txt).

No major changes were made during the process of creating the Internet-Draft, but the new "fo" parameter was added to the DMARC record. This parameter specifies criteria regarding report generation when authentication fails. The values specified for this parameter have the following meanings. "0" is the default value.

"fo=" value	Meaning
0	Generate a DMARC failure report if all underlying authentication mechanisms failed to produce an aligned "pass" result.
1	Generate a DMARC failure report if any underlying authentication mechanism failed to produce an aligned "pass" result.
d	Generate a DKIM failure report if the message had a signature that failed evaluation, regardless of its alignment.
s	Generate an SPF failure report if the message failed SPF evaluation, regardless of its alignment.

DMARC reporting was originally for the purpose of analyzing the cause when sender authentication technology (DKIM or SPF) failed unexpectedly. The newly-added parameter is thought to make it easier to conduct this analysis.

2.4 Conclusion

As was also reported in Japan, DDoS attacks were made on the Spamhaus anti-spam organization in March 2013, and coverage mentioned that this resulted in issues such as high latency in some areas of the Internet*4. As reports indicated, it appears the attacks were a reprisal for Spamhaus blacklisting a Dutch company for sending spam. Similar incidents have occurred in the past, but this one got a lot of coverage because the scale of the attacks peaked at a massive 300Gbps. This seems to be the result of attacks escalating after Spamhaus collaborated with CloudFlare to combat the attacks through wide area distributed processing using Anycast technology. The person behind these DDoS attacks (a Dutch national) was apparently arrested by authorities in Barcelona, Spain on April 25*5.

The impact of these kinds of attacks perpetrated on the Internet is difficult to gauge until it manifests itself in some tangible form. Recent security incidents tend to be carried out covertly so as to attract as little attention as possible. This makes them hard to detect until their effects come to light, and in some cases it is difficult to estimate the scale of damage even when they are discovered.

Incidents of spam being sent using the mail servers of ISPs, etc. as stepping stones have been on the rise in Japan recently as well. In most cases the spam is sent using valid SMTP authentication (SMTP AUTH), so it is possible that IDs and passwords for authentication have been stolen by malicious software (malware). If malware is gaining access to IDs and passwords, then important information on the PCs being operated or other servers being accessed may also be in danger. Spam is garnering less and less attention of late, but by carefully following these trends it may be possible to identify more serious security threats.

Author:

Shuji Sakuraba
Senior Engineer, Strategic Development Center, Product Division, IIJ Mr. Sakuraba is engaged in the research and development of messaging systems. He is also involved in various activities in collaboration with external related organizations for securing a comfortable messaging environment. He is a M3AAWG member and JEAG board member. He is a member of the Anti-Spam mail Promotion Council (ASPC) and administrative group, as well as chief examiner for the Sender Authentication Technology Workgroup.

*4 "Firm Is Accused of Sending Spam, and Fight Jams Internet" (http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html).
*5 OPENBAAR MINISTERIE, "Nederlander aangehouden in Spanje vanwege cyberaanvallen op Spamhaus" (http://www.om.nl/actueel/nieuws-persberichten/@160856/nederlander/) (in Dutch).