Examining the Relationship between Sender Authentication Technology and Spam

In this report we will present an overview of spam trends for week 39 through week 52 of 2010. As was the case for the previous period, the United States was the number one source of spam in this survey. This time we also look at the relationship between spam and authentication results.

2.1 Introduction

This report summarizes the latest trends in spam, covers email-related technologies, and touches on various other activities in which IIJ is engaged. In this volume we focus on data for the period of 14 weeks from week 39 of 2010 (September 27 to October 3, 2010) to week 52 (December 27, 2010 to January 2, 2011), which corresponds to the 3rd quarter for many Japanese companies.

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 by the Spam Mail Filter provided through IIJ's email services.

2.2.1 Decrease in Spam from the Second Half of 2010 Continues

In IIR Vol.9 we reported that the drop in spam ratios was continuing in September and beyond. This downward trend continued throughout the period covered in the current survey. Figure 1 shows spam ratio trends for the period from week 39 to week 52 of 2010 covered by the current survey, as well as those for the previous year and three months (for a total of 66 weeks), which includes the same period for the previous year.

The average spam ratio for the current survey period was 72.1%. This represents a decrease of 6.9% over the previous period (weeks 26 to 38 of 2010), and a decrease of 9.3% over the same period for the previous year (weeks 40 to 53 of 2009). As the current drop in average spam ratios clearly demonstrates, there has been a dramatic change compared to levels for the same period of the previous year, and the trend continues to decrease. Of particular note, the decrease was 63% for week 52, the last week of 2010. This is an even lower ratio than week 47 of 2008, which saw the effects of the McColo network shutdown as reported in IIR Vol.2. The decrease in spam from the second half of 2010 has also been noted in security vendor reports and news articles quoting these reports. The cause is presumed to be a decrease in botnet activity, which is the main technique used for sending spam. Former Washington Post reporter Brian Krebs, who reported on the details of the McColo network shutdown in 2008, also noted a connection between the drop in spam from August 2010 and the Rustock botnet in his blog*1. A drop in spam ratios such as this

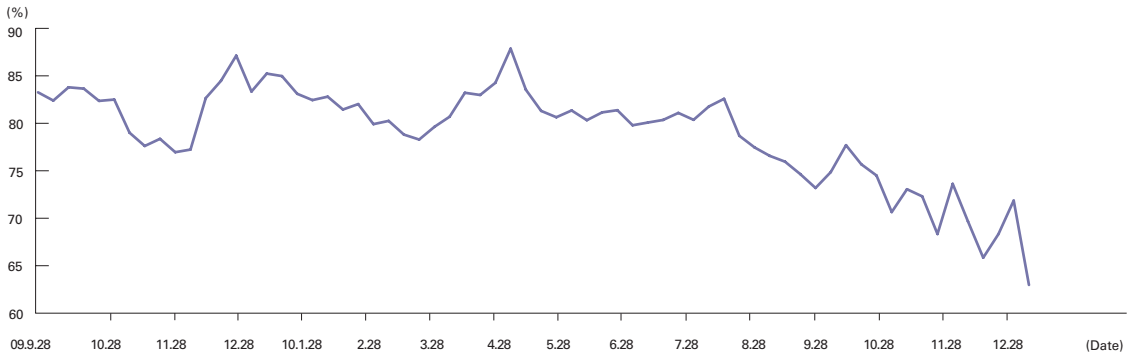

Figure 1: Spam Ratio Trends

*1 Krebs on Security (http://krebsonsecurity.com/2011/01/taking-stock-of-rustock/).

is desirable for those who operate mail services, but unfortunately it does not appear that it will continue for very long. Though still only a quick estimation, spam ratios have begun to increase again from the second week of 2011.

2.2.2 United States the No.1 Regional Source of Spam, Japan's Ratio also Rising

Figure 2 shows our analysis of regional sources of spam over the period studied. As with the previous period, the United States (US) was the number one source of spam in this survey, accounting for 10.3% of total spam. However, its ratio has dropped 1% since the last survey, and as the total ratio of spam has also decreased, the number of spam actually received declined. China (CN) was 2nd at 10.2%, rising from 3rd place in the previous survey. India (IN) was 3rd at 6.2%, dropping from the 7.4% ratio when they held 2nd place in the previous survey. Russia (RU) was 4th at 5.4%, and Japan (JP) 5th at 4.7%. Japan climbed from 8th place in the previous survey. Brazil (BR, 4.6%), Vietnam (VN, 4.6%), and Great Britain (GB, 4.2%) followed behind.

2.2.3 The Relationship between Botnets and Regional Sources of Spam

The reason for Japan's higher ranking in the regional sources of spam is thought to be because spam originating from Japan was not greatly affected by botnet activity. The drop in botnet activity led to an overall decrease in spam. However, most of the spam originating from Japan is sent from static IP addresses, rather than dynamic IP addresses using botnets. This it thought to be why Japan's rank has increased. It is presumed that China also rose in the rankings for this reason. In IIJ Vol.6 we presented analysis results showing that in countries such as Japan and China a higher volume of spam is sent from specific sources. This trend is still continuing today. For this reason we believe that similarly to Japan, China was not affected by botnet activity. Figure 3 shows trends in ratios for the seven main regional sources of spam (US, CN, IN, RU, JP, BR, and VN). The ratio for China (CN) rose rapidly in week 44 (the week of November 11). This is due to an increase in the volume of spam sent from specific sources. On the other hand, this ratio dropped significantly in week 50 (the week of December 13) and week 51 (the week of December 20). These drops were caused when the spam from specific sources that had continued up to that point ceased to be sent. In week 52 (the week of December 27) the ratio for China (CN) shot up quickly once again, and the ratio for the United States (US) dropped dramatically. As shown in the overall ratios in Figure 1, this week had an extremely low volume of spam. In Figure 3 we can see that the reason for this was a drop in the volume of spam sent from the United States (US). Meanwhile, the ratios for countries such as China (CN) and Russia (RU) increased, but this was not an increase

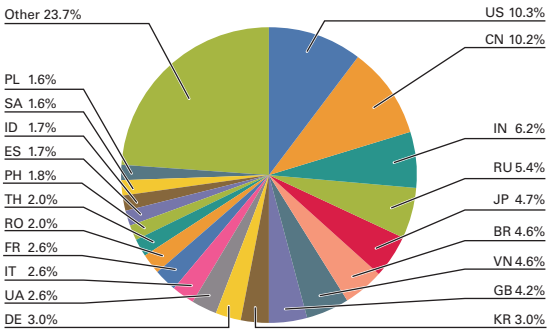

Figure 2: Regional Sources of Spam

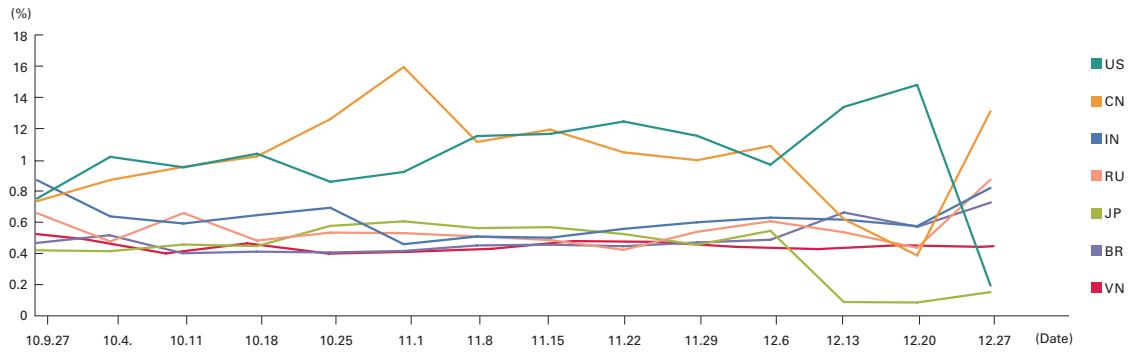

Figure 3: Trends in the Top 7 Regional Sources of Spam

in the actual volume of spam sent, but instead the impact from a drastic drop in the ratio for the United States (US) coupled with a lower overall spam volume. From these trends, it may be possible to analyze regional distribution by botnet type.

2.3 Trends in Email Technologies

Sender authentication is carried out as standard for email received via the email services that IIJ provides. In particular, we implement SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail) technology with the IIJ4U and IIJmio brand email services provided to personal users. In the past we provided a sender authentication filter that used these authentication results, but from December 2010 we began providing a "Fraudulent Email Filter" that can be set up more easily*2. In this report we once again examine the adoption of sender authentication technology.

2.3.1 Volume-Based SPF Implementation on the Rise

Figure 4 shows SPF authentication result ratios for email received during the current survey period (October to December 2010). This time 50.2% of authentication results showed "none," indicating that the sender domain did not declare an SPF record. This is a drop of 5.5% over the results reported in the previous IIR Vol.9. This means that the publication rate of SPF records for senders, or in other words the sender SPF implementation ratio, increased by 5.5%. However, because the overall volume of spam decreased for the current survey period, it could also be said that the increased SPF implementation ratio is only superficial. In response to this, we can point to the 23.6% ratio of authentication results that showed "pass," a 4.8% increase over the previous period.

2.3.2 The Relationship between Authentication Results and Spam

Because it is still often misunderstood by some people, we would like to take another look at the relationship between authentication results and spam. We cannot say for sure that email with sender information given a "pass" in the authentication results is not spam. Similarly, mail with a "fail/hardfail" or "softfail" result is not always spam. Before the spread of sender authentication technology, most spam used widely-known domain names in the sender information (the reverse-path in the SMTP, or the email address in the From: header of the email body). In the past, commonly-used domains were used as forged information to bypass the blocking of incoming mail using sender information and disguise the actual sender. Recently, sender information has also been used to fool recipients for the purpose of redirecting them to fraudulent Web service sites using these domain names to exploit personal information for phishing, etc. Because of this, sender authentication technology was developed and popularized to prevent the misrepresentation of sender information. Meanwhile, more and more spam now uses sender information that produces a "pass" authentication result to bypass filtering that uses only authentication results. We have not completed our analysis of data with many parameters, but looking at the spam received by individuals, over half of recent authentication results have been "pass" results. There are two possible reasons for this. First, it is possible that spam is being sent using legitimate mail servers as stepping stones. Lately there has been an increase in the number of mail services implementing SMTP authentication (SMTP AUTH) when mail is sent. However, the passwords used

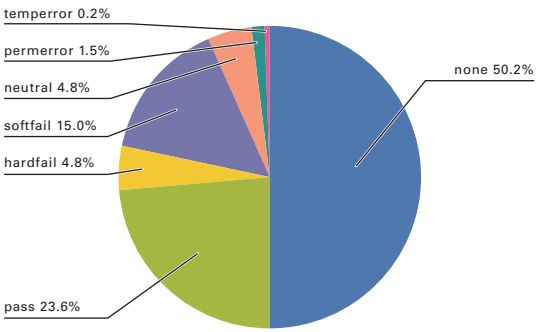

Figure 4: Sender Authentication Result Ratios

*2 Regarding availability of the new "Fraudulent Email Countermeasure Filter" sender authentication filter and discontinuation of the existing sender authentication filter (https://www.iij4u.or.jp/info/iij/20101201-1.html) (https://www.iijmio.jp/info/iij/20101201-1.html) (in Japanese).

for this authentication sometimes contain the same strings as the authentication ID, and it is thought that in some cases authentication IDs appropriated through malicious programs (malware) are being exploited. Secondly, there are cases where rather than misrepresenting the domain name, spammers are openly acquiring their own domain and implementing sender authentication technology to send spam.
In light of the first potential cause, it is important to implement educational measures such as preventing the use of basic passwords and carrying out frequent virus checks. For the second cause, the potential for this kind of activity was originally pointed out during debate over sender authentication technology. However, domain names such as these are practically stating that they are senders of spam, and can be dealt with simply through filtering, etc. In other words, rather than assessing spam through authentication results alone, domain names should also be filtered. Of course there are also cases where confusingly similar domain names are acquired and used to masquerade as legitimate domains. However, these domains can be evaluated automatically using systems such as blacklists. As this demonstrates, it is not possible to determine whether or not email is spam through "pass" authentication results alone. This means that we cannot simply say that sender authentication technology is a complete anti-spam measure. However, we can say that it is possible to deal with spam when it is used in combination with authenticated domain name information. So in other words, it is a kind of infrastructure technology. Additionally, if a domain is properly administrated, creating a whitelist from that domain name and its "pass" authentication results should make it possible to omit other filtering and reduce the load on mail systems. As seen from the above, in order to make it easier for mail to be received, senders of mail must implement sender authentication technology and prevent spam being included in the mail they send. Regarding cases in which legitimate mail fails authentication, we know that this can occur under certain forms of operation such as when mail is redelivered. We have discussed how this kind of problem can be resolved using technology in previous IIR, so this information may be of use to some.

2.4 Conclusion

In the last report we touched upon the Act on Regulation of Transmission of Specified Electronic Mail and the working group held to discuss its revision. According to a media announcement on December 17*3, the operators of a dating service website in Tokyo were arrested on suspicion of violating this act. From the report it seems they were charged with the indiscriminate sending of large volumes of mail using fraudulent sender information and a lack of prior agreement from recipients (opt-in regulation). Both charges relate to parts of the previous act that were made stricter in revisions, so it could be said that these revisions had significance. It has also been reported that this spam was sent from overseas countries such as China and the Philippines. Of course, even if sent from overseas, spam delivered to Japan is subject to its laws, so it is possible to make arrests. That reason that the spam was sent from overseas is thought to be due to the fact that, as we have stated in our IIR to date, through ISP initiatives such as the implementation of OP25B (Outbound Port 25 Blocking) it is now more difficult to send spam from Japan. Through the previous revision of the act, is has now become possible to share information with overseas law enforcement agencies under certain conditions (Article 30). However, because foreign laws and enforcement institutions differ somewhat from those in Japan, the revision of this act alone does not necessary mean that the number of illegal operators caught will increase. But it goes without saying that the Internet is an infrastructure system that connects the entire world, so we believe it is crucial to cooperate and have a more global perspective. From that standpoint, we believe the revision of these parts of the act had meaning. IIJ will continue to contribute to achieving a better Internet environment in a more global sphere, including both technological and legal aspects.

Author:
Shuji Sakuraba
Mr. Sakuraba is a Senior Engineer in the Application Service Department of the IIJ Service Division. He 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 MAAWG member and JEAG board member. He is a member of the Council for Promotion of Anti-Spam Measures and administrative group, as well as chief examiner for the Sender Authentication Technology Workgroup. He is also a member of Internet Association Japan's Anti-Spam Measures Committee. He is a member of the Ministry of Internal Affairs and Communications' Unsolicited Mail Measure Working Group.

*3 Several Million Spam Emails Sent Indiscriminately! 7 Arrested on Suspicion of Advertising a Dating Service (http://sankei.jp.msn.com/affairs/news/110117/crm11011720130102-n1.htm) (in Japanese).