The State of Spam Originating from Japan

In this report we will present an overview of spam trends for week 40 through week 52 of 2011. The ratio of spam has continued to decrease since the last survey, but there has been almost no change in the actual volume of spam from Japan. The ratio of "pass" results indicating that sender authentication was successful climbed to 42.1%, exceeding the ratio of "none" results for the first time.

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 focus on data for the period of 13 weeks from week 40 of 2011 (October 3 to October 9, 2011) to week 52 (December 26, 2011 to January 1, 2012), which corresponds to the 3rd quarter for many Japanese companies. The trend of spam originating from certain specific regions continued due to a drop in botnet activity. In this survey we will report on the results of analyzing the senders of spam originating from Japan in detail.

Additionally, in "Trends in Email Technologies," we report on the penetration rate of sender authentication technologies. We also examine how to use the results of sender authentication to prevent identity theft.

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 The Reduced Ratio of Spam and Security Threats

Figure 1 shows spam ratio trends over the period of one year and three months (65 weeks), including the current survey period and the same period for the previous year. The average spam ratio for the current survey period was 46.8%. This is a significant drop of 25.2% compared to the same period for the previous year, but a drop of just 1.4% compared to the last report (Vol.13). This is a smaller drop than in the last survey, and it is likely that numbers will remain at this level for some time.

However, there is an increased threat of incidents such as targeted attacks exploiting email that can infiltrate an organization from an external network. Appearing as legitimate email, malicious programs (malware) can infiltrate a company when users click links to certain websites or execute an attachment file. Care must be taken when email is received from suspicious senders or when email from a trusted source appears out of the ordinary.

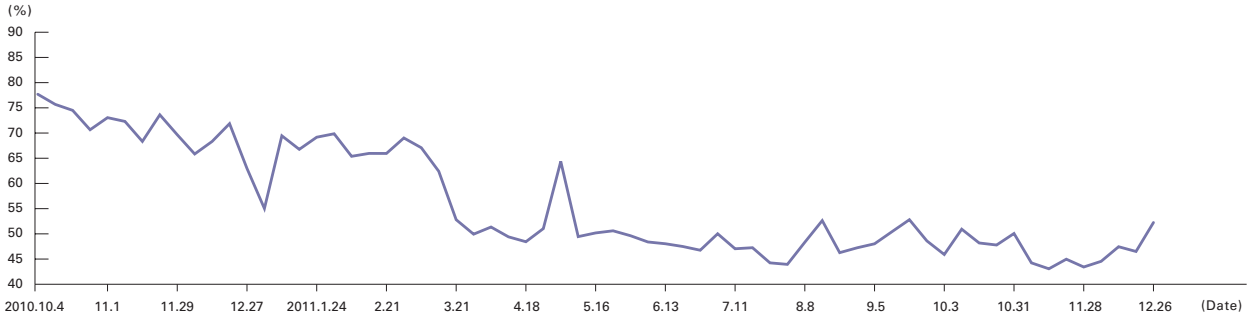

Figure 1: Spam Ratio Trends

2.2.2 An Increase in the Ratio of Spam from Japan

Figure 2 shows our analysis of regional sources of spam over the period studied. China (CN) was once again the number one source of spam in this survey, accounting for 30.0% of total spam. This is a drop of 2.2% compared to the previous survey. The second highest ratio was Japan (JP) at 15.5%, which is an increase of 1.7% since the last report. The United States (US) was 3rd at 10.6%, climbing from 4th place with a 5% increase over the previous survey. These top three countries total 56.1%, accounting for over half of all spam. The Philippines was 4th (PH: 4.9%), India was 5th (IN: 3.7%), and South Korea was 6th (KR: 3.3%), meaning the same lineup of regions took the top places.

Figure 3 shows trends in the ratio of spam sent from the top 6 regions throughout 2011. In early 2011 no regional source of spam stood out from the rest, but in March there was a gradual split, and from May onward China sustained an extremely high ratio, followed by Japan. We can see that most recently the ratio for these two regions as well as the United States and the Philippines has been high.

2.2.3 Details of Senders of Spam Originating in Japan

The ratio of spam originating from Japan detected by IIJ's spam filter in the first volume of this IIR (Vol.1 June to August 2008) was 2%, or 16th highest. This has increased to 15.5%, or 2nd highest, as of this volume (Vol.14 October to December 2011). This is because there has been little drop in the actual volume of spam sent from Japan, despite the overall volume of spam decreasing due to a drop in the activity of botnets that send spam. These botnets were never in common use there, so its ratio relative to others has increased. In this report we will attempt to verify these assertions by examining senders in more detail.

Figure 4 classifies the major senders of spam originating from Japan based on the network name and governing organization in the WHOIS database, and provides a summary of the top 10 senders. Looking at this we can see that the top 6 organizations make up half of the overall volume. Additionally, none of the organizations were ISPs that provide services to consumers, which are a haven for botnets. From this we can surmise that the majority of spam originating from Japan is sent intentionally from specific organizations without passing through a botnet. Although IP addresses were allocated to these organizations by APNIC, some of them were registered with dubious information, including having no address, and a phone number listed as all zeroes after the 81 country code.

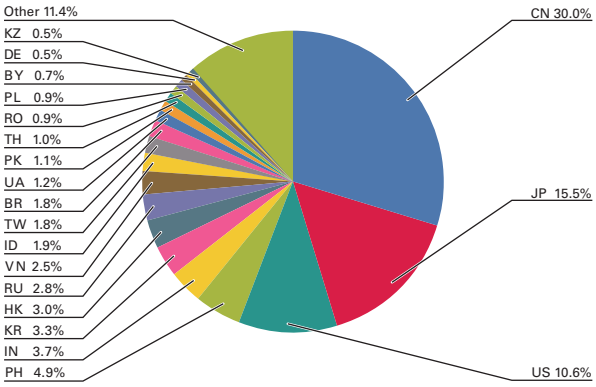

Figure 2: Regional Sources of Spam

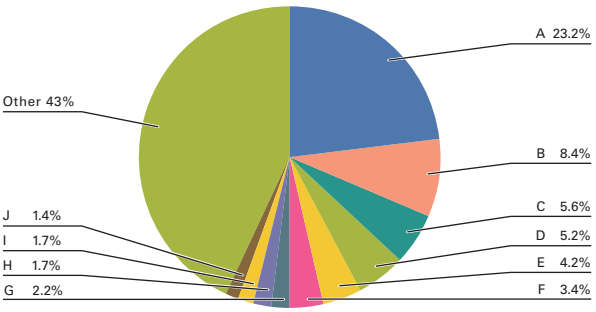

Figure 4: Sender Ratios of Spam Originating from Japan

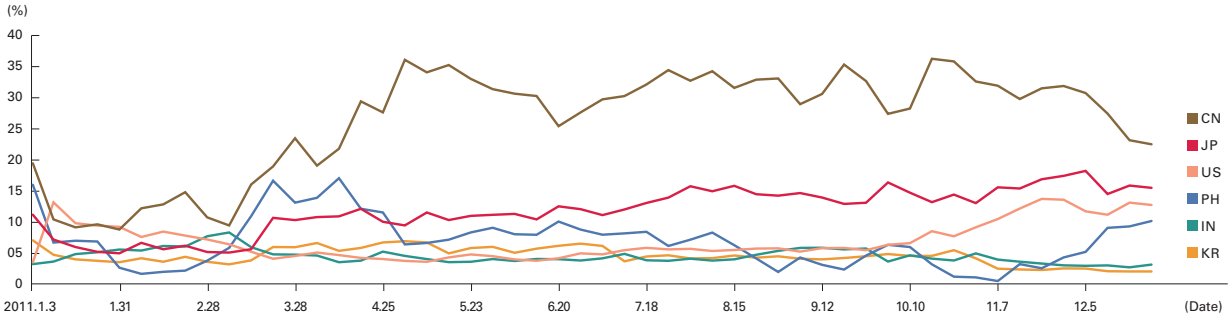

Figure 3: Trends in Ratios for the Main Regional Sources of Spam

Some have pointed out that although the WHOIS database is an important tool for investigating the sending of spam and other misconduct on the Internet, organizations such as APNIC are not managing it properly. MAAWG*1, of which I am a member, has also submitted comments to this effect in the past. We can only hope that improvements are made in the future.

2.3 Trends in Email Technologies

Here we will examine a variety of technological trends relating to email. In this report we present a number of survey results on the adoption of sender authentication technology.

2.3.1 SPF Sender Implementation Status

Figure 5 shows SPF authentication result ratios for email received during the current survey period (October to December 2011). 39.2% of authentication results showed "none," indicating that the sender domain did not declare an SPF record. This was a drop of 4% compared to the previous survey. This indicates that the mail sender adoption rate increased by 4% based on the volume of mail sent. The ratio of "pass" results indicating successful sender authentication was 42.1%. This is the first time in these IIR surveys to date that the "pass" ratio has exceeded "none."

A "pass" authentication result only indicates that the domain in sender information has not been misrepresented, and does not guarantee that mail is not spam. However, because we can be certain that a domain that passes authentication has not been misrepresented, this can be used to filter domains to distinguish between wanted and unwanted email and improve email communication. We will continue to promote the adoption of sender authentication technology.

2.4 Conclusion

Since 2005 the WIDE project has been surveying the deployment ratio of sender authentication technology (SPF and DKIM) in Japan through collaborative research with JPRS. It has been some time since the survey in May 2011, but the survey results for November 2011 have now been published*2. From now on survey results will be published biannually in May and November. According to the November 2011 survey results the deployment ratio for SPF on JP domains was 43.48%, showing a steady increase. The deployment ratio for go.jp domains was particularly high at 93%, indicating that the government is taking these initiatives seriously. Sender authentication technology is an effective way of dealing with fraudulent email that is often used in targeted attacks. We would like to encourage initiatives like this to ensure that mail sent by trusted institutions such as the government is not put to fraudulent use.

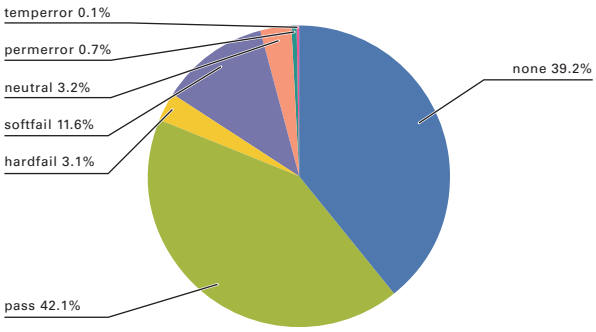

Figure 5: SPF Authentication Result Ratios

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 Anti-Spam mail Promotion Council (ASPC) 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.

*1 MAAWG: Messaging Anti-Abuse Working Group, (http://www.maawg.org/).
*2 Measurement Results on Deployment Ratio of Domain Authentications (http://member.wide.ad.jp/wg/antispam/stats/index.html.en).