

Why Japan Became the 3rd Largest Regional Source of Spam

In this report we will present an overview of spam trends for week 1 through week 13 of 2011.

China was the top regional source of spam. Japan's ranking rose steeply, climbing to 3rd place overall.

Here we examine the reasons for this, and discuss the current relationship between anti-spam measures and IPv6 addresses.

2.1 Introduction

In this report we discuss the latest trends in spam and email-related technologies, and summarize various activities in which IJ is engaged. In this volume we focus on data for the period of 13 weeks from week 1 of 2011 (January 3 to January 9, 2011) to week 13 (March 28 to April 3, 2011), which corresponds to the 4th quarter for many Japanese companies. We also report on trends in authentication results ratios to gain insight into the adoption of SPF (Sender Policy Framework) sender authentication technology. Additionally, we touch on guidelines for the use of IPv6 addresses, which is expected to increase with the exhaustion of IPv4 addresses, as well as anti-spam measures.

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 IJ's email services. In the previous report we noted that despite the downward trend in spam ratios in the latter half of last year, there were indications that they would increase again after the turn of the year. We provide a follow-up in this report.

2.2.1 Spam Decreases Sharply due to Suspended Rustock Activity

Spam ratios dropped precipitously at the end of last year, but began returning to their previous levels from the start of 2011. However, there was another abrupt drop in the ratio of spam in mid-March. 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 65.4%. This represents a drop of 6.7% over the previous report, and a significant drop of 16.7% over the same period for the previous year.

As mentioned in the previous report, it is thought that the decrease in the volume of spam in the latter half of last year is in part due to a drop in the activity of botnets that are the major sources of spam. The suspended activity of the Rustock botnet that accounts for a large portion of spam sent seems to be a primary factor. In the March edition of the

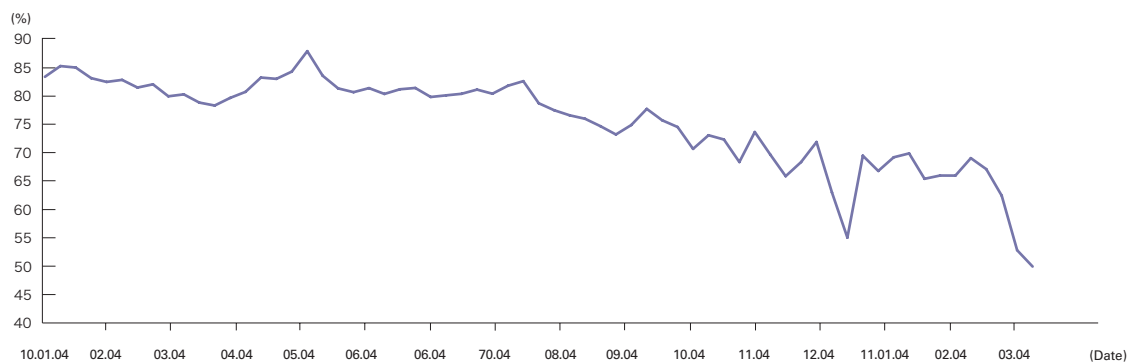


Figure 1: Spam Ratio Trends

Wall Street Journal Online*¹, it was reported that Rustock activity was almost completely shut down due to Microsoft Corporation and federal law enforcement agents seizing the host computers controlling it*². A similar account was published on the Official Microsoft Blog*³.

It is crucial for individual users to take steps to prevent their PCs from being incorporated into a botnet, and for PCs that may have been compromised to be cleaned swiftly. However, as demonstrated by the McColo network shutdown in 2008, finding a way to deal with the controller (herder) of bot PCs is an effective method of stopping botnet activity. If nothing else, it is clear from this example that it has a dramatic effect on spam.

2.2.2 Japan Becomes the 3rd Largest Regional Source of Spam

Figure 2 shows our analysis of regional sources of spam over the period studied. China (CN) was the number one source of spam in this survey, accounting for 12.4% of total spam. This is the first time China has taken the top spot since the 1st quarter of 2010. 2nd in the rankings at 8.0% was the United States (US), which had held the top position up until now. Japan (JP) was 3rd at 6.4%, which is the highest ratio and ranking it has held. The Philippines (PH, 6.1%) was 4th, India (IN, 5.8%) was 5th, and Russia (RU, 5.1%) was 6th.

Figure 3 shows week-to-week changes in ratios for the top 8 regions during the current period. China (CN) maintained a high ratio throughout this entire period, making it clear they were the number one source overall. The ratio for the United States (US), which was 2nd in rank, dropped after mid-January. It is difficult to see the characteristics from the ratio trends, but the period after mid-March when Rustock activity subsided also saw a large drop in actual numbers. The same trend can be seen in India (IN) and Brazil (BR). Meanwhile, the ratio for the Philippines (PH) rose significantly from the second half of February. The ratio for China (CN) also increased abruptly from March.

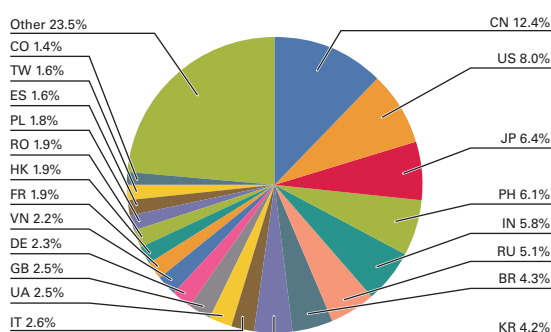


Figure 2: Regional Sources of Spam

2.2.3 Regional Characteristics of Spam Sources as Demonstrated by the Suspension of Rustock Activity

The ranking and ratio of spam originating from Japan rose from 5th place (4.7%) in the previous period. However, comparing numbers with the previous report and the same period for the previous year, there was no significant increase in the actual volume of spam sent. It is thought that the increase in the ratio for Japan is in part due to a drop in the activity of botnets such as Rustock. Figure 4 shows how ratios for the top 8 regions have changed compared to the same period for the previous year (week 1 to week 13 of 2010).

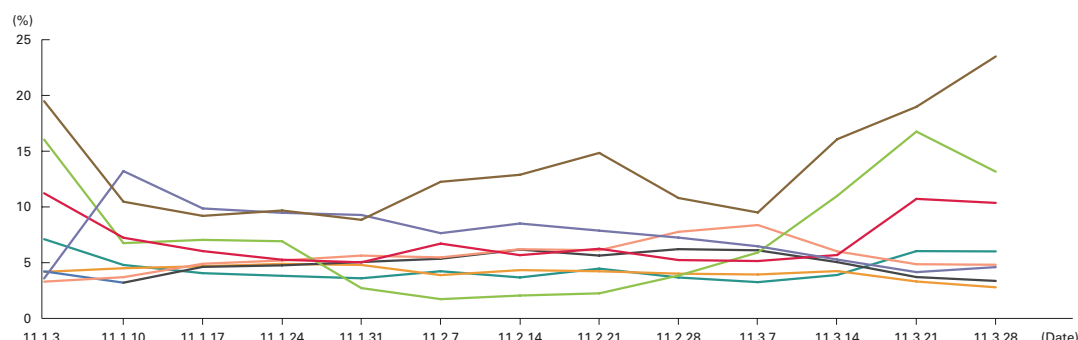


Figure 3: Trends in Ratios for the Main Regional Sources of Spam

*1 The Wall Street Journal (<http://online.wsj.com/public/page/news-tech-technology.html>).

*2 Botnets involve PCs being infected with malicious programs, with said PCs then being controlled via an external host to conduct activities such as the sending of spam.

*3 The Official Microsoft Blog (http://blogs.technet.com/b/microsoft_blog/archive/2011/03/17/taking-down-botnets-microsoft-and-therustock-botnet.aspx).

The figure shows ratios for China (CN), Japan (JP), and Russia (RU) at about 80% of those for the same period the previous year, demonstrating that spam volumes have not dropped significantly. On the other hand, ratios for the United States (US), India (IN), and Brazil (BR) have dropped to below 50%, leading us to believe that the Rustock botnet was active in these regions.

We can also confirm the relationship between botnets and spam volume by examining the Internet environment in Japan. As we have stated several times in the past, Japan has always had low volumes of spam originating from botnets due to the widespread implementation of OP25B*4. In other words, because Japan remained largely unaffected by the shutdown of Rustock, there was little actual decrease in spam volume, with numbers at about 80% of those for the same period of the previous year. Similarly, we believe that the small decrease seen for China (CN) and the large increase in volume sent from the Philippines (PH) point to methods other than the Rustock botnet being used, at least with regard to spam sent to Japan. As mentioned in the previous report, it has been reported several times that Japanese spammers are based in these regions. Regarding geographically isolated Russia, we currently believe it likely that a botnet other than Rustock has spread there.

2.3 Trends in Email Technologies

Here we will examine a variety of technological trends relating to email. In this report we will continue to look at trends in the recipient authentication results for sender authentication technology. We also summarize the current state of the relationship between anti-spam measures and IPv6 addresses.

2.3.1 Volume-Based SPF Authentication Result Ratios

Figure 5 shows SPF authentication result ratios for email received during the current survey period (January to March 2011). As with the previous survey 50.2% of authentication results showed “none,” indicating that the sender domain did not declare an SPF record. The 28.6% ratio of authentication results that showed “pass” was a 5% increase over the previous period. In contrast, the total ratio of results showing “hardfail,” “softfail,” or “neutral” that indicate an authentication failure fell 4.7% compared to the previous period. We believe the increase in successful SPF authentication results is due to the drop in spam ratios and the rise in the ratio of email from legitimate sources that have implemented SPF. Meanwhile, we think the reason that the overall implementation ratio has not increased comes down to the fact that the ratio of spam using the sender information of domain names that have implemented SPF and the ratio of spam not implementing SPF are at comparable levels. In other words, we can surmise that at least with regard to the decreased volume of spam, about half of the domains had already implemented SPF. The decrease in the ratio of authentication failures may point to misrepresentation using legitimate domain names, but considering the drop in spam ratios we believe that a considerable volume of spam openly implements SPF to pass authentication.

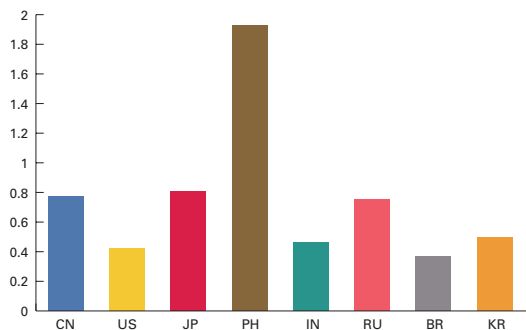


Figure 4: Previous Year Comparison of Major Regional Sources of Spam

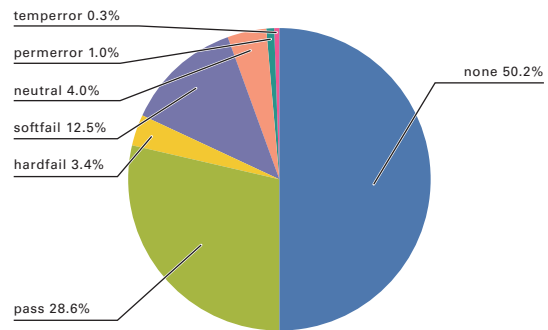


Figure 5: SPF Authentication Result Ratios

*4 OP25B (Outbound Port 25 Blocking) is technology that prevents the dynamic IP addresses used for the Internet connections of consumers from accessing port 25, which is used to connect the mail servers of external networks. It is said to suppress the sending of spam.

2.3.2 Anti-Spam Measures and IPv6

On April 15 as this report was being written, JPNIC announced*5 that the IPv4 addresses available at APNIC and JPNIC for allocation by standard application had been exhausted. Because of this, it is expected that the use of IPv6 addresses will increase. For this reason, we will summarize the relationship between anti-spam measures and IPv6 addresses here.

First, we will discuss the relationship between sender authentication technology and IPv6 addresses. DKIM (DomainKeys Identified Mail) carries out authentication using digital signatures, and because it does not rely on the sender's IP address, there is no impact when sending or receiving email using IPv6 addresses. The SPF records used by SPF and SenderID already include a specification that supports IPv6 addresses. When IPv6 is used for the sender's IP address, "ip6" is added to the SPF record as a mechanism, so there are no issues as long as an IPv6 IP address or network address is added.

Next, we will look at the relationship between frequently used anti-spam measures and IPv6. One function commonly used in anti-spam measures is the content-based detection of spam through email characteristics. As this involves detecting spam from the content of an email, IPv6 has almost no impact.

Another anti-spam measure is the detection of spam based on the sender's IP address. This includes assessing corresponding IP addresses based on a black list, and greylisting in which it is expected that email from a source IP address not identifiable as a threat will be resent. These methods may appear workable provided a database that supports IPv6 addresses is prepared. However, this brings about serious operational issues. Namely, the fact that the IPv6 address space is vastly larger than that of IPv4. Technically, this makes it possible to send a significantly large volume of spam, even if it requires changing the source IPv6 address for each email. When using previous methods such as DNSBL that detect whether or not mail is a threat according to individual IP addresses, it seems highly unlikely that it would be possible to properly manage spam sources. Consequently, we believe that managing IPv6 addresses consolidated to a certain degree by network address would be preferable to managing them individually using a black list. However, when a large range is consolidated together it may also include legitimate mail servers, so care must be taken. Conversely, a white list method of operation whereby all IPv6 addresses are treated as threats and a list of legitimate mail servers with proper anti-spam measures in place is managed could also be a viable option. However, the number of legitimate mail servers existing on the Internet is an unknown quantity, so a significant period of trial and error may be required to generate a suitable list of IP addresses.

Most mail services provided by IJ already allow the receipt of mail sent from IPv6 addresses. We plan to report on the status of these mail services and the relationship between IPv6 and email in the future.

2.4 Conclusion

We would like to express our heartfelt sympathy to those affected by the Great East Japan Earthquake. We pray for the quick recovery of the quake-hit zone. The distribution of information is extremely important during times of crisis. It goes without saying that email and the prevalence of mobile phones, as well as their immediacy and the asynchronous nature of the messages that are exchanged, are invaluable for distributing information. We would like to continue to play a role in providing Internet services that facilitate the distribution of information, as well as email applications widely used on this infrastructure, and we will strive to provide solutions that remain available even when disasters such as this strike.

Author:

Shuji Sakuraba

Mr. Sakuraba is a Senior Engineer in the Application Service Department of the IJ 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.

*5 Regarding the exhaustion of IPv4 addresses (<http://www.nic.ad.jp/ja/ip/ipv4pool/>) (in Japanese).