The Impact of Botnet Countermeasures on Spam Ratios

In this report we will present an overview of spam trends for week 27 through week 39 of 2012.
Spam ratios have settled into a relatively flat range, with a slight increase of 1.4% since the last report,
and a slight decrease of 2.1% compared to the same period the previous year.
We also analyze spam targeting Japan and examine the deployment status of sender authentication technology.

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 27 of 2012 (July 2 to July 8, 2012) to week 39 (September 24 to September 30, 2012), which corresponds to the 2nd quarter for many Japanese companies.

In "2.2 Spam Trends," we analyze trends in spam targeting Japan, which has recently been on the rise. In "2.3 Trends in Email Technologies," we examine the deployment status of sender authentication technologies, comparing both the number of messages received and the number of domains.

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. We also look at changes in the techniques used to send spam based on the analysis results accumulated to date, as well as conclusions from our analysis of recent trends in spam.

2.2.1 Botnet Countermeasures to Date and Their Effect

The average spam ratio for the current survey period (July to September 2012) was 46.1%. This is a slight increase of 1.4% over the previous report (Vol.16), and a slight decrease of 2.1% compared to the same period the previous year (Vol.13). Spam ratios have been relatively stable for some time now. One reason that spam volumes are much lower than they were at one point is because C&C servers*1 have been shut down, preventing large-scale botnet activity. To demonstrate the impact that countermeasures such as this have had on spam ratios, Figure 1 shows the spam ratio trends presented in this report between June 2, 2008 and September 30, 2012.

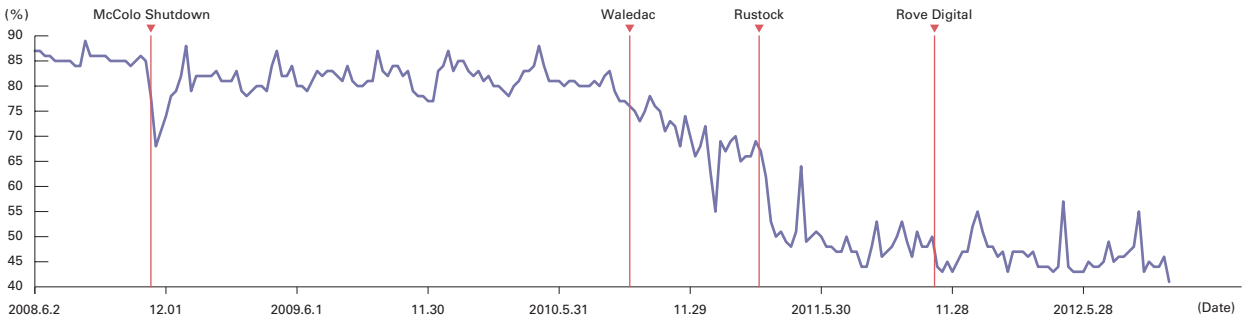

Figure 1: Spam Ratio Trends

*1 Command and Control Servers.

In November 2008, the network of an ISP that was hosting C&C servers was shut down by its upstream ISP (the McColo Shutdown), causing a significant temporary drop in spam ratios. However, spam ratios soon bounced back to previous levels. Following this, Microsoft led moves to shut down a large-scale botnet called Waledac in September 2010, then the Rustock botnet in March 2011. Figure 1 shows that spam ratios gradually dropped from these periods. These results indicate that the shutdown of botnet C&C servers was an effective spam countermeasure.

2.2.2 Changes in the Sources of Spam

Figure 2 shows our analysis of regional sources of spam over the period studied. As with the previous report (Vol.16), China (CN) was again the number one source of spam in this survey, accounting for 24.0% of total spam. Its ratio climbed 3.3% from the previous period. Japan (JP) also remained in 2nd place, at 15.6%. The 3rd highest ratio of 11.1% was held by Saudi Arabia (SA), which has seldom been among the upper rankings in the past. It accounted for 1.4% of spam in the previous survey, so this represents a substantial increase of 9.7%. India (IN) was in 4th place at 7.5%, with both its ranking and ratio higher than in the previous survey. The United States (US) was 5th at 5.4%, and Hong Kong (HK) 6th at 3.3%. The Philippines (PH), which held 4th place last time, slipped all the way down to 21st place in the current survey.

Figure 3 shows spam ratio trends over the period of about a year (November 3, 2011 to September 30, 2012) for the top six regions (CN, JP, SA, IN, US, HK), as well as previous 4th place holder the Philippines (PH). We can see that China (CN) was the top regional source throughout this period. The ratio for Saudi Arabia (SA), which shot up in the current survey, rose rapidly from June 2012. However, its ratio dropped suddenly from September 2012, and its ranking is expected to fall from the next survey if this trend continues. The data shows that during the period that Saudi Arabia had a high ratio, the formerly high-ranking Philippines (PH) accounted for a lower ratio. Because it is difficult to confirm the details of spam in each of these two regions, we cannot draw any conclusions regarding the connection between these fluctuating ratios. However, during the period when the ratio for the Philippines was at its highest, the average number of spam per source (IP address) was about 500 messages, while for Saudi Arabia it was about 12 messages. From this we can speculate that in the Philippines specific sources were sending large volumes of spam to Japan, while in Saudi Arabia botnets were used to send spam, meaning there was no connection, at least with regard to the transmission methods used.

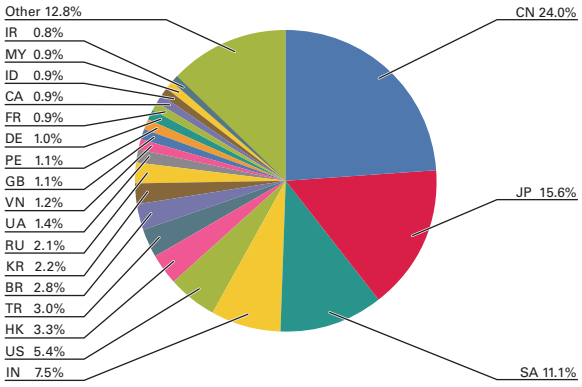

Figure 2: Regional Sources of Spam

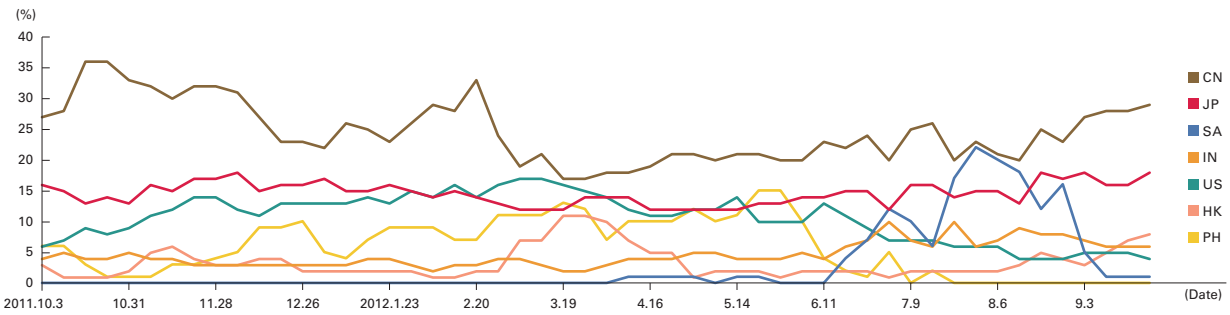

Figure 3: Trends in Ratios for the Main Regional Sources of Spam

2.2.3 Analysis of Spam Targeting Japan

Most of the spam received in Japan until now has been written in English, such as drug-related advertising, or more recently messages purporting to be from major social networking services. However, as shown in Figure 1, the drop in botnet activity has led to a decrease in the volume of this type of English spam sent widely throughout the world. Meanwhile, spam targeting Japan and written in Japanese seems to be on the rise. Here we report on spam advertising cards for unlocking pay TV broadcasts that has been sent in large volumes from around September. There are a number of different patterns, but they generally contain the following sort of advertising pitch.

Subject: 約90チャンネル以上が半永久的に0円で見放題！
From: 噂のB-CAS<support@*****.com>
To: <*****@example.jp>

―――――――――――――――――――――――――――――

【限】【定】【販】【売】▼噂のB-CAS▼数量限定販売

希少価値の高い商品です！お早めに御購入ください！

―――――――――――――――――――――――――――――

豊富な約90チャンネル以上が半永久的に0円で見放題！
もうDVDを借りに行かなくても、お家でのんびり映画・ドラマ三昧！
...

The messages use grammatically-correct Japanese, and feature phrases designed to attract the reader's attention. At first glance they look like email newsletters, but of course no opt-in has been made. There are several versions of the email message, and different text encoding is used to avoid pattern matching. Samples of this spam have been sent from about 100 different regions. China (CN) was the most common, accounting for 40% of samples. Due to the geographical distribution of sources, and the fact that reverse lookup of what is thought to be dynamic IP addresses is carried out, it is likely that bots are being used. However, many examples were sent from Japan (which was the 10th-highest source), so it is possible that a combination of transmission methods are being used. The messages advertise a product that is clearly illegal, so there may be few tangible ill effects. However, the website linked in the spam could turn out to be a malicious site, so it is best to avoid accessing it without careful consideration.

Until now it was thought that most spam targeting Japan and written in Japanese was sent from specific sources in Japan or neighboring regions. However, as this example demonstrates, there may be an increase in spam targeting Japan and sent from a variety of regional sources using a number of transmission methods. We must remain vigilant, and bolster the countermeasures in place.

2.3 Trends in Email Technologies

Here we will examine a variety of technological trends relating to email. In this report we discuss the adoption rate of the SPF*2 and DKIM*3 sender authentication technologies.

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 (July to September 2012). The ratio of authentication results showing "none," indicating that the sender domain has not implemented SPF (no SPF record declared), was 30.7%. This is a 3.1% decrease from the last survey, indicating a corresponding increase of 3.1% in the ratio of email that could be authenticated. In other words, the sender SPF deployment ratio for mail received increased to approximately 69.3% in the current survey period.

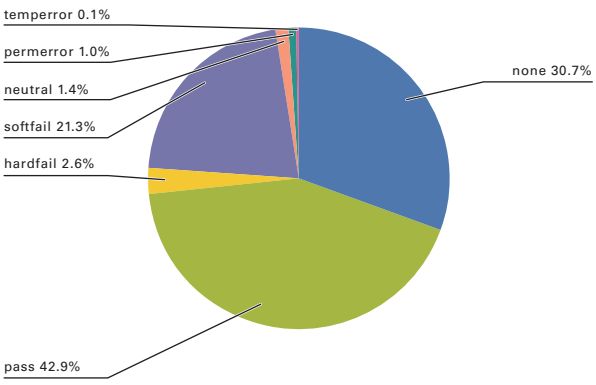

Figure 4: SPF Authentication Result Ratios

*2 SPF: Sender Policy Framework, RFC4408.
*3 DKIM: DomainKeys Identified Mail (DKIM) Signatures, RFC6376.

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 90.3%. The ratio for the previous survey period was 90.6%, indicating that the ratio of mail for which DKIM authentication was possible increased 0.3%.

2.3.2 Analysis of the Number of Authenticated Domains

As shown in Figure 4 and Figure 5, there is still a large gap between SPF and DKIM in the volume of mail from sources that could be authenticated, with SPF about seven times more prevalent. When comparing the number of domains that could be authenticated, the gap widens even more. Looking at mail received in September 2012, SPF is about 45 times more common in terms of the number of domains. This indicates that, for DKIM, specific sources using digital signatures are sending large volumes of mail. Furthermore, although for SPF about 70% of mail received could be authenticated, when comparing the number of domains this figure falls to about 27%. This is because sources that support SPF send more mail. In any case, we believe the fact that mail commonly used deploys either SPF or DKIM sender authentication technology is a step in the right direction. To further popularize sender authentication technologies, it will be necessary to broaden their reach by deploying them on more domains.

2.4 Conclusion

In the previous report, we touched upon the fact that although the volume of spam had dropped, it poses an increasingly greater threat due to an increase in related financial damages and information leaks. In the current survey period there were more reports of incidents in which malicious programs (malware) present on PCs were thought to have posted to external message boards or sent mail after receiving external commands. The PC owners, who had unintentionally become infected with malware, were treated as criminals at first, despite not actually being responsible for any crime. These tactics are similar to the botnet methods used to send spam. This means that once a PC is infected with malware it can become a hotbed for a variety of crime, and once this wrongdoing comes to light the owner of the PC will be held responsible. To avoid being associated with this kind of misconduct, you must take care not to download software of dubious origin such as those mentioned here. It is also necessary to avoid opening attachments or blindly accessing websites linked in mail from suspicious sources. Today, tools such as the Internet, PCs, and smartphones have evolved and become more convenient, but on the other hand this kind of fraudulent behavior using devious and complicated techniques is also on the rise, so caution is required.

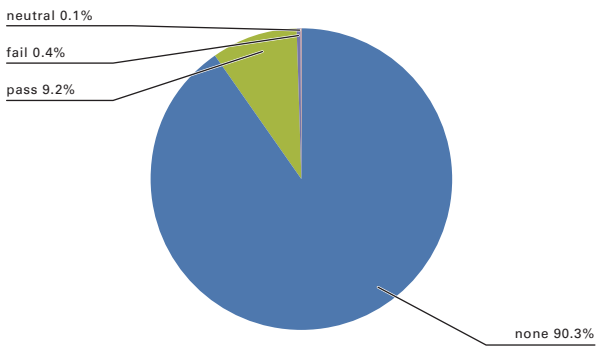

Figure 5: DKIM Authentication Result Ratios

Author:

Shuji Sakuraba

Mr. Sakuraba is a Senior Engineer in the Strategic Development Center at the Application Development Department of the IIJ Product 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 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. 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.