Sender Implementation of Sender Authentication Technology Sluggish

In this report, we will present an overview of spam trends for week 26 through week 38 of 2010. The United States replaced China as the top regional source of spam. We also discuss the implementation status of sender authentication technology and botnet countermeasures.

3.1 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 second quarter of 2010, representing the period of 13 weeks from week 26 (June 28 to July 4) to week 38 (September 20 to September 26).

3.2 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.

3.2.1 No Increase in Spam in September unlike Previous Years

The ratio of spam averaged 79.0% of all incoming emails over the 91-day period from week 26 to week 38, 2010. This compares to an average of 81.3% for our last survey (week 13 through week 25, 2010), and 82.2% for the same period in 2009 (week 27 through week 39), indicating a slight decrease for both. Figure 1 shows spam ratio trends from week 27 of 2009 onward, including the results for the current period.

Trends in surveys for the previous years showed a drop in regular email volume during week 32 (August 9 to August 15), which coincides with a holiday period in Japan, and this caused the ratio of spam to increase. Although the spam ratio subsequently declined, it would rise again in September. During the current survey period the ratio followed a similar pattern up to August, with week 32 showing the highest ratio of spam at 82.6%. However, the ratio stayed low in September, and the overall average spam ratio for the period was lower than in previous years. It is not clear if this is a temporary decline, or if for some reason the decreased spam volume will be sustained in the future. We will continue our analysis and surveys of the situation.

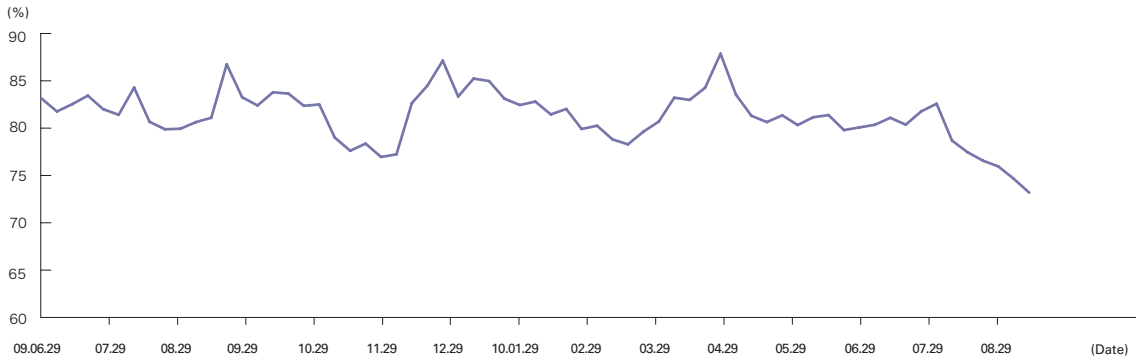

Figure 1: Spam Ratio Trends

3.2.2 The United States Replaces China as the No. 1 Regional Source of Spam

Figure 2 shows our analysis of regional sources of spam over the period studied. The United States (US) was the number one source of spam in this survey, accounting for 11.3% of total spam. It rose from 2nd place in the previous survey to take the top place once more. India (IN) was 2nd at 7.4%, rising from 3rd place in the previous survey. China (CN), which took the top position in the previous survey, was 3rd this time at 7.1%. Additionally, Great Britain (GB) and Germany (DE), which demonstrated upward momentum in the previous survey, maintained high rankings at 5th (5.0%) and 7th (4%), respectively. Other regions that have held high ratios previously remained in the upper rankings, with Brazil (BR) at 4th (5.2%) and Vietnam (VN) at 6th (4.8%). Japan (JP) dropped to 8th, with its ratio falling 0.1% to 3.8%.

Figure 3 shows trends in ratios for the six main regional sources of spam (US, IN, CN, BR, GB, and VN). Though the ratio for previous top place holder China (CN) dropped in July, it began to rise again in August, and there is a chance it will once again become the top regional source of spam in the future. Current 1st place holder the United States (US) had the top ratio for almost the entire period under study, and was highest overall. There were no significant changes for the other 4 top regions (IN, BR, GB, and VN). However, current 2nd place holder India (IN) fluctuated between 1st and 2nd position, and I believe we must continue to keep a close eye on the situation there.

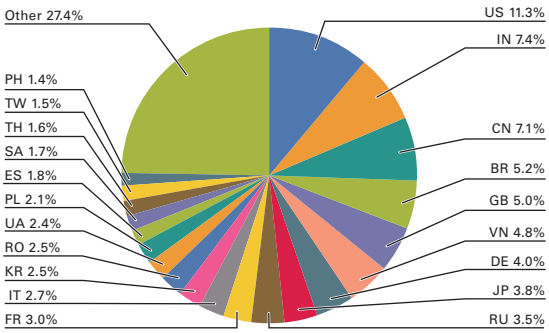

Figure 2: Regional Sources of Spam

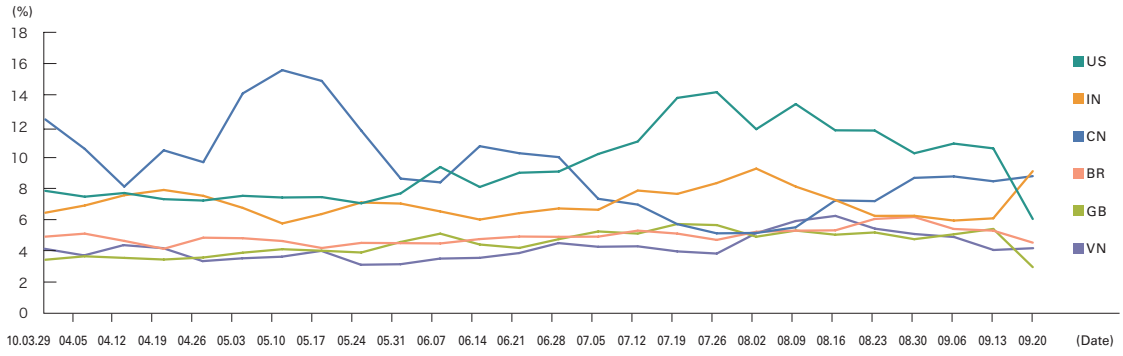

Figure 3: Trends in the Top 6 Regional Sources of Spam

3.3 Trends in Email Technologies

In this section we continue to report on the implementation status of the SPF (Sender Policy Framework) sender authentication technology that has become widely prevalent. We also look at examples of initiatives for eradicating botnets, which play a major role in the sending of spam.

3.3.1 Sender Authentication Technology

Sender authentication is generally carried out as standard for email received via the email services that IIJ provides. Figure 4 shows the ratios for authentication results during the current survey period (July to September, 2010). Of the emails received during this period, 55.7% indicated "none" as the authentication result. This means that the domain for approximately 44.3% of email received declared an SPF record. This is a 0.8% drop compared to results for the previous period. This ratio also dropped in survey results for the JP domain only (Figure 5). The WIDE Project survey*1 also indicated marginal change from the previous period, so we can surmise that domains implementing this technology have not increased significantly.

The Ministry of Internal Affairs and Communications has published statistical data regarding trends in SPF authentication ratio for 6 telecommunications carriers including IIJ since August, 2009*2. The latest data for August 2010 showed authentication results indicating "none" at approximately 18%, meaning that the domain for approximately 82% of email received declared an SPF record.

This result differs greatly from those found in this report. It is thought that this discrepancy arises from differences in the email service user base and aggregation points. For example, the majority of email received on mobile phones is sent from other mobile phones. Most domains for mobile telecommunications carriers declare an SPF record, so we can expect high ratios for this in the authentication results. This means that to ascertain the trends for implementation of sender authentication technology, it would be better to make conclusions based on changes over time for each ratio rather than comparing absolute values for each piece of data. Implementation ratios were already high at the point that data aggregation began, so for both sets of results we can see that the trends indicate implementation is still not progressing.

3.3.2 Botnet Countermeasures

Germany (DE), which was the 7th highest regional source of spam in this report, launched the German Anti-Botnet Initiative*3 in September of this year to eradicate botnets, which are a popular mechanism for sending spam. This is a project jointly operated by the German Internet industry association "eco" and the Federal Office for Information Security (BSI). Through this initiative warnings are sent to users infected by malicious software, and their Internet access is also restricted until the infection is removed. The aim of the project is to help users clean their PCs by providing support such as tools for removing malicious software and a telephone help desk. This may appear very

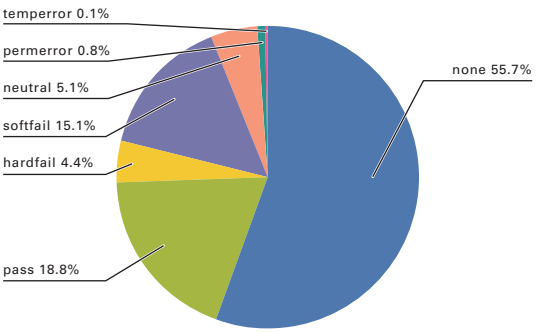

Figure 4: Sender Authentication Result Ratios

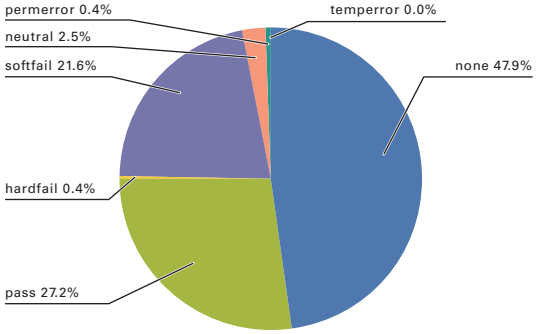

Figure 5: Sender Authentication Result Ratios (JP Domains Only)

*1 Approximate deployment ratios for JP domain authentication technology as of August 2010 (http://member.wide.ad.jp/wg/antispam/stats/).
*2 http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei (in Japanese)
*3 http://www.oecd.org/dataoecd/42/50/45509383.pdf

similar to the initiatives of Japan's CCC (Cyber Clean Center)*4. In actual fact, members of the eco association involved in this project have held hearings and other meetings with CCC participants, and I believe they have applied many aspects of CCC initiatives to their own. The activities of the CCC were also reported on at the MAAWG General Meeting held in June of this year.

When the goal is simply to stop the sending of spam, the OP25B (Outbound Port 25 Blocking) method deployed widely throughout Japan is extremely effective at preventing the direct sending of email from dynamic IP addresses. In addition to the sending of spam, botnets are also used for more serious Internet crimes such as the distribution of malicious software, DDoS attacks, and the exploitation of personal information stored with a PC. Consequently, it is first necessary for telecommunications carriers to implement OP25B to suppress the circulation of spam containing malicious software in attachments, which serves as the primary cause of botnet creation. Infected PCs are then identified using data such as the details of blocked email and DNS queries that malicious software use to receive commands. It is also possible to use honeypot to detect the source of unauthorized access attempts. Then, similarly to the CCC and German Anti-Botnet Initiative activities, removal tools are distributed to remove the malicious software that form botnets.

As demonstrated here, a procedure for eradicating botnets has been established to a certain extent. However, the removal of malicious software involves considerable cost. The cost of the projects in Japan and Germany are born mostly by the government (for the first year in the case of Germany), but ultimately it is the citizens of each country that foot the bill. To reduce this burden it is crucial that individual users maintain vigilance and prevent their PCs from being incorporated into a botnet.

3.4 Conclusion

The Act on Regulation of Transmission of Specified Electronic Mail, which could be considered Japan's anti-spam legislation, incorporates a provision that it be revised three years after it comes into effect. The act was issued in 2002 and amended in both 2005 and 2008, and from September of this year meetings have been held to discuss the anti-spam measures that will be required in the future in light of the act's current enforcement status. An Unsolicited Mail Measure Working Group was established under the Research Group for ICT Service Issues from a User's Perspective, and discussions took place at the meetings of this working group*5. IIJ continues to participate in discussions regarding the revision of the Act on Regulation of Transmission of Specified Electronic Mail, and the author of this report is a member of the working group in question.

The previous amendment introduced drastic changes with an opt-in regulation that makes prior consent necessary when sending specified electronic mail (in other words, email advertising a product or service). However, looking at the email I have received personally, spam advertising various products and services that I have no recollection of opting in for continues to arrive in my inbox. There are many reasons behind the continued prevalence of spam, but I think one of the primary factors is the fact that it is impossible to determine the sender of such email.

I believe the popularization of sender authentication technology will go some way towards resolving this issue. IIJ will continue to actively participate in anti-spam measures, including the legal aspects presented here, while also working towards resolving technological issues.

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.

*4 http://www.ccc.go.jp/en_index.html
*5 http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html (in Japanese)