Email Address Internationalization Approach Considerations

In this report, we will present an overview of trends in the ratio of spam for week 1 through week 12 of 2010, and compare the results with those for the same period the previous year. We will also investigate trends for the major regional sources of spam, report on the implementation status of sender authentication technology, and examine issues with the approach to email address internationalization.

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 period of 12 weeks from week 1 of 2010 (January 4 to 10) to week 12 (March 22 to March 28), as well as data for the whole of 2009. Spam volume fluctuates due to a number of factors, such as the time of year and the timing of spam prevalence, so by presenting spam ratio trends along with those for the same period the previous year, it is possible to make comparisons that take seasonal factors into account. In “3.2 Spam Trends,” we have analyzed the distribution of the regional sources of spam, as well as information regarding transmission methods that can be inferred from this data. We also report on the implementation status of sender authentication technology, which is a core technology for anti-spam measures.

In “3.3 Trends in Email Technologies,” we report on trends in technologies related to email address internationalization that are currently being discussed by the IETF, and examine the issues with EAI (Email Address Internationalization).

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 through IIJ’s Secure MX Service and others.

3.2.1 Spam between Week 1 and Week 12 of 2010 Increased Slightly

The ratio of spam averaged 82.1% of all incoming emails over the 84-day period from week 1 to week 12, 2010. This compares to an average of 81.4% for our last survey (week 40 through week 52, 2009), and 81.5% for the same period in 2009 (week 1 through week 13), indicating a slight increase for both. Figure 1 shows spam ratio trends for 2009, including the results for the current period.

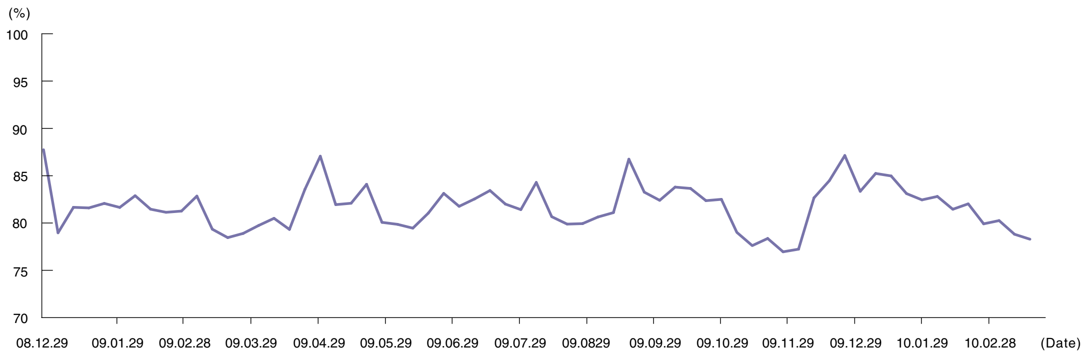

Figure 1: Spam Ratio Trends

As the survey period includes an extended holiday, the ratio of spam for that period is higher as has been the case in previous surveys. However, while in the past the ratio of spam tended to decrease after an extended holiday, for this survey a period of comparatively high activity exceeding 80% continued for some time. The slight rise in the average results for this period is likely to be due to this extended peak. Spam sending trends are affected by seasonal factors, but there are also sometimes sharp increases in spam due to changing transmission methods, such as a boost in botnet numbers resulting from the outbreak of new malware (malicious programs).

In recent years, due in part to hardware performance improvements and increased utilization of network bandwidth, spam has a tendency to increase suddenly when new techniques for sending spam are devised. For companies such as ISPs that constantly receive large volumes of email, these abrupt increases in email volume can serve to impede stable operation. The anti-virus measures and spam detection functions provided by ISP email services are mainly from specialist vendor companies, and they may struggle to handle sudden volume increases such as these. In the years ahead ISPs will need to be able identify trends in the techniques used to send spam, and the email system as a whole will need to be able to react swiftly.

3.2.2 Top Regional Source of Spam Shifts from Brazil to the U.S.

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 9.6% of total spam. China (CN) was 2nd at 7.6%, and India (IN) 3rd at 6.1%. Brazil (BR), which had remained at the top for consecutive surveys, fell back to 4th place at 5.8% in this survey. Similarly, Vietnam (VN), which had previously been in 5th place, fell back to 10th place in this survey at 3.2%. These two countries have dropped in rank significantly, but this is a comparative drop due to an increase in spam from other top regional sources, rather than the result of the number of recipients of spam from these two countries decreasing dramatically. The graph in Figure 2 also demonstrates that there are fewer regions with an extremely high source ratio in comparison to previous survey results. As with the last survey Japan was ranked 7th at 3.9%, which is a slight increase of 0.1% over the previous period. Its ratio rose slightly in the previous survey as well, and the reason for this is an increase in spam from sources thought to be normal mail servers.

Cases in which spam is sent from normal mail servers include those where the mail servers are used as a stepping stone for sending spam, and those where all email including spam is forwarded due to forwarding settings. Of these, for cases in which the servers are used as stepping stones, the outgoing mail servers are likely to be added to a blacklist by external organizations, and once added all incoming mail servers that reference this list will reject email received from those outgoing servers. In Japan, when OP25B*[1] is introduced it is recommended that SMTP-AUTH*[2] be added to mail submission servers, creating a system that prevents email being sent easily. However, there have recently been reports that malicious programs on bot PCs used to send spam are supporting SMTP-AUTH and sending spam, so it appears that applying an authentication system when mail is sent is not sufficient by itself. In addition to using SMTP-AUTH when mail is submitted, measures such as preventing the mass sending of mail by setting upper limits for messages sent per sender and making it possible to trace spam after it is sent by recording sender data in the mail log are necessary.

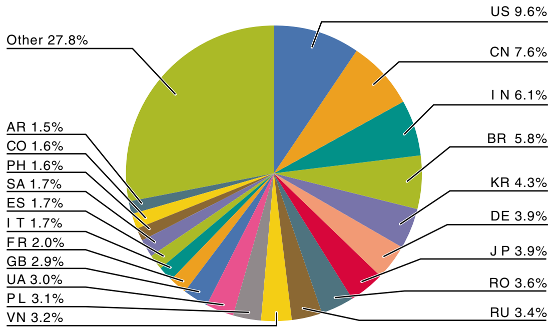

Figure 2: Regional Sources of Spam

*1 OP25B (Outbound Port 25 Blocking) is technology that suppresses the sending of spam by blocking the direct sending of mail from dynamic IP addresses assigned to consumers to external incoming mail servers.

*2 SMTP-AUTH utilizes an SASL (Simple Authentication and Security Layer, RFC4422) mechanism when mail is sent to authenticate the sender. In most cases, authentication is carried out using an Authentication ID and password that identifies the sender. The SMTP-AUTH specification is defined as an extension of SMTP in RFC4954.

3.2.3 Swift Email Receipt through the Implementation of Sender Authentication Technology

It is important for anti-spam measures to provide functions for eliminating spam through the introduction of spam filters and anti-virus functions, as well as a system for receiving legitimate mail without delay. In order to cope with the increasing sophistication of spam and the diversification of virus email in recent years, as well as the rapid spread of new varieties and variants using botnets, there has been a shift toward the introduction of advanced spam detection functions. However, the detection process takes time, and when a large volume of mail is received there is the risk of delivery delays occurring. For example, when the source of an email is evident, such as a business client, users may want to omit part of this spam detection process to receive the email more quickly.

Until now there were no standards or methods for determining whether or not the source of an email was legitimate. However, this can now be achieved by implementing sender authentication technology. As we have noted in our IIR to date, it has been pointed out that the network-based sender authentication technology that is widely in use has the disadvantage of not being able to correctly identify the sender of resent mail, such as forwarded messages. It will be some time before a solution to this problem is widely adopted.

However, even with this issue remaining unresolved, it is possible to utilize the authentication results of sender authentication technology. Erroneous authentication results for mail that has been resent does not represent a very high ratio of the total volume of incoming mail. If the receiving side uses a delivery processing system that gives priority to mail from domains that have been authenticated, it will be possible to receive the required mail more rapidly. Using authentication results from sender authentication technology together with a whitelist for specific senders enables mail to be exchanged more efficiently between trusted parties. To encourage this kind of system, we will continue to push for the adoption of sender authentication technology.

3.2.4 Sender Authentication Technology Implementation Up Slightly, Aiming for Efficient Mail Delivery

Figure 3 shows the authentication result ratios for SPF on a particular mail service, a network-based sender authentication technology, during the current survey period (January 1 to March 31, 2010). Of the emails received during this period, 55.6% indicated “none” as the authentication result. This means that the domain for 44.4% of email received declared an SPF record. This result is a slight increase of 0.7% over the survey for the previous period.

Additionally, the ratio of incoming mail that indicated “pass” as the authentication result stood at 16.3%, resulting in a marginal rise of 0.4%. This is approximately 1/6th of all incoming mail, so if these sources were all added to a whitelist, it would make more efficient mail delivery possible. However, senders of spam have also recently been using domains that pass SPF, so when introducing a whitelist it is necessary to configure it to process authentication results together with the applicable domain name.

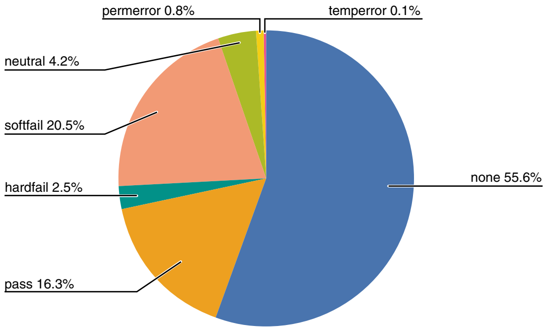

Figure 3: SPF Authentication Result Ratios

3.3 Trends in Email Technologies

3.3.1 Email Address Internationalization

For email addresses used over the Internet, such as taro@example.jp, the parts to the left and right of the “@” sign serve different purposes. The part to the right of the “@” sign is the domain name, and the part to the left indicates the local mail recipient. In general, only ASCII strings can be used for this kind of email address. Internationalization of the domain name placed to the right of the “@” sign is already possible due to a system called IDN (Internationalized Domain Name). The IDN system is explained in detail in JPRS Topics and Columns No.7, “3 Technologies that Enable Internationalized Domain Names,”[3] issued by Japan Registry Services Co., Ltd. (JPRS). We will provide an overview of this system here.

Domain name internationalization support is achieved by making the use of Unicode characters possible. The adoption of Unicode enables domain names such as “日本語.jp” to be utilized without adjustment in languages not based on ASCII characters. However, it was feared that using Unicode as-is would have a significant impact on existing protocols, in particular the DNS system. For this reason, the existing system combining alphanumeric characters and hyphens (-) was maintained by introducing a conversion system called “punycode” to encode Unicode characters and add an ACE prefix to indicate IDNs. This encoding method makes it possible for domain names encoded with punycode to be queried when a Web browser obtains the IP address for a website from the DNS, even if the URL typed into the browser includes a Japanese domain name. Figure 4 shows an example of the IDN notation for “日本語.jp” when using punycode.

As a result of numerous discussions over domain name internationalization, a method with minimal impact on the existing system was selected. The adoption rate for this system will depend on market factors such as how much demand there actually is for it.

There are also few issues with email, as there is no impact on existing mail servers provided that the MUA (Mail User Agent) implements encoding similar to Web browsers when internationalized domain names are used in an email address. However, there are currently moves to internationalize the local portion of an email address to the left of the “@” sign in addition to the domain name. The proposed method also utilizes Unicode without encoding it, complicating the issue further.

The Email Address Internationalization (EAI) that is currently proposed is covered in detail in JPRS Topics and Columns No. 11, “A Summary of Email Address Internationalization (EAI)”[4]. The IETF has defined the EAI framework in the experimental RFC4952, in addition to SMTP (Simple Mail Transfer Protocol, RFC5321) extension specifications in the experimental RFC5336.

3.3.2 Serious Issues with Email Protocols and EAI

When using EAI over SMTP, like previous SMTP extensions the receiving mail server’s support for EAI is determined by its response to the EHLO command sent when an SMTP session begins. When the response to the EHLO command includes “UTF8SMTP,” it means the receiving mail server supports EAI. If EAI is supported, Unicode can be included in the reverse-path parameter of the MAIL command that indicates the email sender and the RCPT command that indicates the recipient. Similarly, Unicode can be used in the From: and To: headers in the header section of the email body. Because extended functions are only used after negotiating mutually supported functions when email delivery begins, there are no significant problems with this process.

Encoding Example:

“日本語.jp”

↓

“xn--wgv71a119e.jp”

Figure 4: Example of Punycode Encoding

[3] http://jpinfo.jp/topics-column/007.pdf

[4] http://jpinfo.jp/topics-column/011.pdf

The problematic aspect of EAI is the processing that takes place when the receiving mail server does not support EAI. For example, consider a case in which a mail submission server (MSA: Mail Submission Agent) that supports EAI receives EAI as-is from the MUA, but the receiving mail server does not support it. When mail that is received cannot be delivered, it is normally bounced back to the sender as an error notification. This kind of processing may lower the availability of mail systems as a whole when the gradual deployment of EAI takes place, but it is not a very serious issue.

A more serious problem is the fact that a conversion mechanism called downgrading has been added to EAI to maintain backward compatibility. This mechanism attempts to downgrade mail instead of bouncing back an error so that mail can be sent to receiving mail servers that do not support EAI whenever possible. There are a number of minor issues related to SMTP, but the most significant problem relates to the conversion of email headers. When the receiving mail server does not support EAI, the original EAI header information is rewritten to headers starting with the string “Downgraded-,” and the existing From: and To: headers are rewritten with the downgraded email addresses. The issue with this process is the fact that DKIM sender authentication technology references these key email headers for signature verification. If the headers that are used for the signature are rewritten, the signature will naturally be treated as invalid, causing authentication to fail.

Up until now mail-related protocol extensions, including sender authentication technologies such as SPF, SenderID, and DKIM, as well as MIME (Multipurpose Internet Mail Extension, RFC2045) for attachments, have been carefully designed to be backward compatible and have minimal impact on existing protocols. EAI could be called overly rough in its current state, as its extension specifications appear to completely ignore the previous care taken, in particular with regard to downgrading. It appears that EAI will be considered as a candidate for adoption as an international standard, and we feel that a more careful approach is needed for discussion of the extension mechanism and its procedures.

3.4 Conclusion

In this volume’s Messaging Technology we reported on spam ratio trends, analysis results for regional sources of spam, and the adoption of the SPF sender authentication technology. High spam ratios continue, and these have the potential to soar even higher, so continued vigilance is necessary.

With regard to trends in email technologies, we took a look at EAI instead of the sender authentication technology that we have focused on in the past. EAI is not completely unrelated to sender authentication technology, as we believe the extension of specifications could potentially have significant impact, so we elected to shed some light on the subject. In this volume we emphasized the problems with EAI, but we support its original purpose of broadening the email user base. In fact, we feel that it is important to actively explore mechanisms that make it easier for regions and people that do not normally use ASCII text to use email, in order to expand the user base. However, when the method of achieving this is not well thought out, and ignores existing protocol extensions, there is a risk of segmenting the email environment itself. When introducing new specifications, they must be considered carefully, as has been done up to now. Alternatively, there may be a need for a new message delivery framework that meets the requirements of a larger group of regions or people.

Author:
Shuji Sakuraba
Mr. Sakuraba is a Senior Engineer in the Application Service Department of the IIJ Service Division. Mr. Sakuraba is engaged in the research and development of messaging systems. He is 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.