The DMARC Technical Specification Promoted by DMARC.org

In this report we will present an overview of spam trends for week 1 through week 13 of 2012. As was the case in the previous study, China was the top source of spam. We also discuss DMARC.org*1, a joint initiative of 15 companies announced on January 30, 2012, and examine the DMARC*2 technical specification promoted by this organization.

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 1 of 2012 (January 2 to January 8, 2012) to week 13 (March 26 to April 1, 2012), which corresponds to the 4th quarter for many Japanese companies.

Spam ratios have been in a declining trend over the past two years, but recently the degree of this decline has slowed. We have anticipated that it would stop falling at some point, and we touch upon the current status in this volume.

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 Ratio of Spam Climbs for the First Time in Two Years

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 47.2%. This is a slight increase of 0.4% over the previous report (Vol.14).

The last time that the average ratio exceeded that from the previous survey period was the first quarter of 2010 (Vol.7). This means that spam ratios declined for a full two years. Only a slight increase was observed, so rather than an indication that spam volumes will rise rapidly in the coming months, this should merely be interpreted as a sign that the declining trend has halted. We believe that the ratio will continue to remain at current levels until new methods for mass transmission spread.

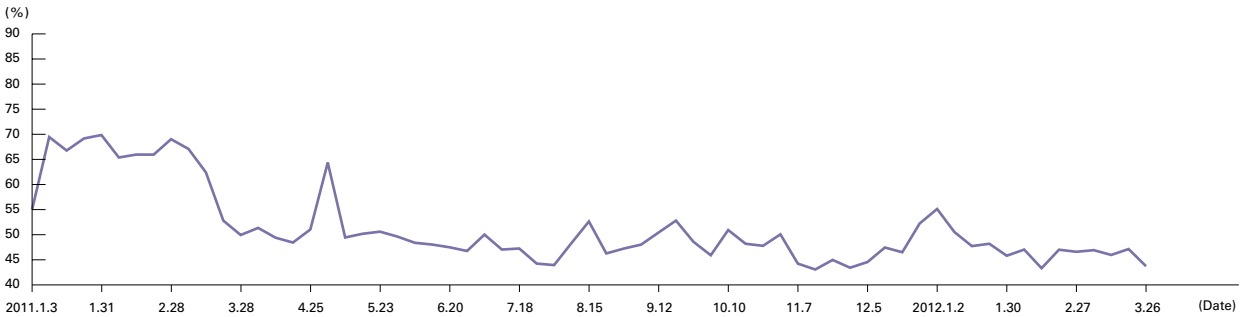

Figure 1: Spam Ratio Trends

*1 DMARC.org (http://www.dmarc.org/).
*2 DMARC: Domain-based Message Authentication, Reporting & Conformance.

2.2.2 The Philippines Continues to Rise as a Main Regional Source of Spam

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 23.7% of total spam. This is a drop of 6.3% compared to the previous survey. The United States (US) was second highest at 14.9%, an increase of 4.3% over the previous period. This led to it climbing from third place to second. Japan (JP) was third highest at 14.0%, a decrease of 1.5% compared to the previous survey. These top three regions totaled 52.6%, once again accounting for over half of all spam. The Philippines (PH) was 4th at 9.0%, a significant increase of 4.1% over the previous survey. The 5th highest ratio was Hong Kong (HK, 4.2%), and the 6th highest was Thailand (TH, 3.4%), each climbing in ranking since the previous period.

Figure 3 shows trends in the ratio of spam sent from these top six regions for the period of a year up to the end of the current survey period (April 4, 2011 to April 1, 2012). China (CN) held the top position throughout the year, but its ratio began dropping from late February 2012. On the other hand, Hong Kong (HK) rose sharply at around the same time. The figure shows that the ratio for the United States (US) has risen steadily over the past year. Looking at the previous and current results for the Philippines (PH), which has climbed in the rankings recently, we can see that it also had a high ratio at around the same time a year ago.

2.3 Trends in Email Technologies

Here we will examine a variety of technological trends relating to email.

In this report we present survey results on the adoption of the SPF sender authentication technology at receiving mail servers.

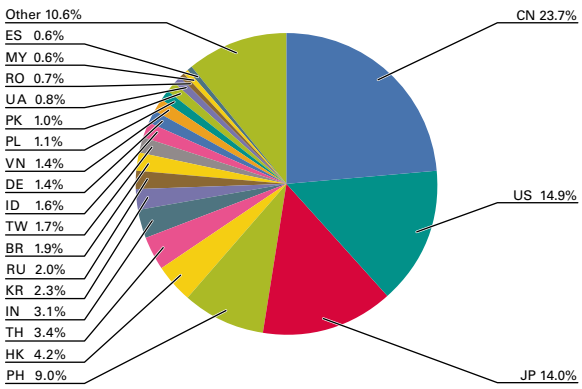

Figure 2: Regional Sources of Spam

We also discuss DMARC.org, a joint initiative of 15 companies announced on January 30, 2012, and examine the DMARC technical specification promoted by this organization. DMARC was discussed in a number of articles in Japan due to the participation of major companies that provide email services such as Google and Comcast, but unfortunately none of these articles provided an accurate picture of the technology. Here we will explain its purpose and technical content in detail from the perspective of a regular participant in M³AAWG*3, which played a part in the early discussion of DMARC.

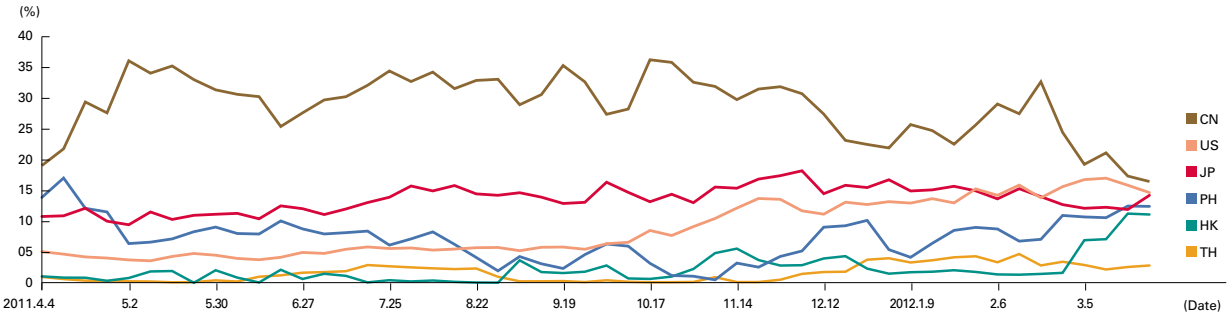

Figure 3: Trends in Ratios for the Main Regional Sources of Spam

*3 M³AAWG: From February 14, 2012 it became the Messaging, Malware and Mobile Anti-Abuse Working Group, widening the scope of discussion that had previously focused on messaging.

2.3.1 SPF Sender Implementation Status

Figure 4 shows SPF authentication result ratios for email received during the current survey period (January to March 2012). The ratio of authentication results showing "none," indicating that the sender domain has not implemented SPF (no SPF record declared), was 36.5%. This is a drop of 2.7% compared to the previous survey, indicating that for the total volume of mail received the ratio of senders that have implemented SPF increased 2.7%.

2.3.2 DMARC Overview and Background

DMARC is a mechanism that allows senders of mail to indicate policies for how spoofed mail should be handled on the recipient side using existing sender authentication technology. Ultimately, spoofed mail should of course be rejected, but legitimate mail may not always pass authentication when using existing sender authentication technologies such as SPF or DKIM due to differences in configurations, delivery routes, and implementations. To make matters worse, only the mail recipient can determine whether or not sent mail has passed authentication or not, and there is no standard method for the sender to confirm this. This mechanism makes it difficult to detect and rectify any configuration problems on the sender side. Similarly, it is hard for recipients to determine whether mail that fails authentication has been spoofed, or if the failure was due to technical factors of some kind. This could prevent authentication results from being utilized effectively depending on the inbound policy, even if sender authentication technology becomes widespread.

In answer to this, the DMARC specification enables senders to publish a point of contact for receiving feedback on the recipient authentication results. At the same time, it also makes it possible for the sender to indicate tiered action levels (policies) for when authentication fails.

This enables configurations with the policy specified as "none" in the initial stages when recipient authentication status is not known, and then raised to "quarantine" or "reject" in stages based on the feedback reported. If a strong inbound policy that rejects receipt of mail that fails authentication can be implemented, we expect it will be possible to eliminate malicious techniques such as phishing that rely on forged sender information.

In other words, DMARC is not a technology for proposing new authentication methods and standards; it is a mechanism for indicating policies that the sender expects recipients to follow when handling mail that fails authentication using the current SPF and DKIM standards. This mechanism enables mail recipients to provide information that streamlines feedback during the policy transition process to make it easier to reject mail that has failed authentication.

2.3.3 DMARC Policy Indication

Like SPF and DKIM, a DMARC record is also configured on a DNS to indicate where policies and feedback should be directed. To give a specific example, a DMARC record for the "example.com" domain would be indicated as a TXT record named "_dmarc.example.com". This begs the question of how domains are determined. Unlike SPF, which uses existing sender information (reverse-path), DMARC poses a similar problem to DKIM with no signature information. For DKIM, the signature information (DKIM-Signature header) indicates a signing domain name, and a subdomain name (selector) that contains information required for signature verification. This means it is not possible to determine whether mail without signature information was

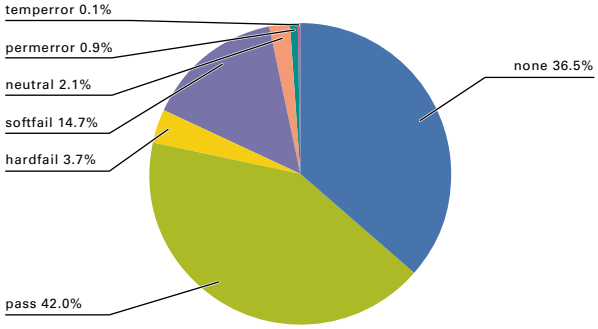

Figure 4: SPF Authentication Result Ratios

Policy	Action Expected when Authentication Fails
none	No action specified
quarantine	Isolate from standard delivery route by quarantining, etc.
reject	Reject receipt

Table 1: DMARC Policies

intentionally left unsigned by the sender or whether it was spoofed. DKIM ADSP*4 was created as a framework to bridge this gap. With DKIM ADSP, the domain for the email address in the From: email header (Author Address, RFC5322.From) is used as the ADSP record location. DMARC also configures the DMARC record on the RFC5322.From domain.

The parameters currently proposed for configuration in DMARC records are shown in Table 2.

The “adkim” and “aspf” parameter values mean s (strict) and r (relaxed). If “strict” is used, the authenticated domain must match the RFC5322.From domain exactly. If “relaxed” is used, then subdomains of that domain are also accepted.

```
_dmarc.example.com  IN TXT  “v=DMARC1; p=reject; pct=100; rua=mailto:dmarc-feedback@example.com”
```

DMARC records are configured using TXT records on the sender domain (RFC5322.From domain) as mentioned above.

Tag Name	Purpose	Sample
v	Protocol version	v=DMARC1
pct	Percentage of messages subject to filtering	pct=100
ruf	Reporting URI for forensic reports	ruf=mailto:dmarc-authfail@example.com
rua	Reporting URI of aggregate reports	rua=mailto:dmarc-aggrep@example.com
p	Policy for organizational domain	p=quarantine
sp	Policy for subdomains of the OD	sp=reject
adkim	Alignment mode for DKIM	adkim=s
aspf	Alignment mode for SPF	aspf=r

Table 2: DMARC Record Tags

2.4 Conclusion

DMARC records and DKIM ADSP records do not use the RFC5322.From domain merely because there is no other place to store them. The final mail recipient references this RFC5322.From information in the mail header as sender information. Using DKIM alone, when a spoofed email address (domain) is set to RFC5322.From, mail will pass authentication even if it is signed by a completely unrelated domain. Many mail recipients have no way of knowing what the signing domain is, even if closely related to the apparent sender (RFC5322.From). As a result, it is difficult for mail recipients to determine whether mail they receive can be trusted or not.

This is why the DMARC record indicating sender policies including DKIM ADSP and SPF uses the RFC5322.From domain that mail recipients are able to reference. Of course, with the diversity of mail usage, it is difficult to stay consistent with this kind of mechanism in some cases. However, email is a tool that provides an easy way to compromise organizations. With email used for an increasing number of malicious purposes such as targeted attacks, it may be time to consider systems for ensuring that legitimate mail is delivered, including re-examination of technical specifications related to the use of mail.

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.

*4 DKIM ADSP: DomainKeys Identified Mail Author Domain Signing Practices, RFC5617.