Anti-Spam Measure Technology and DMARC Trends

In this volume we report on spam trends incorporating the 52 weeks' worth of data from March 31, 2014, to March 29, 2015, while referencing data from IIR Vol.1.

Additionally, in our commentary on email technologies we discuss the RFC for DMARC that was authored recently, as well as the email framework for using DMARC, and the email ecosystem including domain reputation and feedback.

2.1 Introduction

In this report we discuss the latest trends in spam and email-related technologies, and examine a variety of anti-spam measures in which IIJ is involved. In "Spam Trends," we cover spam ratio trends since IIR Vol.1, including FY2014. We also discuss security topics arising from spam.

Under "Trends in Email Technologies," we take the opportunity to examine the benefits of introducing DMARC to aid it in becoming more widespread, in light of a DMARC RFC being authored. We also look at how sender authentication technology such as DMARC can be used effectively in email systems. We have already presented these concepts at events such as the Internet Association Japan's Anti-Spam Conference. In the future we would like to continue discussions in detail to work toward implementation, together with a number of organizations involved with anti-spam measures.

Last year, there were a number of events that became milestones for activities related to anti-spam measures. I will touch upon these at the end.

2.2 Spam Trends

In this section we examine spam trends, based on trends in the ratios of spam detected by the spam filter provided through IIJ's email services. Spam ratios are collated by week, because email usages rates differ for email users between weekdays and weekends. That said, spam ratios tend to be relatively higher on weeks that include long holidays such as the summer vacation and New Year periods, as the number of legitimate emails is significantly lower.

2.2.1 Spam Ratios Decline Further in FY2014

Figure 1 is a graph showing spam ratio trends for 356 weeks' worth of data from the initial IIR period (Vol.1, June 2008), including the 52 weeks between March 31, 2014, and March 29, 2015, which covers the year since the previous IIR (Vol.23). This indicates that average spam ratio for the past year (FY2014) was 31.7%. The average ratio stood at 47.4% the year before last (FY2013), so this represents a drop of 15.7%. The ratio of spam has fallen sharply since 2010, first remaining in the 40% range for some time with averages of 48.1% for FY2011 and 44.3% for FY2012, and now in FY2014 it has decreased further.

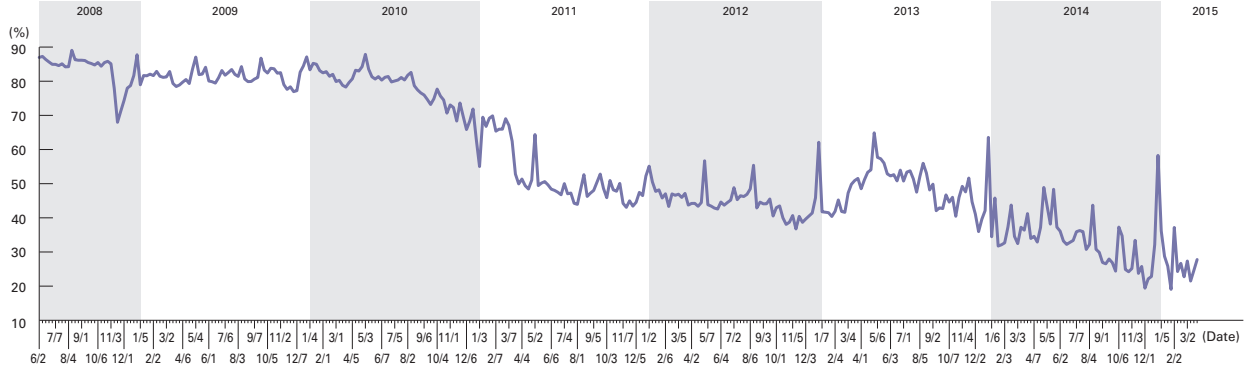

Figure 1: Spam Ratio Trends

Let us compare spam ratios over a longer period of time. The average ratio was 78.6% in FY 2009, so spam ratios, or in other words the volume of spam itself, has dropped considerably in the past five years. To give a more detailed explanation, because the ratio has fallen by 46.7%, if we were to suppose the number of standard, non-spam emails received remained constant over these five years, it would mean the overall volume of email received has fallen to a third of that before.

2.2.2 Higher Risks Despite Lower Volumes

These figures demonstrate that the volume of spam itself is on the decline, but as we have said in the past, it does not appear the risks that spam can pose have diminished. According to a report*1 published by the National Police Agency on February 12, 2015, there were 1,876 cases of illegal remittance in 2014, an increase over the previous year. Total damages came to 2,910 million yen, which is about double the 1,406 million yen in damages from the year before. Regarding the type of damages incurred, it was reported that there had been an increase in corporate bank accounts affected, rather than personal bank accounts. Regarding illegal remittance methods, it was reported that the technique of using viruses to automatically process illegal remittances was become increasingly sophisticated. This is thought to indicate that malware*2 is still being employed.

Let us examine how this kind of malware infiltrates the PCs of individuals and companies. Data on unauthorized access in the report*3 also published by the National Police Agency, among others, on March 19, 2015, listed two arrests for exploiting security holes, or in other words targeting vulnerabilities (security hole attacks in the report). Meanwhile, there were 336 arrests for the use of identification codes without permission. Of course, it is likely a considerable amount of malicious activity did not result in arrests, but from the data that we have at hand we can surmise that incidents exploiting vulnerabilities on a PC directly from an external source are (as yet) uncommon. These materials also listed the following points to note regarding defense against such incidents.

1. Appropriate configuration and management of passwords
2. Caution regarding phishing
3. Caution regarding malicious programs

Because the caution regarding phishing discussed taking care with email, it appears that email is being used to redirect users to phishing sites. Similarly, with regard to malware (malicious software), it was indicated that users should not open email attachments or files downloaded from untrustworthy websites. In short, we can see that email is used as a trigger for these malicious activities, and that accessing malicious sites listed in emails is a major cause of malware infections.

Regarding phishing, the Council of Anti-Phishing Japan*4 provides information such as lists of phishing sites that mimic actual websites and the sample phishing email text used to lure users to those sites. If you receive a suspicious email, we recommend you check whether it has been registered there. From a global perspective, APWG*5 publishes regular reports that I believe will prove useful for gauging recent trends.

2.3 Trends in Email Technologies

Here we will examine a variety of technological trends relating to email. This time we discuss the RFC for DMARC that was authored recently, as well as the email framework for using DMARC, and the email ecosystem including domain reputation and feedback.

2.3.1 The DMARC RFC

We have discussed the specifications of DMARC (Domain-based Message Authentication, Reporting, and Conformance) in this IIR since its origin and Internet-Draft ("I-D") stages. In March 2015, the core portions of DMARC were published as

*1 Status of Incidents of Illegal Remittance Related to Internet Banking in 2014 (http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf) (in Japanese).
*2 Software created for certain malicious purposes, such as the theft of information, the sending of spam, or the processing of illegal remittances, is sometimes called malicious software or malware to differentiate it from the more widely-used term "viruses."
*3 Status of unauthorized access incidents and research and development for technology related to access control functions (https://www.npa.go.jp/cyber/statics/h26/pdf041.pdf) (in Japanese).
*4 Council of Anti-Phishing Japan (https://www.antiphishing.jp/) (in Japanese).
*5 APWG: Anti-Phishing Working Group (https://apwg.org).

RFC7489*6. Initially, the DMARC I-D was published and discussed as a standards-track item, but in the end it became an Informational RFC. I did not follow all the discussions of the IETF DMARC Working Group, so I am not fully aware of the reasons for it becoming an Informational, but it appears the change from I-D to Informational was made in April 2014.

As has been pointed out in the past, DMARC has an issue with authentication failing in a number of cases where use was normally possible. It is likely this issue had an impact during the standardization process, and it is also cited as a point requiring ongoing attention by the IETF DMARC Working Group. The issue originates from the fact that DMARC and the SPF and DKIM checks used as the basis for DMARC authentication each authenticate a different sender domain. We discussed this in Vol.16 of this report*7, which was published in August 2012.

2.3.2 Problems with DMARC and Reporting

One problem currently listed in the charter of the IETF DMARC Working Group as an issue that needs to be tackled is "indirect mail flows." Cases given as examples include the use of the following functions, which have been widely utilized as convenient email operations.

- Mailing list managers
- Automated mailbox forwarding services
- MTAs that perform enhanced message handling that results in message modification

In each case, the underlying cause is that the original email creator and the most recent sender from the perspective of the final recipient of that email are different, or that an intermediary function has changed the message. In April 2014, there was an actual incident in which U.S. company Yahoo! changed the DMARC record policy to "reject," resulting in the email of users participating in mailing lists via Yahoo! to fail DMARC authentication at delivery destinations from the mailing list. This caused receipt to be rejected according to the DMARC record policy. Meanwhile, after publishing that the DMARC record policy was to be changed to "reject," I heard from a staff member with a major U.S. bank who was pleased with the dramatic drop in complaints related to email that misrepresents its domain.

The goal of DMARC is to identify email that has the sender domain spoofed in this way, and prevent it from being delivered. However, to achieve this it is necessary to set the DMARC record policy to "reject." As shown in a previous example, this may have a significant impact. However, DMARC also features policies such as "none" and "quarantine," which are designed as transitions for a "reject" policy configuration. A domain administrator can configure policies with limited impact such as these, while utilizing the reporting function that reports authentication results to the sender. Based on this report, domain administrators can determine in advance whether authentication for legitimate email failed in any cases, and confirm about how many spoofed emails are in circulation to gauge the impact if the policy were to be changed to "reject." This kind of reporting is achieved by authenticating the sender domain for email received by the email recipient, and notifying the sender domain of information on email that fails authentication in the form of a report. Reporting is a new burden placed on the recipient side. However, to popularize the use of DMARC it will be necessary for more email recipients to provide this kind of reporting function.

2.3.3 Use of DMARC by Email Recipients

It could be said that from a sender's perspective there are significant advantages to DMARC, as publishing DMARC records prevents spoofed email from being delivered to the recipients. Then let us examine whether DMARC provides any benefits to recipients, who must add a new authentication function and report information on failed authentication to senders.

Up to now, we have stated a number of times that sender authentication technology such as SPF and DKIM are technologies for authenticating sender information, rather than for determining whether or not email is spam. This merely indicates that an authenticated sender domain has not been spoofed, so an authorization process is required to determine whether or not an email should be received. In the world of email, it has long been said that a reputation system for evaluating whether or

*6 Domain-based Message Authentication, Reporting, and Conformance (DMARC) (https://datatracker.ietf.org/doc/rfc7489/).

*7 "Messaging Technology 'Sender Authentication Technology Deployment and Authentication Identifiers'" in Vol.16 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol16_EN.pdf).

not email should be received based on the authenticated domain would be required to perform this authorization. DMARC enables a system in which domains are authenticated using SPF and DKIM, then ultimately DMARC, so it is at last possible to extract a domain using unified methodology. In other words, you could say it is now possible to perform an authorization process to determine whether or not to receive email using reputation based on individual domains.

Implementing DMARC benefits email recipients because clarifying the sender via sender authentication and evaluating them (the domain) reduces the number of unnecessary emails with a low reputation that should not be received. Preventing email recipients from receiving unnecessary email can lighten the load associated with a number of processes normally applied to received mail, such as virus checks and spam filter detection. It also means they do not need to be stored in the message spool. This reduces the burden of viewing and deleting unnecessary email for recipient users, too, improving user satisfaction.

2.3.4 Domain Reputation

The term "domain reputation" is still not clearly defined. In the past, there were examples of domains from which email should not be accepted being expressed as a domain blacklist, and conversely, domains from which email should be accepted were expressed as a whitelist. In general, domain reputation is thought of as a value that takes a more graded approach, rather than being limited to the two values of black or white (or three values if you including domains not included on either list).

For example, this makes it possible to automatically judge even domains with no clear data showing they had sent spam, based on information such as the amount of time that has passed since they were created, or the identity of administrators. That enables us to express their tendencies as a certain range. That said, to raise the accuracy of domain reputation, information on the authentication results of email actually received, and on detection of whether email is spam (or whether this is necessary) by the recipient is very helpful. Recently, I have seen records specifying domain names other than the corresponding one as the target for DMARC record reporting. It appears these reporting targets are also utilized as data for a company's own domain reputation by aggregating reporting emails, and collating cases in which DMARC authentication failed as a useful report, instead of providing them together. This demonstrates how it is possible for domain administrators and companies who collate reporting information to build a mutually beneficial relationship, so the number of businesses providing this kind of report analysis and reputation data may increase.

There are already cases of systems for reporting email received by a recipient as spam in Japan. For example, the Anti-Spam Consultation Center of the Japan Data Communications Association (JADAC) accepts information on spam by way of forwarded email or Web-based input. The Anti-Spam Consultation Center takes measures such as notifying the Ministry of Internal Affairs and Communications (MIC) if there are any violations indicated by this information. The MIC sends warnings to senders or implements administrative measures based on the information it has gathered*8.

If spam along with definitive sender information (domains) can be gathered using this system, it will be possible to further improve the accuracy of domain reputations. Until now, spam was sent to recipients in a one-sided manner, and the recipients had to exert effort individually to exclude it. However, once the use of DMARC becomes more widespread, and spam sender (domain) information can be aggregated over a wide area, enabling domain reputations to be provided as feedback, it may become possible to exclude unwanted spam in a more proactive manner.

*8 Ministry of Internal Affairs and Communications: Anti-Spam Measures (http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html) (in Japanese).

2.3.5 Email Ecosystems

Figure 2 is an overview (framework) showing the relationships between the DMARC implementation of sender authentication, the domain reputation evaluating authenticated domains, and the feedback reporting received email. This is an ecosystem that covers roles of each and sustainable systems for creating a better environment for email use, including the anti-spam measures we have discussed to date. Allow me to go over the basics of each role.

First, when email is received, domain authentication is performed using SPF and DKIM, as well as DMARC. At this stage, assuming the various issues can be resolved using technology, and DMARC authentication fails with the sender policy configured as reject, it may be possible to block receipt (from a technical perspective). Next, the received and authenticated domain is evaluated using domain reputation. If an authenticated domain is registered to a whitelist in advance, it can be delivered to the mail recipient without processing the spam filter, depending on the situation. The difficult aspect of spam filters is how to exclude clever spam that makes itself hard to identify. On the other hand, it is necessary to take measures to prevent false positives in which normal email that should be received is detected as spam. Email like this that is hard to detect based on its content alone can be delivered to recipients easily if the authenticated domain name is included in a whitelist.

Additionally, if it is known that an authenticated domain is clearly one that sends spam, it can be excluded easily without passing it through the spam filter. This shows that if the number of cases detectable in advance increases, it may also be possible to keep spam filter equipment costs in check.

We have reported cases in the past where IDs and passwords subject to SMTP authentication when mail was sent were exploited to use legitimate mail submission servers as stepping stones. To sum up, because the message passes over a legitimate email delivery route, even under this framework, spam would be delivered if that sender were registered to the whitelist. In this case, as long as the recipient can report the false negative (as feedback) to the sender managing domain reputation, it will be possible to detect the transmission server being used as a stepping stone. If the sender-side company references the SMTP authentication records for when an email is sent, it is possible to look up where that email was actually sent from, and who the physical sender is. For example, the PC may be infected with malware, or that subscriber may be explicitly sending spam, but in either case the source of the email can be confirmed, so measures can be taken.

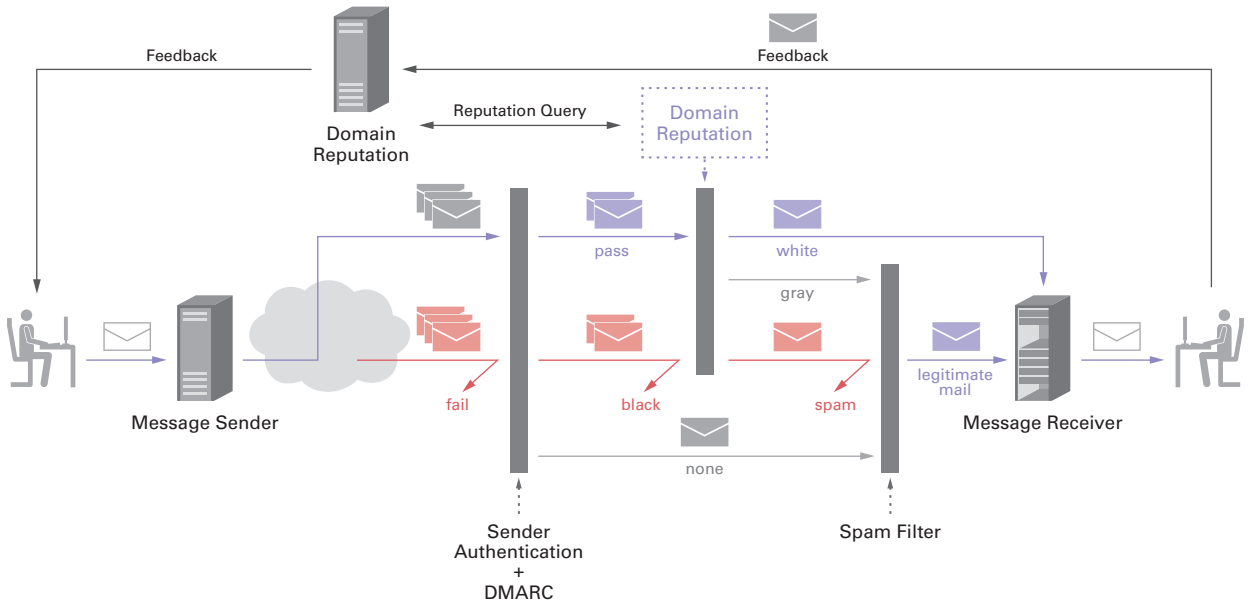

Figure 2: Email Ecosystem

2.4 Conclusion

Last year, in October 2014, the 10th annual conference of the London Action Plan (LAP*9), LAP 10 Tokyo was held at Keio Plaza Hotel in Tokyo. LAP is an organization that brings together administrative agencies from various countries involved with anti-spam measures, and there are currently 27 countries participating. From Japan, the Ministry of Internal Affairs and Communications (MIC) and the Consumer Affairs Agency take part as members. This is closely related to the M³AAWG that I am a member of, and as we have previously held joint meetings on occasion, for the past few years I have taken part in independent LAP meetings together with MIC members. Past LAP conferences have only been held in Europe or North America, but last year the 10th annual conference took place in Japan, the first time it has been held in Asia. To build up this milestone conference, the Anti-Spam mail Promotion Council (ASPC) that I belong to formed a committee to prepare for the LAP 10 Tokyo conference. We put together a panel exhibition at an adjoining exhibition hall, and held the Internet Association Japan's Anti-Spam Conference at the same venue, with the aim of encouraging the general public to attend as well. During the LAP conference I also gave a presentation on the anti-spam measure activities carried out in Japan to date, as a representative of the ASPC. Thanks to the efforts of many contributors, the LAP 10 Tokyo conference ended in success, and participants also voiced their approval of how it turned out.

M³AAWG, which was established in 2004, also reached its 10-year milestone last year. The 32nd General Meeting was held in October 2014 in Boston, USA, the same place where I took part in the initial Founding Meeting. To commemorate the 10th anniversary, the original agenda was presented at the opening, and speeches were given by the three members who have taken part in the most conferences, including me.

When administrative agencies and private organizations came together 10 years ago, I had no inkling that our anti-spam measure activities would still be ongoing a decade later. We launched JEAG*10 in Japan in 2005, and if you include its predecessor organization, 10 years have passed since then. This was another activity I did not expect to last so long at first. I didn't think the problem of spam would be so protracted. For that reason, JEAG was not set up as a formal organization, and everyone involved with it has acted as a volunteer all this time. Still, there is no way a group like that can sustain itself forever, and it has pretty much run its natural course, but the purpose of these activities and the importance of organizations such as these appear to remain unchanged 10 years on. That may be because the system known as email has grown in importance, transforming from a supplementary tool that only a few use into one of the foundations of society.

Naturally, I believe it would be best if these anti-spam measures were no longer needed one day, but at this point in time that may be difficult. I would like to at least help develop an environment where email can be used with a little more peace of mind.

Author:

Shuji Sakuraba
Mr. Sakuraba is a Senior Engineer in the Service Development Section No.2 of the Application Development Department of the IIJ Product Division. He is engaged in the research and development of communication systems. He is also involved in various activities in collaboration with external related organizations for securing a comfortable messaging environment. He has been a member of M³AAWG since its establishment. He is acting chairperson of the Anti-Spam mail Promotion Council (ASPC) and a member of its administrative group, as well as chief examiner for the Sender Authentication Technology Workgroup. Additionally, he is a member of Internet Association Japan's Anti-Spam Measures Committee.

*9 London Action Plan (http://londonactionplan.org).
*10 JEAG: Japan Email Anti-Abuse Group (http://jeag.jp) (in Japanese).