The Background and Characteristics of Email Authentication Technology

In this report we will present an overview of spam trends for week 40 through week 52 of 2012. Spam ratios have once again started to decline after a recent period of little change, with a drop of 5.6% since the last report, and a decrease of 6.3% compared to the same period the previous year. However, as mentioned in this report, security threats resulting from spam such as phishing attacks targeting Japanese users are becoming more serious.

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 report the results of our analysis of survey data for the period of 13 weeks from week 40 of 2012 (October 1 to October 7, 2012) to week 52 (December 24 to December 30, 2012), which corresponds to the 3rd quarter for many Japanese companies.

We look at spam trends, including analysis of changes in spam ratios and the regional sources of spam, as well as incidents in which phishers posed as financial institutions. Regarding trends in technology, we give an overview of email authentication technology and examine its relationship with sender authentication technology.

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 Spam Ratios Declining but Threats More Severe

The average spam ratio for the current survey period (October 1 to December 30, 2012) was 40.5%. This is a drop of 5.6% compared to the previous report (Vol.17). The ratio of spam has also decreased 6.3% compared to the same period the previous year (Vol.14), suggesting a shift to further drops after the recent trend of little change. However, as we also describe in detail later, we believe that security threats resulting from spam are becoming more serious. Spam appears to be evolving from conventional methods of indiscriminate mass-mailing that do not reach all recipients to more subtle techniques focusing on select targets. Figure 1 shows changes in the spam ratio between the same period the previous year (Vol.14) and the current survey period.

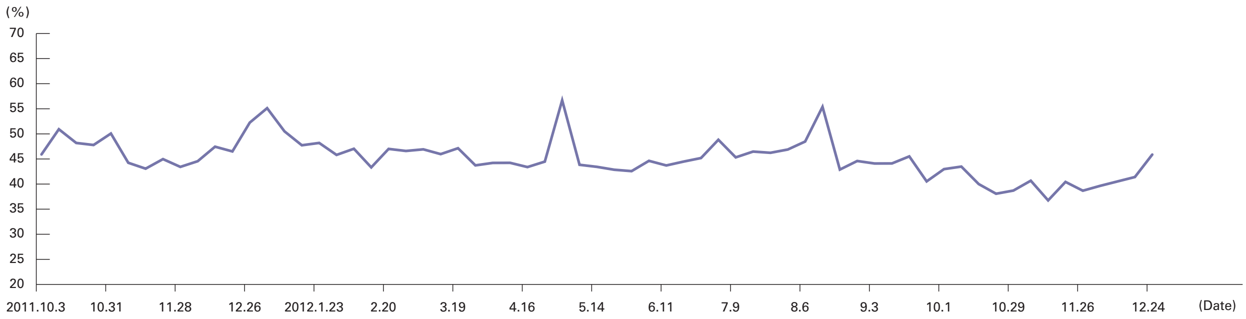


Figure 1: Spam Ratio Trends

2.2.2 Phishers Posing as Banks

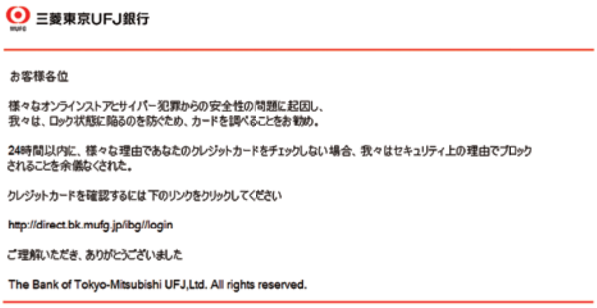
In the past we have touched upon fraudulent activity related to financial institutions, such as the theft of security information through phishing sites disguised as bank websites or fraudulent pop-up screens that appear when accessing actual online banking services[*1]. In this report, we look at incidents in which large volumes of fraudulent mail posing as the Bank of Tokyo-Mitsubishi UFJ were sent in January 2013.

A large volume of email purporting to be from "Mitsubishi UFJ Financial Group" was sent from January 2013. All the email was HTML format, and included information for external image files with links to other websites (Figure 2). The images displayed actual domain names, but because the images as a whole were associated with links, clicking any part of them would launch a site unrelated to the bank (the site itself no longer exists). The Bank of Tokyo-Mitsubishi UFJ[*2] and a number of other banks have issued warnings about this kind of email.

The fraudulent mail involved in this incident contained unnatural Japanese expressions in the image text, and the sender information was inaccurate. Many emails received during this period used the following domain names in the sender information.

- mitsubishiufj.com
- financeufj.com
- ufjnet.jp
- ufjtokyo.com
- ufj.jp

Of these, only the "ufj.jp" domain name exists. This means that mail servers set to block mail from domains that do not exist should not have even received the mail. Typical modern mail servers should be set to block this kind of mail, so we would suggest that mail server administrators double-check their settings. Even when domain names that actually exist are used, authentication of these domain names can show whether or not they were used fraudulently. Authentication methods and their meanings are explained in detail in "2.3 Trends in Email Technologies".



三菱東京UFJ銀行

お客様各位

様々なオンラインストアとサイバー犯罪からの安全性の問題に起因し、
我々は、ロック状態に陥るのを防ぐため、カードを調べることをお勧め。

24時間以内に、様々な理由であなたのクレジットカードをチェックしない場合、我々はセキュリティ上の理由でブロック
されることを余儀なくされた。

クレジットカードを確認するには 下のリンクをクリックしてください

http://direct.bk.mufg.jp/ibg//login

ご理解いただき、ありがとうございました

The Bank of Tokyo-Mitsubishi UFJ,Ltd. All rights reserved.

Figure 2: Content of Email Posing as the Bank of Tokyo-Mitsubishi UFJ

2.2.3 Trends in the Regional Sources of Spam

Figure 3 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 26.6% of total spam. Its ratio also increased 2.6% since the previous period. Japan (JP) was 2nd as in the previous report, with its ratio rising to 18.6%. Hong Kong (HK) was 3rd at 7.9%, climbing from 6th place in the previous survey. South Korea (KR, 7.4%) was 4th, the United States (US, 4.6%) was 5th, and Bangladesh (BD, 3.2%) was 6th.

Saudi Arabia (SA), which was 3rd in the previous report (Vol.17), fell to 31st place in the current survey, meaning that its previous ranking was a temporary increase. Meanwhile, Bangladesh rose dramatically in the current survey. Figure 4 shows trends in the ratio of spam sent from these top six regions (CN, JP, HK, KR, US, BD) for the period of a year (January 2, 2012 to December 30, 2012).

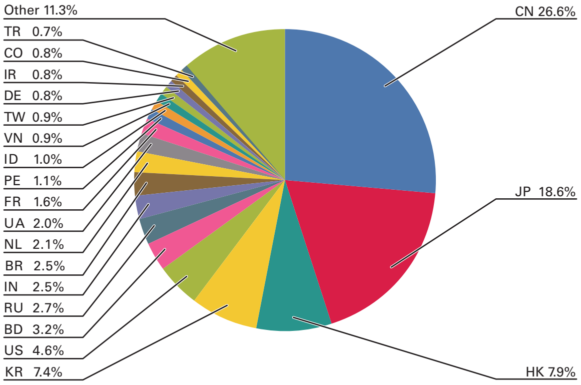


Figure 3: Regional Sources of Spam

[*1] National Police Agency: "Regarding the Development of New Criminal Techniques Targeting the Financial Information of Internet Banking Users" (http://www.npa.go.jp/cyber/warning/h24/121026.pdf) (in Japanese).

[*2] Beware of Suspicious Email Seeking to Obtain Internet Banking Passwords, etc. by Deception (http://www.bk.mufg.jp/info/phishing/notice.html) (in Japanese).

China (CN) was the top regional source throughout the year. On the other hand, the ratio for the United States (US) is gradually falling. We can see that the ratio for Bangladesh (BD) shot up rapidly after November of last year. Upon examination we discovered a large amount of the spam sent from Bangladesh was in Japanese, so there is reason to believe that a hub targeting Japan has been set up there. Regions with established communication environments such as the United States and Europe were the main sources of spam in the past. While progress in spam countermeasures in these developed regions has led to a drop in their spam ratios in recent years, an increasing amount of spam is sent from regions where the communications environment is still developing, as demonstrated by the rise in spam from Saudi Arabia (SA) seen in the previous report. We strongly feel that expanding the use of anti-spam measures around the world will continue to play a crucial role in eradicating spam.

2.3 Trends in Email Technologies

Here we will examine a variety of technological trends relating to email. In this report, we look at a number of technologies related to email authentication.

2.3.1 Email Authentication Technology

Email authentication technology is now used as a basis for determining whether incoming mail should be received and whether it is spam. We have previously detailed SPF and DKIM sender authentication technology in this report, along with applied technology such as DMARC. The sender authentication technology is designed to authenticate email sender information, but before its inception other authentication methods were proposed as email-related technology. Here we give an overview of these authentication technologies, take a look at their background, and examine how they differ from sender authentication technology.

2.3.2 The TLS (Transport Layer Security) Protocol

TLS[*3] and the SSL technology it is based on is commonly used to encrypt HTTP communications and authenticate domains using third party certificate authorities. TLS can also be used with the SMTP mail delivery protocol to encrypt communication paths and authenticate the mail servers of both parties[*4].

To use TLS with SMTP, the "STARTTLS" command is sent at the start of an SMTP session. This initiates a TLS handshake, and subsequently normal SMTP communications continues over an encrypted communication channel.

The BITS[*5] roundtable made up of mostly U.S. financial institutions recommends the use of TLS along with SPF and DKIM sender authentication technology for email security[*6]. Some global companies also require that clients use TLS on their mail servers.

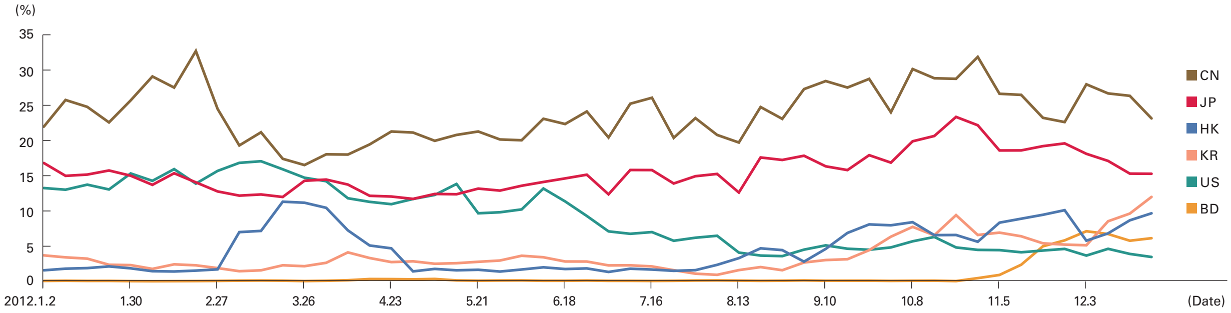


Figure 4: Trends in Ratios for the Main Regional Sources of Spam

[*3] RFC2246, The TLS Protocol Version 1.0.

[*4] RFC3207, SMTP Service Extension for Secure SMTP over Transport Layer Security.

[*5] BITS (http://www.bits.org).

[*6] BITS Email Security Toolkit: Protocols and Recommendations for Reducing the Risks (http://www.bits.org/publications/security/BITSSecureEmailApr2007.pdf).

2.3.3 S/MIME and DKIM

File attachments such as images or application data files sent along with email are implemented via a formatting standard called MIME (Multipurpose Internet Mail Extensions), which splits messages into parts. A number of RFC documents have been added based on the data type of parts, but the basic structure is laid out in RFC2045*[7]

S/MIME defines a system for encrypting email body text and attaching email signature information using this MIME structure*[8]. Mail can also be authenticated by verifying this signature information.

S/MIME is similar to DKIM*[9], with a digital signature used to authenticate mail. However, as is also mentioned in the RFC for DKIM, their approaches differ in the following ways.

- The message signature is written as a message header field so that neither human recipients nor existing MUA (Mail User Agent) software is confused by signature-related content appearing in the message body.
- There is no dependency on public- and private-key pairs being issued by well-known, trusted certificate authorities.
- There is no dependency on the deployment of any new Internet protocols or services for public-key distribution or revocation.

S/MIME was first documented in an RFC by the IETF in RFC1847 in 1995. The first RFC for DKIM was RFC4869, proposed about 12 years later in 2007. As demonstrated by how DKIM came about, if S/MIME became popular during this period and was used effectively for authentication, we believe that DKIM would not have been proposed. We believe a key reason that S/MIME did not become more popular was operational issues, including certificate authority problems (especially cost, etc.), and the lack of a reduction in the amount of mail that cannot be authenticated due to authentication being carried out via the MUA used by the mail recipient. Another issue is the decision of how authentication results should be used is left up to the recipient.

We think that instead of promoting use among individual mail recipients such as MUA users, it is necessary to establish a framework that builds reliability between providers who use mail, providing an environment where key email can be sent and received easily. To achieve this, it will be important to popularize sender authentication technology, share reliable domain names using this technology, and provide a foundation for maintaining domain reliability. We see DMARC*[10] as a promising technology that covers these objectives well.

2.4 Conclusion

In the past mail recipients generally accepted the mail sent to them without question. However, as detailed in this report to date, spam now accounts for most of the mail received, and with the security threats faced by mail users on the rise, it is becoming difficult to maintain this practice. For this reason, we feel it is time to look at shifting from a model in which all mail users are trusted to a model in which rules for the use of mail are set, and trusted partners are filtered or prioritized within this framework. We believe it is first necessary to popularize sender authentication for authenticating senders as a foundation for achieving this.

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 M^{3}AAWG 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.

*[7] RFC2045, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies.

*[8] RFC5751, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification.

*[9] RFC6376, DomainKeys Identified Mail (DKIM) Signatures.

*[10] See Vol.15 of this report for a more detailed explanation of DMARC (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol15_message_EN.pdf).