An Increase in Fraudulent SMTP Authentication for Sending Spam

The issue of third parties using IDs and passwords for SMTP authentication to exploit email accounts for sending spam is on the rise. Botnets are used in many cases, and these attempt to send spam using valid SMTP authentication. Here we discuss trends in access via fraudulent SMTP authentication observed on IIJ's email services.

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. This time we present the results of our analysis of data observed on IIJ's email services.

Recently there have been a series of incidents in which third parties attempt to log in to certain services using the account and authentication information of legitimate users. For portal sites and web services, it seems that in many cases the goal was to steal or alter account information. Meanwhile, fraudulent use of accounts for email services has been a problem for some time. In 2012 the JPCERT Coordination Center reported that the unauthorized use of email accounts had been observed on the email services of a number of ISPs*[1]. It is said that most fraudulent use of email accounts is for sending spam, and botnets are often used for this.

In this report, we cover issues stemming from the fraudulent use of email accounts, and look at trends in access via fraudulent SMTP authentication that we have observed on IIJ's email services.

2.2 Trends in Access via Fraudulent SMTP Authentication

2.2.1 Fraudulent SMTP Authentication

SMTP authentication is essentially used to confirm that a legitimate user was the sender of an email. However, in recent years there have been issues with the ID and password information used for this SMTP authentication being stolen by some means, such as through virus infections, and exploited by an illegitimate third party to send spam. In this report, we refer to SMTP authentication carried out by a third party using the authentication information of a legitimate user as "fraudulent SMTP authentication." For the email services that IIJ provides, we observe and respond to access via fraudulent SMTP authentication by applying our own service standards, and we are seeing an increasing number of these incidents.

2.2.2 Identifying Fraudulent SMTP Authentication

It is not easy to identify access via fraudulent SMTP authentication accurately in real time. This is because it is necessary to take into account a comprehensive range of factors, such as geographic trends for the source IP addresses of mail accounts, the number of emails sent, and destination address trends. Geographic trends in source IP addresses serve as a particularly important lead for identifying access via fraudulent SMTP authentication. This access is often carried out from a large number of geographically distributed sources, and shares the same characteristics as spam sent from botnets. Botnets are becoming more devious each year in an attempt to spread them further and make them more difficult to track, and recently the threat of P2P botnets like ZeroAccess*[2] has been reported. IIJ detects and responds to access via fraudulent SMTP authentication on a daily basis by applying our own service standards.

*1 JPCERT Coordination Center, "A Request for Information about Unauthorized Use of Mail Accounts" (http://www.jpcert.or.jp/pr/2012/pr120003.html) (in Japanese).

*2 Over 9 million PCs infected - ZeroAccess botnet uncovered (http://nakedsecurity.sophos.com/2012/09/19/zeroaccess-botnet-uncovered/).

2.2.3 Observing Fraudulent SMTP Authentication

Figure 1 shows the number of accounts targeted by access via fraudulent SMTP authentication observed on IIJ's email services over a set period of time. This figure demonstrates that mail accounts accessed via fraudulent SMTP authentication are detected on a daily basis. On average a few incidents are detected each day, and this number climbs to several dozen incidents on heavy days.

In many cases no trends were seen in the accounts accessed via fraudulent SMTP authentication, but we did observe multiple accounts on a specific domain accessed simultaneously in this manner at times. We estimate that ID and password information for the mail accounts used in SMTP authentication were stolen through virus infections on internal networks.

The mail accounts detected were all accessed by an extremely large number of source IP addresses, which were widely distributed geographically.

■ Geographic Trends in IP Addresses for Sources of Access

Next, we examined geographic trends in IP addresses for sources of access. Figure 2 gives a chronological overview of source IP addresses for account access detected during the current survey period, focusing on the top regions represented.

We can see that for this period access from Poland (PL) and India (IN) accounted for a larger portion than other regional sources of access.

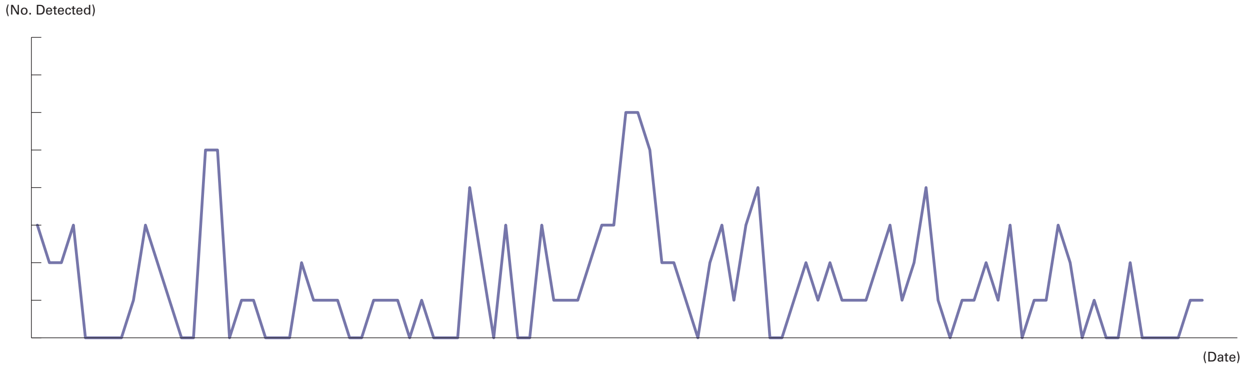

Figure 1: No. of Accounts Accessed Via Fraudulent SMTP Authentication

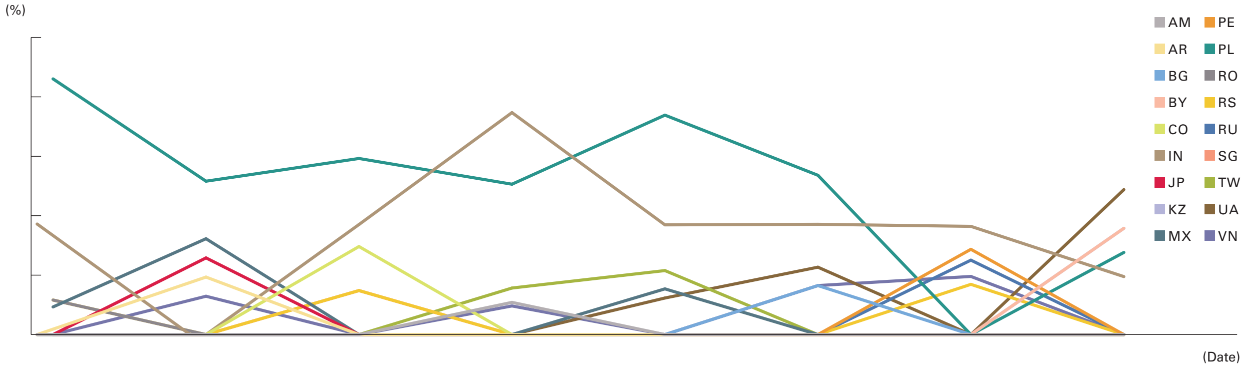

Figure 2: Trends in the Ratio of Regional Sources of Access

A report from the JPCERT Coordination Center*1 suggests that most fraudulently used mail accounts are exploited to send spam. A Sophos report*3 that periodically publishes rankings of the top spam-relaying countries also ranked Poland (PL) as the 10th highest source of spam for 2012, while India (IN) ranked 1st. We can surmise that large volumes of spam continued to be sent from these countries in the current survey period.

In addition to the Central and Eastern European regions mentioned previously, large-scale access exceeding several thousand source IP addresses was also observed from up to 30 countries at peak times, including Argentina (AR) and South Africa (ZA). Although Central and Eastern European regions stand out among the top regional sources of access, with access coming from almost all regions of the world, we estimate that botnets are being used for access via fraudulent SMTP authentication.

■ Trends in Numbers of IP Addresses for Sources of Access

Figure 3 shows trends in the number of IP addresses for sources of access to mail accounts detected to have been accessed via fraudulent SMTP authentication. An average of several hundred IP addresses for sources of access were detected during the current survey period, ranging up to several thousand.

■ IP Addresses for Sources of Access and Number of Spam Sending Attempts

We identified two patterns when examining the frequency with which IP addresses for sources of access were used to send spam during the current survey period. In some cases attempts were made to send several thousand emails from a single IP address, while in others attempts were made to send just a few emails from a single IP address. This latter pattern accounted for 90% of the cases detected in the current survey period, and the former pattern made up the remaining 10%. Figure 4 shows the number of attempts to send mail via fraudulent SMTP authentication per access source IP address for a given mail account in cases fitting the former pattern. Figure 5 shows the same for cases fitting the latter pattern.

Additionally, after examining the interval between access times for each source IP address accessing the accounts covered in Figure 4, we found evidence of continued attempts to send mail several times per second over the period of about an hour for each IP address. Meanwhile, no evidence of continued attempts to send mail from the same IP address was uncovered when performing a similar examination of the accounts covered in Figure 5.

Sending just a few emails from a large number of IP addresses, rather than a large volume of email from a single IP address, is a typical technique used by spammers to make it more difficult to trace sources of access.

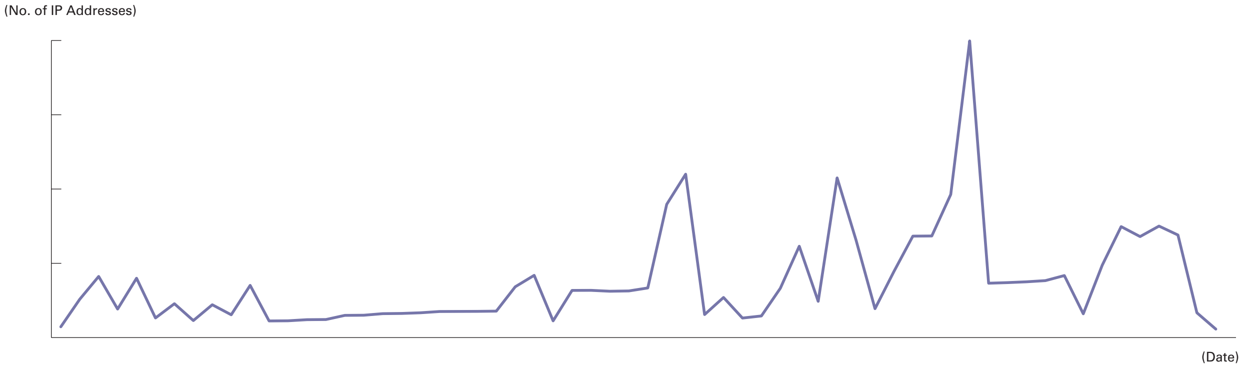

Figure 3: Trends in No. of IP Addresses for Sources of Access

*3 Sophos Security Threat Report 2013 (http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf).

2.3 Conclusion

In this report we examined the issue of fraudulent use of mail accounts, and presented our observations of trends in access via fraudulent SMTP authentication for IIJ's email services. Because our observations of access via fraudulent SMTP authentication indicate that sources are distributed across almost the entire globe, and involve large numbers of IP addresses, we believe it is highly likely that access was carried out using botnets. The geographic trends for source IP addresses also suggest there is a good chance that attempts to send spam continue to be made from areas reported to be top regional sources of spam. Additionally, we observed that attempts to send mail via fraudulent SMTP authentication were not uniform in nature. It is not easy to accurately perceive evidence of fraudulent SMTP authentication access, but IIJ detects and deals with fraudulent access promptly by applying our own service standards.

Meanwhile, according to a report*[1] from the JPCERT Coordination Center, typical methods used by attackers to steal SMTP authentication information for mail accounts include dictionary attacks on POP servers, phishing, and virus infections. This means it is crucial for users to take appropriate protective measures on a continuous basis, such as periodically updating the anti-virus and passwords used on devices, and deleting mail accounts that are no longer needed.

IIJ will continue to analyze and respond to trends in access via fraudulent SMTP authentication for stable operation of email services.

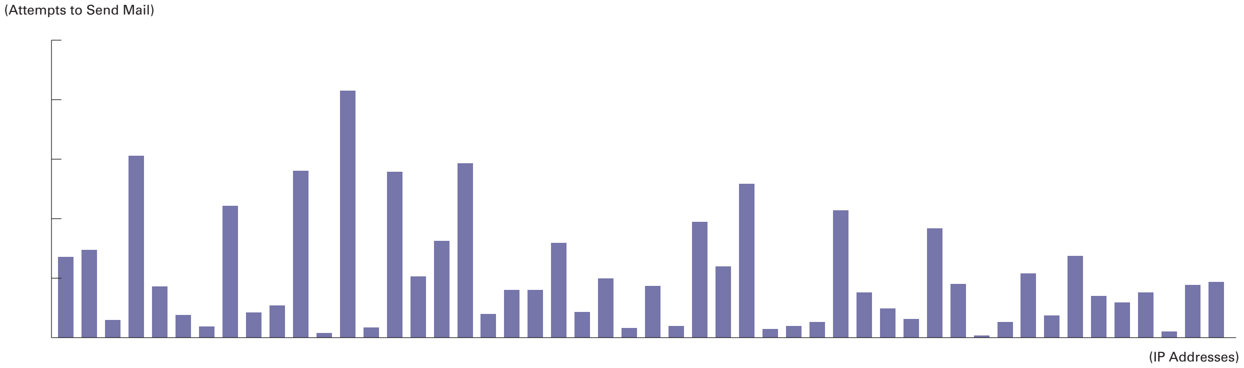

Figure 4: No. of Attempts to Send Mail Per Access Source IP Address

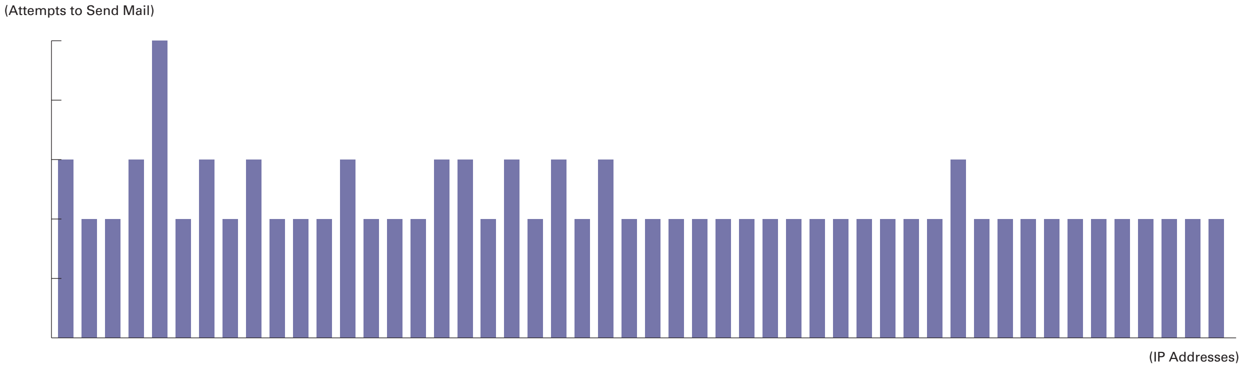

Figure 5: No. of Attempts to Send Mail Per Access Source IP Address

Author:

Takafumi Watanabe
Messaging Service Section, Product Development Department, Product Division, IIJ. Mr. Watanabe joined IIJ in 2009. He is engaged in the development of IIJ's email services. He is also a member of M3AAWG.