An automatic training system against Advanced Persistent Threat

Kazuki Iwata
Graduate School of Systems Information Science
Future University Hakodate
Hakodate, Japan
g2116005@fun.ac.jp

Yoshitaka Nakamura
Graduate School of Systems Information Science
Future University Hakodate
Hakodate, Japan
y-nakamr@fun.ac.jp

Hiroshi Inamura
Graduate School of Systems Information Science
Future University Hakodate
Hakodate, Japan
inamura@fun.ac.jp

Osamu Takahashi
Graduate School of Systems Information Science
Future University Hakodate
Hakodate, Japan
osamu@fun.ac.jp

***Abstract*— In recent years, APT attack (Advanced Persistent Threat) puts out a lot of damage. There is method to train the "human" who received attack emails as a countermeasure of this type of attack. However, the training technique that is currently performed is not in the effective training for individual trainee to be trained. In this thesis, I propose an automatic training system for countermeasure against APT attack to solve those problems. The proposed system can enhance a training effect by repeating training and collecting data.**

Keywords—Network security, Advanced Persistent Threat, Training system, Malware, Training email

I. INTRODUCTION

In recent years, the damage of APT attack (Advanced Persistent Threats) is increasing [1][2]. The attack procedure is shown in Fig 1 below.

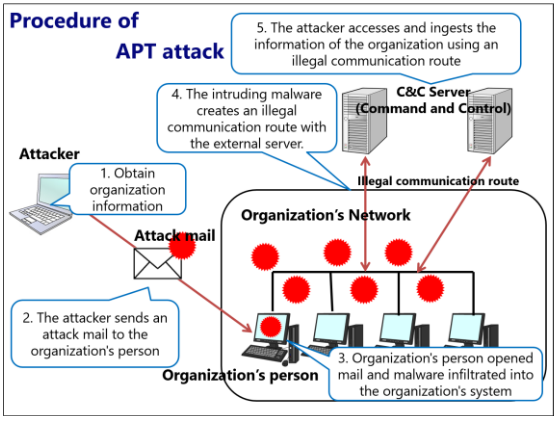
Procedure of
APT attack
5. The attacker accesses and ingests the information of the organization using an illegal communication route
4. The intruding malware creates an illegal communication route with the external server.
C&C Server
(Command and Control)
Attacker
1. Obtain organization information
Illegal communication route
Organization's Network
Attack mail
2. The attacker sends an attack mail to the organization's person
Organization's person
3. Organization's person opened mail and malware infiltrated into the organization's system

Figure 1: Attack Procedure

Because APT attacks are mostly made by malware that is not detected by existing antivirus software, it is difficult to detect APT attacks. In addition, the content of the mail used for the attack is hard to notice that it is an attack mail. Therefore, we rarely notice that we are being attacked. For these reasons, we need countermeasures against these type of attacks. We propose a method to prevent intrusion rather than detecting malware.

II. RELATED WORK

There are studies of measure to detect the malware that invaded by attacker. There are "entrance control" and "exit control" in APT measures. "Entrance control" is a measure to prevent intrusion of malware. "Exit control" is a measure to prevent illegal communication with the outside. In general, exit control such as detecting C & C communication [3] is done. However, in this research we are researching "entrance control". At present, there are countermeasures for entrance control, such as detection of malware by antivirus software and removal of suspicious mail by spam filter. However, unknown malware is often used for APT in recent years. In addition, attack mails are often disguised to some extent in ordinary mail. Therefore, it is difficult to prevent APT by "entrance control". Training for recipients of mail is a solution to these problems. Training is a method of attaching resistance to APT by having "human" experience the attack. As an example, JPCERT / CC (Japan Computer Emergency Response Team Coordination Center) conducted training on APT measures in 2008 and 2009 [4][5]. The training procedure is as follows.

1. Notification of the training
2. Education on APT
3. 1st delivery of training mail
4. 2nd delivery of training mail
5. Questionnaire survey for trainees

In this experiment, it was confirmed that the opening rate of the attached file in the 2nd training is lower than that of the 1st training. However, since it is difficult to create training mails manually, it is also difficult to repeat training. Furthermore, the effect of the training may change depending on the situation of each trainee. Therefore, it is necessary to prepare training mail specialized for each trainee.

III. METHOD

A. Purpose of the study

The purpose of this research to train humans as a countermeasure against APT attacks. This is because it is difficult to cope with unknown attacks with mechanical

978-4-907626-31-0/17/$31.00 ©2017 IEEE

countermeasures, but there is a possibility that countermeasures against unknown attacks by improving the knowledge of security of the trainee. In addition, the other purpose of this research is to carry out training that is appropriate for each trainee be performed. This is to respond to the APT attack that sends an attack mail tailored to the individual who is attacked. For this reason training is carried out using the system to be described later.

B. Automatic training system

The configuration of the proposed system is as shown in Figure 2 below.

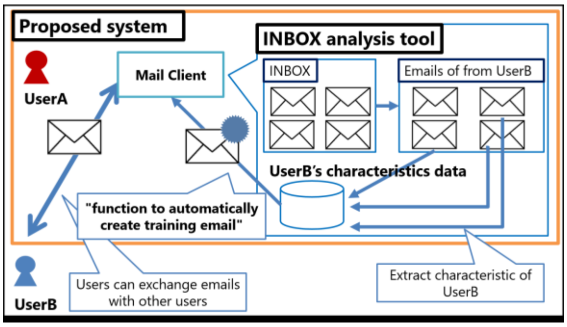
Proposed system
INBOX analysis tool
UserA
Mail Client
INBOX
Emails of from UserB
UserB's characteristics data
"function to automatically create training email"
UserB
Users can exchange emails with other users
Extract characteristic of UserB

Figure 2: System Configuration

In the mail client, it is also possible to exchange and view ordinary mails. In addition, it has the function to automatically train by creating and displaying attack mail for training. An attack mail for training needs to consist of sentences which are not suspicious even trainee receives it. A certain file is attached to this attack mail. When the trainee opens this attached file, it means that the attack by the training mail has succeeded. The system has INBOX analysis tool. This tool analyzes trainee's INBOX, and get the characteristics of mail contents sent from trainee's trusted mail address. The system creates a training email using this analysis result. This function is called "function to automatically create training email". There are some "Unnatural points" in training mails made with this function. Such points often appear in mails used for actual attacks. Therefore the "Unnatural points" need to be reproduced. The "Unnatural points" are created by system based on IPA document [6], and inserted so that the user can notice that it is an attack mail. Automatic generation of mails in this way makes it easier to create training mails that can repeat training. Furthermore, since training emails are created by using personal mail information and training data, the system can carry out specialized training for each trainee. It is considered that the trainee will be able to open mails while paying attention when similar mails are sent.

C. Evaluations

The purpose of this evaluation is to verify whether the result of training is the same as in the past or more than the conventional effect by training methods that we described this paper. The experiment was conducted for three third graders of Department of Media Architecture at Future University Hakodate. The subjects have gained knowledge of information security to some extent. We went as follows with reference to JPCERT / CC 2009 materials [4][5]. First, we explained to the subjects how to conduct training on APT. Next, we taught to the subjects about APT attacks by a trainer. The content is the outline of APT attack and countermeasures. Subsequently, questionnaire to the subjects was carried out. After three days of training, another training started. Training was done three times in 2 days. When opening the attached file of the training mail, contents to educate attention and attacks are displayed. After the training period, a post questionnaire was conducted.

IV. DISCUSSION

As a result of this evaluation, the opening rate of the attached file in third training was lower than that of the first training overall. Also, it seems that the opening rate changes depending on the contents of the training e-mail. In the future, we need to implement the proposed system and evaluate the results of the training using that system and its trends.

V. CONCLUSION

In recent years, there are countermeasures to train "human" to receive attack mails against APT attacks (Advanced Persistent Threats) that will cause damage. In this research, we proposed an automatic training system to train efficiently for each trainee. The automatic training system has a mail client. In the mail client part, there is a function to analyze the mail of the reception BOX and use the data for automatic generation of the training mail. Therefore, the system can generate training mails similar to the e-mail normally received. Thus, it is possible to perform highly effective training for each trainee. In addition, we conducted a basic experiment to confirm the usefulness of the proposed method. The results of this experiment suggest that the opening rate of the attached file is lower and the training effect is improved by repeating the training. In the future, we want to implement the proposed system and evaluate the usefulness of the proposed system.

REFERENCES

[1] IPA, “Survey Report on Damage to Information Fiscal 2014,” [Online] http://www.ipa.go.jp/files/000043418.pdf, [Accessed:2015/11/10]

[2] IPA, “Survey Report on Damage to Information Fiscal 2013,” [Online] http://www.ipa.go.jp/files/000036465.pdf, [Accessed:2015/8/10]

[3] K. F. Hong, C. C. Chen, Y. T. Chiu, and K. S. Chou, “Ctracer: Uncover C&C in Advanced Persistent Threats Based on Scalable Framework for Enterprise Log Data,” *2015 IEEE International Congress on Big Data,* pp. 551-558, June. 2015. [Online].

[4] JPCERT/CC, “2008 Security Immunization Study Report,” [Online], http://www.jpcert.or.jp/research/inoculation2008html, 2009, [Accessed: 2015/11/10]

[5] JPCERT/CC, “2009 IT Security Immunization Study Report,” [Online], http://www.jpcert.or.jp/research/inoculation2009.html, 2011, [Accessed: 2015/11/10]

[6] IPA, “How to distinguish from examples of APT,” *IPA Technical Watch*, [Online], https://www.ipa.go.jp/files/000043331.pdf, [Accessed: 2015/11/18]