T. Hirashima et al. (Eds.) (2011). Proceedings of the 19th International Conference on Computers in Education. Chiang Mai, Thailand: Asia-Pacific Society for Computers in Education

A practice of anti-BOT education for high school students

Kazumitsu MASUYAMA[a*,b], **Naoshi SATO**[a]
[a] *INSTITUTE of INFORMATION SECURITY, Japan*
[b]*Kanagawa sogo sangyo high school, Japan*
*dgs104102@iisec.ac.jp

Abstract: Recently, BOT has caused many security incidents and given us serious damage. Information security incidents often occur based on computer user's lack of knowledge and/or false recognition on BOT, and anti-BOT education is essential especially for young generation. This paper shows our experience of practical anti-BOT education for high school students, and describes how to improve their information security capabilities.

Keywords: anti-BOT education, Information security education, BOT

Introduction

When BOT, a kind of malicious software, infects a user computer, the computer could be controlled remotely through the Internet. The computers infected by BOT cooperatively configure a BOT network, and are employed to practice systematically information security attacks such as sending spam mails, DDoS(Distributed Denial of Service) and password exploitation. Even if a computer is infected by BOT, no symptom of the infection appears generally. So the user can't find the infection until the above attacks get realized and the user recognizes his own assistance to the attacks. In particular, most of high school students have never experienced the threat of BOT and don't have sufficient knowledge about BOT.

Considering the situation, we discussed anti-BOT education scheme in a high school; Kanagawa sogo sangyo high school and put it into practice as a special lesson program. That is, the anti-BOT education scheme is deployed as a school setting subject "Information Security" at Kanagawa sogo sangyo high school. The following in this paper outlines and evaluates effect of the anti-BOT education.

1. School setting subject "Information Security"

Kanagawa sogo sangyo high school developed the school setting subject "Information Security". The school setting subject is specially arranged by the school itself, which is different from the usual subjects designated by official education authorities. According to the government course guidelines in Japan [1], school setting subject is defined to be set up with the purpose to contribute formation of unique curriculum that features regionality and reflects reality of concerned schools and students.

Objectives of "Information Security" are "Acquiring the basic knowledge of information security, to enable implementation and analysis of information systems security policy." Curriculum of the school setting subject "Information Security" is constructed from anti-malware measures, incident response, encryption, authentication and management.

2. Practice of anti-BOT education

This chapter describes anti-BOT education in "Information Security". The lesson includes 56 students at second grade and third grade. The lesson for the anti-BOT education was executed on November 18 and 26, 2010. The content of this lesson is shown in Table 1. First, BOT's operation for DDoS attacks and mail spamming was presented for discussion in the lesson. It seems difficult for high school students to understand details of BOT because most of them are beginners in terms of information security. Therefore, we promoted understanding of the outline of BOT activities, rather than its technical configuration. Concretely, a representative operation of BOT was explained graphically, which consists of herder, control server and the PC infected by BOT. Chain of commands used for BOT was also shown to assist further understanding.

Preceding to learning of BOT threats, the students studied computer viruses and their countermeasures. Based on the study, we asked if the students can control infection of BOT. As a result, many students answered effective measures were antivirus software. Actually it is hard to detect BOT infection by the antivirus software. So, we illustrated some methods to check the infection. Investigation of hosts file, as the first method, is introduced [2]. That is, content of hosts file in C:\WINDOWS\system32\drivers\etc (for Windows XP) is examined to detect an illegal connection. This method is thought a simple way for student, and can prevent the threat of BOT reliably. The second method is usage of CCC (Cyber Clean Center) cleaner, a tool developed by just to remove BOT [3]. Here, CCC is anti-BOT organization running in cooperation with the Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry. CCC monitors BOT operations in the Internet and distributes the CCC cleaner to the PC users supposed to be infected. We instructed the students how to use the CCC cleaner.

Table1 Contents on BOT lesson.

Item	Contents
Previously survey	- Survey for BOT awareness
Overall understanding of the BOT	- Overview of BOT - Behavior features of BOT - BOT Network Configuration - Examples of threats caused by BOT
Measures of BOT	- measures to prevent BOT infection - method to detect BOT infection Investigation of hosts file Use of CCC Cleaner
Posterior survey	- Survey with a questionnaire

3. Result of posterior survey

At the end of lesson we conducted a survey by using a questionnaire. Table2 contains the six survey items from Q1 to Q6. The answers for each question is ranked from 1 to 5 and their average rank are shown in the table. As for Q1 and Q2, it can be said that the comprehension about lesson contents and threats to BOT are good.

For Q3, it can understand that the students cannot practice measures to BOT very much. And for Q4, It is clear that students do not receive direct or indirect damage from BOT. These responses have been brought about by features of BOT. Therefore, it is necessary to practice effective measures to BOT for the students. In concrete terms, we instructed the students to practice about an investigation method for BOT infection treated in this lesson.

At result, it is reported from the students that approximately 74% of them carried out the investigation methods. This fact shows that the students were highly concerned about BOT. As further reports, it is shown that approximately 8% of students (three) were infected. For a concrete investigation method, three students checked hosts file, and one student of those used CCC cleaner.

On the other hand, as for Q5, a pessimistic answer is conspicuous about social measures of BOT. And for Q6, it is made a low reply for the question about whether the problem for BOT is solved in the near future. From such situation, students feel that malware measures including the computer viruses do not advance as whole society.

From these results, the students were able to understand information security incident measures of BOT through this lesson.

Table2 A result of posterior survey.

Survey item	Average Rank
Q1.Were you able to understand lesson contents?	4.24
Q2.Do you feel information security threats to BOT?	4.50
Q3.Do you practice BOT measures?	3.01
Q4.Have you encountered damage by BOT?	1.56
Q5.Do you think that social measures of BOT advance?	3.29
Q6.Will you think that the problem for BOT is solved in the near future?	2.70

4. Issue

The school setting subject "Information Security" is thought effective to let the student be aware of BOT threats as one of the information security incidents. However, an inappropriately interested student for BOT may appear and misuse the knowledge obtained in the lesson. Such a dilemma accompanies the practice of the information security education. This is because the consideration for both of the defense side and the attack side is indispensable to understand information security. Therefore, in the practical lesson of “Information Security”, it becomes the issue to instruct the students that they would observe information ethics.

5. Conclusion

In this paper, we described about lesson practice about BOT as the school setting subject "Information Security" in Kanagawa sogo sangyo high school and its education effect. We hope that we would realize the lesson jointly with security vendors as industry-academia collaboration and want to expand information security education.

References

[1] Ministry of Education, Culture, Sports, Science and Technology (2010). The government course guidelines. higashiyama syobou (in Japanese)

[2] Information-technology Promotion Agency (2006). Countermeasures on Bots. http://www.ipa.go.jp/security/english/virus/antivirus/pdf/Bot_measures_eng.pdf

[3] Cyber Clean Center (2010). https://www.ccc.go.jp/en_index.html