Basic Study on Targeted E-mail Attack Method Using OSINT

Basic Study on Targeted E-mail Attack Method Using OSINT

Kota Uehara [1], Kohei Mukaiyama [1], Masahiro Fujita [1], Hiroki Nishikawa [2], Takumi Yamamoto [2], Kiyoto Kawauchi [2], Masakatsu Nishigaki [1]
[1] Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011 Japan
E-mail: nisigaki@inf.shizuoka.ac.jp
[2] Mitsubishi Electric, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501, Japan

Abstract. In recent years, attackers have easily gained considerable information on companies and individuals using open source intelligence (OSINT), thereby increasing the threat of targeted attacks. In light of such a situation, modeling the synergistic effect of OSINT and targeted attacks will be an effective measure against these attacks. In this paper, we formulate a state transition model that defines the process by which attackers gather a target's information by using OSINT tools. Then we categorize the targeted e-mails that the attackers can generate in each state. The results of the analysis can be used by the victims to estimate the extent of attacks from the contents of the targeted e-mails, and to take appropriate measures.

1 Introduction

In recent years, the damage due to targeted e-mail attacks has increased rapidly. Targeted e-mail attacks are a typical example of social engineering, causing damage (for example, exploiting information and money, or manipulating PCs illegally) to the targets by deceiving them. To accomplish a targeted e-mail attack, it is essential to make the target believe that the targeted e-mail is a regular e-mail, and thus the attacker attempts to collect information about the targeted person.

Regarding information gathering, previously attackers had to gather information on the target through their own exertions. Typical data collection methods include human intelligence (HUMINT), which pretends to be an administrator or officer to get close to the target to hear information directly from them or to collect information from persons around them, and signals intelligence (SIGINT), which eavesdrops information and communication of the target person. However, in recent years it has become common practice for companies and users to send information about themselves over the internet, such as through owned media and social media. It has been reported that the Web and social media is overflowing with information

pertaining to companies and individuals, and personal identifiable information and privacy information can be obtained by combining public personal information [1], [2]. This information-gathering method is called Open Source Intelligence (OSINT), and there are several tools that support OSINT activities. By using OSINT tools, attackers can create targeted e-mails that are more credible (the target can be more easily deceived), and hence, the threat of targeted e-mail attacks is much greater than before. From the defender's point of view, it is important to consider the target e-mail attacks that use OSINT techniques beforehand [3].

In view of this situation, this study attempts to model the synergistic effect of OSINT and targeted e-mail attacks. Specifically, assuming a targeted e-mail attack [3] using OSINT tools, we formulate a "state transition model" that defines the process by which attackers gather information of the target person using OSINT tools. Furthermore, in each state, we categorize targeted e-mails that the attackers can generate. The results of this analysis provide effective knowledge for the victims to estimate the depth of the attack from the contents of targeted e-mails, and to take measures for restoration accordingly. Moreover, in the future, because OSINT tools will be developed and fully supported by artificial intelligence (AI), attackers will carry out targeted e-mail attacks by misusing AI. The findings of this study can be a foothold in analyzing the synergistic effect of AI and targeted e-mail attacks.

2 Targeted E-mail Attack Using OSINT

2.1 Advancement of Social Engineering by OSINT

OSINT is an abbreviation for open source intelligence, and refers to intelligence activities collecting necessary information from published information. The published information (hereinafter referred to as "OSINT data") includes a wide range of information, for example, newspaper reports, and information written from government officials to telephone directories. In recent years, many individuals and companies have transmitted information related to themselves on the social media and Web, and enormous OSINT data related to individuals and companies is now easily available.

OSINT data is useful information for purposes such as economic forecasting and epidemic analysis. However, OSINT data is also useful in targeted e-mail attacks, more precisely, for attackers who utilize social engineering. It is reported that personal and privacy information can be obtained by combining OSINT data [4], and tools that support OSINT activities are also available [5]. Attackers can now collect information on target persons using OSINT data without performing "troublesome intelligence activities" such as HUMINT and SIGINT. By using the information, an attacker can create a targeted e-mail with high credibility (the target can be deceived easily).

Below, we explain these threats with concrete examples. The underlined parts correspond to the OSINT data.

[Concrete Examples]

Assume that the attacker sends a targeted e-mail to Mr. A who is a university professor in Japan.

1. The attacker uses the name of Mr. A to search the e-mail address on the Web, and obtains the e-mail address whose domain is "*.ac.jp".
2. The attacker searches related web pages using names and e-mail addresses, and examines his researches and achievements from his website.
3. The attacker continues to investigate the related web pages and obtains information that Mr. A previously gave a lecture at company X.
4. The attacker searches the Web about company X to examine the related web pages, and obtains information such as the e-mail naming convention that the employee use or the business that they are focusing on currently.
5. The attacker pretends to be an employee of company X by e-mail spoofing. The e-mail body includes something like the following; “your lecture was great,” “our project currently focused on is related to Mr. A's research,” “we wish you to talk again for our company,” “we would like you to see the attached file for details.” Then the attacker attaches a PDF file containing the exploit code and sends the e-mail to Mr. A.

Although the attacker in this scenario initially had only information on Mr. A's name and profession, they were eventually able to collect considerable OSINT data from the Web. As a result, the attacker succeeded in creating a targeted e-mail with high credibility as shown in Step 5.

2.2 OSINT Tools

OSINT tools are software used to obtain OSINT data related to the search object efficiently, from the enormous OSINT data available on the Web. Numerous OSINT tools (such as Maltego and Creepy) have already been released. Below, detailed operation of OSINT tools will be explained using Maltego and Tinfoleak, which are representative examples of OSINT tools.

Maltego is a data collection and visualization tool developed by Paterva. When you enter a name, domain, URL, or a combination these elements, it automatically collects all kinds of information related to it from the Web. For instance, if you enter the name "Masakatsu Nishigaki" for Maltego, you will receive a list of phone numbers, e-mail addresses, and related Web sites in the format shown in Fig. 1. In this instance, although the social media account could not be found, if there is a matching account name on Twitter or Facebook, information on the corresponding account can also be acquired.

In addition, by further inputting the information obtained here, it is possible to collect information in a chain reaction. For instance, if you enter the domain name "minamigaki.cs.inf.shizuoka.ac.jp" (Fig. 1) obtained by entering a name in Maltego, you can obtain the PDF file, related web site, related domain, web server software information, e-mail address, IP address, and location information obtained from the IP address (Fig. 2).

In this way, it can be seen that the search operations defined in points 1 to 4 (in the scenario described in the previous section) can be semi-automatically executed by Maltego.

Tinfoleak can obtain Twitter ID input information and the following information. While Maltego searches the whole Web on the Web, Tinfoleak collects information limited to a specific service (Twitter).

Tinfoleak can obtain the following information by entering a TwitterID. While Maltego searches on the whole Web, Tinfoleak collects information limited to a specific service (Twitter).

- User basic information (name, image, location, followers, etc.)
- Device and operating system
- Applications used, and linked social media
- Location information (coordinates) given to tweets
- Photographs submitted by users
- Hash tag used by user and time used
- Identification of other users closely related to the user
- Topics on which the user is interested (such as hobbies)

These pieces of information can be obtained by thoroughly checking and analyzing profiles and tweets of target users and interactions with other users, and manually searching for tweets using location information. Tinfoleak provides such information automatically and instantaneously.

These OSINT tools are very useful for authorized users to check to what extent the personal information of its own diffuses, and diagnose the vulnerability of the server that is used (check the daemon and application version). However, in some cases, it has other aspects, such as being used by attackers as a tool to support targeted e-mail attacks (more precisely, for social engineering).

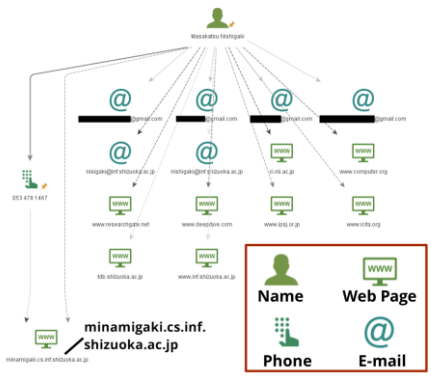

Fig. 1. Result 1 by Maltego (Input: Name)

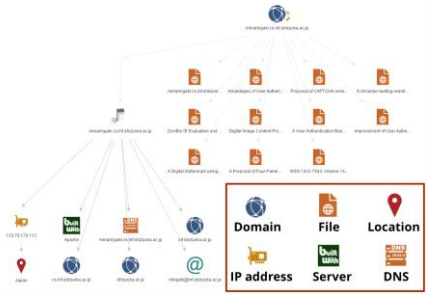

Fig. 2. Result 2 by Maltego (Input: Domain)

3 Synergistic Effect of OSINT and Targeted E-mail Attack

3.1 Threat Analysis by State Transition Model

Considering targeted e-mail attacks using the OSINT tools, this paper attempts to model "the synergistic effect of OSINT tools and targeted e-mail attacks". First, we formulate the process of gathering information of attack targets using OSINT tools by attackers as a state transition model. Then, in each state, we categorize targeted e-mails that the attackers can generate.

In this paper, which is the first step of this research, we focus on the case where the attack target of the targeted e-mail attack is a "specific individual," and model it accordingly. We believe that it is possible to model a targeted e-mail attack by targeting "any member belonging to a specific department" as well, but we prefer to treat that as the subject of our analysis from now on.

3.2 Transition of Information Held by Attackers

In a targeted e-mail attack using OSINT tools, regarding an attacker,

1. Initially, the attacker enters information about the target that he possesses into the OSINT tools, and then obtains new information.
2. Furthermore, the attacker enters the information obtained in step 1 into the OSINT tools to gather information in a chain reaction.

Considering the procedure of attacking, we formulate the process by which the attackers gather information of the target person using OSINT tools as a "state transition model."

In the initial state, "information relating to the attack target person," which is owned by the attacker, is written as {X0}. When an attacker inputs {X0} to the OSINT tool and new information X1 related to the attack target can be obtained, the state changes to {X0, X1} (from {X0}). The attacker continues to input {X0, X1} to the OSINT tools, then further (new) information X2 related to the attack target can be obtained, the state changes to {X0, X1} (from {X0}). After that, this operation is repeated.

For instance, in the state in which the attacker possesses the information {name, phone number} of the target, when information of "address" can be obtained by inputting "name," "phone number" or both in the OSINT tools, the state transitions change from {name, phone number} to {name, phone number, address}.

The attacker freely uses arbitrary OSINT tools and repeats the OSINT activities of the above steps 1 and 2. Here, the OSINT tools group (Recon-NG, Maltego, Creepy, Metagoofil, Tinfoleak, EmailHarvester, the Harvester, SpiderFoot, and ExifTool), which are included in Buscador [6], which is a Linux virtual machine for OSINT collection, is assumed.[1]

[1] Each OSINT tool has its own characteristics, and "input information" for the OSINT tool and "collectable information" obtained as output from the input information are partially different

3.3 Formulation of State Transition Model

When the authors took the attacker's position and tried OSINT activities by actually using the nine kinds of OSINT tools named in the previous section, it was possible for "Process of using the OSINT tool by an attacker to collect information on targets one after another" as a state transition model (Fig. 3).

In the state transition model to be formulated this time, the following assumptions are provided for simplifying the model.

- The type of OSINT data to be considered is confined to name, phone number, e-mail address, social media account, hobby, location information, friendship, affiliation organization name, managerial name in the organization, and organization's public information.
- Build a state transition model with the assumption that the attacker holds only the attack target {name} as the initial state.
- Do not consider information that can be inferred from the held information. (For example, it can be easily guessed that the subject belongs to the educational institution at the time when it is found that the domain of the mail address to be attacked is "ac.jp," but this time, do not perform such deductions.)
- If you enter the social media account into the OSINT tools, you can always acquire information on hobbies, location information, and friendships of people in that account (*a in Fig. 3). (Actually, some people include location information in tweets on Twitter, whereas some people do not include them at all. However, for simplicity this time, we will assume that these three pieces of information are known from the social media in general.)
- Several organizations currently publish IR information and the like in web pages, therefore if you enter an organization's name in the OSINT tools, you will be able to acquire information related to the names of the executives, business contents, and group companies (affiliates) (*b in Fig. 3).

Presently we will focus on targeted e-mail attack (targeted attack via e-mail), therefore we exclude "address," which is information related to postal mail from the OSINT data handled.[2]

---

for each tool. Due to space limitations, the list of "input information" and "collectable information" of each OSINT tool is omitted.

[2] When we actually tried OSINT activities, it was rare (only when the customer management database is in an open state etc., due to misconfiguration etc.,); the case where the address could be acquired by the OSINT tool. Therefore, excluding addresses in this analysis is reasonable, also from the meaning that the address is not "information that can be easily acquired by the OSINT tool."

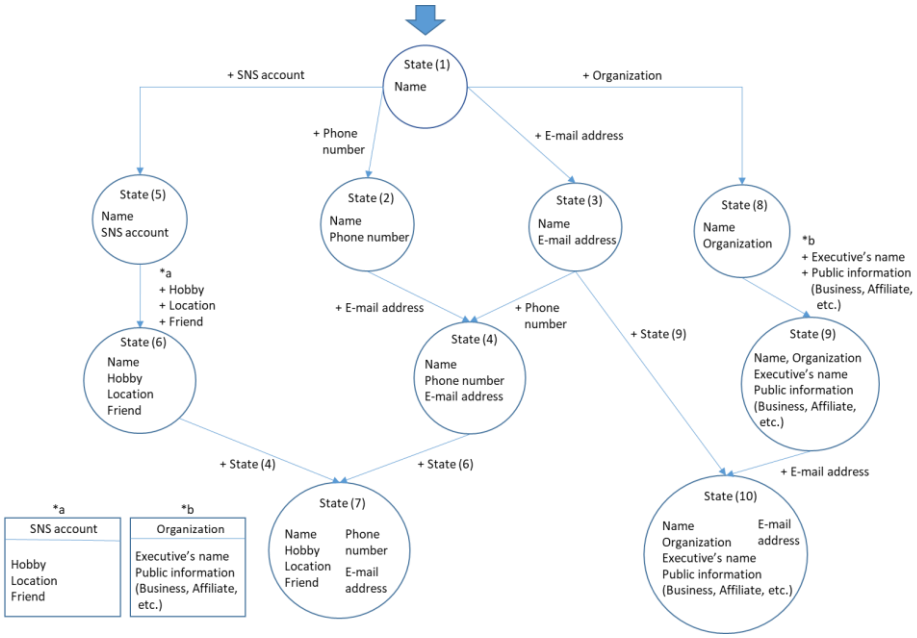

Fig. 3. State transition model of the process by which attackers gather information

3.4 Targeted E-mail that Attackers can generate in each State

Typical examples of targeted e-mails that an attacker can create in the four states (states (3), (4), (7), (10)) in which e-mails can be sent in the state transition model shown in Fig. 3 are shown in Figs. 4 to 8.

- State (3) (Fig. 4):

In state (3), because the information on the attack target held by the attacker is only "mail address" and "name," the content of the mail is not dependent on the attack target person. Although it can be said to be targeted mail because the name is written in the text of the mail, it is close to the content of general phishing mail.

- State (4) (Fig. 5):

In state (4), an attacker can include the "phone number" of the attack target in the text of the mail. Even if you have nothing to do with the e-mail, the information contained in the body of the e-mail is certainly yours, so the possibility that target is deceived (they may access the link in the e-mail) is thought to be increased. Moreover, the fear that his/her phone number is known to the sender of the e-mail may cause anxiety in the target person, and calm judgment will be lost.

In this case, the "address" of the target person was excluded from consideration, but if the attacker could obtain the address (instead of the telephone number) of the attack target person, targeted e-mail can be created as shown in Fig. 6.

- State (7) (Fig. 7):

In state (7), the attacker has acquired information on his/her hobby, position information, and friendship from the social media account name of the target person,

such that it is able to create a targeted e-mail impersonating a friend of the target. In this state, it is possible to include the private information of the attack target in the mail, and it is possible to create a targeted e-mail with high credibility. Furthermore, it is known that mail sent by a sender impersonating an intimate person is effective to make the recipient blind [7], hence, the degree of the threat is considered to be high.

- State (10) (Fig. 8):

In state (10), the attacker can create a targeted e-mail like that was a trigger of the massive information leakage incident [8] that the Japan Pension Service caused in May 2015. In case of this incident, the subject and body of the e-mail is included in the contents of the business and the executive's name in which the Japan Pension Service published on the web page, thus a highly reliable targeted e-mail was created and used.

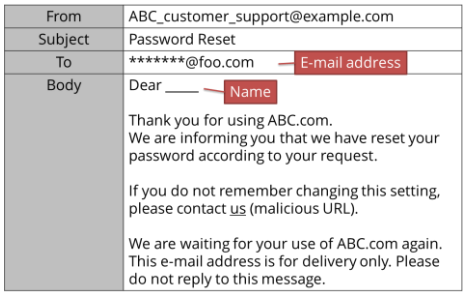

Fig. 4. Targeted e-mail in state (3)

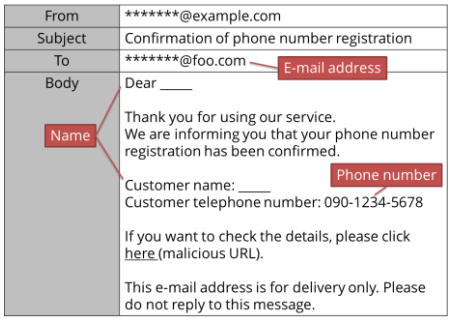

Fig. 5. Targeted e-mail in state (4)

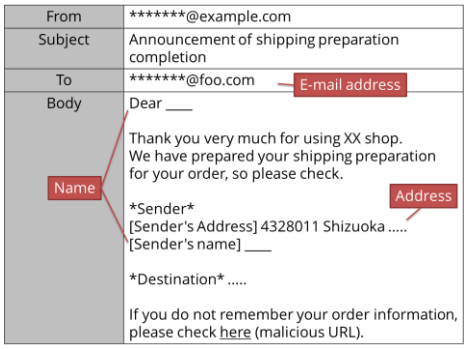

Fig. 6. Targeted e-mail in state in which an attacker has {name, email address, address}

Fig. 7. Targeted e-mail in state (7)

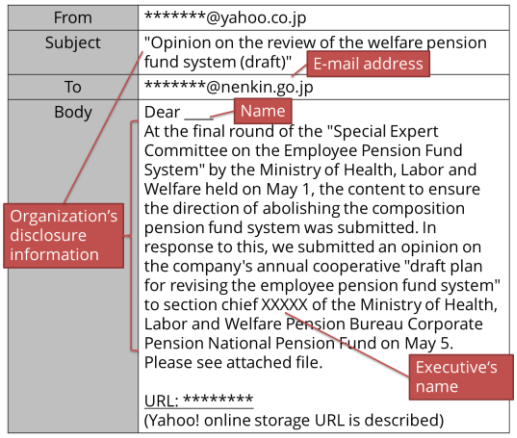

Fig. 8. Targeted e-mail in state (10) [8]

4 Discussion

4.1 Type of Targeted E-mail in each State

As mentioned in Section 3.1, in this paper, we narrowed down the target of targeted e-mail attack to "specific individuals," but here we classify "specific individuals" into three more categories (Table 1). First, the "specific individual" is divided into two depending on whether or not the attack target is "an individual belonging to a specific organization." Then, depending on whether or not the attack target is uniquely specified (whether the number k of persons who can be an attack target is 1 or 2 or more), the two are further divided into two. As shown in Table 1, the three types among these are referred to as "specific individual type," "carpet bombing type," and "specific member type."

For instance, even if an attacker in state (1) could acquire "Gmail address related to the name of the target person" by the OSINT activities, it is also possible that it is the mail address of another person with the same name. In other words, in state (3) it cannot be said that the attack target person can be uniquely identified (Fig. 9). Such a situation can arise, for instance, when the attacker's purpose is "to deceive one of multiple persons of the same name." That is, the target type mail in state (3) is sent to the target of the same name in the same sentence (carpet bombing type).

On the other hand, it can be said that phone numbers and affiliated organizations are unique information for identifying specific individuals (Fig. 10).[3] Therefore, the target type e-mail in the state (4) and the state (8) aims only at the attack target for the purpose of the attacker "deceiving a specific person" or "deceiving a specific person belonging to a specific organization" (Specific personal type, specific member type).

[3] In the case of a large-scale organization, there may be people with the same first and last name, but here we consider an organization of moderate scale.

The tendency of the targeted e-mail type in each state is shown in Fig. 11.

Table 1. Type of targeted mail

Attack target	Number of attack target indicated by k	
	k = 1	k >= 2
Specific individual	Specific individual type	Carpet bombing type
Individual belonging to organization	Specific member type	

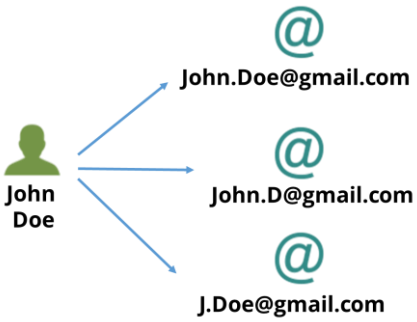

Fig. 9. State in which an individual cannot be uniquely identified

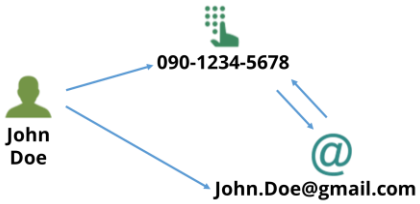

Fig. 10. State in which an individual can be uniquely identified

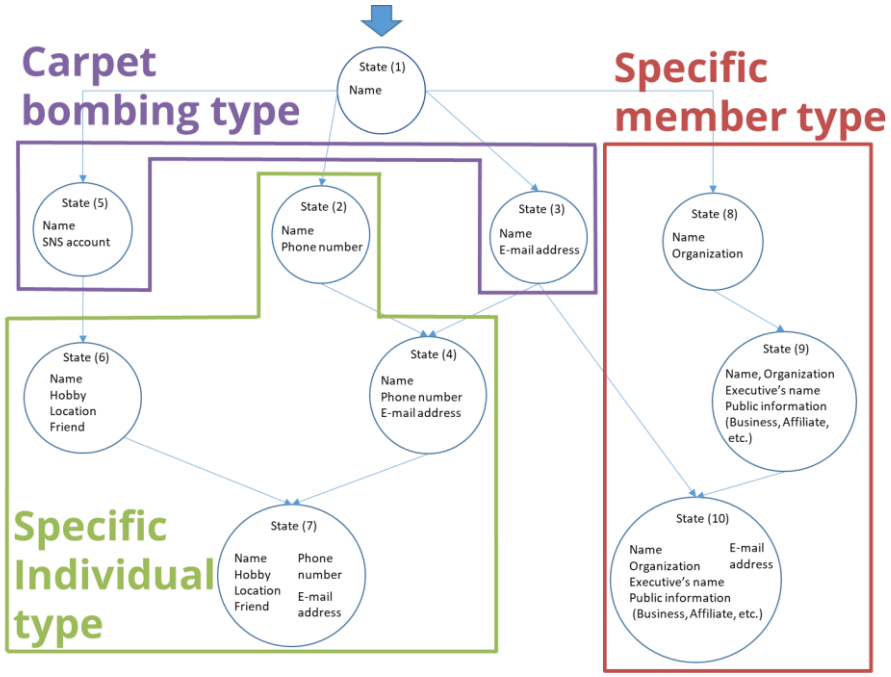

Fig. 11. Type of targeted e-mail in each state

4.2 Use of This Model and Template

It is expected that state transitions in the process of attackers collecting information on target persons and typing of targeted e-mails created in each state can be utilized as the following three findings.

First, it is to grasp the depth of the targeted e-mail attack. When a targeted e-mail is sent to you, the amount of information the attackers are collecting about you can be estimated. Moreover, in the future, it is possible to predict what type of targeted e-mail will be sent when attackers' information gathering progresses. This allows you to pay attention to the expected target type e-mails, and you can know the possibility that another attacker will send similar targeted e-mails. Namely, it is considered useful for risk analysis and advance measures.

Second, it is to grasp what "information about yourself" is disclosed and should be stopped to prevent attackers from creating highly reliable targeted e-mails. From the state transition model shown in Fig. 3, for example, it can be seen that it is effective to refrain from disclosing information in the form of co-occurrence of your name (real name) and social media account so as not to bring the attacker to the state (7).

Third, it is possible to introduce countermeasures for targeted e-mail attacks according to the degree of information disclosure of individuals and organizations. Considering the possibility that targeted e-mail with high credibility may be sent using more information obtained by OSINT, it is necessary to raise countermeasures against targeted e-mail attacks.

5 Related Work

Regarding the effectiveness of OSINT in social engineering, studies with respect to references [3], [9], [10] are being conducted.

Ball et al. mention that there is the possibility that OSINT will be used for social engineering and criminal activity because the amount of data accumulated all over the world is exponentially increasing, and further discuss ways to launch spear-phishing mail attacks on organization employees using OSINT [3]. In the paper, they state that attackers introduce the OSINT tools for information gathering and describe a method to use a dedicated tool for spear phishing. Edwards et al. categorized the OSINT data into two categories, Bootstrap (data used as a trigger for attack) and Accentuator (data supplementary used to increase the effectiveness of attacks), and they showed how the data is used in social engineering [9]. They also investigated the extent to which information such as name of employee, phone number, or e-mail address can be gathered from OSINT about enterprises responsible for utilities such as water supply, gas, and electricity. Further, they revealed the threat of social engineering caused by them.

Silic et al. examined the effectiveness of social engineering using social media for Fortune 500 companies [10]. Specifically, they utilized OSINT, and created a "fake social media account" to impersonate an employee of the targeted company, and became a member of the social media private group composed of regular employees, then revealed whether it is possible to obtain information from the group. As a result,

it is clear that employees are easily deceived, vulnerable to social engineering, and that organizations currently do not have any methods to control over security threats from social media.

In this paper, we survey multiple OSINT tools, and formulate the information gathering process by attackers as a "state transition diagram," focus on targeted e-mail attacks and concretely explain how to utilize information in each state (to create targeted e-mail). Therefore, this paper complements or reinforces the existing research above-mentioned.

Research on machine learning and social engineering is also being conducted [11].

Singh et al. propose a learning model in which target of targeted attack is CFO (Chief Financial Officer) of a company and machine prediction predicts whether person is "able to be targeted (easy to be cheated)" by machine learning [11]. The learning data is the age and gender of CFO, the number of followers and Tweets on Twitter, whether phishing is successful via Twitter or LinkedIn, and so on. By machine learning, it is possible to identify a person who is targeted (deceived) with 80% accuracy, and it is clarified that the evolution of social engineering using it.

Regarding automatic generation of targeted e-mail, Iwata et al. propose analysis methods of received mails for automatic generation of training e-mails in targeted e-mail attack training [12]. After analyzing the user's received e-mail BOX, they confirm what kind of e-mail you trusted and opened, and give a comment such as "It is similar to an everyday e-mail, but its unnaturalness makes you notice that it is a targeted e-mail" to the e-mail, then a training e-mail is created. Research conducted by Singh et al. and Iwata et al. shows that attackers can perform sophisticated social engineering by utilizing big data technology and AI technology. From now on, it is important to prepare for sophisticated social engineering and targeted e-mail.

6 Conclusion

In this paper, we formulate the process by which attackers gather information of targets using the OSINT tools as a state transition model, and categorize targeted e-mails that attackers can generate in each state.

The obtained findings are used for risk analysis such as grasping the depth of attack, assuming what type of targeted e-mail may be received by disclosing information, and selection of required security measures. Briefly, the pre/post-action measures mentioned above are expected to be possible.

Here, we mainly analyzed "targeted e-mail attacks by targeting a specific individual." However, we shall further investigate "targeted e-mail attack targeting organizations" in the future. In addition, although presently only the information that can be mechanically collected by the OSINT tools was taken into consideration, information that can be inferred from the information and information that the user unintentionally made public (for example, such as metadata of the public file) should also be considered. In the future, we will improve these state transition models by taking this information into consideration.

References

1. Acquisti, A., Gross, R., Stutzman, F.: Face recognition and privacy in the age of augmented reality. Journal of Privacy and Confidentiality, (2014) 1-20
2. Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., Dabbish, L.: Anonymity, privacy, and security online. Pew Research Center, (2013)
3. Ball, L.D., Ewan, G., Coull, N.J.: Undermining-social engineering using open source intelligence gathering. In: Proc. of 4th International Conference on Knowledge Discovery and Information Retrieval (KDIR), SciTePress-Science and Technology Publications, (2012) 275-280
4. Best, C.: OSINT, the Internet and Privacy. In: EISIC, (2012) 4
5. INFOSEC, "Top Five Open Source Intelligence (OSINT) Tools," [Online], Available: https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/, [Accessed: 30 Jul. 2018]
6. IntelTechniques.com, "Buscador OSINT VM," [Online], Available: https://inteltechniques.com/buscador/index.html, [Accessed: 3 Aug. 2018]
7. Chen, S.E.R.E N.A., Fitzsimons, G.M., Andersen, S.M.: Automaticity in close relationships. Social psychology and the unconscious: The automaticity of higher mental processes (2007) 133-172
8. Japan Pension Service, "Investigation result report on information leakage cases due to unauthorized access," [Online], Available: https://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf, [Accessed: 7 Aug. 2018] (In Japanese)
9. Edwards, M., Larson, R., Green, B., Rashid, A.,Baron, A.: Panning for gold: automatically analysing online social engineering attack surfaces. Computers & Security, (2017) 18-34
10. Silic, M., Back, A.: The dark side of social networking sites: Understanding phishing risks. Computers in Human Behavior, (2016) 35-43
11. Singh, A., Thaware, V.: WIRE ME THROUGH MACHINE LEARNING. Black Hat USA 2017, Black Hat, (2017)
12. Iwata, K., Nakamura, Y., Inamura, H., Takahashi, O.: An automatic training system against advanced persistent threat. In: 2017 Tenth International Conference on Mobile Computing and Ubiquitous Network (ICMU), IEEE, (2017) 1-2