Multi-layered Defense against Advanced Persistent Threats (APT)

● Satoru Torii ● Masanobu Morinaga ● Takashi Yoshioka ● Takeaki Terada
● Yuki Unno

Recently, crafty cyber-attacks such as advanced persistent threats (APT) have become a menace to systems in enterprises. The APT attack usually uses a variety of intelligent techniques to gain access to a specific target based on elaborate preliminary research on the target. Therefore, the risks involving the intrusion of such malicious unauthorized code (malware) have increased greatly. To confront such novel cyber-attacks, a new approach is needed. The new approach aims to reduce the damage of the cyber-attack by using technologies of early detection and avoidance. Fujitsu Laboratories is developing and commercializing technologies to enable comprehensive countermeasures against each stage of APT, from the initial spying stage of malware to the breakout stage via the system research stage, within an organization's network. This paper presents four research activities concerning cyber-security based on this approach. First, as an inlet measure to prevent APT at its initial spying stage, this paper describes the countermeasure implemented by a client against the targeted e-mail. Then, techniques to optimize security measures implemented by employees and organizations are described by giving consideration to human behavioral characteristics. Further, the techniques to appropriately detect intelligence activity conducted by the malware such as system research are described as an organization's network measure after malware has intruded. In the end, the paper covers the exit control measure after malware has intruded, and this detects the malware's attempt to communicate with an externally controlled server.

1. Introduction

Recently, crafty cyber-attacks such as advanced persistent threats (APT) (i.e., cyber-attacks directed at specific organizations or individuals) have become more cunning than ever. APT is a highly stealthy cyber-attack comprised of diverse attack approaches that can infiltrate an organization with the purpose of stealing confidential information. The APT usually attacks target organizations or individuals persistently based on elaborate preliminary research on the target. Therefore, the risks involving the intrusion of such malware into an internal network greatly increase. To confront such cyber-attacks, a new approach is needed. The new approach aims to minimize the damage of the cyber-attack through early detection and avoidance based on the assumption that intrusions will occur.

Fujitsu Laboratories is developing and commercializing technologies to enable comprehensive countermeasures against each stage of APT, from the initial spying stage of malware intrusion to the breakout stage and research stage within the network after it has intruded, up to the information theft stage. First of all, this paper describes the countermeasure implemented by a client against the targeted e-mail as an inlet measure to prevent APT at its initial spying stage. It is technology to issue alerts and it detects any risk factor in incoming e-mails, and calls for the receiver to be vigilant. Further, techniques to optimize security measures implemented by individual employees and organizations are described by giving consideration to human behavioral characteristics. Then, the techniques to appropriately detect intelligence activity conducted by the malware such as system research are described as an organization's network measure after the malware has intruded. In the end, this paper covers the outlet measure at the boundary of

an organization's network after malware has intruded. In this approach, a technology to detect the malware's attempt to communicate with an externally controlled server is introduced.

2. Measures to prevent malware intrusion: countermeasure against targeted e-mail

With regard to a targeted e-mail attack, which is a typical initial attack approach in APT, the targeted e-mail uses a deceptive subject name or e-mail text and appears to be from an actual individual, organization or acquaintance who is trying to talk to the target about some authorized job or request. Further, it urges the receiver to open an attached file which is embedded with malicious unauthorized code called "malware" by using words that make him or her interested in the file. In many cases, the receiver cannot detect the risk of the e-mail at first sight and carelessly opens the attached file. As a consequence, the system becomes infected with malware and confidential information is stolen.

2.1 Technology to be applied

The targeted e-mail is characterized by the fact that the attack is focused on a specific target and its approach varies depending on the receiver. Different from ordinary spam e-mails that are sent in an indiscriminate manner and in large quantity, the attack is hardly detected by existing spam mail filters, because the sender or e-mail text differs for each individual target. Even sender domain authentication technology has some challenges to overcome to address this issue. If a sender address is disguised, this technology cannot verify the authenticity of the sender, and introducing a server for verification is very expensive.

Accordingly, Fujitsu Laboratories has developed the following two technologies to detect whether a received e-mail poses a risk and alert the receiver, as client-side countermeasures against the targeted e-mail attack (**Figure 1**).[1)]

1) Accurate detection technology based on tie-up between sender and receiver

A common countermeasure tool is introduced to both the sender terminal and receiver terminal in a mutual tie-up with the purpose of preventing a targeted e-mail attack by attackers disguised as a third party. To be more specific, a piece of unique identification information based on the mail header or mail text is created automatically on the sender's terminal and this ID information is added to the e-mail at transmission. The attacker's disguise can be detected by examining how well this ID information matches on the receiver terminal.

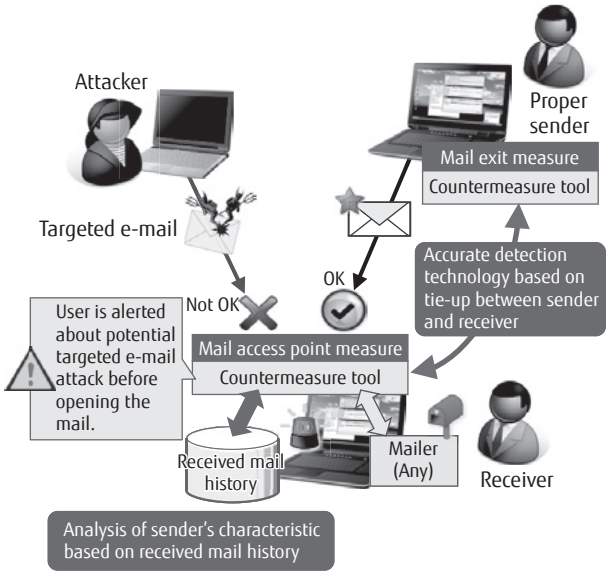

Figure 1
Countermeasure against targeted e-mail attack to prevent malware intrusion.

2) Analysis of sender's characteristics based on received mail history

Even if an e-mail is sent from a sender terminal on which no countermeasure tool has been introduced, it is possible to analyze and determine whether or not it is a targeted e-mail attack by using the characteristics of the e-mails received from the same sender. To be specific, the characteristics of the e-mails from each sender are accumulated as received mail history, and the technology examines how similar a received e-mail is by checking against the received mail history of the relevant sender. For instance, if any deviation from a sender's ordinary characteristics is identified such as a change in transmission route, it is possible to detect a targeted e-mail attack by attackers in disguise.

2.2 Effect

By combining these two technologies, a countermeasure tool has been commercialized that detects and alerts a potential targeted e-mail attack on a

real-time basis before a suspicious e-mail is received by the mailer system.[2)]

By introducing this countermeasure tool, it is possible to call for e-mail receivers to be vigilant without changing the existing e-mail environment and reduce infections through targeted e-mail attack.

3. Measures to prevent malware intrusion: countermeasure based on risk perception

In the previous section, a client-side countermeasure that determines and alerts them against a potential targeted e-mail attack based on mail information was introduced as a technology-based countermeasure. In this section, a technique to enhance the receiver's sense of danger is introduced as a technique to optimize the security measures for each employee or organization so that they are unlikely to be deceived by suspicious e-mails.

3.1 Targeted e-mail attack that takes advantage of psychological bias

It has been known from many psychological studies that human beings have various biases in terms of cognition (cognitive bias). People tend to have a familiar feeling toward things they frequently see or hear or persons they often communicate with. They are likely to see these things or persons in a positive light. It is considered that the attackers take advantage of such a cognitive bias in creating APT e-mails. For instance, they try to catch the receiver off-guard by disguising themselves as someone whom the receiver often communicates with or a contact of the client. This trick makes the targeted e-mails look less suspicious.

Because the attackers take advantage of the psychological bias of receivers in this way, it is imperative to develop countermeasures that take account of human behavior besides the above-mentioned technological countermeasures. It is necessary to optimize security measures to address the situation of each individual employee or function in addition to having organization-wide, uniform countermeasures.

3.2 Risk perception-based countermeasure against targeted e-mail attack

As a countermeasure against a targeted e-mail attack for individuals, there is hands-on training called "targeted e-mail training" (hereafter "mail training") or "IT vaccination".[3)] In this mail training, participants experience simulated targeted e-mail attacks by receiving a mock targeted e-mail. This training has the benefit of enhancing the security awareness of individuals as well as organizations. Meanwhile, it should be noted that there are people who open the mock targeted e-mails and those who do not. It has yet to be clarified how people detect suspicious e-mails, what factors enhance the risk perception of the receivers exposed to a targeted e-mail attack, and what factors lead to actual vigilant behavior. Therefore, Fujitsu Laboratories developed a series of hypotheses about the factors that cause people to be deceived by targeted e-mails. Then, the relationship between the behavior of the mail receiver and the various characteristics of the individual was analyzed based on the results of an experiment conducted on Fujitsu's employees during the mail training and a questionnaire.[4)]

The analysis results revealed that individuals with a higher risk perception are less likely to open a mock targeted e-mail. Further, some of the cognitive characteristics that decrease the level of psychological vigilance were identified. To be specific, it was found that the group of subjects who opened the mock targeted e-mails tends to show a high "self-efficiency" level. Here, "self-efficacy" refers to high self-esteem and overconfidence (for instance, the tendency to believe that you can overcome any difficult challenge, if you do your best). Besides, it was found that those who opened the mock targeted e-mails were reluctant to share information with the people around them (for instance, they were reluctant to share with colleagues their experience of negative events such as being infected with a virus or being deceived by a targeted e-mail).

3.3 Effect

Ideally, these findings will be used to develop countermeasures against targeted e-mail attacks or to automatically detect and provide intensive support for employees who have cognitive characteristics associated with a lower vigilance level. This would make it possible for an IT administrator in an organization to detect and address security risks at an early stage with regard to the security risks of employees. Meanwhile, employees would be freed from excessive pressure

generated by conventional security measures that they all face when doing their job. Based on these benefits, it would be possible to expect more flexible security governance (**Figure 2**).

4. Countermeasures against intruding malware: detection of intelligence activity

Malware that has intruded inside a network is called a Remote Access Trojan/Remote Administration Tool (RAT), and it allows the attacker to gain remote access to the infected host PC. This RAT malware establishes a connection with the attacker's command and control server (C&C server) located in an external network, and the attacker carries out intelligence activity to obtain the targeted information. In this section, technologies to detect these intelligence activity by such malware are described.

4.1 Characteristics of intelligence activity by malware

Through intelligence activity by malware, attackers can gather information on a network, host and applications to steal targeted information. They can also acquire account information. After they have acquired the account information, they try to access it by repeating a node exploration attack (an activity to seek the next target from the host PC that they first infiltrated) and a remote control attack (an activity to steal information by infiltrating the next target) (**Figure 3**). In the node exploration attack and the remote control attack, a protocol called a server message block (SMB) is misused; this protocol is normally used for sharing files or printers in a network environment.

4.2 Technical challenges to be addressed

The attack in the intelligence activity uses the same SMB protocol as the one used in routine works. Therefore, the malicious communications slip into the communications for routine operations, making it difficult to discern them from normal operations.

To address this challenge, it is essential to establish a monitoring method that takes the action mechanism of RAT malware into account. Namely, it is necessary to understand how the RAT malware gathers information, how it transmits the collected data to the external network, and so forth.

4.3 Attack detection technology based on choke point

Misuse of the SMB protocol is one of the attack approaches (choke points) that attackers are forced to adopt in their intelligence activity. Therefore, Fujitsu Laboratories has developed a method to detect the

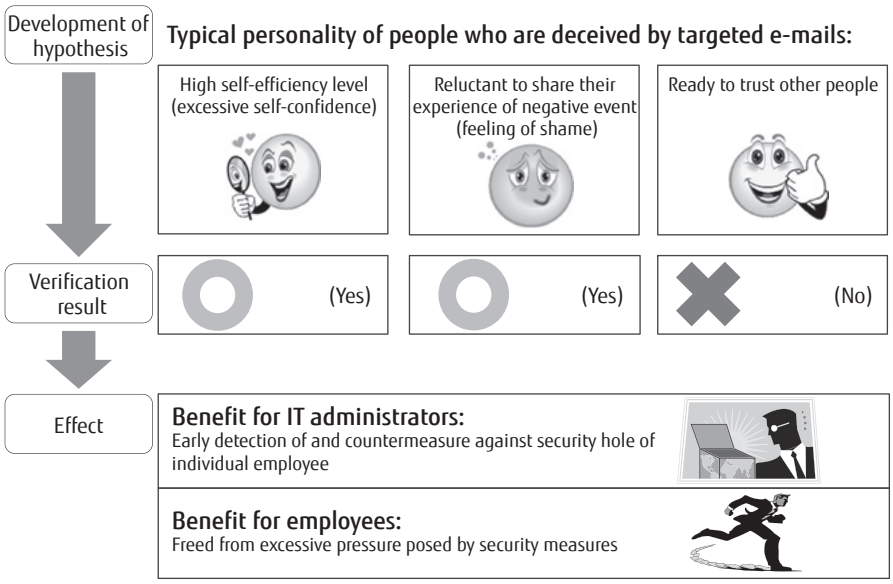

Figure 2
Risk perception-based countermeasure against targeted e-mail attack.

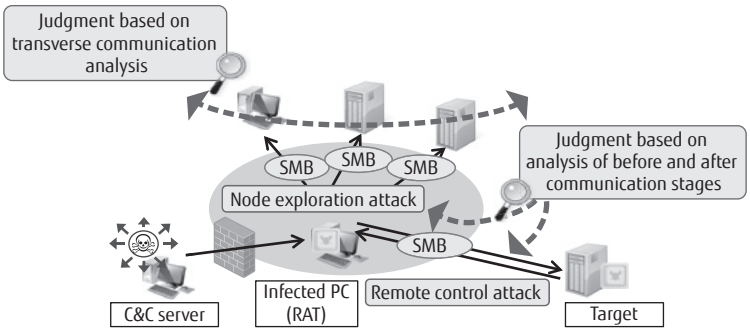

Figure 3
Monitoring of intelligence activity by analyzing intra-organization communications.

intelligence activity of malware by collecting intra-organization communications, capturing these choke points and analyzing the system behavior.[5)]

In this way, the behaviors of an entire system are examined instead of monitoring a single behavior such as an individual communication. To be specific, communications with various counterparts are analyzed on a transversal basis, or, a series of flows before and after a communication is analyzed on a chronological basis (Figure 3). This approach shows to observers any inconsistency and abnormality of all the system's behaviors, even if an individual communication looks normal. Based on this approach, it is possible to find intelligence activity that are different from normal operations.

1) Detection of node exploration attack

In a node exploration attack, attackers misuse the authentication function of the SMB protocol. They repeatedly scan the candidate target nodes and carry out log-in trials using this authentication function. To detect this attack, any inconsistency or abnormality of the authentication request of the SMB protocol is analyzed on a transversal basis for the entire system to determine if this type of attack is occurring.

2) Detection of remote control attack

In the remote control attack, attackers misuse the authentication function, transfer function and execution function to enter the next target. To detect this attack, it is necessary to identify the SMB communication used as signaling. Then, from the reverse connection communication for remote controlling that occurs in the signaling, a series of flows before and after this communication is analyzed to determine if this type of attack is occurring.

4.4 Effect

By analyzing the intra-organization communications as mentioned above, it is possible to swiftly detect the intelligence activity of malware such as a node exploration attack and remote control attack without depending on the signature or operation definition of malware, and attackers can be prevented from stealing confidential information.

5. Countermeasure against intruded malware: monitoring of communication with external network

In recent years, malware that has entered an internal network has established a tunneling route to communicate with improper external control servers and this route allows the attackers to remotely control the victim's IT equipment. It has been difficult to detect this process by using conventional detection technologies. Therefore, Fujitsu Laboratories has developed a "Detection System for Malicious HTTP Communications" to detect any communication with improper external control servers by focusing on the characteristics of communication sessions with external servers (**Figure 4**).

5.1 Detection System for Malicious HTTP Communications

The tunneling route to communicate with improper external control servers should be found among the huge amount of Web accesses that occur in routine operations. However, the control servers are not fixed

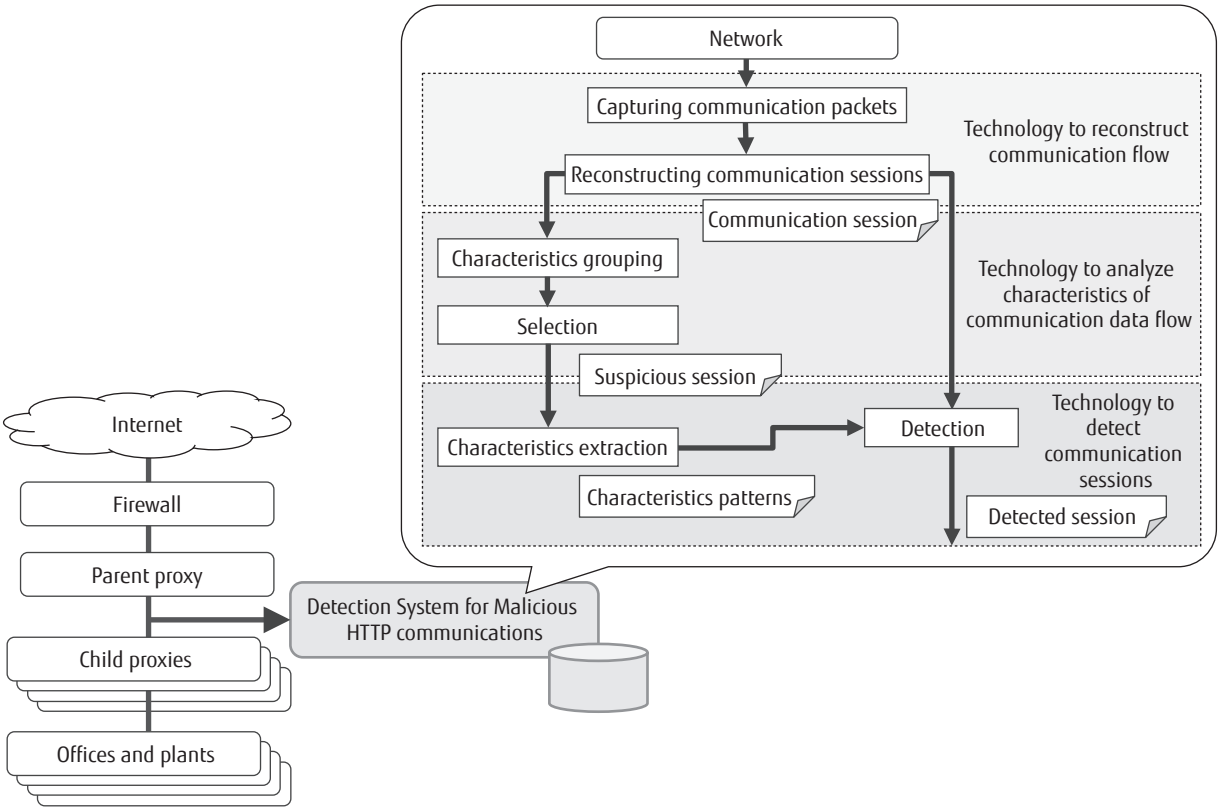

Figure 4
Detection System for Malicious HTTP communications.

and crafty camouflage makes it difficult to identify the server. Even an elaborate check of the access log of proxy servers that relay communication with external networks does not reveal any useful information for identification.

To overcome these difficulties, the following three technologies were developed to discern the difference between communication with a control server and Web access communication by focusing on the characteristics of the improper communication sessions:

1) Technology to reconstruct communication flow

Communications with external servers are conducted via a proxy and continued communication routes are established. Therefore, communication packets for external communication are collected at the preliminary stage of the parents' proxy. Based on the collected packet, a series of communication flows between the concerned servers and the client is analyzed to reconstruct the communication sessions. The communication requests reconstructed in this way should be included in the scope of the monitoring.

2) Technology to analyze characteristics of communication data flow

It is considered that some heart beat to maintain the sessions or control code to indicate some processing request are loaded on the communication route for continuing the communication session. Therefore, the characteristics of the data flow in the collected communication sessions are numerically processed by using various indicators.

3) Technology to detect communication sessions

Observing the communications with external sites for several months and analyzing the characteristics revealed that it is possible to establish a correlation based on composite indicators of the communication status. Further, placing the communications into several characteristic groups was also possible. The presence of some suspicious communication sessions that deviated from the aforementioned correlation or groups were also confirmed.[6)]

It is considered to be feasible to detect communications with suspicious control servers by defining and

registering the patterns of these characteristics.

5.2 Effect

After carrying out a detection experiment within a virtual environment that simulated a local communication network, this approach is currently running in a real environment on a pilot basis. It has been demonstrated that the approach has decreased the false detection rate to about 1/300 versus the level achieved by conventional approaches with regard to cases where normal communication is misjudged as improper communication.[7)]

6. Conclusion

In this paper, we introduced Fujitsu Laboratories' approaches to technologies for multi-layer defense with the purpose of offering safe and secure services. They are comprised of technologies to protect inlet, intra-organization networks and exit points. These technologies are offered in combination with technologies to optimize the security measures for individual employees and functions within the framework of countermeasures against advanced Persistent Threats.

It is considered such Advanced Persistent Threats will be more persistent and crafty in future, and their threats will increase. To address them, we are committed to enhancing countermeasure technologies. Further, we are seeking more sophisticated protection by using a systematic combination of various countermeasure technologies and developing innovative technologies.

References

1) T. Yoshioka et al.: A Client-side Solution for Protection Against Targeted Email Attacks Using Email Feature Information, IPSJ SIG Technical Report, Vol. 2012-CSEC-58, No. 37, 2012 (in Japanese).
2) Fujitsu Social Science Laboratories: Shield Mail Checker targeted e-mail countermeasure (in Japanese). *http://www.ssl.fujitsu.com/products/network/netproducts/shieldmail-ta/*
3) Research Report on IT Security Inoculation FY2009, JPCERT Coordination Center, 2011 (in Japanese).
4) T. Terada et al.: Examination of Targeted-Mail Attack Countermeasure based on Risk Perception, IPSJ SIG Technical Report, Vol. 2013-SPT-5, No. 9, 2013 (in Japanese).
5) Y. Unno et al.: Proposal for a method for detecting the intelligence activity of targeted cyber-attack in the internal system, Computer Security Symposium 2012 (CSS2012), 2012 (in Japanese).
6) S. Torii et al.: Proposing the method for detecting an improper HTTP tunneling communication, IPSJ SIG Technical Report, 2009-CSEC-46(15), 2009 (in Japanese).
7) S. Torii et al.: Extrusion Detection for Remote Access Trojan, Computer Security Symposium 2012 (CSS2012), 2012 (in Japanese).

Satoru Torii
Fujitsu Laboratories Ltd.
Mr. Torii is currently engaged in research and development of cyber security.

Takeaki Terada
Fujitsu Laboratories Ltd.
Mr. Terada is currently engaged in research and development of cyber security.

Masanobu Morinaga
Fujitsu Laboratories Ltd.
Mr. Morinaga is currently engaged in research and development of cyber security.

Yuki Unno
Fujitsu Laboratories Ltd.
Ms. Unno is currently engaged in research and development of cyber security.

Takashi Yoshioka
Fujitsu Laboratories Ltd.
Mr. Yoshioka is currently engaged in research and development of cyber security.