Fujitsu's Know-how and Latest Technology for Measures against Information Leakage by Cyber Attacks

● Michio Masuno ● Atsushi Wataki

While the scope of application of information and communications technology (ICT) is expanding, finding a way to take measures against cyber attacks, which are becoming increasingly advanced and sophisticated, is posing a significant challenge for enterprises. These cyber attacks call for measures premised on intrusion, not to mention measures to prevent intrusion. In the event that a company's defenses are breached, the speed and reliability with which it can respond has a great impact on the risk of information leakage and spread of infection. Fujitsu has developed and offered FUJITSU Software Systemwalker Security Control, which navigates and automates the response according to the specified operation process as a means to deal with this problem. This middleware reduces the cost of the procedure from formulating an operation process to actual security management and allows reliable operation with the elimination of human error by automating response. This paper uses an information leakage accident caused by a cyber attack that occurred in Japan in 2015 as a case example to describe measures that utilize Fujitsu's know-how in internal operation. It also describes the latest technology for measures against cyber attacks, and presents middleware that integrates such operational know-how and the latest technology of Fujitsu.

1. Introduction

Targeted cyber attacks mainly take the form of "targeted e-mail attacks" that seek to steal information and begin with an e-mail, and the number of such attacks grew rapidly from the second half of 2014.

Targeted e-mail attacks deliver malware by e-mail in a bid to infect the terminals within an organization by using the infected terminal as a springboard for deep penetration of the organization, with the ultimate aim of stealing the targeted confidential information or system destruction (**Figure 1**).

In recent years, targeted e-mail attacks have been characterized by increasing sophistication, featuring for example content that forces recipients to open them, based on company regulations or corporate related events. Further, such attacks have been found to be carefully designed based on detailed research on the targeted company or organization, for example specifying only e-mail addresses that are not revealed on the Internet.

Moreover, the malware used in the attacks consists only of content designed exclusively for the target in order to avoid detection by security systems such as anti-virus software. For this reason, malware intrusions in companies and organizations are difficult to prevent. By way of remedy, the introduction of suspicious behavior detection technology that detects intrusions from malware behavior and communication behavior is proceeding.

The purpose of attackers is either the theft of confidential information or system destruction. To penetrate deep inside the target organization, attackers use compromised terminals infected by malware as a springboard to expand the scope of malware infection while snooping inside the organization, gradually getting nearer the confidential information and mission-critical systems that are the target, until they achieve their purpose.

Countering increasingly sophisticated cyber attacks requires raising the level of security operations using information and communications technology (ICT) in addition to improving threat literacy and threat defending skills through education and training (human resource development) and enhancing threat

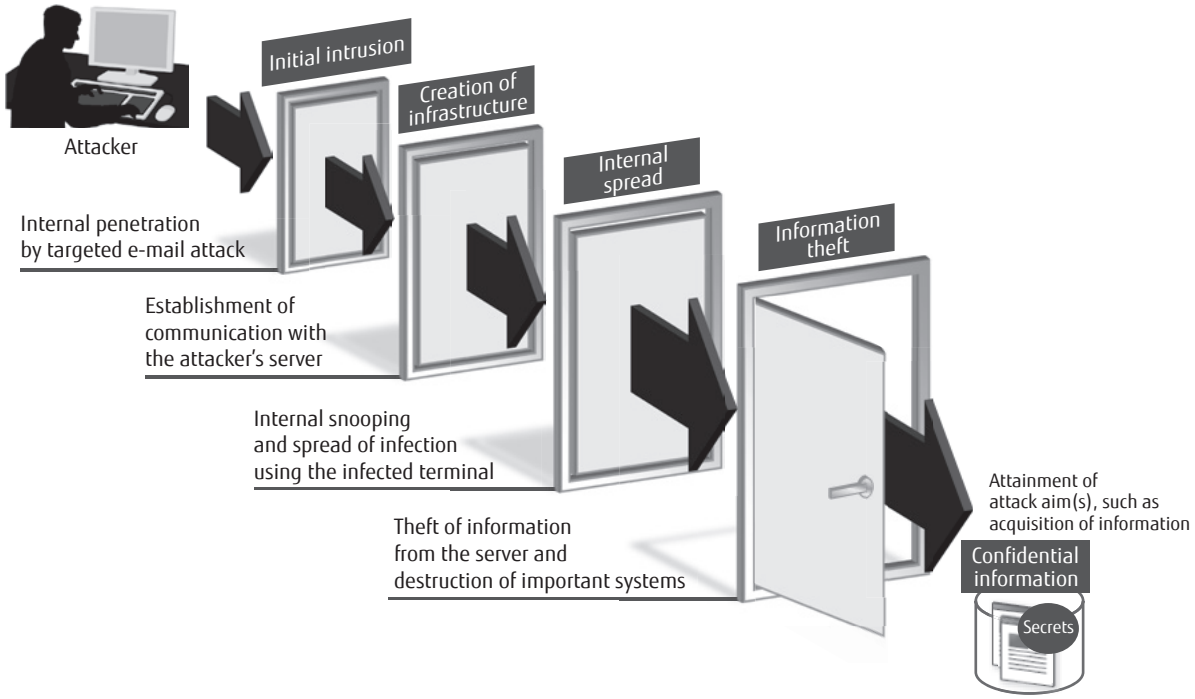

Figure 1
Targeted cyber attack technique.

detection capabilities. Upon detection of a threat, it is important to break the progress of the attack through prompt and reliable response. Further, considering that attackers aim for surprise attacks, it is also important to clearly show the progress of attacks and implement countermeasures accordingly.

This paper describes Fujitsu's internal operations know-how and the latest cyber attack defense technology for measures against information leakage caused by cyber attacks.

2. Cyber attack process and main points of defense

The main points of measure against cyber attacks are described below, taking as an example an actual case of information leakage caused by a targeted cyber attack in Japan in 2015.

1) Delivery of a suspicious e-mail to a public address

The e-mail was opened and infected one terminal with malware. An external security organization detected the suspicious communication and notified the public corporation that received the e-mail in question. The compromised terminal was disconnected from the network.

2) Delivery of a large number of suspicious e-mails to private addresses

Ten days after the initial attack, approximately 100 e-mails with malware attachments reached private e-mail addresses (later, 30 terminals were confirmed to have been infected by malware). Based on the fact that terminals that did not receive e-mails were infected by malware, secondary infection via neighboring terminals is suspected.

3) Leak of approximately one million items of personal information

A few days after the delivery of the large number of suspicious e-mails, a large amount of external communication took place. Files containing personal information that had been stored on file servers were leaked out. Later, it was found that 99% of the leaked files were not encrypted and were stored in plaintext format.

Three main points of defense that can be identified from this information leakage accident are discussed in the following sections (**Figure 2**).

- Response to detected attacks
- Response to undetected attacks
- Strengthening of management of important data

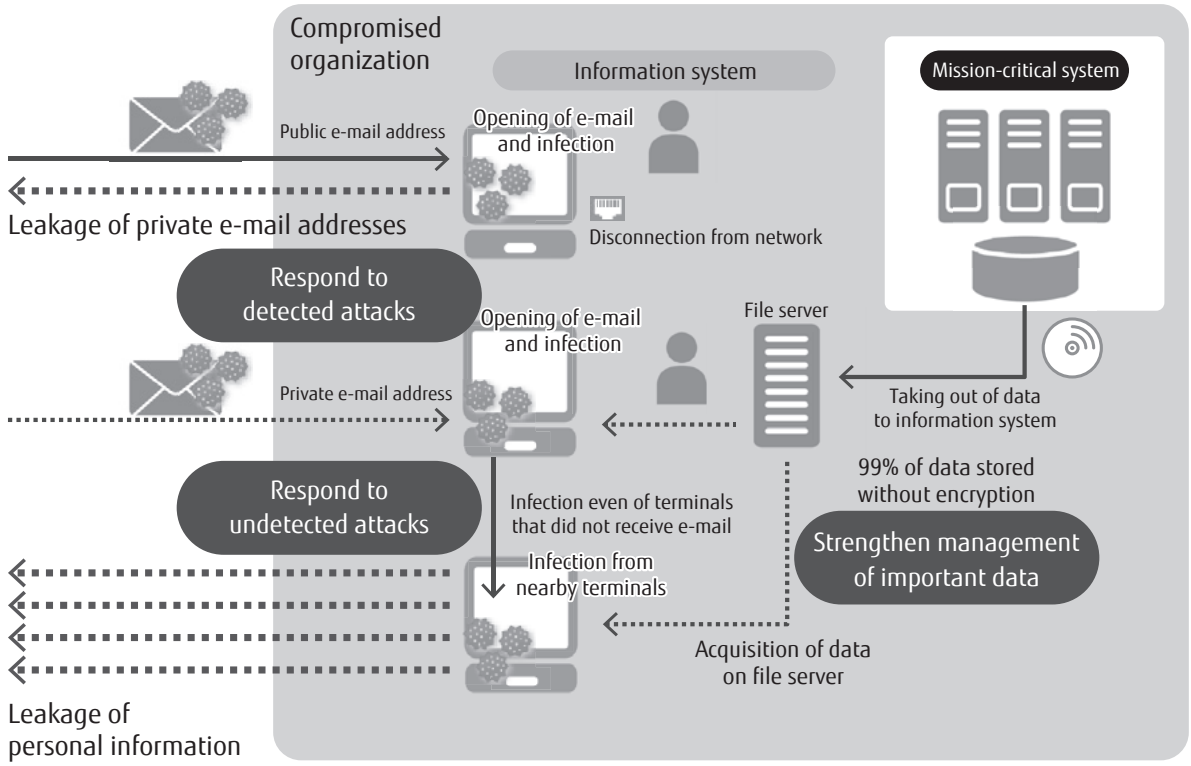

Figure 2
Defense points for cyber attack.

3. Response to detected attacks

In the initial targeted attack, the compromised terminal was disconnected from the network approximately 4.5 hours following detection of suspicious communication from the malware infected terminal. Ten days after the initial attack, a second targeted e-mail attack was launched against private addresses, a fact that suggests that the initial attack achieved the leakage of personal e-mail addresses from inside the organization. The lapse of 4.5 hours from the initial attack until the compromised terminal was disconnected from the network is believed to have led to the subsequent attacks.

3.1 Causes of the accident

The response delay of 4.5 hours until disconnection of the compromised terminal is believed to have happened because, once the person in charge at the attacked organization was notified that unauthorized communication had taken place, the various tasks (confirmation of the response procedure, notification to the concerned parties, assessment of necessity of response, and identification of terminal involved in unauthorized communication) were addressed manually by the concerned parties, including the person in charge.

Thus quick response to cyber attacks must be required, but the response is limited in terms of speed when it is carried out by human operators. Therefore, operations that do not depend on the skills and resources of the persons in charge must be established to ensure the quick execution of measures upon detection of threats.

3.2 Security management practices at Fujitsu

Fujitsu implements security controls for approximately 300 companies both in Japan and overseas that are all connected to the Fujitsu corporate network.

As targeted cyber attack countermeasures, which are one aspect of security control, Fujitsu standardizes the response content and procedures (operational processes) to be applied upon detection of cyber attack threats, and further incorporates automated processes

in the form of middleware in standardized operational processes. Automation makes it possible to shorten the time required from threat detection until determination of the infected terminal(s) and notification of the administrator to one thirtieth (from 30 minutes to 1 minute) compared with the conventional human operations.

Fujitsu began offering its FUJITSU Software Systemwalker Security Control, which incorporates operation scenarios developed through such in-house security operations in August 2014 (**Figure 3**).

An operation scenario is a system for achieving quick and reliable response to detected malware by systematizing the response procedure (flow) and automating parts of the procedure. The following are examples of operations that have been automated.

- Identification of the terminal(s) suspected of infection and the terminal's administrator(s) and/or user(s) based on the IP address(es) of the terminal(s) notified by a malware detection tool, and issuance of response instructions to the terminal
- Communication blocking between the suspicious URL indicated by the malware detection tool and the other terminals within the organization

Operational scenarios can also be customized according to the corporate/organizational structure and operations, including the addition of notification destinations and changes to the external communication cut-off method for compromised terminals.

4. Response to undetected attacks

The response to the case described in the previous section consisted in analysis of the terminal first infected by malware by a security vendor, and the distribution of virus signature codes (virus patterns) for the identification of malware to all terminals. Notwithstanding this, the malware sent 10 days after the beginning of the infection failed to be detected and removed, resulting in information leakage.

4.1 Cause of infection by the secondary attack

The attacker used the information obtained from the initially infected terminal to launch secondary and tertiary attacks not detectable by the security system through the use of different techniques and new malware.

The inability of security detection systems introduced as an entry/exit point defense poses the following problems for companies.

- Companies do not know that they have been internally infected by malware and that confidential information has been stolen from them.
- The status of infection of terminals other than those where the malware infection was detected is not known.

To prevent damage from such malware that escapes detection, Fujitsu and Fujitsu Laboratories have developed diagnostic technology to assess damage caused by targeted cyber attacks.

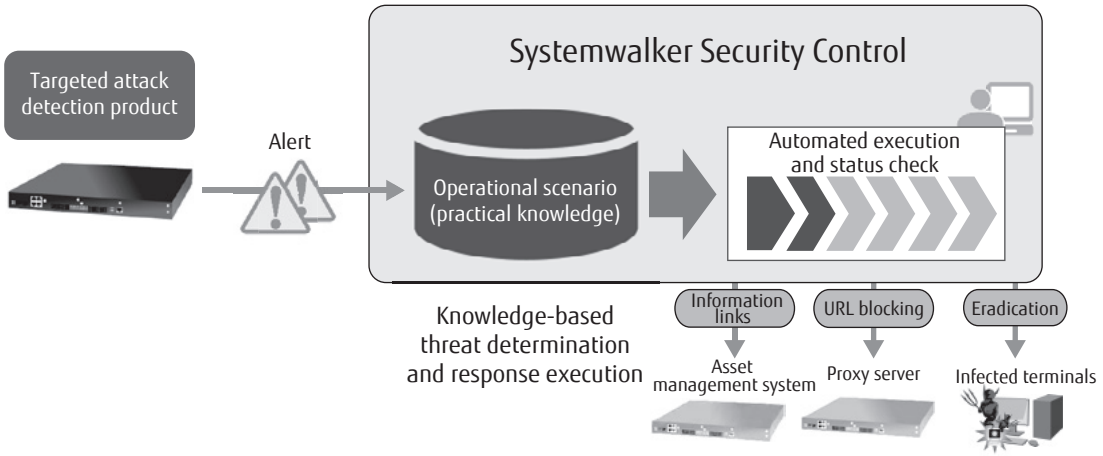

Figure 3
Response to detected attacks.

4.2 Damage assessment technology

This damage assessment technology is designed to assess the presence of damage from cyber attacks on terminals, by comparing and analyzing multiple logs on terminals, using the attack signatures of malware as keys. Specifically, the following points are determined.

- Has the terminal fallen under unauthorized remote control?
- Has information been illegally leaked out from the terminal?

The damage assessment technology can also be applied to terminals where a malware infection has been detected in order to determine the terminals to which the infection may have spread.

When applied to actual accidents, the damage assessment technology allows detection of the terminals that may have been subjected to unauthorized remote control from malware infected terminals. Moreover, using the terminal subjected to unauthorized remote control as the starting point, it can track also terminals that have suffered secondary infection. It can also determine the names of the files that are leaked out from the terminal and thus reveal the actual nature of the damage (**Figure 4**).

This damage assessment technology has been incorporated in FUJITSU Software Systemwalker Security Control as an exclusive Fujitsu technology that constitutes a new defense against targeted cyber attacks.

5. Strengthening of management of important data

The third problem was violation of the business process rule that all information taken outside the organization must be reported and encrypted, which is a standing rule. Although this does not directly compromise measures against the two aforementioned targeted cyber attacks, this is still an important and fundamental problem in view of the aftermath of the kind of information leakage that resulted from the case described here.

5.1 Cause of business process rule violation

Users taking out personal information from mission-critical systems were supposed to perform the following work procedures in order to use that information.

1) Encryption of the file when it is taken out from the mission-critical system to a shared server
2) Copying of the encrypted file from the shared server to the user's terminal
3) Deleting of the files following completion of use from the PC and shared server

However, under their own judgment, users give priority to operational efficiency over compliance with rules, and it can be surmised that step 1) (encryption of files) and step 3) (deletion of files) were not followed.

Thus it is important that established rules not be made to be complied with based on personal judgment, but instead to achieve automatic rule compliance through the use of an ICT system.

5.2 Rule compliance through ICT system

Through the adoption of an ICT system for rule compliance, the work required per the established rules is done by the ICT system, thereby minimizing the scope of the tasks that users need to do. The work

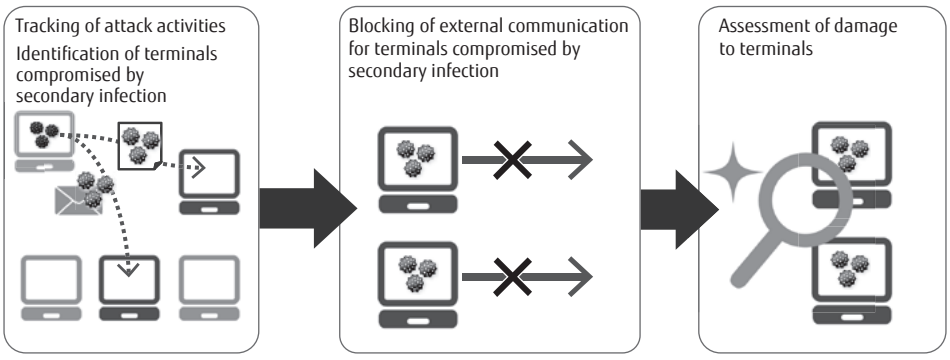

Figure 4
Application of damage assessment technology for terminals compromised by secondary infection.

procedure to achieve this is described below.

1) The user uses the ICT system to apply to the administrator for the use of personal information.
2) The administrator uses the ICT system to check the content of the application and approve the application.
3) When the application is approved, the user obtains the permissions grant to the requested files from the ICT system.
4) The user uses the ICT system to apply for permission to take out personal information.
5) The user obtains the requested files encrypted by the ICT system.
6) The user decrypts the obtained files and uses them.

Rule compliance using the ICT system can be realized with FUJITSU Software Systemwalker Security Control, which incorporates workflow technology (**Figure 5**).

Furthermore, used in combination with FUJITSU Software Systemwalker Desktop Keeper, it is possible to authorize manipulations of files that are taken out such as the following, and to perform control checks.

- Copying of files decrypted by the user to external media, forced encryption of files, logging of information that is taken out, and storage of the original files
- Tracking the copy destination of files when the user copies decrypted files to other terminals
- Tracking of the original files of files that are taken out (for example, files that are e-mailed)

6. Conclusion

Using an actual case of personal information leakage as an example, this paper has introduced Fujitsu's operational know-how (rapid and reliable implementation of response following the detection of malware), measures that use the latest technologies (assessment of damage caused by undetectable malware intrusion), and the FUJITSU Software Systemwalker Security Control and FUJITSU Software Systemwalker Desktop Keeper defense solutions, which incorporate these measures. These middleware products curtail the spread of cyber attack threats and minimize damage from information theft.

As cyber attack techniques continually evolve, it is important to implement new defenses in a timely manner, and to maintain and extend security management. Along with these middleware products, Fujitsu aims to protect the ICT environment of customers from new threats through the operational know-how it has developed in house and the timely provision of technologies for the detection of new threats.

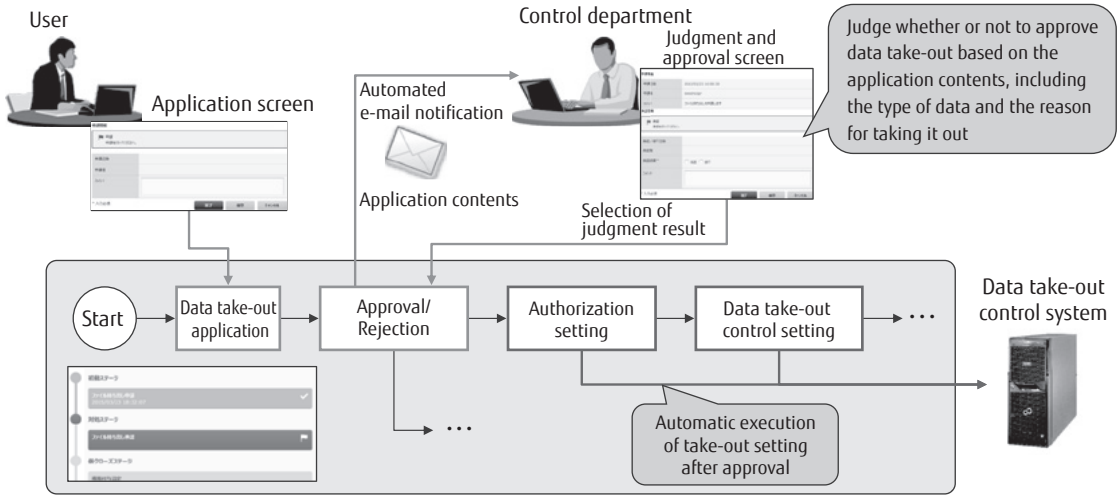

Figure 5
Strengthening of data take-out management.

Michio Masuno
Fujitsu Ltd.
Mr. Masuno is currently engaged in security product development.

Atsushi Wataki
Fujitsu Ltd.
Mr. Wataki is currently engaged in security product development.