Fujitsu's Security Technology Based on Practical Knowledge

● Takayoshi Kurita ● Michio Masuno ● Atsushi Wataki

Information and communications technology (ICT) is leveraged in wider applications today, and enterprises are faced with an ever-growing need to protect themselves against cyber-attacks, which continue each day to become technically more sophisticated. Measures against these attacks should aim to not only prevent malicious intrusions, but also implement possible countermeasures in case such intrusions take place. It is crucial to respond to a security breach quickly, and the response time significantly impacts security risks such as those relating to data leakage and network contamination. Fujitsu has developed a software suite, FUJITSU Software Systemwalker Security Control (SSC), which follows a preprogrammed operation process and navigates through automated responses against cyber-attacks. This product has already been launched on the market. It helps enterprises to reduce the costs of process programming and actual security operation, and it can automate operation process to enhance flawless security operations by eliminating human error. Fujitsu has integrated its operation management technology with response scenarios developed through the company's practical knowledge. This paper describes a software product with built-in operational processes against standard cyber-attacks based on this technology. It also outlines its features that significantly reduce the response time by automating a series of actions upon detecting malware (network shut-down, identification of infected terminals, response alert to operators, etc.).

1. Introduction

Corporations and other organizations have been implementing a multitude of security measures to combat the threats of malware[note 1)] intrusions and data leakage. They install firewalls and proxy servers to protect a company's intra-networks, run antivirus software, manage OS/application patches, ensure access control and encryption, and implement access/operation monitoring and analysis, while educating users about data security.

A new threat has been gaining prevalence worldwide in recent years—targeted attacks that aim to gain access to confidential information or destroy business infrastructure.[1)] Such damage has been reported in Japan, too, and a wide spectrum of sectors from governmental to corporate ones have fallen victim. In this type of attack, perpetrators prepare their offense by researching their target company or organization thoroughly and succeed in infiltrating the security system that the victim has built up over the years (**Figure 1**).

In view of this new threat, Fujitsu is developing a systematic operation process that presupposes malware infiltration, aiming to minimize security risks.

2. Major types of system intrusions in targeted attacks

The following describes the major and popular intrusion methods employed in targeted attacks.

1) Targeted e-mailing attacks

E-mails are sent to target organizations or individuals, usually impersonating an existing person or business and often with fake messages appearing to be relevant to the victim. Malware is embedded in the e-mail, and it contaminates the recipient's computer system. A developed version of this type is called a targeted correspondence attack, beginning with an uncontaminated e-mail. The perpetrator conducts correspondence for a while to gain the victim's confidence

note 1) Malicious program codes including computer viruses, worms and Trojans.

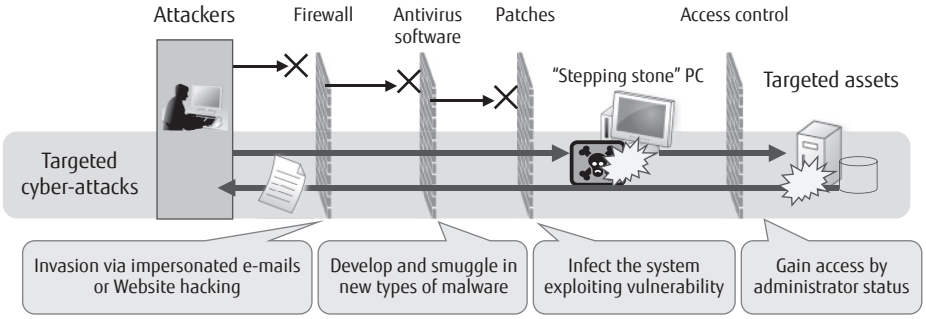

Figure 1
Targeted cyber-attacks.

before sending a malicious e-mail, hoping for a higher chance of successful infection.

2) Watering hole attack

The perpetrator investigates or predicts the Websites its victim regularly visits in business, then hacks one of those Websites to set up a trap that will let him or her infiltrate the victim's system.

As described above, these attacks are typically executed without arousing the victim's suspicions of the attack. In addition, the malware in these attacks tends to be more difficult to detect using conventional antivirus products.

Conventional antivirus software uses virus signatures (static characteristics), extracted from malware samples. The system verifies malware infection (invasion) by scanning hard disk drives or stored data in a memory space and looks for matching patterns. Previously, malware was often intended to infect computers randomly and therefore distributed widely over the Internet. This made it easy for antivirus vendors to obtain samples and analyze them, facilitating countermeasures with signatures. In targeted attacks, however, the culprits launch specified offenses on a specific enterprise or industry for invasion using malware variants with different static program characteristics or malware specifically developed for the targeted victims. This makes it difficult for the vendors to sample the malware and create signatures from them. Therefore, these attacks are increasingly difficult to detect not only by the users of the computers, but also by conventional antivirus systems.

A new system to counter this problem has been developed; instead of relying on virus signatures, it detects an invasion by recognizing suspicious "system behavior" of computer programs. This behavioral-based detection is a method based on technology to monitor programs and identify unusual behaviors (dynamic characteristics) such as suspicious outbound accesses and execution commands occurring within a data space.

In response to the recent prevalence of targeted attacks, many enterprises are introducing security products with this behavioral-based detection technology. However, users often find the system difficult to manage due to, for instance, the detection results being too complex since it takes a long time to investigate and understand the situation, or because it is not clear what the necessary actions are to be taken against the detected problems.

Behavioral-based detection is designed to identify suspicious phenomena, and it involves probable false positives. This necessitates human judgment as to the actions to be taken when certain threats are found. The required actions must also be executed by human operation. In other words, installing a product that employs behavioral-based detection means an increased operational workload is created in terms of the manual tasks required to eliminate the threats after they have been detected, and such tasks would have been automatically executed with conventional antivirus programs. In addition, operators are required to have appropriate and precise knowledge about the product alerts, and they are expected to continue updating their knowledge and skills in interpreting the detection results and executing the necessary counteractions.

3. Fujitsu Group's measures to combat cyber-attacks

The Fujitsu Group has strengthened its internal security system against targeted attacks through improving detectability and optimizing operationability as described below.[2)]

1) System reinforcement

The system has been newly installed with an antivirus gateway, unauthorized access detection device, and antivirus system which prevents unauthorized outbound e-mails, for the purposes of detecting viruses, shutting down unauthorized accesses, and further tracking down the viruses.

2) Operational optimization

Group-wide security incident information is centrally managed for a unified security system. Information on security incident response has been rolled out to overseas operations so that countermeasures can be executed swiftly after a security threat is detected.

A new issue emerged while implementing these measures of security reinforcement. That is, the enhanced detectability through system reinforcement resulted in a torrent of event alerts being issued by the detection system. Soon the situation was one in which there began to be a lack of personnel who were required to analyze the alerts and implement appropriate actions based on them. This also made it difficult to ensure speedy, error-free operations.

In malware-enabled targeted attacks, the attacker, once successfully inside the victim's system, will penetrate deeper and spread the attack to other connected devices, and there is a higher risk that he or she will reach the information he or she seeks to obtain (**Figure 2**). Therefore, a quick response is crucial to disable the attack after it has been detected.

Taking a long time to analyze the incident and formulate the necessary action may lead to a loss of confidential information and/or other gravely serious issues.

4. Approaches to solving operational issues

As stated above, it is crucial to stop malware from causing damage as soon as it is detected. This is referred to as an initial response. Two approaches were adopted to tackle the task of expediting the initial response: standardization and automation.

4.1 Standardization of operation process

Event analysis is standardized through the following stages from selecting the events that need

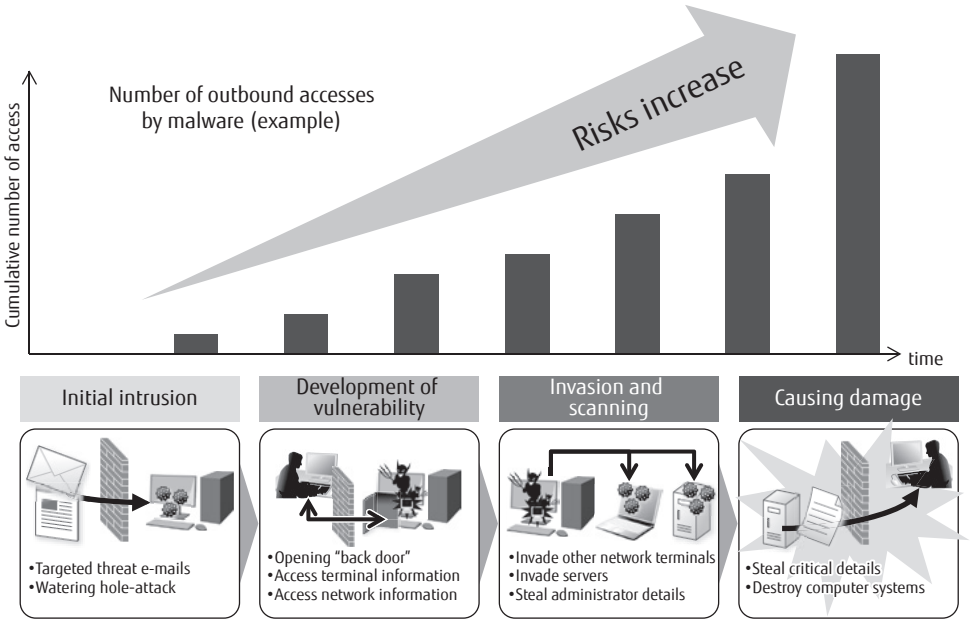

Figure 2
Correlation of response time and risks.

addressing out of all events found by the detection system to executing the necessary actions.

1) Analyze the event log to assess the security risk level.
2) Identify the terminals for which a security alert has been issued and the responsible administrators from inventory and personnel data.
3) Determine the necessity and/or priority of actions based on the risk level and information on identified devices.
4) Ensure that the device administrator is notified of the security countermeasures to be taken.

4.2 Automation of standardized operation process

The next step was to incorporate the automation technology that we have cultivated in the operational management middleware developed so far into the standardized operation process[3]. This has fully automated the process from event alert to device administrator notification.

These two approaches have made it possible to solve operational issues, and produced the following effects:

1) Reduction of the initial response time by 97%, stopping the infected terminal from spreading damage.
2) Reduction of incident response time by 60%, lowering the risk of information leakage and further infection from an infected terminal.
3) Reduction of the personnel required to operate the system down to a third.

5. Progress on Fujitsu middleware

FUJITSU Software Systemwalker Security Control (SSC)[4] is a middleware product with a standardized and automated operation process based on the counter-cyber-attack system Fujitsu has developed for itself. SSC is Fujitsu's brand-new product. It was announced in May 2014, and it was launched in the following August. It incorporates Fujitsu's know-how on systems to combat cyber-attacks.

5.1 Specifics of SSC

SSC is an accumulation of Fujitsu's system security measures embodied in product form. The following summarizes the product's characteristics (**Figure 3**).

1) Shortened response time prevents infection from spreading

Based on the practical knowledge Fujitsu has hitherto accumulated, a swift initial response is enabled by automated operation from discriminating attacks to executing counteractions, lowering security risks.

2) A reliable security system operation can be run without the operator having highly technical security knowledge

By providing the know-how developed within the company, Fujitsu has realized a system that can be operated by people without special skills in security operation suites.

3) Continued provision of action templates

Practical knowledge on how to identify new types of attacks and take countermeasures against them is provided in the form of an on-going detection product update template, keeping the system always up-to-date against newer threats.

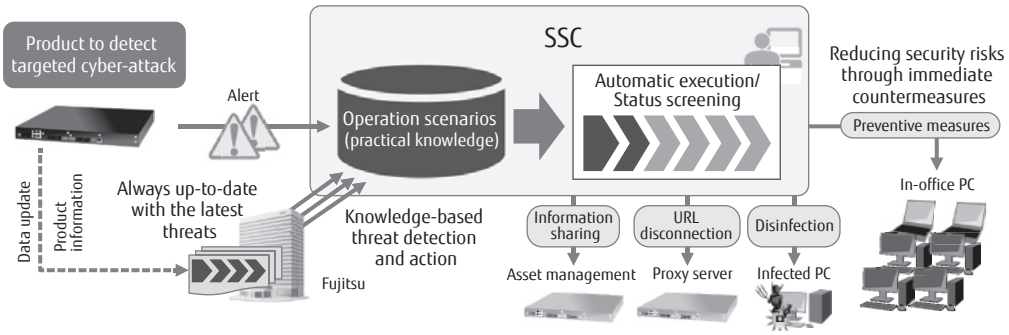

Figure 3
SSC overview.

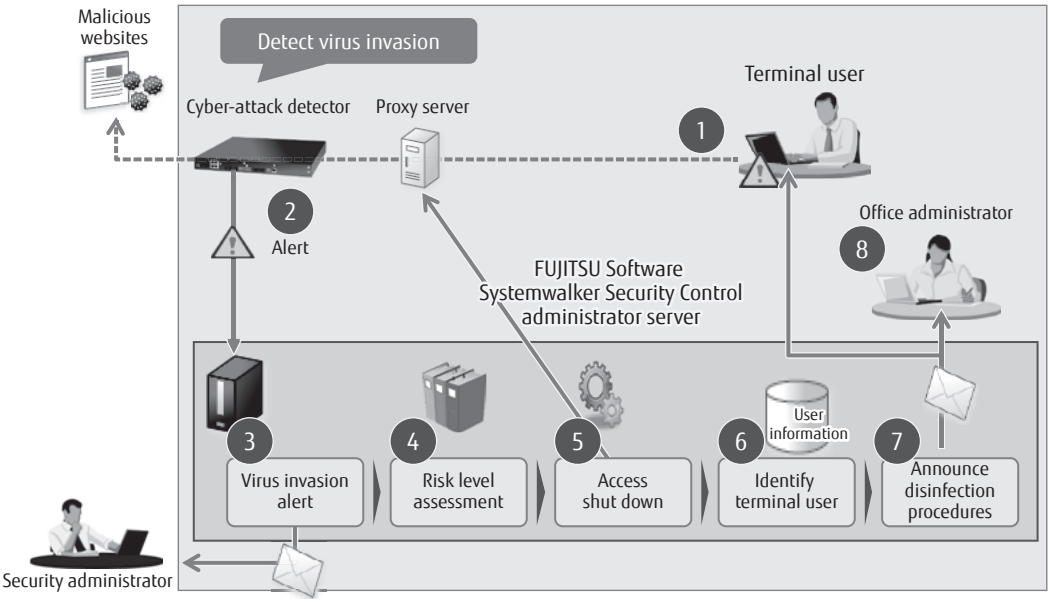

Figure 4
Operation overview of SSC-enabled system.

5.2 SSC-enabled operation

Initial response procedures with SSC are explained below, based on an example of responding to a threat that has arisen by accessing a malicious Website (**Figure 4**).

1) A computer user clicks on a URL link contained in a malicious e-mail, and a virus is downloaded from the Website to infect the terminal.
2) The detection product (Cyber-attack detector) detects the virus's intrusion in the corporate network, and alerts the SSC administrator server.
3) The SSC management server sends an e-mail alert to a security administrator, notifying him or her of the virus intrusion.
4) The administrator server diagnoses the risk level, and identifies the necessity and/or methods of countermeasures.
5) The administrator server commands the proxy server to prohibit the infected terminal from making any outbound access.
6) The administrator server identifies the section manager and terminal user based on the alert message.
7) The administrator server sends an e-mail to the section manager and terminal user, notifying them of the procedures to remove the virus.

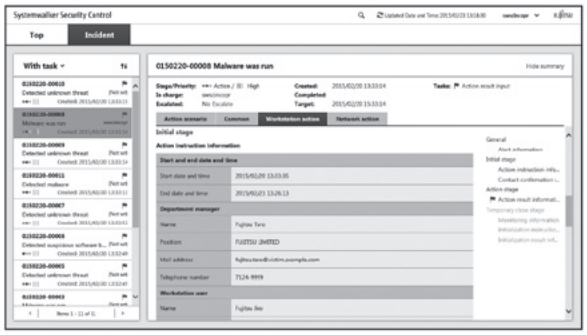

Figure 5
Visualization of security threat by SSC.

8) The section manager and terminal user follow the instructed procedures to segregate the infected terminal from the network, remove the virus, etc.

5.3 Support features of SSC operation

1) Visualization of security threat (**Figure 5**)

SSC discriminates targeted cyber-attack alerts sent from the detection product, and extracts the following information:

- Date and time of alert issuance
- Risk level
- Alert summary
- Terminal information (host name, IP address)

- Administrator information (name, phone number, e-mail address)
- Procedures to be implemented

This enables security administrators to narrow down the terminals that are suspected of being infected, and give instructions as to what actions to take, without requiring much specialist knowledge in system security.

2) Security incident management

SSC manages all instances of alerts from the detection product that need responding to as security incidents, and visualizes the process and progress of the countermeasure implementation. This visualization is an effective way to understand the progress in dealing with threat at a glance, and to maintain a shared understanding of the progress in the response scenario implementation.

3) Automation of countermeasure implementation

Upon receiving threat alerts, SSC selects an appropriate countermeasure scenario, and notifies it to the relevant servers and terminal administrators, together with details on the procedures to be taken at each step in the scenario. The system executes the complex set procedures automatically, thereby achieving standardizing counter actions, reducing response time, and minimizing the workload of the security administrators.

Automation helps to operate timely and reliable security management, by replacing human efforts in, for example, notifying terminal users and server administrators of the actions to take upon detecting a cyber-attack, and disconnecting the terminal within which malware is detected and disabling its access to Websites.

6. Conclusion

This paper has described Fujitsu's experience in building up in-house security measures against cyber-attacks, and SSC, the product created by using the know-how gained from that experience.

SSC helps users to minimize security risks such as those related to spreading cyber infections and having confidential information stolen. The system allows operators to manage cyber-attack countermeasures without having highly technical knowledge of cyber security.

Fraudsters are developing their attack methods day by day, and in order to combat them, it is crucial to maintain effective security operation management through timely provision and execution of up-to-date countermeasures.

Fujitsu will strive to protect customers' business environments from ever-evolving cyber threat through SSC, and continue providing its unique operational know-how in a timely fashion together with its threat detection technology armed against new threat.

References

1) IPA: 10 Major Security Threats 2014.
https://www.ipa.go.jp/security/english/vuln/10threats2014_en.html
2) Fujitsu: Fujitsu's measures to combat cyber-attacks (in Japanese).
http://jp.fujitsu.com/solutions/safety/secure/solution/sol36.html#measures
3) Fujitsu: FUJITSU Software Systemwalker Runbook Automation (in Japanese).
http://systemwalker.fujitsu.com/jp/runbook/
4) Fujitsu: FUJITSU Software Systemwalker Security Control (in Japanese).
http://systemwalker.fujitsu.com/jp/securitycontrol/

Takayoshi Kurita
Fujitsu Ltd.
Mr. Kurita is currently engaging in development of security products.

Atsushi Wataki
Fujitsu Ltd.
Mr. Wataki is currently engaging in development of security products.

Michio Masuno
Fujitsu Ltd.
Mr. Masuno is currently engaging in development of security products.