Cyber Attack Countermeasure Technologies Using Analysis of Communication and Logs in Internal Network

● Masanobu Morinaga ● Yuji Nomura ● Kazuyoshi Furukawa ● Shoji Temma

The threat of cyber attacks is continuously on the increase and causing major social issues. In particular, cyber attacks intended to steal information by targeting specific corporations and individuals, which are called targeted attacks, are becoming increasingly clever and persistent. With conventional inbound and endpoint measures such as firewalls and antivirus software, it is not possible to completely prevent malware from intruding into organizations. This paper presents internal countermeasure technology that detects any targeted attack in an organization and analyzes the extent of impact of the attack. This technology is composed of high-speed capture technology for efficiently analyzing a large number of packets that flow in the internal network, attack detection technology based on analysis of the context of malware communications that intruded into the internal network and technology for validating the impact of the attack by analyzing malware detection information and peripheral device log information. An advanced countermeasure solution against targeted attacks can be realized by combining these technologies.

1. Introduction

The ever-increasing threat of cyber attacks toady is becoming a major social issue. In particular, cyber attacks known as targeted attacks, which intend to steal information from specific corporations or individuals, are becoming increasingly sophisticated. Targeted attacks are often highly stealthy, combining several offensive methods. Conventional inbound and outbound measures, such as firewalls and antivirus software, cannot offer perfect protection against malware that may intrude into the targeted organization's internal network. Once it has successfully penetrated the system, malware proceeds to multiply and spread the infection, repeating unauthorized accesses, and this is difficult to counteract with those preventive measures. This means that it is necessary to have some internal measures in place against possible malware intrusions. The importance of having these internal measures is emphasized by the National Information Security Center (NISC) in its Outline of the Standards for Information Security Measures for the Central Government Computer Systems.[1)] The NISC considers it critical to detect possible attacks at an early stage and minimize damage from such attacks. Fujitsu takes a comprehensive approach to targeted attacks, from detection to countermeasures, with steps of attacks in mind, that is, from initial intrusion to post-intrusion espionage activities.

This paper presents new anti-cyber-attack technology that offers security measures for intra-networks by analyzing access and log data within an organization's internal networks. We first describe the high-speed capture technology, designed to efficiently collect a large volume of packet data within the internal network, which will serve as the basis of the data analysis. Then we describe the attack detection technology that extracts the contexts of malware communications upon intrusion into the internal network. This is followed by giving accounts about the technology for verifying the extent of the intrusion by analyzing malware detection information and peripheral devices' log information.

2. Capture technology for monitoring internal network communication

Packet capture is a superior technology that neither depends on the types of servers, client terminals or networks for collecting data, nor puts stress on these

components for data collection. In this section, we will describe this packet capture technology for malware communication analysis.

2.1 Challenges in packet capturing

Telecommunication packets are large-volume data, which take up much CPU capacity if processed entirely with computer software. Meanwhile, software on conventional multi-purpose hardware can only process them partially. This makes it unsuitable for malware communication analysis, which would require the entire data. Additionally, taking up much of CPU memory resource for packet capturing would leave malware communication analysis with a resource shortage. Therefore, it is necessary to keep the data to a minimum but sufficient amount for malware analysis.

2.2 High-speed, real-time packet capture technology

Fujitsu Laboratories has so far developed technology that allows real-time packet analysis at 200 Gbps on a single piece of multi-purpose hardware.[2)] We employ this technology in the packet data collection platform for malware analysis (**Figure 1**).

The conventional *libpcap* interface[note)] is commonly used for packet capturing on multi-purpose hardware, but its performance is low. In order to address this, we developed the following three technologies, and made it possible to receive data packets without placing much load on the system:

1) Using a high-speed packet-receiving process by bypassing the heavy-load TCP/IP packet reception at the OS kernel level,
2) Ensuring high-speed memory access to avoid unnecessary packet data copying, and
3) Adopting a parallel CPU core arrangement between the packet receiving process and data analysis process to enhance performance efficiency.

2.3 Data generation function for analysis

Chronological packet capturing alone is not enough to obtain data sufficient for malware analysis, as the aforementioned *libpcap* interface does. Thus, we developed the following three features:

4) Decoding packet headers to identify communication sessions,
5) Configuring data to ensure that all the necessary data (i.e., packet payload), and no more, are provided for malware communication analysis, and
6) Discovering and removing data with errors such as packet loss and communication interruption.

2.4 Impacts

With the above-stated technologies and features, packet capturing is realized without placing a heavy load on the system. Furthermore, the malware analysis function does not require logic analysis or data access for the data packets because the data needed for malware analysis has been prepared. Packet capturing and data generation are improved in this way, and they help to miniaturize the hardware as well as enhance its resource-effectiveness.

3. Technology for malware analysis and detection

Ordinary cyber attacks employ remotely controlled malware known as a remote access Trojan or remote administration tool (RAT). Attackers use such methods as targeted e-mails to infect the host computer (hereafter, the terminal) within the targeted network/system with a RAT. They take the terminal as a jump host (infected server or terminal), and intrude further and execute commands or computer programs on other devices to repeat espionage acts. We will describe the technology to detect such RAT spying activities by correlating

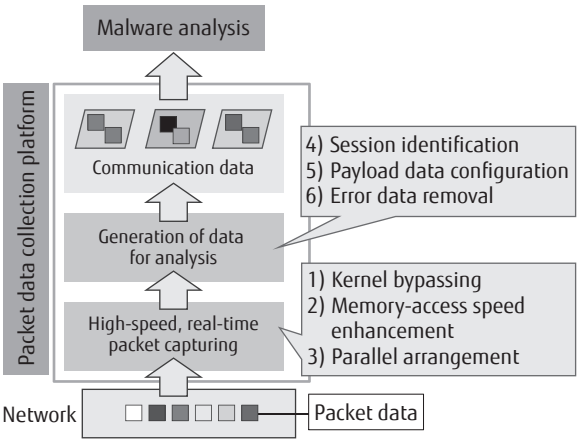

Figure 1
Platform to collect packet data.

note) This is a standard application programming interface (API) for capturing data packets.

information on internal communications.

3.1 Technical challenges

The spying communications are divided into two categories: remotely operated communication between the attacker and the jump host's RAT (hereafter "RAT communication"), and communication to penetrate another terminal from the jump host and execute a command or program (hereinafter "internal attack communication"). RAT communication is difficult to detect with high accuracy because it is often disguised as ordinary Web accesses using encrypted communications. The internal attack communication often abuses administrator tools and commands that are commonly used, in order to gain access to other devices within the network. Therefore, it is also difficult for conventional technology to discern RAT infiltration from the true administrator's operations.

3.2 Technology to detect RAT activities within the internal network

Fujitsu Laboratories has developed a method to detect espionage activities through collating and analyzing internal network communications and extracting the communications with RAT or internal-attack characteristics, and tag them.[3)]

The remotely controlled RAT communications typically hide in the jump host, waiting for a command from the attacker, and respond as soon as they receive such instructions, sending back the outcomes of their actions. It is also characteristic of a RAT that it keeps the external connection open once it is established, so that access may continue to be made at any time. These characteristics may be used to narrow down the possible RAT communications.

Internal attack communication often abuses Windows administrator services and disguises itself as work-related commands. Typically, these services use the server message block (SMB) protocol. By separating SMB packet headers into user authorization and operation details, it is possible to filter suspicious administrative operations linked to the internal attack communication. This would typically have executed file sharing and/or network searches. These marked communications are tagged based on indicators such as IP addresses and access times. This will enable the identification of SMB administrator operations executed by SMB management operations related to remote-RAT communications.

3.3 Coordination of sensors to expand the scope of risk detection

In actual networks, it is not always possible for a single sensor to monitor both RAT and internal attack communication against spying activities across different network segments. Fujitsu Laboratories has developed a technology for coordinated detection, making it possible to expand the scope of security monitoring. This can be done as several sensors installed in the network each detect RAT and internal attack communication separately. The technology then sends the information to a coordination server, where those communications are tagged accordingly (**Figure 2**).[4)]

This coordinated detection technology is made possible by installing monitoring sensors at network gateways and segments to be monitored. These sensors send information on suspicious communications. The server analyzes the received information, and requests other sensors to provide further information if necessary. This interactive arrangement enables comprehensive and real-time detection of spying activities over all segments with the sensors installed.

3.4 Impacts

We believe that this risk detection technology can detect RAT-based spying activities that have penetrated through inbound and endpoint protection measures

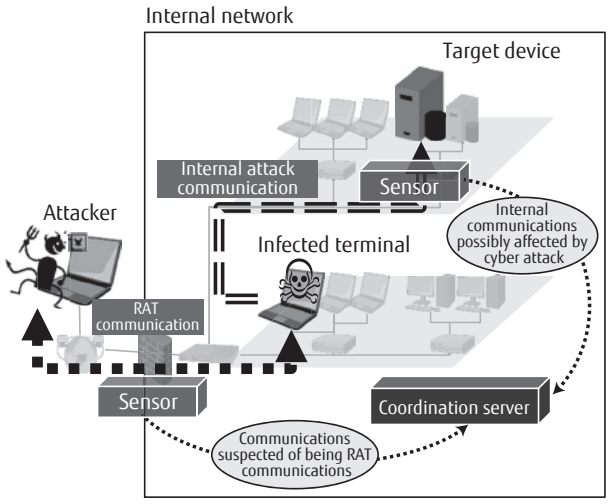

Figure 2
Technology to detect RAT espionage activities.

into the intra-network. It also enables the user to implement countermeasures before the attacks cause serious damage.

4. Technology to identify the extent of malware intrusion

As we have stated above, targeted cyber attacks cause malware infection in certain terminals within the target network, and, using them as an infected terminal, repeatedly access other devices and/or servers to steal information, causing more damage. It is considered that it takes 146 days on average before targeted attacks are found after the initial malware intrusion,[5] during which period a wide range of important information could well have already been stolen.

Therefore, the victim of targeted attacks must investigate the full extent of the intrusion, and implement countermeasures. It is customary to employ expert services, but such specialist investigations usually take a long time, forcing the organization to suspend its operations. There are commercially available new products that provide agent software to be installed on all terminals, facilitating a quick investigation in the event of cyber intrusion. While these products offer quick investigations, they require every single terminal to be managed, which means a significantly large operating resource must be secured for that at all times.

We present totally new technology that enables automated assessment of damage from targeted attacks. The quality of the investigation performed is at the same level as security experts, and it identifies security threats still remaining within the network very quickly.

4.1 General damage analysis of targeted attacks

Generally speaking, targeted attack detection can only detect infected terminals, but not other devices and servers that may have been accessed from such terminals. For this reason, security experts will, first of all, identify infected terminals, then repeat searches for further targets of the attacker's spying activities beyond those terminals. They also evaluate the found malware in terms of its static and dynamic attributes by scanning the malware as well as the traces left in other data files, registries and log files, to elucidate what passed within the affected terminals. These expert investigations often take six to twelve months. For this reason, it is rare for these investigations to be employed, save only for very serious cases. Meanwhile, a customary practice has been to reform infected terminals and implement preventive measures against infection to avoid recurrence.

4.2 Technology to identify the impact of malware intrusion

The newly developed technology can perform investigations as well as security experts, and without requiring agent software to be run on the terminals. To achieve this, we have developed technology to enhance efficiency in two phases of the processes: information collection and analysis. In the information collection phase, the volume of information to use in analysis is minimized. Experts would collect voluminous information including a portion irrelevant to the malware categories or behavior. The technology is designed to filter information to extract only data segments that are relevant to the malware processes and accessed files.

In the information analysis phase, highly accurate analysis is made possible by leveraging data other than the infected terminals' IP addresses (such as data from the exploited account or tool name). With the technology presented in the previous section, it is possible to obtain, through the analysis of malware communications, information such as account data and tool names targeted outside the infected terminals' IP addresses. Targets of the spying activities can be identified with accuracy by analyzing data from the exploited account or tool name that is obtained from the collected information in the key. The information required for the investigation can be collected remotely using the standard features of Windows. This makes it possible to use Windows' standard functions and automate the investigation into the extent of intrusion from the infected terminals into the intra-network (**Figure 3**).

4.3 Impacts

This technology enables the user to elucidate the extent of intrusion upon malware attacks as effectively as security experts, without requiring agent software to be installed on every terminal, and the investigation is performed very quickly. According to our simulation,

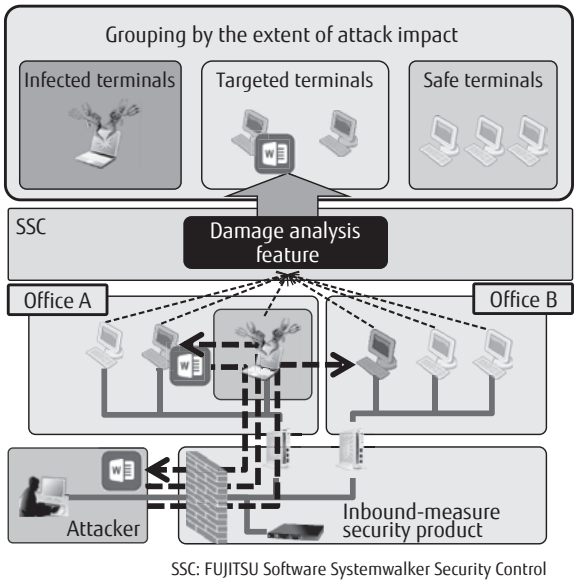

Figure 3
Feature to identify intrusion extent.

the time required for an investigation to identify the extent of the attack can be significantly reduced, to a few hours or a few days from over six months. This makes possible what was before impossible—to include in the scope of the investigation the terminals subjected to espionage activities beyond the initially infected terminals.

5. Conclusion

This paper presented technologies for high-speed packet capturing, attack detection, and impact analysis that Fujitsu developed for internal network security, aiming to detect targeted attacks for the network, and analyze the extent to which the attack has affected the network. These technologies combined can offer a reliable high-security response solution that captures and analyzes a large volume of packet data communicated within the network, and verifies the scope of damage as well as evidence of information leaks in early stages of the attack.

This research is partly conducted by commission for the R&D for analysis and detection of cyber attacks of the Ministry of Internal Affairs and Communications.

References

1) The National Information Security Center: Outline of the Standards for Information Security Measures for the Central Government Computer Systems (2014) (in Japanese).
http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf
2) Yuji Nomura, et al.: Software Technology Offers Real-time Analysis of Super-fast Telecommunications at 200 Gbps. FUJITSU Sci. Tech. J., Vol. 52, No. 1, pp. 41–45 (2016).
http://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol52-1/paper06.pdf
3) Masahiro Yamada, et al.: A Detection Method against Espionage Activities of Targeted Attack on the Internal Network: The 31st Symposium on Cryptography and Information Security (SCIS), 2014.
4) Masahiro Yamada, et al.: Cooperating Multi Sensors for Behavior Detection of Targeted Attack in Intranet: The 32nd Symposium on Cryptography and Information Security (SCIS), 2015.
5) FireEye: FireEye Releases Mandiant M-Trends Report with Insights from Advanced Attack Investigations, February 2016.
https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

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

Yuji Nomura
Fujitsu Laboratories Ltd.
Mr. Nomura is currently engaged in research and development of operations management for ICT systems.

Kazuyoshi Furukawa
Fujitsu Laboratories Ltd.
Mr. Furukawa is currently engaged in research and development of cyber security.

Shoji Temma
Mr. Temma is currently engaged in research and development of NFV, network security and IoT.