High-Speed Forensic Technology for Promptly Analyzing Damage After Targeted Attacks

● Yuki Unno ● Takanori Oikawa ● Kazuyoshi Furukawa ● Masanobu Morinaga
● Masahiko Takenaka

The number of targeted attacks aimed at stealing information from government and municipal offices, specific enterprises, and individuals is growing year by year, and the attack methods are becoming more and more clever. In a targeted attack, the attacker stubbornly attacks the target after thoroughly investigating it beforehand. The risk of malware (malicious and illegal code) infecting an internal network is thus increasing. Therefore, there is a pressing need for countermeasures against malware infection that detect attack activity as soon as possible and respond effectively to prevent or minimize damage before the attack proceeds further. We have developed high-speed forensic technology that promptly analyzes the situation after an attack has been detected. Previously, such analysis took a long time. Application of this high-speed forensic technology enables inclusive countermeasures to be promptly implemented before the damage expands.

1. Introduction

In targeted attacks aimed at government and municipal offices, specific enterprises and individuals, the attacker typically uses malware (malicious and illegal code) to infiltrate the organization's intranet and then controls the malware remotely to spread the infection and collect network and system information. In the worst cases, confidential information and personal details are leaked outside the organization, causing major damage to the targeted organization and its partners.

Many organizations prevent malware from infiltrating their intranets by installing an intrusion prevention device such as a firewall or intrusion prevention system (IPS) at the boundary between the organization's intranet and the Internet, by installing antivirus software on terminals, and by other means. However, by using communications channels such as Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP), which are typically configured to penetrate firewalls, an attacker can send remote-control malware known as a RAT ("Remote Access Trojan" or "Remote Administration Tool") into the organization's intranet. "Social engineering," which exploits people's psychological blind spots and careless mistakes, is another method commonly used to infect intranets.

Avoiding detection by antivirus software, the attacker can send in a customized RAT that adapts to the targeted network environment, enabling espionage activities to be initiated without being noticed by the targeted organization. Espionage activities can also escape notice by being carried out under cover of legitimate operations using standard operating system (OS) commands. In many cases, therefore, the targeted organization does not become aware of the attack until it receives notification from an external body such as a third-party monitoring center.

With the aim of damage minimization, Fujitsu Laboratories has developed a technology for early detection of RAT-based espionage activities.[1),2)] This technology collects and analyses internal communications, detects espionage activities by using communication characteristics to abstract and correlate remote-control communications between the attacker and the RAT-infected terminal and internal attack communications that infiltrate other terminals from the infected terminal, and then executes commands and programs.[3),4)]

Advice on what to do after an attack has been detected is set out in the "incident response life cycle"

described in the Computer Security Incident Handling Guide[5], Special Publication 800-61, a security standard created by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. According to the Guide, after an attack is detected, analysis needs to be carried out with the aim of containing and eradicating the activity of the malware and enabling the intranet to recover. If early detection of the attack is promptly followed by this analysis phase, and if appropriate measures are implemented before the harm spreads, major damage can be prevented. We have developed a high-speed forensic technology for promptly analyzing the status of the damage after an attack has been detected. This technology makes it possible to rapidly identify how many terminals have been impacted by the attack and to obtain details of the impact of the attack on each terminal.

After explaining conventional targeted-attack analysis methods and technological challenges posed by attack analysis, we go on to explain our high-speed forensic technology system and its characteristics and benefits and to introduce the integrated analysis system in which this technology has been applied.

2. Conventional method for analyzing targeted attacks

The conventional method for analyzing a targeted attack uses digital forensics. Digital forensics is a means of analyzing traces left by the attacker on network devices and terminals. In this section, we explain the general digital forensic method used in analyzing espionage activities on an intranet.

1) Analysis of suspicious external communications

Having infiltrated an intranet, a RAT uses communications channels such as HTTP or Hypertext Transfer Protocol Secure (HTTPS) to connect to the command and control (C2) server installed externally by the attacker. The attacker then sends espionage commands to the RAT from the C2 server, collects information from the infected terminal and the peripheral network and terminals, and expands the attack (**Figure 1**). The incident responders examine the log of the domain name system (DNS) server for suspicious name resolution queries and examine the proxy server log for communications involving suspicious URLs, IP addresses, port numbers, and user agents.[6),7)]

2) Analysis of unauthorized account usage

Every OS has an authentication and authorization system for preventing unauthorized usage. When an attacker executes standard OS commands or runs the

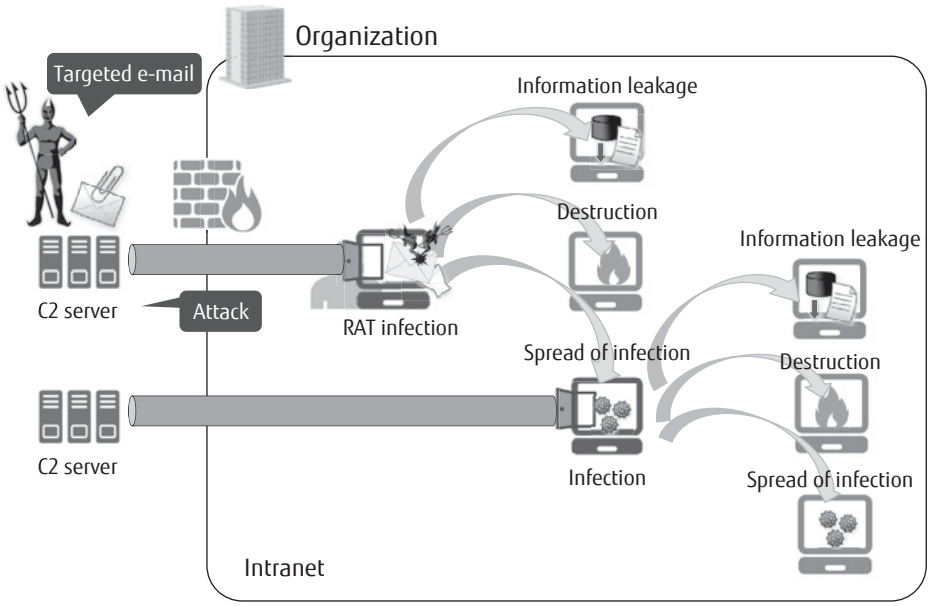

Figure 1
Typical targeted attack.

remotely installed malware, this system requires them to input account names, passwords, tickets, and other authentication information. Oftentimes, therefore, the attacker uses the RAT's key logger function or a security inspection tool such as Windows Credentials Editor (WCE) and Mimikatz to steal legitimate authentication information and then executes standard OS commands and runs free tools to steal information from the network and peripheral terminals. To track such unauthorized usage of accounts, the responders analyze authentication logs. These include Active Directory event logs and other event logs for auditing authentication servers[8] and Windows terminal auditing logs, which retain records of authentication success/failure and permission usage.

3) Analysis of attack procedure and scope of damage

The individual log inspections described in 1) and 1) yield only fragmentary information, so although it is possible to tell whether an attack has taken place and to decide whether a detailed inspection is required, it is difficult to get an overview of the attack. To make up for this, a copy of the hard disk is taken and the file system is analyzed. The files are restored, and emails, browser histories, device connection logs and other information is obtained from them. The restored malware is then examined to find out exactly what it has done. Although details of the attack procedure can be identified by using this method, the responders need to have sophisticated security knowledge and technology. The same analysis has to be repeated for each terminal affected by the attack, so obtaining an overview of the whole attack can take weeks or even months (**Figure 2**).

3. Technical challenges in attack analysis

To clarify the damage done by an attack in which an intranet has been infiltrated by malware, the most obvious approach would be to collect the communications data flowing around the intranet on a non-stop basis and analyze it in its unmodified state. However, this would amount to a huge volume of data, so high-capacity storage media would be required. Judging from past case histories, the initial attack is typically traced back to a point up to a year prior to its detection. Japan's National center of Incident readiness and Strategy for Cybersecurity (NISC) therefore recommends retaining logs for over a year.[9] However, retaining all of an organization's communications data for over a year would require a data storage capacity ranging from several petabytes to several tens of petabytes. Securing and managing the storage media would probably involve considerable costs. Within such a huge volume of communications data, it would also be difficult to narrow down the range of data to be analyzed.

The analysis described above would also require knowledge of the specifications of various network protocols. It would therefore be difficult and time-consuming to find out, from the communications data, who did what (in other words, when a particular account logged into the OS, and so on). Moreover, the standard OS commands executed in the course of espionage activities and the protocols used within the malware are typically the same as those used in an organization's normal work. Looking at operation communications individually is insufficient to tell whether they are attack-related.

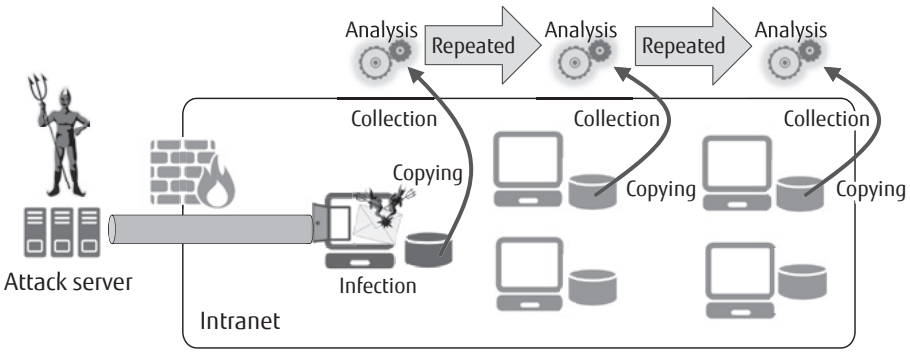

Figure 2
Conventional method for analyzing targeted attacks.

4. Features and benefits of high-speed forensic technology

To solve the technical problems outlined in the previous section, we have developed a high-speed forensic technology consisting of a technology for collecting traces in real time at the command level, a technology for automatically correlating accounts with operations, and a technology for tracking the progress of the attack (**Figure 3**). The features of these technologies are described below.

1) Technology for collecting traces in real time at command level

This technology continuously captures communications data flowing through the network and analyses the protocols common to internal attack-related communications included in the data. By evaluating the features of the packets–a packet being the basic unit of communication data–it identifies remote control commands executed on each affected terminal and captures each one along with its associated execution result (success or failure). By summarizing the huge volumes of communication data at the command level before recording them, this technology enables the trace log to be compressed. Although the compression

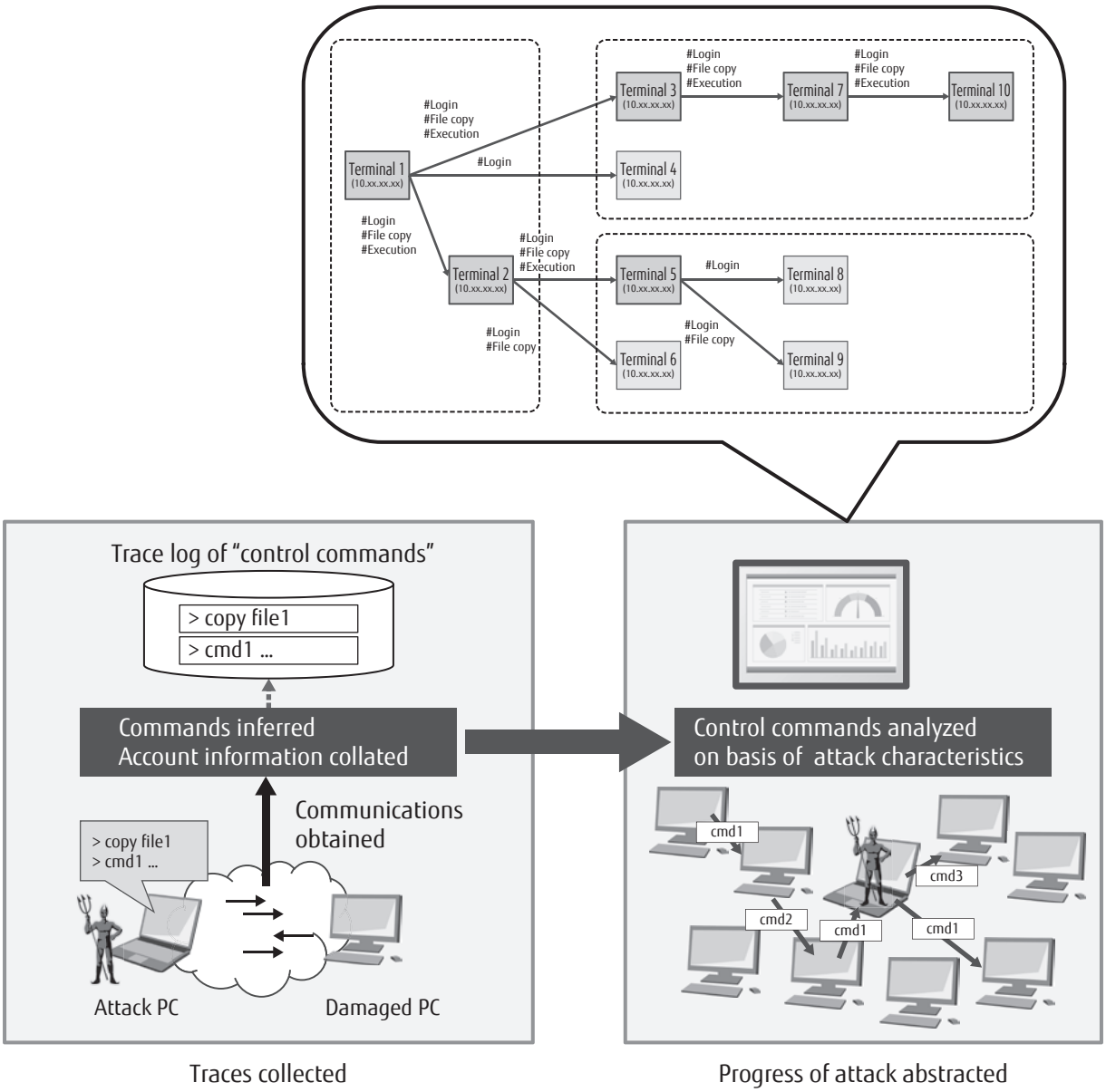

Figure 3
High-speed forensic technology.

ratio depends on the distribution of protocols in the communications data, the data can usually be compressed to approximately one ten-thousandth of its original size before being stored.

2) Technology for automatically correlating accounts with operations

This technology analyzes the authentication protocols included in the communications data, identifying account names and other authentication information. It then efficiently works out the specific authentication information used to authenticate specific remote control commands. Any improperly used accounts can then be frozen and subjected to swift and reliable countermeasures such as changing their passwords. The permission level of the accounts in question can also be identified, enabling the scope of the damage to be accurately grasped.

3) Technology for tracking progress of attack

A primary characteristic of targeted attacks is that a RAT is used to execute remote control commands on peripheral terminals rather than the initially infected terminal. The technology uses this characteristic to distinguish operations that are highly likely to be attack-related, separate them from the organization's legitimate work-related operations, and analyze them. Using operation methods and other attributes to filter out the suspicious communications, it also continuously abstracts them in chronological order. From a day's worth of trace-log data, the sequence of remote control commands on a specific terminal can be analyzed in a few seconds or several tens of seconds at most. This means that the progress of the entire attack can be extracted in a short period of time, ranging from several tens of minutes to a few hours.

5. Technology application example: integrated analysis system

In this section, we introduce an integrated analysis system featuring the high-speed forensic technology described in the previous section.

The integrated analysis system consists of a network trace server on which attack trail collection technology has been installed and a trace analysis server on which attack progress tracking technology has been installed. In the system configuration shown in **Figure 4**, the network trace server is installed in such a way that it can capture the traces of espionage activities carried out by means of the attacker's remote control commands between the head office, where important information is stored, and branch offices and between branch offices.

Suppose, for example, that a terminal at branch office B has been infected by a RAT and then remotely controlled by the attacker to carry out espionage activities on a head office terminal. In the example in Figure 4, technology for detecting RAT-based espionage activities has been installed on an appliance. As soon as an incident is detected, this appliance registers the incident on the trace analysis server. This incident registration alerts an analyst at the Security Operation Center (SOC). The analyst then uses the analysis console of the integrated analysis system to find out what happened (**Figure 5**). On the analysis console, traces relating to the incident can be identified, and the content of remote-control commands executed on the head office terminal from the terminal at branch office B can also be checked in chronological order. This makes it possible to obtain detailed information, such as the account that was improperly used by the attacker, the files that were remotely accessed, and the settings that were changed and to ascertain whether these actions succeeded or failed.

Furthermore, by taking the terminal at branch office B, where the attack took place, as the point of origin for the purpose of attaining an overview of the attack, and by performing a manual analysis in the same way on terminals with which the originally infected terminal communicated, the analyst can identify traces related to attacked terminals other than the head office terminal and identify the attacked terminal at branch office B (**Figure 6**). In this way, by shifting to the next infected terminal and recursively carrying out the same kind of automatic analysis, the analyst can analyze the entire attack process. The automatic plotting of the results of these analyses as a node graph produces a bird's eye view of the entire attack process (**Figure 7**).

By using this integrated analysis system, even someone who is not an advanced specialist can quickly create an overview of the entire attack process by viewing the details of the attack on the analysis console. This enables appropriate measures to be taken promptly.

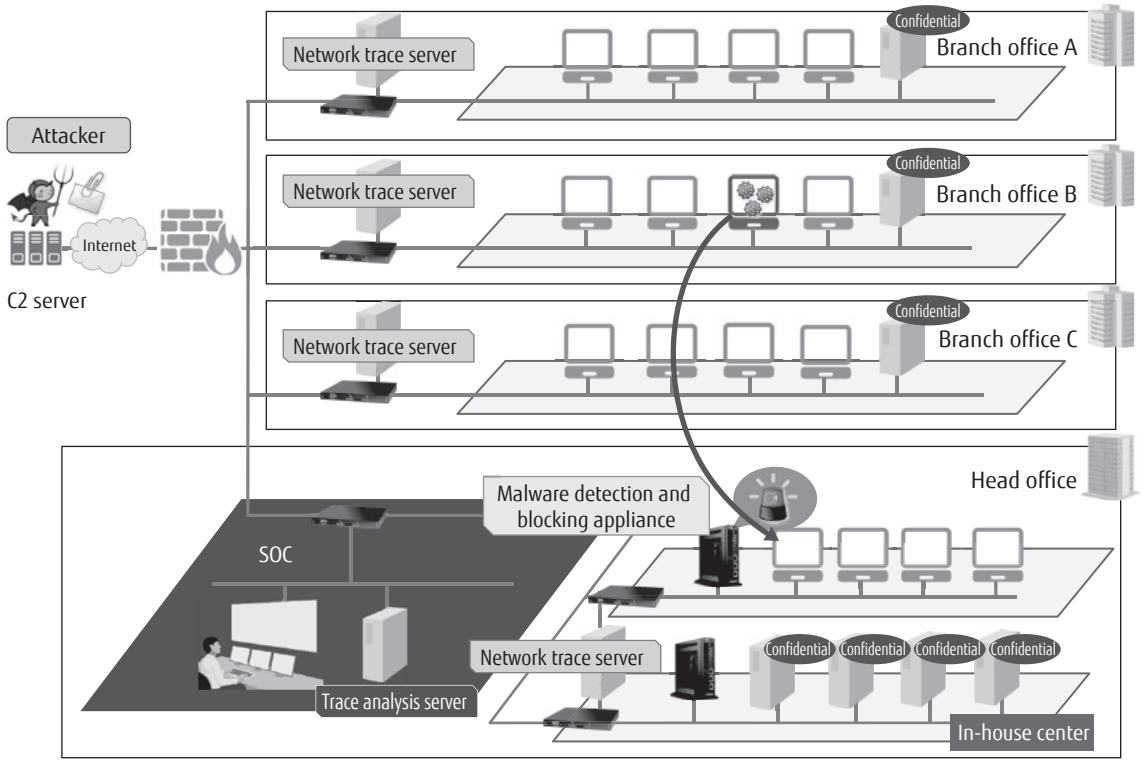

Figure 4
Configuration of integrated analysis system.

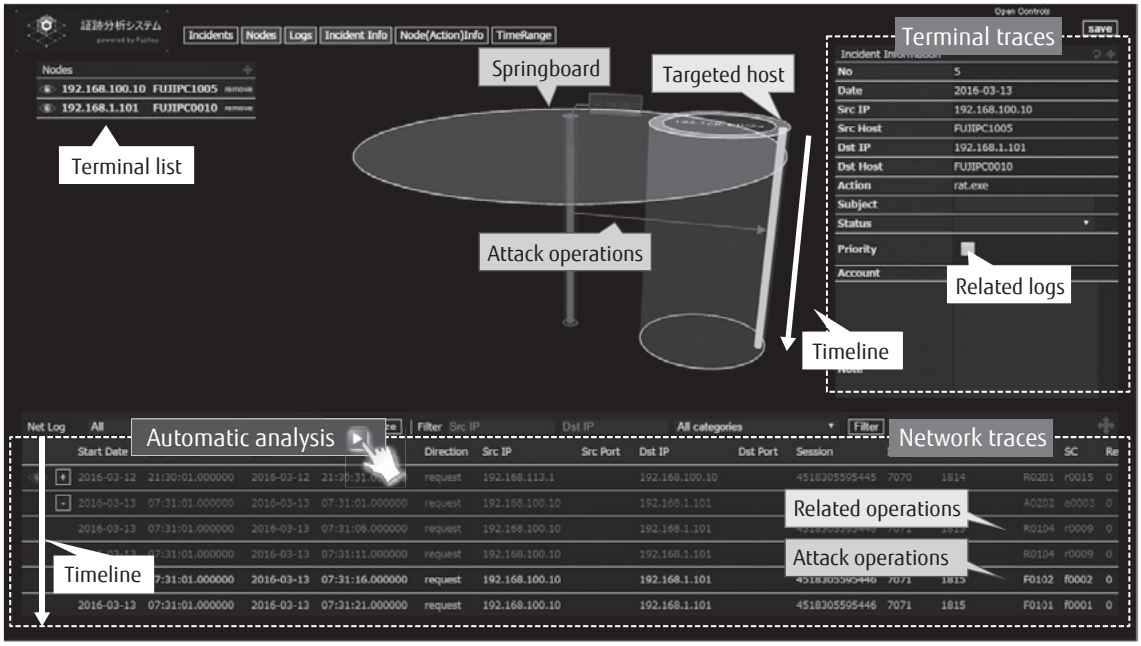

Figure 5
Analysis console.

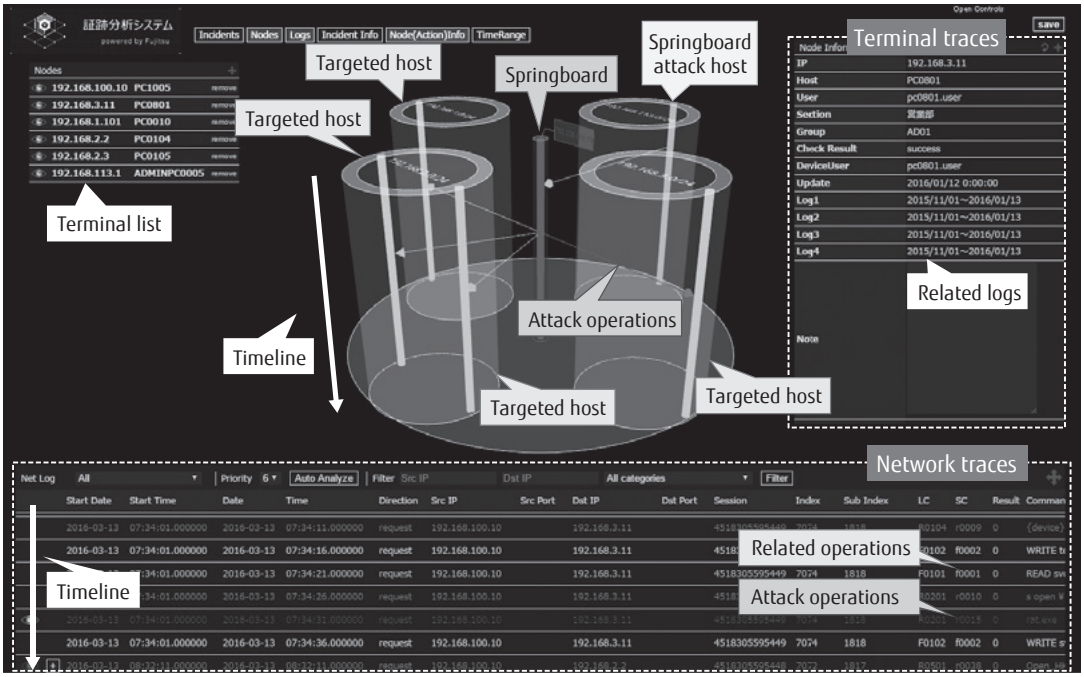

Figure 6
Analysis console (after automatic analysis).

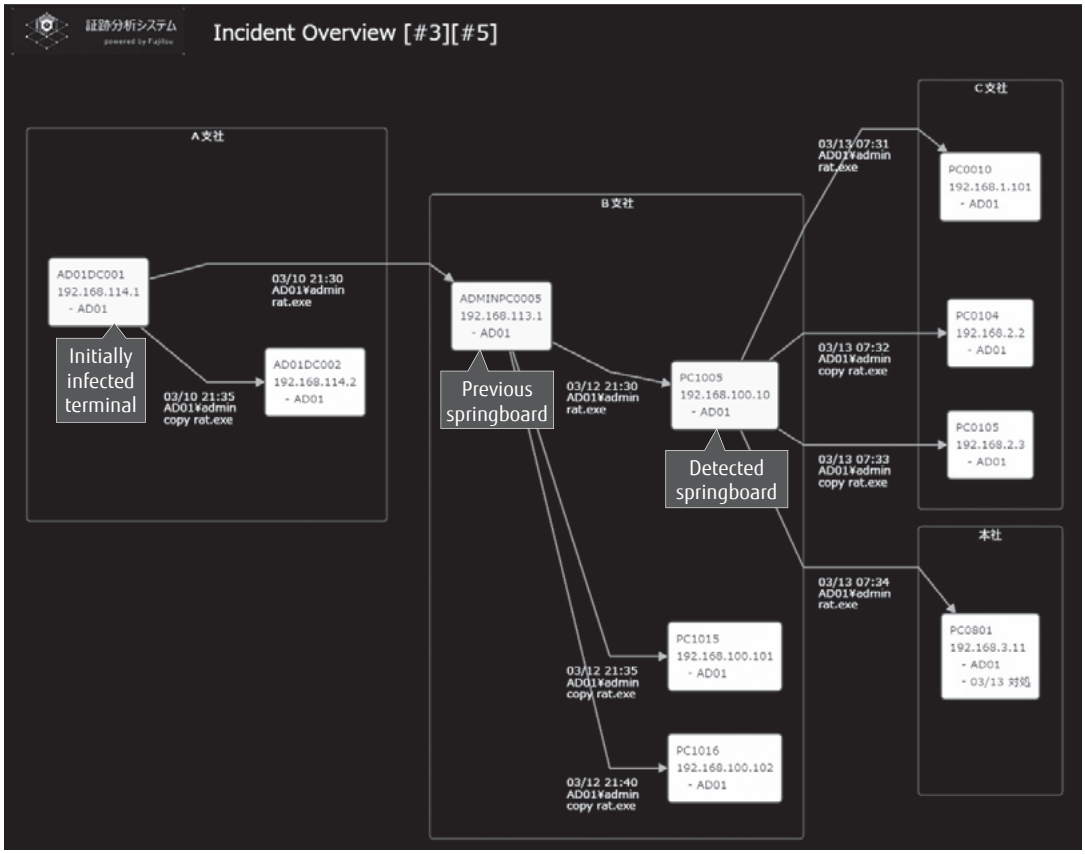

Figure 7
Overview of attack.

6. Conclusion

In this article, we have explained the world's first high-speed forensic technology developed at Fujitsu Laboratories and the integrated analysis system featuring this technology. This integrated analysis system enables traces of an attack to be continuously collected while minimizing the volume of trace data collected and the damage caused by the attack to be examined. When a targeted attack is detected, the terminals involved are abstracted as a daisy chain, and an overview of the progress of the attack is automatically plotted, thus enabling an overall picture of the attack to be grasped at a glance. This enables security incident analysis, previously a time-consuming process, to be carried out swiftly even by persons who are not specialists possessing advanced knowledge. This in turn enables comprehensive countermeasures to be promptly put in place before the damage spreads. After internal verification at Fujitsu, we aim to commercialize this integrated analysis system by the end of fiscal year 2017.

References

1) S. Torii et al.: Multi-Layered Defense against Advanced Persistent Threats (APT). Fujitsu Sci. Tech. J., Vol. 50, No. 1, pp. 52–59 (2014). *http://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol50-1/paper09.pdf*
2) M. Morinaga et al.: Cyber Attack Countermeasure Technologies Using Analysis of Communication and Logs in Internal Network. Fujitsu Sci. Tech. J., Vol. 52, No. 3, pp. 66–71 (2016). *https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol52-3/paper10.pdf*
3) M. 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) M. 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) P. Cichonski et al.: Computer Security Incident Handling Guide. National Institute of Standards and Technology, Special Publication 800-61 Revision 2, August 2012.
6) Japan Computer Emergency Response Team Coordination Center (JPCERT): Methods for Utilizing and Analyzing Logs in Countermeasures Against Sophisticated Cyber Attacks, Version 1.1. October 19, 2016. *https://www.jpcert.or.jp/research/APT-loganalysis_Report_20161019.pdf*
7) T. Mitsunaga: Utilizing Logs for the Early Detection and Analysis of Sophisticated Cyber Attacks. 2015. *https://www.jpcert.or.jp/research/APT-loganalysis_Presen_20151117.pdf*
8) B. Mathers: Best Practices for Securing Active Directory. Microsoft, February 2017.
9) National center of Incident readiness and Strategy for Cybersecurity (NISC): Survey Report on an Investigation of the Obtaining and Management of Information System Logs at Government Institutions in Fiscal Year 2011, March 2012.

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

Takanori Oikawa
Fujitsu Laboratories Ltd.
Mr. Oikawa is currently engaged in research and development related to cyber security.

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

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

Masahiko Takenaka
Fujitsu Laboratories Ltd.
Mr. Takenaka is currently engaged in research and development related to information security, cryptography implementation, and cyber security.

