High-Speed Forensic Technology Against Targeted Cyber Attacks (Extended Abstract)

Yuki Unno, Takanori Oikawa, Kazuyoshi Furukawa, Masanobu Morinaga,
Masahiko Takenaka, and Tetsuya Izu(✉)

FUJITSU Laboratories Ltd., Kawasaki, Japan
izu@jp.fujitsu.com

Abstract. This paper introduces the high-speed forensics technology that promptly analyzes the damage after the targeted cyber attack had been detected and visualizes the whole picture of the attack by binding the communication packets and users' logs.

1 Introduction

The targeted attacks to aim to steal information from government and municipal offices and specific enterprises and individuals keep increasing every year, and the way of the attack is becoming clever more and more. In the targeted attacks the attacker obstinately attacks the target after investigating it enough beforehand and the risk that the malware (malicious and illegal codes) intrude into an internal network rises. Therefore, there is a pressing need for countermeasures predicted on malware intrusion. It is important to detect the attack activity as soon as possible and make a suitable response to suppress damage to the minimum before the attack extends. To achieve appropriate response, the authors developed the high-speed forensics technology that promptly analyzes the situation of damage after the attack had been detected. Up to now it had taken long time for the analysis of the security incident and accident, but it is able to do it by applying the high-speed forensic technology in a short time and take inclusive measures promptly before damage expands.

L. Barolli et al. (eds.), *Advances in Network-based Information Systems*,
Lecture Notes on Data Engineering and Communications Technologies 7,
DOI 10.1007/978-3-319-65521-5_85