Chapter XLVI
Cyber Forensics

Stéphane Coulondre
University of Lyon, France

ABSTRACT

Nowadays, terrorists master technology. They often use electronic devices that allow them to act without being physically exposed. As a consequence, their attacks are quicker, more precise, and even more disastrous. As cyber-terrorism relies on computers, the evidence is distributed on large-scale networks. Internet providers as well as government agencies around the world have set up several advanced logging techniques. However, this kind of information alone is not always sufficient. It is sometimes paramount to also analyse the target and source computers, if available, as well as some networking elements. This step is called cyber-forensics, and allows for precisely reconstructing and understanding the attack, and sometimes for identifying the intruders. In this paper, we present the basics and well-known issues, and we give some related perspectives.

INTRODUCTION

When a crime is committed, the police resort to scientific methods in order to track down the culprit. These methods largely rely on traces that have been left unconsciously or unintentionally, either on or around the victim. When a suspect has been identified, the very same methods are used to gather proof on the suspect or in his/her environment (home, work, etc.).

Nowadays, electronic devices are extensively used in terrorist attacks. For example, mobile phones are used for bomb ignition; and the chemical industry's computer systems are very often the target of intrusion attempts in order to launch uncontrolled chemical reactions, either directly or indirectly, by using a specially tailored malicious code sent as Trojans to particular users. As a consequence, a new discipline is born: cyber forensics.

BACKGROUND

In the mid-1980s, various law enforcement agencies began to examine computer evidence. By analogy, examining the traces left by a user in computers and, more generally, in electronic devices (mobile phone,

personal digital assistant (PDA), videotapes, etc.) and reconstructing the evidence is called computer forensics (Shinder, 2002). The term computer forensics was coined in the first training session held by the International Association of Computer Investigative Specialists (IACIS) in Portland, OR.

As the FBI states (FBI, 2004):

Computer crimes can be separated into two categories: (1) crimes facilitated by a computer and (2) crimes where a computer or network is the target.

When a computer is used as a tool to aid criminal activity, it may include storing records of fraud, producing false identification, reproducing and distributing copyright material, collecting and distributing child pornography, and many other crimes. Crimes where computers are the targets can result in damage or alteration to the computer system. Computers which have been compromised may be used to launch attacks on other computers or networks. (p. X)

Cyber forensics is a larger term than computer forensics and applies essentially to point 2 of the above definition. Indeed, cyber terrorism very often relies on the networking aspect of forensics. Cyber forensics includes network forensics and focuses on evidence that is distributed on large-scale networks.

Forensics is a paramount step in the investigation that can reveal a lot of precise and useful information, depending on the criminal's skills, for example, the weapons and methods that have been used, the precise attack time, and what has been destroyed, stolen, or hidden. When the terrorist's origin is not known, this step can sometimes reveal both location and identity (Middleton, 2004). Whenever the attacker's electronic devices can be seized, this step enables the collection of trivial evidence.

This chapter will focus on networking aspects of cyber forensics, which are central to cyber terrorism. We first describe the basic types of traces that can be left by a terrorist or an automated process, intentionally, or unintentionally, in a target computer system or in his/her own computer. We then explain how to gather them and how they can be used, in conjunction with external information sources, to reconstruct precisely the attack scenario and track down the culprit. Then we try to give some perspectives on the future of cyber forensics, especially with reference to encryption and anonymization techniques and identity issues. Note that we do not focus here on dedicated monitoring techniques (which have to be deployed prior to any attack, i.e., intrusion detection systems, traffic recording, etc.) or incident response handling, which are outside the scope of this chapter.

DATA LIFE

A computing device (computer, PDA, digital camera, smart phone) can manipulate four types of data (Jones, Bejtlich, & RoseReal, 2005):

- Active data, which is recorded willingly and can be hidden willingly
- Temporary data, which is recorded by the system itself
- Latent data, which is considered as useless or erasable
- Archival data, which is located on an isolated media

Most computer users think that accessible data is only composed of active and archival data. Indeed, for sake of usability and simplicity, most operating systems do not mention to users the existence of temporary or latent data. However this data is of great importance.

Virtually any computing activity generates temporary and latent data. Internet browsers, word processors, mailers, games, music players, video edition software, and even intrusions or malicious code (spyware, viruses, Trojans, etc.), all leave traces of activity. The amount of disseminated information depends on the kind and duration of activity. It is important to notice that temporary and, especially,