Chapter 3
Cyber Criminal Profiling

Mohammed S. Gadelrab
National Institute for Standards, Egypt

Ali A. Ghorbani
New Brunswick University, Canada

ABSTRACT

New computing and networking technologies have not only changed the way traditional crimes are committed but also introduced completely brand new "cyber" crimes. Cyber crime investigation and forensics is relatively a new field that can benefit from methods and tools from its predecessor, the traditional counterpart. This chapter explains the problem of cyber criminal profiling and why it differs from ordinary criminal profiling. It tries to provide an overview of the problem and the current approaches combined with a suggested solution. It also discusses some serious challenges that should be addressed to be able to produce reliable results and it finally presents some ideas for the future work.

INTRODUCTION

Nowadays, a lot of crimes occur in the cyberspace; classical crimes in addition to new kinds of information-related or computer-service-related crimes. Cyber crimes may range from mail spam to war crimes passing by cyber terrorism and pedophile or child abuse. Some have roots in the physical world (e.g., financial fraud) while others completely take place in the cyber space (e.g., data theft or cyber espionage). In fact, it represents a serious threat of our modern societies and life. Fighting against cyber crime requires a multifaceted approach. The toughest part is detecting its occurrence and catching the people behind; for example who created a malware, controlled a botnet, directed a financial fraud, or a cyber espionage.

Cyber criminal profiling could be a major contributor to the resilience of our societies against cyber threats as it provides a direct deterrent of cyber crimes if perpetrators risk of being identified and prosecuted. Besides that, knowing the profile of the adversary and what (s)he is targeting, allows the owner of the data to make strategic decisions on what to put on the network and how to store it. Moreover, from law enforcement perspective, this improves prosecuting and convicting perpetrators. During ordinary crime investigations, crime investigators or forensic experts collect informa-

DOI: 10.4018/978-1-4666-8793-6.ch003

tion about potential perpetrators so that they can portray a profile with characterizing features. If the profile is well sketched it may directly reveal the identity of the person who conducted the crime. Otherwise, it may cut down the number of suspicious persons if it matches few existing profiles belonging to several criminals who have registered criminal records.

In parallel with the rise of cyber crimes, new fields such as digital forensics and cyber criminal profiling have emerged to cope with such a new kind of crimes. Both adopt fundamental concepts and try to adapt approaches from its traditional counterpart while relying mainly on digital evidences. However, importing ideas from traditional fields could be sometimes difficult and not straight forward. There exist some challenges inherent in applying the traditional approaches on digital evidences and correlating such evidences with other non-technical information. As a result, the field of cyber criminal profiling still immature despite a lot of research work that has been carried out in this area.

The ultimate goal of cyber criminal profiling is to help in identifying or determining the real identity of individual attackers or an attacker group involved in cyber crimes by identifying their characteristics, their tools and their relationships. In other words, the final objective would be the attribution of cyber crime(s) to criminal person(s). However, given the current state of the literature, having a trustworthy cyber profile that is sufficient by itself and alone for cyber criminal attribution could be an ambitious goal in most of the cases. If more effort and resource can be assigned to this problem and thanks to technology advancements, it may become feasibly more effective in short time.

While adopting more technical perspective, this chapter explains the key concepts of cyber criminal profiling. In particular, it begins by introducing the background of cyber crimes while presenting some examples from the real world. Besides that, it presents a brief literature review on research activities. From this point, it explains the basics of traditional criminal profiling and explain how it differs from cyber criminal profiling as well as presenting various types of cyber criminals. Then, the chapter describes a simple approach for cyber criminal profiling. Furthermore, it identifies relevant cyber attacker features and data sources from which we can build cyber profiles and explains the operations that should be run to maintain cyber profiles, (i.e., through profile computing). After that, a framework to collect data on cyber criminals that is necessary to build cyber profiles is presented and followed by a brief exploration of enabling technologies such as honeypots, malware analysis, security incident and event management systems, open source intelligence systems, etc. Finally, the challenges that may be confronted when dealing with this subject is discussed before the chapter concludes by some words about the new trends and some thoughts on possible future work.

A list of target audience of this chapter includes but is not limited to: security analysts, security incident handlers, computer forensics experts, network administrators, law enforcement officers, IT and security managers, government officials, etc.

BACKGROUND

A study carried out in 2014 by the Center of Strategic and International Studies, on behave of Mcafee, estimates the annual cost of cyber crimes and economic espionage to the world economy at more than $445 bilion, approximately 1 percent of the global income [CSIS, Mcafee].

During the last two years, we have witnessed attacks against big-name retailers like eBay, Michael's, Neiman Marcus and numerous other websites. Data breaches used to represent a precursor to subsequent money or information theft. eBay is one of the most notable victims of a devastating data breach, one of the biggest data breaches yet reported by an online retailer. Attackers compromised a "small number of employee log-in