# Chapter 3
# Emerging Cybercrime Trends:
## Legal, Ethical, and Practical Issues

**Sean M. Zadig**
*Nova Southeastern University, USA*

**Gurvirender Tejay**
*Nova Southeastern University, USA*

## ABSTRACT

*The issue of cybercrime has received much attention of late, as individual and organizational losses from online crimes frequently reach into the hundreds of thousands or even millions of dollars per incident. Computer criminals have begun deploying advanced, distributed techniques, which are increasingly effective and devastating. This chapter describes a number of these techniques and details one particularly prevalent trend: the employment of large networks of compromised computers, or botnets, to conduct a wide variety of online crimes. A typology of botnets is provided, and the supporting infrastructure of botnets and other online crime, including bulletproof hosting providers and money mule networks, are described. The chapter also relates a number of the practical, legal, and ethical challenges experienced by practitioners, law enforcement, and researchers who must deal with these emergent threats.*

## INTRODUCTION

Cybercrime in the 21st century is rapidly evolving, with new techniques being developed and exploited by criminals worldwide. This new type of crime is no longer the exclusive domain of the Information Systems (IS) security professional; now, every person who interacts with technology in some fashion, from the IS manager, to the end user, to the shareholder of a company which utilizes technology, needs to have an awareness of these dangerous new trends. Furthermore, modern cybercrime poses various technical, legal, and ethical challenges to those whose job it is to focus upon it, from scholarly researchers who study cybercrime, to IS security professions who defend against it, and to the law enforcement officers and prosecutors who investigate it.

DOI: 10.4018/978-1-61350-132-0.ch003

Complicating matters significantly is the ever-expanding internationality of the cybercriminals themselves. The advent of the Internet and the diffusion of computer technologies worldwide have resulted in an unprecedented global expansion of computer-based criminal activity (Salifu, 2008). Now, criminals in one country can easily conspire with other criminals in another country to defraud a victim in a third country. Or to complicate matters further, those criminals can rent (or compromise) a server in a fourth country from which to launch their attacks, which may involve compromised victim computers acting as "zombies" in dozens of other countries. In this hypothetical scenario, there are at least four international jurisdictions to deal with, each introducing different legal systems and possibly different languages and diplomatic relations into any attempt to investigate into the activity. This worldwide nature of cybercrime involves significant and unresolved issues related to the application of national laws to international crime, such as differing definitions of criminal conduct in affected countries (Podgor, 2002), making it difficult for law enforcement and prosecutors to apprehend these criminals.

The very nature of these attacks is also shifting. Traditional Internet-based cybercrime once involved attacks by lone hackers against monolithic targets, such as the notable example of British hacker Gary McKinnon in 2001, who conducted attacks against NASA and the Pentagon (Arnell & Reid, 2009). However, many of the attacks which will be discussed in this chapter are instead aimed at individual users, both corporate and residential. These users are also geographically dispersed, like the criminals who target them, and some of these attacks involve millions of victims at a time. For investigators and prosecutors, incorporating the losses experienced by these victims into criminal cases is difficult enough on a national level, but when the victims are foreign, obtaining statements or interviews can often be impossible. Attackers have also become much more focused upon financial motives; while in the past hackers may have attacked for fun, notoriety, or to challenge themselves (Hoath & Mulhall, 1998; Leeson & Coyle. 2005), more recently, making money from cybercrime victims is a major driving factor (Choo, 2008; Ianelli & Hackworth, 2006).

The remainder of the chapter is organized into five sections. The next section introduces the historical perspective of cybercrime and discusses some of the literature surrounding this perspective. The third section introduces one of the types of malicious software commonly utilized by organized cybercrime groups, botnets, and describes the emerging issues faced by this threat. The fourth section details other common threats, such as bulletproof hosting, mule networks, and other emergent trends. The fifth section describes future research opportunities in the cybercrime field, and the sixth section concludes the chapter.

## BACKGROUND

While multiple types of emerging cybercrime will be discussed, the major focus of this chapter will be on the usage of malicious software, or malware, so a brief introduction to malware would be appropriate. The first computer viruses emerged in the 1980's (Cohen, 1987), but spread slowly due to the reliance upon manual disk-to-disk infection (Highland, 1997) as a result of the lack of network connectivity between infected computers. One notable exception to this was the Morris Worm, a fast-spreading computer worm which infected one in twenty computers on the Internet in 1988 (Orman, 2003). The creator of the Morris Worm, once identified, received a sentence of three years of probation and a fine of $10,000, becoming the first individual to be tried by a jury for violating then-new federal hacking laws (Markoff, 1990).

Since the introduction of the World Wide Web in the 1990s (Berners-Lee, et. al, 1994), and the corresponding increased usage of IS by businesses and individuals, the occurrence of malicious software infections and other computer crimes have risen dramatically. For example, the Melissa Virus, a macro virus which infected Microsoft