Chapter 2
Trends in Crime Toolkit Development

Ansam Khraisat
University of Ballarat, Australia

Ammar Alazab
Deakin University, Australia

Michael Hobbs
Deakin University, Australia

Jemal Abawajy
Deakin University, Australia

Ahmad Azab
University of Ballarat, Australia

ABSTRACT
Cybercriminals continue to target online users of banks. They are improving their techniques and using high levels of skill in their attacks. Their continued search for different methods to commit crime makes the existing protection system less effective. They have developed crime toolkits which have become more accessible and simpler to use, and this has attracted more cybercriminals to cybercrime. In this chapter, the authors study the methods that are used in crime toolkits. They present the development and current trend of crime toolkits and reveal the methods that have been used to commit cybercrime successfully.

INTRODUCTION
Cybercriminals are people who use digital devices to commit crimes in cyberspace. The current prevalence of cybercrime is a major threat to information security. Initially, cybercriminals were hackers (often professional technical coders) who trespassed into the cyber world by implementing simple malware to conduct attacks. These attacks were generally aiming at gaining a reputation in the underground market, or to cause financial loss to a targeted user by deleting system data or stealing personal passwords. While occasionally their actions resulted in significant financial losses to victims it usually brought little or no financial gain to them (Sood & Enbody, 2013).

Currently, users and organizations are using Internet services heavily on their daily transactions because of the ease of attaining high speed Internet connections as Digital Subscriber Line (DSL), third Generation (3G) and others. Such new Internet services as e-commerce, online banking, online advertisements and others which moved the economy online. This economy movement shifted the motivation of Cybercriminals from getting individual reputations in the underground
market and working as individuals into working as organized large groups with more money profit driven intentions.

However, Cybercrimes are becoming more serious. The underground market has allowed criminals to achieve cybercrime intentions in different ways. Unlike before, where a Cybercriminal needed to have a strong computer technical background, today the naïve user can conduct Cybercrime using tools which are sold in the underground market. These user friendly tools are called crimeware toolkits and can be used to create sophisticated malware binaries or to propagate these malware binaries. Figure 1 demonstrates a simple underground market scenario (Hogben, Plohmann, Gerhards-Padilla, & Leder, 2011) that reflects how Cybercriminals are using strategy as organized groups which are profit driven. It also demonstrates the ease of being a Cybercriminal or purchasing a Cybercrime service. Malware writers create a Crimeware toolkit that can be used to create malware binaries or to distribute malware with a simple interface where naïve criminals can use it. After that, the malware distributor distributes and sells the Crimeware toolkit to Cybercriminals. Services and support may be offered with the toolkit where help is required. Finally Cybercriminals can infect devices and distribute attacks using these toolkits. It should also be noted that services may be offered to criminals who are ready to pay for an attack service without the need to buy any type of toolkit.

Different studies and reports demonstrate the distribution and losses caused by Cybercrime. Symantec stated that, on average, 42 billion spam messages a day are sent around the world (Symantec, 2011). In 2012, $110 billion worldwide was lost to cybercrime, with Australia recording $2 billion in losses (Norton, 2012). HP Enterprise Security, showed different losses for different countries, in which US scored highest loss with $8.9 million in just 2012 (Ponemon, 2012). Finally, 13% of North America home networks were

*Figure 1. Underground market*
Related Content

Information Systems Security: A Survey of Canadian Executives
www.irma-international.org/chapter/information-systems-security/6867

Bitcoin Hype Analysis and Perspectives in the South Asian Market
www.irma-international.org/article/bitcoin-hype-analysis-and-perspectives-in-the-south-asian-market/261206

Secure Data Hiding Using Eight Queens Solutions
www.irma-international.org/article/secure-data-hiding-using-eight/75322

Privacy Preservation Based on Separation Sensitive Attributes for Cloud Computing
www.irma-international.org/article/privacy-preservation-based-on-separation-sensitive-attributes-for-cloud-computing/226952

A New Fuzzy-Based Approach for Anonymity Quantification in E-Services
www.irma-international.org/article/a-new-fuzzy-based-approach-for-anonymity-quantification-in-e-services/136364