Chapter 3
Botnet Threats to E-Commerce Web Applications and Their Detection

Rizwan Ur Rahman
Maulana Azad National Institute of Technology, India

Deepak Singh Tomar
Maulana Azad National Institute of Technology, India

ABSTRACT

Security issues in e-commerce web applications are still exploratory, and in spite of an increase in e-commerce application research and development, lots of security challenges remain unanswered. Botnets are the most malicious threats to web applications, especially the e-commerce applications. Botnet is a network of BOTs. It executes automated scripts to launch different types of attack on web applications. Botnets are typically controlled by one or more hackers known as Bot masters and are exploited for different types of attacks including Dos (denial of service), DDos (distributed denial of service), phishing, spreading of malware, adware, Spyware, identity fraud, and logic bombs. The aim of this chapter is to scrutinize to what degree botnets can cause a threat to e-commerce security. In the first section, an adequate overview of botnets in the context of e-commerce security is presented in order to provide the reader with an understanding of the background for the remaining sections.

INTRODUCTION

Electronic Commerce is a transaction of purchasing, selling and marketing online. E-commerce makes use of computer technologies such as Internet, World Wide Web, EFT (Electronic Funds Transfer), Internet marketing, and online transaction. Current electronic commerce usually uses the World Wide Web for one part of the life cycle of transaction even though it could also use e-mail systems (O'Leary, 2000).

E-Commerce uses different Business models such as B2B (Business - to - Business), C2C (Consumer - to - Consumer), C2B (Consumer - to - Business), B2C (Business - to - Consumer). The main objective of this chapter is to study the perception of security in different business models of e-commerce

DOI: 10.4018/978-1-5225-3646-8.ch003

such as B2B, B2C, C2B, and C2C web application from both organizational and consumer viewpoint (Combe, 2012).

Security is one of the principal and ongoing concerns that limit clients and organizations engaging with e-commerce. E-commerce Security is a part of the Computer Security and is particularly applied to the components that concern e-commerce applications including Information Security and Data security. This chapter addresses the vulnerabilities, threats, and detection methods in the context of e-commerce applications. This chapter explores the perception of security in e-commerce websites from Bot and Botnet attacks viewpoint.

E-Commerce applications have numerous components including web server, database server, and payment gateway for online transaction. In Cyber world each component of e-commerce application is targeted by different attacks. According to numbers of survey reports, almost ninety percent (90%) of the attack comes from either Bot or Botnet. The given figure (Figure 1) shows the typical components involved in simple life cycle of e-commerce with different attacks on each component (Wokosin, 2002). For instance, attacks particularly targets customers are account takeover and account lockout. Similarly, the attacks that target the application are price scraping, content scraping, and database scraping.

The first section introduces the overview of Bots including basic and advanced Bots, good and bad Bots, generalized and specialized Bots. Further, this section elaborates the attacks on different components of e-commerce application such as Price Scarping, Content Scrapping, and Man in the Browser attack on e-commerce transaction.

The next section presents the more malicious form of Bot known as Botnet i.e., network of Bots. In this section technologies related to Botnet are explored and different architecture of Botnet including centralized and decentralized architectures is presented. Additionally, this section explores the taxonomy of attacks which are executed by Botnets including, Malware, DoS, Phishing, Injection attacks.

Figure 1. E-commerce components and cycle