Chapter 3
A Survey of Botnet-Based DDoS Flooding Attacks of Application Layer: Detection and Mitigation Approaches

Esraa Alomari
Universiti Sains Malaysia (USM), Malaysia & University of Wasit, Iraq

Selvakumar Manickam
Universiti Sains Malaysia (USM), Malaysia

B. B. Gupta
National Institute of Technology Kurukshetra, India

Mohammed Anbar
Universiti Sains Malaysia (USM), Malaysia

Redhwan M. A. Saad
Universiti Sains Malaysia (USM), Malaysia & Ibb University, Yemen

Samer Alsaleem
Universiti Sains Malaysia (USM), Malaysia

ABSTRACT
A Botnet can be used to launch a cyber-attack, such as a Distributed Denial of Service (DDoS) attack, against a target or to conduct a cyber-espionage campaign to steal sensitive information. This survey analyzes and compares the most important efforts carried out in an application-based detection area and this survey extended to cover the mitigation approaches for the Botnet-based DDoS flooding attacks. It accomplishes four tasks: first, an extensive illustration on Internet Security; second, an extensive comparison between representative detection mechanisms; third, the comparison between the mitigation mechanisms against Botnet-based DDoS flooding and fourth, the description of the most important problems and highlights in the area. We conclude that the area has achieved great advances so far, but there are still many open problems.

DOI: 10.4018/978-1-5225-0105-3.ch003
INTRODUCTION

In the past decade we have seen the phenomenal growth in the Internet use, this increasing illustrates the increasing importance of the Internet to the general society. Actually, the Internet is not only an important tool for researchers but also a major part of the infrastructure of general society, this growth proves all these valuable meanings. The influence of the Internet on society is illustrated in Figure 1, which depicts the huge number of hosts interconnected through the Internet (Aiello, Papaleo, & Cambiaso, 2014; Consortium, 2014).

One of the major and widely used service after the email is the World Wide Web (WWW). The (WWW) is can be defined as a system of interlinking hypertext documents these documents are accessed by the Internet. When the user use a Web browser, he can view the Web pages, the content of the Web pages could be text, images, videos and other multimedia, in the other hand will be the navigation between Web pages across hyperlinks (T. Berners-Lee / CN, 1990). The rapid growth of the WWW can be attributed to changes in traditional roles and in the way business is conducted using the Internet, which allows all transactions going back to Internet. The government uses the Internet to provide its citizens and the world at large with information and governmental services. The Internet enables companies to share and exchange information among their divisions, suppliers, partners, and customers to increase operational efficiency. Research and educational institutions depend on the Internet as a medium for collaboration to enhance their research discoveries.

Unfortunately, the growing dependence of business on the Internet, security problems have begun to pose main problems to the future of the Internet. Since the Internet use increase, the number of attacks also increased against the Internet. The Internet is especially vulnerable to attacks because of its public nature and because it has virtually no centralised control. Therefore, network attacks have become more sophisticated because the attackers have shifted from physical attacks (direct sabotage of digital resources) to remote attacks (disruption or disabling of one or more targets, e.g., Web servers). According to (Team, 2015) statistics, the number of the vulnerabilities were 171 that have been reported in 1995. However, this number had increased to 7,236 by 2007. Moreover, in the third quarter of 2008, this number increased to 6,058, and it reached over 10,000 in 2013, as shown in Figure 2.

Figure 1. Number of hosts connected through the Internet