Chapter 7
Detection of Botnet Based Attacks on Network:
Using Machine Learning Techniques

Prachi
The NorthCap University, India

ABSTRACT

This chapter describes how with Botnets becoming more and more the leading cyber threat on the web nowadays, they also serve as the key platform for carrying out large-scale distributed attacks. Although a substantial amount of research in the fields of botnet detection and analysis, bot-masters inculcate new techniques to make them more sophisticated, destructive and hard to detect with the help of code encryption and obfuscation. This chapter proposes a new model to detect botnet behavior on the basis of traffic analysis and machine learning techniques. Traffic analysis behavior does not depend upon payload analysis so the proposed technique is immune to code encryption and other evasion techniques generally used by bot-masters. This chapter analyzes the benchmark datasets as well as real-time generated traffic to determine the feasibility of botnet detection using traffic flow analysis. Experimental results clearly indicate that a proposed model is able to classify the network traffic as a botnet or as normal traffic with a high accuracy and low false-positive rates.

INTRODUCTION

Scalability in computer networks, its architecture and a variety of software applications allows people to carry out their most mundane of tasks to most complex activities from remote locations in time efficient manner with great ease. There is the tremendous change in people's daily lives and business model of organizations across the world. More and more people are getting connected to the Internet in order to complete their daily chores and get benefits of the new business model. Although Internet brings lots of new ways to reach the end users it also brings the risk associated with it. Unfortunately, criminals have gained these revolutionary technological advances to commit offenses against an individual or groups of individuals in order to physically or mentally harasses victim for personal gains using modern tele-

DOI: 10.4018/978-1-5225-4100-4.ch007

communication systems in form of Cyber Crimes (Shrivastava, 2016). Acceleration in growing usage of Internet and technological advances leads to integration of information from multiple sources that reflects scaling of volume and type of information (Matallah et al., 2017). Constant advancement in Next Generation Internet enhances the requirement of secure and efficient communication against the new sort of challenges posed by the emerging applications (Kimbahune et al., 2017). In recent times, botnets are used to launch a number of distributed cyber-attacks such as ransomware, Distributed Denial of Service (DDoS) (Shrivastava et al., 2010), distributed computational tasks, spam emails, etc. The high infection rate, a large number of unlawful activities and strong comebacks make botnets one of the most destructive attacks (Cox, 2013; David, 2012). Destruction impact of the botnet is becoming more and more critical nowadays (Guntuku, 2014).

In general, botnets can be characterized based on the characteristics of Command & Control server that is used for the communication between the bot-master and bot-client. Command & Control server facilitates a bot-master to issue some queries and waits for their responses in a time efficient manner while evading the security measures deployed by the victim to detect a botnet. Although, the different types of command and control are presented in literature two of them are most significant: centralized and distributed. In case of the distributed botnet, individual bots are hard to detect and hence increase the resiliency of botnet. However, both of them have their own benefits and drawbacks. To address their drawbacks, peer-to-peer botnets came into existence. Till date, these are most robust and hard to detect by most of the existing security mechanisms.

Although a significant number of security solutions have been developed in recent past in terms of firewall and cryptographic solutions they have their limitations in terms of security solutions. Defense solutions that identify network intrusions are another way of identifying the recent type of attacks (Shrivastava et al., 2016). The research community is actively working towards detection of botnets and a number of detection techniques have been proposed in the literature. Botnet mitigation techniques can be classified into 2 categories: active botnet detection and passive botnet detection.

Active botnet detection involves all sorts of analysis techniques that inform Command &Control server or bot-master either directly or indirectly about botnet analysis. Although, active botnet detection techniques appear promising they suffer from the drawback of early detection. Once identified, they can easily circumvent any actions taken against the botnets.

During passive analysis of network traffic, the analysis is performed without interrupting the activity of botnet. In such type of scenario, network activities are traced (Shrivastava, 2017). Most common technique in a passive analysis is the inspection of network packets. Parameters of network packets are analyzed against a large database of malicious behavior for identification of botnets. Packet inspection techniques can be easily incorporated into existing Intrusion Detection Systems (IDS). Intrusion Detection System is considered as most effective technology against the network attacks by identifying and analyzing the traffic (Denning, 1987). Most of the Intrusion Detection System designed for botnet detection is rule-based. Performance of such Intrusion Detection System depends on the rule set defined by the experts (Zhang et al., 2005; Roesch, 1999). In this type of Intrusion Detection System, signatures of incoming network traffic are compared against signatures of previously identified botnets. Such detection mechanism may work well for existing botnet but fail against rapidly changing network traffic. Such dependencies make rule-based Intrusion Detection System inefficient, time-consuming and tedious process against botnets.

Behavior or anomaly based Intrusion Detection System (Huang et al., 2016) cannot perform the complete inspection of packets when network flow is high. Techniques such as packet filtering and packet