Chapter 1
Inevitable Battle Against Botnets

Ibrahim Firat
University of Reading, UK

ABSTRACT

It is undeniable that technology is developing and growing at an unstoppable pace. Technology has become a part of people's daily lives. It has been used for many purposes but mainly to make human life easier. In addition to being useful, these advancements in technology have some bad consequences. A new malware called botnet has recently emerged. It is considered to be one of the most important and dangerous cyber security problems as it is not well understood and evolves quickly. Communication of bots between each other and their botmaster results in the formation of botnet; this is also known as a zombie army. As botnets become popular among cybercriminals, more studies have been done in botnet detection area. Researchers have developed new detection mechanisms in order to understand and tackle this growing botnet issue. This chapter aims to review working principles of botnets and botnet detection mechanisms in order to increase general knowledge about botnets.

INTRODUCTION

When it comes to talk about cyber security and its possible consequences, botnet is one of the most common word that pops in people's mind who are specialised in cybersecurity. Botnets can be considered as network of bots as they consist of more than one bot working together. Botnets use command and control (C&C) communication channels to talk with the cybercriminal who controls them. During this communication process, bots receive commands from the cybercriminal and then report back to that cybercriminal. This is one of the most distinctive characteristics of botnets which separates them from other malwares. Botnets have different architectures and cybercriminals choose any of these architectures depending on their purposes. Cybercriminals have a range of different options ranging from client-server model to peer-to-peer networks (Botnet, 2018). In general, botmasters try to collect more devices as possible to increase the strength of botnet. Through infection process, botmasters add new devices to their army. Botmasters infect new devices by using viruses, worms, trojan horses and many other malicious techniques. Once a device gets infected by any of the mentioned malicious technique, it

DOI: 10.4018/978-1-7998-5348-0.ch001

becomes a part of the botnet and can be labelled as a bot. Bots can be any device as long as cybercriminals can infect them such as computers and smartphones. On the other hand, it is well known that botnet detection is an on-going problem. It is very challenging to detect botnets as they use small amounts of computing power and they can update their behaviours. They can be very dangerous as they are capable of carrying out distributed denial-of-service (DDoS) attacks, stealing sensitive data and performing a number of different malicious behaviours. They can cause a range of different and serious problems if they are not successfully detected and neutralized. To be more precise, leakage of sensitive data can lead to conflicts at different levels. If cybercriminals leak government secrets, this can cause a crisis at a national level. On the other hand, DDoS attacks can make important online services unavailable. For example, if cybercriminals decide to perform DDoS attacks on online banking system, this can lead to money transaction problems, money fraud and even more serious financial issues. These are only some of the few problems that botnets can cause. Therefore, it is important to detect and understand botnets. This chapter aims to increase the knowledge about botnets by giving information about different types of botnets with their uses and formation. Also, it aims to explain botnet's working principles, architecture, life-cycle, possible threats, infection and detection processes.

BACKGROUND

Many researches have been done in the areas of botnets and botnet detection in order to strengthen the domain knowledge about botnets and protect innocent users from possible attacks of botnets. Cooke et al. published a paper in order to draw attention to the current botnet problem and determine the origins and structure of bots and as well as botnets. The authors stated that, monitoring IRC communication or other command and control activity was not sufficient enough to detect botnets effectively. The authors concluded the paper by describing a system which was able to detect botnets with advanced command and control mechanisms by using secondary detection data from more than one sources (Cooke, Jahanian & McPherson, 2005). In 2014, Sebastián Garcıa presented three new botnet detection methods in his PHD thesis. These detection methods were SimDetect, BClus and CCDetector. SimDetect method focused on finding structural similarities, BClus focused on clustering network traffic based on connection patterns and CCDetector focused on training a Markov Chain to detect similar traffic in unknown networks. Also, he presented a new model for botnet behaviour analysis in the given network (Garcia, 2014). On the other hand, Muthumanickam K. et al. proposed a decentralized three phased botnet detection model for the detection of P2P based botnets. The first phase was the identification of P2P node, second phase was about collecting suspicious P2P nodes together and the final phase was the detection of botnets (Muthumanickam, Ilavarasan & Dwivedi, 2014). This is followed by a study in which the authors compared the outputs of three popular botnet detection methods by executing them over a range of different datasets (Garcia, Grill, Stiborek, Zunino, 2014). In another study, the authors proposed a new technique to detect botnet activity with the help of machine learning. The authors detected botnet activity based on traffic behavior analysis by identifying network traffic behavior. Also, the authors worked on the feasibility of locating botnet activity without having access to a complete network flow by identifying behavior based on time intervals (Zhao, Traore, Sayed, Lu, Saad, Ghorbani & Garant, 2013). In another paper, the authors presented an event-driven log analysis software that helped researchers to detect botnet activities and identify if an end-user's machine has become part of the botnet (Ersson & Moradian 2013). In another study, the researchers presented a method which used artificial fish swarm

Related Content