Chapter 5

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.

DOI: 10.4018/978-1-5225-8976-1.ch005

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
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 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.
Eriksonian Analysis of Terrorism in West Africa
[www.igi-global.com/chapter/eriksonian-analysis-of-terrorism-in-west-africa/251489?camid=4v1a](www.igi-global.com/chapter/eriksonian-analysis-of-terrorism-in-west-africa/251489?camid=4v1a)

Aligning Two Specifications for Controlling Information Security
[www.igi-global.com/article/aligning-two-specifications-for-controlling-information-security/123512?camid=4v1a](www.igi-global.com/article/aligning-two-specifications-for-controlling-information-security/123512?camid=4v1a)