Chapter 18
Retrieval of Information Through Botnet Attacks:
The Importance of Botnet Detection in the Modern Era

Zahian Ismail
https://orcid.org/0000-0003-4143-6305
Universiti Malaysia Pahang, Malaysia

Aman Jantan
Universiti Sains Malaysia, Malaysia

Mohd. Najwadi Yusoff
Universiti Sains Malaysia, Malaysia

Muhammad Ubale Kiru
Universiti Sains Malaysia, Malaysia

ABSTRACT

Services and applications online involve information transmitted across the network, and therefore, the issue of security during data transmission has become crucial. Botnet is one of the prominent methods used by cybercriminals to retrieve information from internet users because of the massive impact cause by the bot armies. Thus, this chapter provides a study of Botnet and the impact of Botnet attacks especially on the security of information. In order to survive, Botnet implemented various evasion techniques, and one of the notorious ones is by manipulating an encrypted channel to perform their C&C communication. Therefore, the authors also review the state of the art for Botnet detection and focus on machine learning-based Botnet detection systems and look into the capabilities of machine learning approaches to detect this particular Botnet. Eventually, they also outline the limitations of the existing Botnet detection approach and propose an autonomous Botnet detection system.

DOI: 10.4018/978-1-6684-5250-9.ch018

INTRODUCTION

Information is an asset to many organizations. These organizations rely on the information especially for problem solving and decision making. Other organizations use information to observe the patterns and do the prediction for future exertions. For most organizations, their information is crucial and need to be protected, thus making the security of information is one of the areas that need special attention. To make things worse, recently many attackers started to use advance attacks for example the attack through Botnet, which compromised the computers in organizations and finally able to steal the organization's data.

Botnet is a vector to launch the attacks and amplify the impact of the attacks. Previously, Botnet attacks focused on the prevention of access and destruction of infrastructure through DDoS attacks, spamming and malware spreading. Nowadays, Botnet attacks mostly focusing on information stealing. Botnet itself is short for robot and networks (Jakalan et al., 2014), referring to the automated nature of Botnet operation in the network and the fact that all bots follow the instruction of the attacker (botmaster). Hence, this Botnet mechanism allows the attacker to give command through Botnet and launch the attack automatically, regardless the time and locations. In fact, if Botnet has been used to steal the information, it was in large scale and greatly affected the organizations (cloudbric, 2018).

Botnet that usually associated with information stealing mostly use encrypted channel for example SSL and TLS to launch the attacks. For instance, the attacks that targeting banking institutions, social media, and email applications (Gooley, 2017 and Desai, 2017). These applications are mostly using SSL or TLS to secure their communications and transactions. However, Botnet use the encrypted channel to hide their command and control (C&C) and to evade the detection. For that reason, this article emphasis on the discussion of the Botnet attacks over the encrypted channel.

Observing the scenario of Botnet attacks and the destructive effects cause by the attacks, the authors focus on Botnet attacks to steal the information and the detection of Botnet. The authors review the mechanism on how Botnet able to launch the attacks especially via encrypted channel and the Botnet detection techniques to suggest better detection techniques. The effective and efficient Botnet detection techniques can reduce the Botnet attacks especially the attacks targeting to steal the information. The study of Botnet detection is crucial as one of the steps for Botnet mitigation efforts. The authors study the various Botnet detection techniques and review whether the detection techniques capable to detect Botnet over the encrypted channel.

The authors organized the remainder of this article as follows. In section 2, the authors discuss the background of Botnet and possible scenarios which enable Botnet to launch the attacks over the encrypted channel. To show the severity of Botnet attacks especially for information stealing, the authors provide the example of Botnet attacks happened globally in section 3. Also in section 3, the authors are going to show Botnet variants associated with information stealing. Section 4 explains the impact of Botnet attacks to social, technical, and economy. Section 5 explains Botnet detection techniques and the limitation of Botnet detection especially for the encrypted channel. In section 6 the authors suggest the criteria for better Botnet detection system. Finally, the concluding remarks has been drawn up in section 7.