A proposed framework for P2P botnet detection

Abstract

Botnet is most widespread and occurs commonly in today‘s cyber attacks, resulting in serious threats to our network assets and organization’s properties. Botnets are collections of compromised computers (Bots) which are remotely controlled by its originator (BotMaster) under a common Command-and-Control (C&C) infrastructure. They are used to distribute commands to Bots for malicious activities such as distributed denial-of-service (DDoS) attacks, spam and phishing. Most of the existing botnet detection approaches concentrate only on particular botnet command and control (C&C) protocols (e.g., IRC,HTTP) and structures (e.g., centralized), and can become ineffective as botnets change their structure and C&C techniques. In this paper we proposed a new detection framework which focuses on P2P based botnets. This proposed framework is based on our definition of botnets. We define a botnet as a group of bots that will perform similar communication and malicious activity patterns within the same botnet. In our proposed detection framework, we monitor the group of hosts that show similar communication pattern in one stage and also performing malicious activities in another step, and finding common hosts on them.