A survey of botnet detection based on DNS

Kamal Alieyan, Ammar ALmomani, Ahmad Manasrah, Mohammed M Kadhum

Botnet is a thorny and a grave problem of today's Internet, resulting in economic damage for organizations and individuals. Botnet is a group of compromised hosts running malicious software program for malicious purposes, known as bots. It is also worth mentioning that the current trend of botnets is to hide their identities (i.e., the command and control server) using the DNS services to hinder their identification process. Fortunately, different approaches have been proposed and developed to tackle the problem of botnets; however, the problem still rises and emerges causing serious threat to the cyberspace-based businesses and individuals. Therefore, this paper comes up to explore the various botnet detection techniques through providing a survey to observe the current state of the art in the field of botnet detection techniques based on DNS traffic analysis. To the best of our knowledge, this is the first survey to discuss DNS-based botnet detection techniques in which the problems, existing solutions and the future research direction in the field of botnet detection based on DNS traffic analysis for effective botnet detection mechanisms in the future are explored and clarified.