ABSTRACT

A botnet is a collection of compromised computers, each of which is known as a 'bot', which communicate using the Internet. When a computer is compromised by an attacker, there is often code within the malware that commands it to become part of a botnet. The "botmaster" or "bot herder" controls these compromised computers via standards-based network protocols such as IRC and HTTP. Botnets are emerging as threats with hundreds of millions of computers already infected. They have become the main vehicle to conduct online crimes such as DDoS, spam, phishing and identity theft etc. Botnets have been utilizing the DNS heavily just like any legitimate host. Therefore, it is difficult to distinguish between the legitimate and illegitimate DNS traffic. Building a suitable solution for botnet detection and subsequently protecting the network from the malicious activities is a challenging problem which needs design of an accurate method. In this dissertation work, we have implemented four different methods based on analysis of DNS traffic and evaluated the effectiveness of each of the method in detection of botnet activities. Out of the four methods considered, two of them are based on similarity ratio analysis (Jaccard Similarity Ratio Method, Kulczynski Similarity Ratio Method), one is on domain clustering with hypothesis test (X-means Clustering Method) and the last one is on prior knowledge based Bayesian statistical method (Bayesian Bot Detection Method). Based on our analysis, we have also proposed and implemented a hybrid mechanism which shows better detection results. For experimental purpose, we have collected DNS logs for five consecutive days from our campus DNS server.

Only DNS based detection methods are not adequate to detect all different kind of bots, so incorporating network traffic based detection method with the DNS based method can yield better results. And this could be done as future work.