DNS rule-based schema to botnet detection

Kamal Alieyan, Ammar Almomani, Mohammed Anbar, Mohammad Alauthman, Rosni Abdullah, BB Gupta

Botnets are considered a serious issue today. They have several negative economic impacts as well. Such impacts are affecting organizations and individuals. Recent botnets–such as Zeus and Citadel's Conficker–use the Domain Name System (DNS) to avoid detection. These botnets use the DNS server to prevent the network administrator from locating and shutting down the C&C servers. Therefore, this paper proposes a DNS rule-based approach for Botnet Detection (DNS-BD) that can improve the accuracy of DNS traffic-based detection of botnets. This approach is based on DNS query and response behaviours; it aims to detect any abnormal DNS query and response behaviours by applying the proposed DNS query and response rules. The result showed that the proposed approach can detect the botnet with an accuracy of 99.35% and a false-positive rate of 0.25%. A comparison with well-known DNS-based approaches evaluates the effectiveness of the proposed approach. It has been concluded that the approach proposed outperforms other approaches that can be implemented as part of any anti-viruses IDS product.