Botnets are considered one of the most dangerous and serious security threats facing the networks and the Internet. Comparing with the other security threats, botnet members have the ability to be directed and controlled via C&C messages from the botmaster over common protocols such as IRC and HTTP, or even over covert and unknown applications. As for IRC botnets, general security instances like firewalls and IDSes do not provide by themselves a viable solution to prevent them completely. These devices could not differentiate well between the legitimate and malicious traffic of the IRC protocol. So, this paper is proposing an IDS-based and multi-phase IRC botnet and botnet behavior detection model based on C&C responses messages and malicious behaviors of the IRC bots inside the network environment. The proposed model has been evaluated on five network traffic traces from two different network environments (Virtual network and DARPA 2000 Windows NT Attack Data Set). The results show that the proposed model could detect all the infected IRC botnet member(s), state their current status of attack, filter their malicious IRC messages, pass the other normal IRC messages and detect the botnet behavior regardless of the botnet communication protocol with very low false positive rate. The proposed model has been compared with some of the existing and well-known approaches, including BotHunter, BotSniffer and Rishi regarding botnet characteristics taken in each approach. The comparison showed that the proposed model has
made a progress on the comparative models by not to rely on a certain time window or specific bot signatures.

References


Index Terms

Computer Science

Network Security
**Keywords**

IRC Botnet  IRC Botnet detection  Monitoring of Network Activities  IDS alerts  correlation