MULTI-PHASE IRC BOTNET AND BOTNET BEHAVIOR DETECTION MODEL

ABSTRACT

Nowadays, 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 such, the process of detecting botnet members is a challenging problem. IRC protocol is widely used for normal IRC chatting services, but it has also been exploited maliciously for botnet communication. Generally, the current solutions to botnet problem are either honeynet-base or IDS-base solutions. In this thesis, we propose an IDS-based and multi-phase IRC botnet and botnet behavior detection approach based on the C&C responses of the bots and their typical botnet behavior (botnet attack traces). The proposed model uses the C&C responses messages of the IRC servers captured by Snort IDS and then correlating them with both of the other C&C responses that belong to the same IRC server, and the detected botnet attacks traces inside the network environment. A spatial-temporal correlation and similarity method has been used on the proposed model. We evaluated the proposed model using six network traffic traces from three different network environments (Virtual network, DARPA 2000 Windows NT Attack Data Set and CAIDA "DDoS Attack 2007" Dataset). 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 detection accuracy and 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. Finally, the new features of the proposed model will be adapted with IAQF (Intrusion Alert Quality Framework) to enhance its functionality as a network monitoring framework based on Snort IDS.