Abstract

Being well aware of the drastic changes brought by the Internet to the world there exists an explosion of network traffic. This burst traffic brings in lots of unwanted communication as a side-effect from the infected machines also called victims. Bots are such type of infected machines which work under a super power called botmaster. A botnet is a collection of compromised machines or bots receiving and responding to commands from the Command and Control (C&C) server that serves as a rendezvous mechanism for commands from a human or controller i.e., the bot master. The aim of our work is to detect the presence of the bot in the network traffic. This is accomplished in a two-step process. The work first captures network traffic from the infected host, and second step analyzes the captured traffic and detects the presence of a bot. To meet the goal we experimented on CTU-13 data set, a data set of botnet traffic captured in the CTU University, Czech Republic. Our work uses decision trees, Naïve Bayes, SVM and K Nearest Neighbor to detect the presence of bot. We found that decision trees gives 99.9% positive detection rate compared to other algorithms.
Detecting Bots inside a Host using Network Behavior Analysis

References

17. Francisco Villegas Alejandro, Nareli Cruz Cortés and Eleazar Aguirre Anaya, 2017. Feature Selection to Detect Botnets using Machine Learning Algorithms, IEEE, and
Detecting Bots inside a Host using Network Behavior Analysis


Index Terms

Computer Science  Networks

Keywords

Bots, SVM, KNN, Decision tree, bot detection