Abstract

Malwares on the websites can be harmful for the host machine. It may result in security breach, data loss, or denial of service at the host end. Many approaches for malware prediction have been applied in the past. Supervised machine learning approaches are popular and efficient in terms of accuracy. These techniques can be very useful for malware prediction using web traffic. Alarm for malware can be generated well before the attack and damage by simply just monitoring the web traffic. In this paper comparative analysis of supervised machine learning approaches which includes Naïve bayes, Support vector machine, PART and J48 is done. These methods are compared in terms of accuracy of prediction, false positive, false negative, true positive and true negative. This analysis is done using Weka tool.

References


Index Terms
Computer Science Software Engineering

Keywords
Web Based Malware, Supervised learning, Naive Bayes, SVM, J48, PART