Abstract

Botnet is considered a multifunctional malware. It can be leveraged by criminals to launch variety of malware attacks such as click fraud, DDOS, spam, etc. Moreover, the botnets pretend the normal traffic by leveraging common protocols such as IRC, HTTP, DNS and P2P for command control. Therefore, distinguishing botnet behavior is challenging because it has similarities with normal protocols behaviors. Most of previous researches focus on detecting specific type of botnet. Moreover, they rely on limited number of features. In addition, they do not select the optimal model by tuning the hyperparameters of machine learning algorithms. In this paper we use a recent dataset that containing a diverse set of botnet traces and wider flow features. We select the relevant features using several ranking algorithms. Eventually, the optimal models are selected by tuning the hyperparameters of machine learning algorithms.

References

Efficient Botnet Detection using Feature Ranking and Hyperparameter Tuning


Index Terms

Computer Science
Security

Keywords

Botnet, Hyperparameter Tuning, Random Search