Paper Title:

Website Navigation Behavior Analysis for Bot Detection

Paper Link:

https://ieeexplore.ieee.org/document/8259764

1 Summary

1.1 Motivation

This paper focuses on finding malicious bots on the internet and to attain their goal they choose a machine learning approach.

1.2 Contribution

The paper proposed a better machine learning approach comparatively and their approach is easy to implement and sustain. Every website can be adjusted specifically and bots will have a harder time, if not completely unable to bypass their security model.

1.3 Methodology

. The researchers took data from two websites and extracted features from it . With the dataset prepared, the researchers used 10 fold cross validation to find a suitable model. With the model selected, they tried different combinations of features in order to improve the accuracy and ultimately put forth a model that performs the tasks efficiently and outperforms existing ones.

1.4 Conclusion

The finding suggests that the machine learning approach introduced in this paper has a 14% better accuracy compared to other competitive machine learning approaches. Overall, the model had 83% accuracy in detecting malicious bots.

2 Limitations

2.1 First Limitation

In order to differentiate, humans and bots researchers provided system admin with special tools. If the bots can bypass these tools, the dataset will be inconsistent and trained models will have a harder time detecting bots.

2.2 Second Limitation

The model can only keep up if trained often using updated data. Hence, the dataset needs to be updated every now and then. As long the activity is not automated, updating the datasets will be a hindrance.

3 Synthesis

As data is an important commodity, bots specializing in mining data will only increase in the future, not to mention the harmful bots that are meant for attacking. Thus, integrating the model in every website will allow the website owners to save their work/business and also allow users a smooth experience.