An Analysis of Recurrent Neural Networks for Botnet Behavior Detection

Pablo Torres*[1], Carlos Catania †[2] and Sebastian Garcia‡[3]

*Facultad de Ingenieria, Universidad de Mendoza
Mendoza, Argentina
[1]pablo.dtorres@gmail.com
†FCEN-ITIC, Universidad Nacional de Cuyo
Mendoza, Argentina
[2]ccatania@itu.uncu.edu.ar
‡CTU - Czech Technical University
Prague, Czech Republic
[3]sebastian.garcia@agents.cvut.fel.cz

***Abstract*—With the advent of new technologies and the investment in connectivity around the globe comes an increment of internet ready devices. However, an undesired outcome is the increased interest around cyber criminals to target these devices, often infecting them with malware giving unwittingly access and control as part of a botnet. We can conceive a malignant botnet as a group of compromised computers which can be controlled remotely to execute coordinated attacks or commit fraudulent acts.**

The fact that botnets keep continuously evolving means that traditional detection approaches are always one step behind. Recently, network traffic behavior analysis has arisen as a way to tackle the botnet detection problem. The behavioral analysis approach aims to look at the common patterns followed by botnets across their life cycle, trying to generalize in order to become capable of detecting unseen botnet traffic.

In this work, we propose a recurrent neural network (RNN) to analyze the behavior of network traffic by modeling it as a sequence of states that change over time. The recent success applying RNN to sequential data problems makes them a viable candidate on the task of sequence behavior analysis.

We evaluated our trained network using stratified k-fold cross validation and performed our tests on captures from two different botnets. Preliminary results reveal that the RNN is capable of classifying the traffic with a high attack detection rate while maintaining an almost negligible false alarm rate, which makes it a possible candidate for implementation and deployment on real-world scenarios.