Detecting and classifying IoT botnet attacks using Deep Learning methods

Sergei Tsimbalist

2019

Abstract

The growth of the Internet-of-Things device adoption, brings with it increased risks of these devices being infected with malware and becoming a part of the botnet. This suggests the development of novel ways for detection and prevention of these attacks. This work shows how Deep Learning methods can be used to detect and classify malicious IoT network traffic. DL methods are still considered novel when compared to more established ML methods. It will be shown how using Deep Autoencoders it is possible to detect anomalous traffic and then predict to which attack type this traffic belongs using Deep Neural Network with Softmax. The resulting algorithm very accurately predicts the malicious botnet network traffic.

Contents

1 Introduction

As the number of IoT devices grows, it creates more incentives for attackers to create malware that targets them and for example turns them into part of a botnet. Due to a multitude of different types of devices from different manufacturers it is not always feasible to use more traditinal methods of attack detection, that rely on custom attack signatures. Moreover installing and managing security for each device separately can be very burdensome, as more and more devices are added to the network.

One possible approach that solves these problems is to detect an attack using Machine Learning methods on network traffic data. In this case the model learns what a normal traffic in the network looks like and when an attack happens, it is classified as an anomalous traffic, then this data can be inspected in more details, again using Machine Learning, to determine for example which type attack it belongs to.

Recently, Deep Neural Networks have been enjoying a lot of attention for many reasons. In general, Deep Learning (the training of Deep Neural Networks) appears to be a lot more efficient on big volumes of data, and moreover it benefits from more data resulting usually in better prediction metrics. More traditional ML approached usually require some feature selection and engineering, and sometimes also the sampling of training data, in cases when there is alot of it. Performance-wise, however, both Deep Learning and classical Machine Learning can have their own advantages. Traditional ML such as decision trees, random forests, SVMs also offer good interpretability of their results, the feature that is lacking in Deep Neural Networks. However, with the development of frameworks like LIME (Local Interpretable Model-Agnostic Explanations) in becomes possible to explain the model's decision post factum.

For the purpose of One particular type of Neural Netowork, called Autoencoder suits very well for the task of anomaly detection

2 Methods

References