Project: Static/Dynamic Analysis and Machine Learning

Overview

The purpose of this project to use machine learning to improve the effectiveness and efficiency of static and dynamic malware analysis. As part of the project, we will submit several malicious files (e.g., binaries and documents) to Cuckoo, open source software for automated malware analysis, that will help gain an understanding of how malware operates. Cuckoo provides reports that summarize static, behavioral and network analysis of the malware. Radare2 is another open source software tool that can be used to extract static information from malware.

Project Idea

Static analysis can be extracted from malware in less than a second, while dynamic analysis can take several minutes because one has to run the malware and observe its behavior. We will build a predictor using fast static analysis that can determine the time that malware should be executed (dynamic analyzed) to reveal its malicious behavior is critical and should be studied, as well as deviations in the behavioral profile of malware that has been analyzed in different environments. As a result, this project will act as the foundation for evasive malware detection and automated static and dynamic analysis research.

A training set will be created with static analysis information, as well as labels indicating the time needed to uncover the malicious behavior of the malware, which will be the input for a deep neural network (DNN). Finally, we will use a preexisting database of static analyses to test our DNN and predict the time needed to run the malware. We will then proceed to execute the malware for each of the predictive times and compare the results with the reports obtained from Cuckoo.

Objectives

1. Develop an automated framework that predicts the time needed to execute malware and reveal its malicious behavior.
2. Construct a dataset of evasive malware.

Technology

- Modification of Cuckoo’s main code should be performed using Python.
- The use of AWS cloud instances in conjunction with Cuckoo.