**Research plan**

## Analysis of Machine learning methods for malware detection and classification

**Research goals**

Assess the performance of various Machine Learning methods in relation to malware detection and classification. Research which features of malware should be used for best performance.

**Problem statement**

Signature-based methods are currently most used by antivirus software. However, not only it cannot detect unknown malware families, but also the new samples (polymorphic etc.) of known malware families. Machine learning is based on the behavioral analysis of each sample and can result in better detection of new malware samples.

In this paper, the goal is to research the current state of the field, actual methodologies and solutions. A set of classifiers based on different algorithms will be trained and their performance will be tested. We will use the dataset of several hundred samples of malware of different families and several hundreds of benign files. The behavior of samples will be extracted from the reports, obtained after each sample has run in the sandbox environment. Cuckoo Sandbox will be used for this purpose. After obtaining the reports, we will research the most suitable features and perform feature extraction and selection. Data will be preprocessed and normalized. After that, different classifiers will be trained on that data and the overall performance of the classifiers will be evaluated and compared. The overall goal of this research can be formulated with the following questions:

* What is the current state of the field?
* What are the problems of signature-based methods? Can Machine Learning solve them?
* How exactly Machine Learning should be applied?
* Which methods result in best performance?
* How to perform feature extraction of the samples?
* Which features are the most suitable?
* What are others things that should be taken into account?

**Resources:**

1. Cuckoo Sandbox server
2. Some powerful server for faster data extraction
3. Python 2.7
4. R 3.3.1
5. Malware samples (now 150 samples of 5 families), benign samples (now 200 samples)

**Rough plan of final report:**

1. Introduction
2. Theory part
   1. Malware definition and types
   2. Detection methods
   3. Machine learning overview
   4. Current state of field and recent researches
3. Practical part
   1. Overview of the experiments

2.1.1 Cuckoo Sandbox

* 1. Data gathering and preprocessing
     1. Feature extraction
     2. Feature selection
     3. Other things (large files, multitasking, ????)
     4. Data scaling and normalization
  2. Clustering and classification methods
     1. K-means
     2. Support Vector Machine
     3. Naive Bayes
     4. Random Forest
     5. Multilayer perceptron??
     6. Smth else???
  3. Validation and evaluation of results (Cross-validation, maybe something else)
  4. Results

1. Conclusion and Future work