MFDCA Official Challenge

Daniel Portnoy 307889287

Erez Segev 025226655

Tomer Avitzur 025248170

**Feature Engineering Process**

In order to transform our segments to a vectorized presentation, we used a traditional method for text feature extraction: TF-IDF.

**Data Mining Methods**

At first, we tried the Supervised Classification approach to learn from our labeled data what differentiates between 'Benign' and 'Malicious' samples. We tested Naive Bayes, Linear, Forest and Neural Network models, without much success.

Then, we decided to try an Anomaly/Outlier Detection approach to learn from our un-labeled data who are the small group of suspicions 'Malicious' samples amongst the large group of 'Benign' samples.

Furthermore, we decided that every user should be tested individually, as there is no guarantee that all users share the same or common characteristics.

1. We used **K-means** classifier to find outliers, based on Euclidian distance:

* We calculated a single cluster that represents the 'Benign' samples.
* We calculated the average distance from the center for every sample.
* If a samples' distance from the center was more than some threshold we defined (115%) of the average distance, we classified it as 'Malicious'.

1. We used **4 single classifiers** with outlier detection algorithms:

* IsolationForest
* OneClassSVM
* EllipticEnvelope
* LocalOutlierFactor

1. We used a Grid search to tune the hyper-parameters of every estimator:

* We used a custom score function based on the challenge grading (1 point for 'Benign' and 9 points for 'Malicious' out of the total possible 180 points).
* We used a 3-Fold cross-validation method on our labeled users.

1. Majority voting:

* After we tuned and trained our classifiers, we combined [1] + [2] for a total of 5 different classifiers.
* The final prediction was based on the majority of the votes - if 3 or more of the 5 classifiers classified a sample as 'Malicious', we chose 'Malicious', otherwise, we chose 'Benign'.