Detecting Phishing URLs Using Machine Learning Algorithm

Mohamed Abdelhamid

Shruti Pingale

Extended Abstract

As the Internet and electronic mail continues to be utilized by an ever-increasing number of users, so does fraudulent and criminal activity via the Internet and email increase. Phishing is one of the top cybercrime in the united states and the world at large. Phishing is becoming more prevalent and is a growing concern that can take different forms. Phishing can generally be described as an attempt by cybercriminals to deceive users into disclosing credentials and sensitive. A phishing attack can be initiated by sending an electronic mail message to a user that is crafted to appear to originate from a known and trusted entity. In the past few years, phishing attacks and mechanism have been evolving and growing. Therefore, research in the context of phishing is expected to keep adapting and evolving in order to mitigate the impact of phishing attacks.

Prior research can be divided into technical and behavioral aspect of phishing. Behavioral aspects include user awareness, training, motivations among other. In this paper, we focus on the technical aspects of detecting phishing URLS. The objective of this preliminary study is to develop and train a machine learning model that can detect phishing URLs automatically. In addition, features can be added to improve the model detect accuracy as phishing URLs evolve.

We utilize a recent phishing dataset from “openphish” website. The dataset contains over 3800 phishing URLs. In addition, we added over 5000 of trusted URLs. The outcome variable is phishing (=1 if the URL is phishing, 0=if trusted). Then, we created several feature variables (i.e. based on number of characters, special characters, encryption, domain type, etc.). Then, we divided the dataset into training and testing data. We utilized Python 3 and ML libraries to train five ML models. The five algorithms were: Decision Tree, Random Forest, K Nearest Neighbors, Logistic Regression, and Multi-layer Perceptron.

Of the five algorithms, three (Decision Tree, Random Forest, and Logistic Regression) provided an accuracy that exceeded %90. More specifically, random forest performed the best with an accuracy of over %94.

Finally, this is a work in progress. We aim, to include more features and increase the number and diversity of both phishing and trusted URLs.

Keywords: Phishing, Machine Learning, Cybercrime