Enhancing Phishing Detection on Websites: A Hybrid Approach Combining Signature-Based Detection and Classic Machine-Learning Methods

Marcin Latawiec, Jakub Romanek, Ph.D. Bartosz Chaber

Faculty of Electrical Engineering, Warsaw University of Technology

Faculty of Electrical Engineering
WARSAW UNIVERSITY OF TECHNOLOGY

Introduction

The increasing sophistication and frequency of phishing attacks outpace traditional detection methods, pushing the need for more advanced solutions. While machine learning models offer adaptability and behavioral insight, they can be resource-intensive and prone to false positives. Signature-based methods, in contrast, are efficient but limited to known threats. Our research introduces a hybrid phishing detection approach that integrates both machine learning and signature-based detection, aiming to combine precision with adaptability for a lightweight, effective solution in real-time threat analysis.

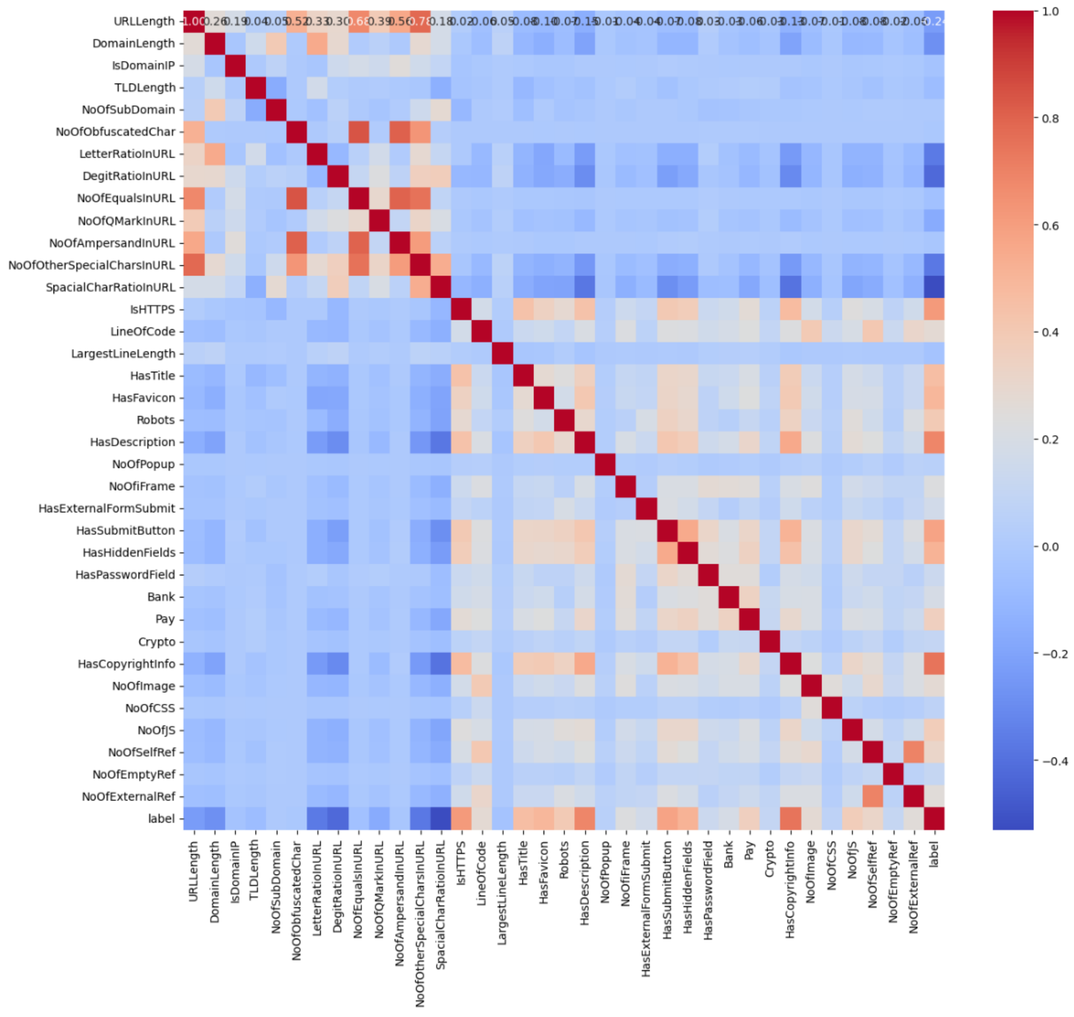

Figure 1. Two distinct regions of correlation can be observed: one corresponding to URL-based features and the other to HTML-based features. The matrix clearly dissolves into two areas of features which are correlating (url & html features).

Proposed Approach

Our study presents a detection framework that leverages a combination of classical machine learning models and a signature-based API using VirusTotal. The machine learning component is trained on a rich dataset (PhiUSIIL), comprising over 230,000 labeled URLs and 36 extracted features across URL structure and HTML content. For detection, the system extracts URLs from EML (email) files, processes them through a feature extraction pipeline, and then classifies them using a trained model. Simultaneously, the same URLs are queried via the VT API to retrieve aggregated reputation and detection scores.

Comparison of models

Three machine learning models—Decision Tree, Multilayer Perceptron (MLP), and Support Vector Machine (SVM)—were evaluated based on accuracy and training time. Results can be seen in Table 1.

Table 1. Performance comparison of chosen machine learning models.

Machine Learning Model	Accuracy [%]	Building time [s]
Decision Tree	99.823	0.69
Multilayer Perceptron	99.936	114.72
SVM	99.778	941.33

Coherence

For the sake of the research, the process includes utilizing the machine learning model, and the API wrapper to the phishing data engine. The flow of the phishing detection is presented below:

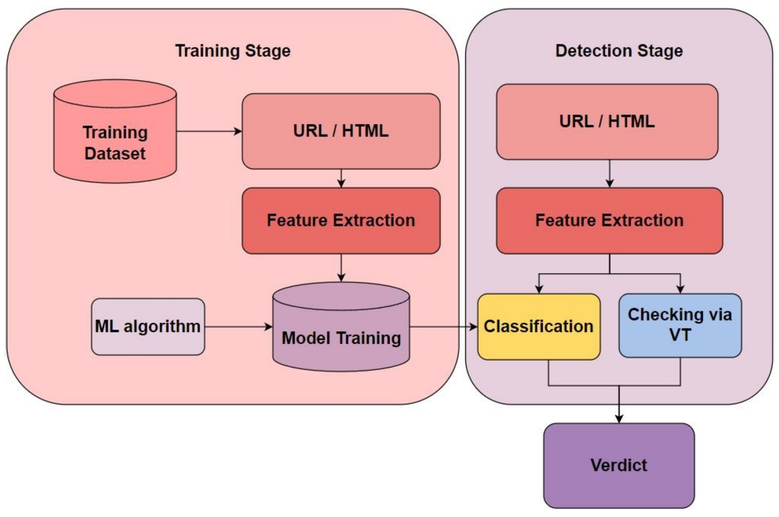

Figure 2. The process includes utilizing the machine learning model, and the API wrapper to the phishing data engine. The advantage of using two types of detections instead of one is that the user of the prototype can benefit from getting more comprehensive results.

Results

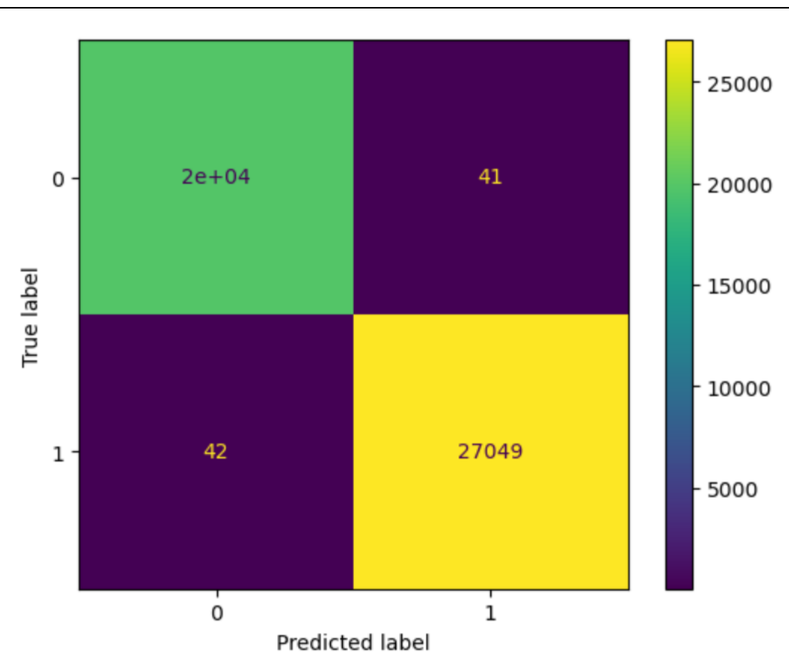

Figure 3. Confusion matrix of data classified by the decision tree confusion indicates that out of 46,914 total records, there were only 42 adequately classified False Negatives and 41 False Positives.

Conclusions

This study successfully integrated two detection methods into a single workflow, using a recent and representative dataset of phishing URLs - mostly from 2023 - which enabled accurate model training. Access to real phishing websites allowed for reliable validation in near-real-world conditions.

The links to the dataset and to the code repository are attached below:

https://github.com/Nixam01/phishsandbox

References

[1] "VirusTotal Official Documentation,", [Online]. Available: https://docs.virustotal.com/.

[2] A. Prasad and S. Chandra, "PhiUSIIL: A diverse security profile empowered phishing URL detection framework based on similarity index and incremental learning,", Jan. 2024.

[3] T. Singh, M. Kumar, and S. Kumar, "Walkthrough phishing detection techniques,", Aug. 2024.