Machine Learning Technique for Phishing Website Detection

Nurul Amira Binti Mohd Zin
Faculty of Computing
Universiti Malaysia Pahang Al-Sultan Abdullah,
26600, Pekan, Pahang, Malaysia
nurulamira2617@gmail.com

*Mohd Faizal Ab Razak
Faculty of Computing
Universiti Malaysia Pahang Al-Sultan Abdullah,
26600, Pekan, Pahang, Malaysia
faizalrazak@ump.edu.my

Ahmad Firdaus
F*aculty of Computing*
Universiti Malaysia Pahang Al-Sultan Abdullah,
26600, Pekan, Pahang, Malaysia
firdausza@ump.edu.my

Ferda Ernawan
Faculty of Computing
Universiti Malaysia Pahang Al-Sultan Abdullah,
26600, Pekan, Pahang, Malaysia
ferda@ump.edu.my

Nor Saradatul Akmar Zulkifli
Faculty of Computing
Universiti Malaysia Pahang Al-Sultan Abdullah,
26600, Pekan, Pahang, Malaysia
saradatulakmar@ump.edu.my

2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS) | 979-8-3503-1093-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSECS58457.2023.10256280

***Abstract*—** The Internet has emerged as an indispensable tool in both our personal and professional life in our modern day. As a direct consequence of this, the number of customers who make their purchases over the Internet is quickly increasing. Internet users may be vulnerable to a wide variety of web threats because of this fact. These threats may result in monetary loss, fraudulent use of credit cards, loss of personal data, potential damage to a brand's reputation, and customer mistrust in e-commerce and online banking. Phishing is a sort of cyber threat that may be defined as the practice of imitating a genuine website for the purpose of stealing sensitive information such as usernames, passwords, and credit card numbers. This research focuses on strategies for detecting phishing attacks. This study apply a machine learning approach to detect a phishing attack. As a result, this study able to detect phishing with accuracy 94%.

Keywords—phishing attack; phishing; website detection; malware; machine learning

I. INTRODUCTION

Phishing attacks are prevalent cyber threats that exploit any communication channel to trick individuals into divulging sensitive information. Attackers manipulate victims in fake scenarios to obtain data for personal harm or corporate damage. The attacker's objective and the data type determine the communication mode choice.[1] In addition, it involves ransom demands and threats of account cancellation. Another deceptive technique, email spoofing, targets customers, leading them to disclose sensitive information like credit card numbers and passwords. Phishing primarily aims to obtain critical data such as bank login credentials and credit card details. These fraudulent activities erode trust in online transactions, damaging the reputation of Internet organizations. Despite data encryption measures, computer systems remain vulnerable to attacks.[2] Awareness and vigilance are key to avoiding phishing attacks. Developing the habit of carefully browsing the Internet and verifying the trustworthiness of links can prevent harm. Browser extensions and technologies can alert users to fraudulent websites that aim to steal credentials. Implementing network systems that lock down everything except designated sites enhances security, albeit at the expense of user convenience.[1] In this work, machine learning was used to identify phishing.

Phishing website detection techniques used are heuristic-based methods that collect information from websites to identify authenticity. Unlike blocklists, heuristics can detect phishing sites in real time during their construction. Successful heuristic methods rely on discriminatory criteria for differentiating website types. Using HTML or URL signatures, the heuristic approach identifies phishing websites. Ongoing studies are exploring the effectiveness of this method.[3]

In evaluating machine learning and data mining algorithms for predicting phishing sites, Logistic Regression (LR), Bayesian Additive Regression Trees (BART), Classification and Regression Trees (CART), Random Forests (RF), and Neural Networks (NN) are compared. Experiments with a dataset of 1171 phishing emails and 1718 real emails utilized 43 functions for training and testing classifiers. Results show RF with the lowest error rate of 7.72%, followed by CART (08.13%), LR (08.58%), BART (09.69%), Support Vector Machines (SVM) (09.90%), and NN (10.73%). However, according to the findings, no single classifier emerges as the best for predicting phishing sites.[4] The research evaluates and compares the effectiveness of machine learning-based detection methods (MLBDMs), including Bagging, AdaBoost, SVM, CART, NN, RF, LR, NB, and BART. The dataset comprises 1,500 phishing websites and 1,500 trustworthy websites. Evaluation factors conducted by CANTINA encompass a total of eight criteria.[4]

II. PHISHING WEBSITE ATTACK TRENDS

The Anti-Phishing Working Group (APWG) documented 316,747 attacks in the month of December 2021, making it the month with the greatest monthly total in the organization's history of reporting. Phishing scams have been more common since the beginning of the year 2020. In the fourth quarter of 2018, the financial industry was the industry that was the most often targeted by phishing, accounting for 23.2% of all attacks. The amount of cyberattacks directed against suppliers of SaaS and webmail has remained quite high. The percentage