IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

Prediction of Phishing Websites Using Machine Learning

Revathi Pandi[1], Shruthi Suresh[2], Shruthi Siva[3], Dr. Kumaresan G[4]
Students, Department of Computer Science and Engineering[1,2,3]
Assistant Professor, Department of Computer Science and Engineering[4]
SRM Valliammai Engineering College, Chengalpattu, India

Abstract: *The Internet has become an indispensable part of our life, However, It also has provided opportunities to anonymously perform malicious activities like Phishing. Phishers try to deceive their victims by social engineering or creating mock-up websites to steal information such as account ID, username, password from individuals and organizations. Although many methods have been proposed to detect phishing websites, Phishers have evolved their methods to escape from these detection methods. One of the most successful methods for detecting these malicious activities is Machine Learning. This is because most Phishing attacks have some common characteristics which can be identified by machine learning methods. In this paper, we compared the results of multiple machine learning methods for predicting phishing websites.*

Keywords: Phishing, Websites, Machine Learning, Logistic Regression, Random Forest, Decision tree classifier, Naive Bayes Algorithm, SVM, KNN.

REFERENCES

[1]. Wentao Zhao, Jianping Yin, "A Prediction Model of DoS Attack's Distribution Discrete Probability",2008.
[2]. Jinyu W1, Lihua Yin and Yunchuan Guo, "Cyber Attacks Prediction Model Based on Bayesian Network",2012.
[3]. XiaoyongYuan , Pan He, Qile Zhu, and Xiaolin Li,"Adversarial Examples: Attacks and Defenses for Deep Learning",2019.
[4]. Zhen Yang, YaochuJin, Fellow, and Kuangrong Hao , 2018," A Bio-Inspired Self-learning Coevolutionary Dynamic Multi objective",2018.
[5]. Seraj Fayyad, Cristoph Meinel, "New Attack Scenario Prediction Methodology",2013.
[6]. "Anti-Phishing Working Group (APWG) ", https://docs.apwg.org//reports/apwg_trends_report_q4_2019. pdf.
[7]. AlEroud A, Karabatis G, "Bypassing detection of URL-based phishing attacks using generative adversarial deep neural networks. In: Proceedings of the Sixth International Workshop on Security and Privacy Analytics",2020 Mar 16.
[8]. Gupta D, Rani R, "Improving malware detection using big data and ensemble learning", Computer Electronic Engineering, vol. 86, no.106729, 2020.
[9]. E. Sri Vishva and D. Aju, "Phisher Fighter: Website Phishing Detection System Based on URL and Term Frequency-Inverse Document Frequency Values",2021.
[10]. J. Anirudha and P. Tanuja, "Phishing Attack Detection using Feature Selection Techniques ", Proceedings of International Conference on Communication and Information Processing (ICCIP), 2019,
[11]. Maher Aburrous, M. A. Hossain, Keshav Dahal, Fadi Thabtah, "Predicting Phishing Websites using Classification Mining Techniques with Experimental Case Studies",2010.
[12]. Alnajim, A., and Munro, "Ananti-phishing approach that uses training intervention for phishing websites detection",Sixth International Conference on Information Technology: New Generations (pp. 405–410). IEEE,2009.
[13]. Zhuang, W., Jiang, Q., and Xiong, T , "An intelligent anti-phishing strategy model for phishing website detection" ,In 2012 32nd International Conference on Distributed Computing Systems Workshops (pp. 51–56). IEEE,2012.