Research Exhibition in Mathematics and Computer Sciences (REMACS 6.0)/
ISBN: 978-629-97440-5-4

ANALYSIS OF THE FAKE WEBSITES USING ACTIVE URL IDENTIFYING METHOD

Muhammad Nasriq Ikmal bin Abdul Rahman, Zulfikri Paidi and Hafizah Hajimia
College of Computing, Informatics and Mathematics,
Universiti Teknologi MARA, Perlis Branch
nasriqikmalabdulrahman@gmail.com, fikri@uitm.edu.my and hafizah.hajimia@gmail.com

ABSTRACT - In the modern era, the use of Internet has been increased a lot. The Internet made the world instant therefore anyone can access and get whatever they need. However, there are an existence of fraudulent website available on the Internet and nowadays fake websites has been one of a method in cyberattack to hijack. The main use of this fake website is to trick users into fraud or malicious attacks. Several websites require users to enter sensitive information for authentication process. However, some fake websites make use of this information for miserable purposes such as blackmailing, selling the data in the black market and more. Thus, this project is carried out to simulate on how the fake website can be done using BlackEye and analyse the variety links to determine which tools has a best accuracy to detect a fake website. Two scenarios are examined; one is to simulate on ow fake website can fraud victims, while the other hand is to compare which three main tools can detect on the fake websites with higher accuracy. By studying these aspects, improved security measures and protocols can be developed to ensure people browsing on the Internet without getting trapped into fake websites.

Keywords: Fake websites, BlackEye

1. INTRODUCTION

Website is a collection of web pages and the related content that can be identified by a common and familiar domain name. Every web pages has at least one web server. Server is a software or hardware device that accepts and responds the request that has been made by the users over the network. On the other hands, fake websites are unlicensed or unauthorized websites on the Internet. Scammer misused the namelessness of the Internet to hide their true identity and intentions behind multiple unrecognizable. These fake websites work in many ways such as promising big rewards in a financial exchange. Several websites require users to enter sensitive information for authentication process. To protect against these attack, suitable security measures can be done. This project aims to develop, simulate and analyse the fake websites using BlackEye and three main tools which are URLVoid, CheckPhish and ScamVoid. Two scenario will be done which are to simulate on how fake websites can make victims fall into it and secondly on how to analyse the fake website by using different tools. This project's significance lies on the ability to recognise and list every phoney website, protecting users' data and preventing them from being victims of fraud.

2. METHODOLOGY

The method includes information gathering, planning, design, simulation, performance evaluation and documentation. Two scenario are simulated; The first scenario is simulate on how fake websites can be done by using BlackEye while the second scenario is to trace on which three tools can have a better performance on accuracy by using 20 different links combining legitimate and fraudulent links. The simulation process comprises setting up the environment, configuring the BlackEye as the main tool to create the fake website and Hydra as a tool for penetration testing. Microsoft Word is used for project documentation, facilitating accurate record-keeping and future reference. Overall, The first scenario does not meet the objectives as the link that should be sent to the victim is cannot be produced because of uncertain issues while the second scenario runs smoothly as it give a good results.

3. RESULT AND DISCUSSION

Based on three tools that has been identified; URLVoid, CheckPhish and ScamVoid, they showed a different results of accuracy on detecting the fake websites by using the same 20 links combining from legitimate and fraudulent links respectively. For URLVoid and ScamVoid, it shows 0.7 of accuracy which are 14 links out 20 links can be detected correctly. While CheckPhish, it has 0.85 of accuracy which are 17 out of 20 links which are close to get 1.0 of accuracy.

Table 1 Comparison of URLVoid, CheckPhish and ScamVoid

OL	CURACY
LVoid	
eckPhish	5
mVoid	

4. NOVELTY OF RESEARCH / PRODUCT

A scanning tool that can trace fake websites can be a valuable asset in the fight against phishing attacks. Such a tool can be created by researchers with expertise in website design, network security, and programming. The tool would need to be able to scan websites for suspicious activity, such as hidden scripts or links to known phishing sites. It could also use machine learning algorithms to identify patterns and anomalies in website design and structure that are indicative of phishing attacks. By creating such a tool, researchers can help prevent cybercrime and protect individuals and organizations from the harm caused by phishing attacks.

5. CONCLUSION

In conclusion, this project is partially successfully as the simulation of fake websites cannot be finished even after several trial with different kind of configurations and tools. The analysis of fake websites is successfully investigated and the evaluation of performance metric revealed that CheckPhish has a better accuracy than URLVoid and ScamVoid. Future research can concentrate on advancing the tools by develop a scanning tool to detect and trace fake websites through links.

REFERENCES

Blackeye Phishing Tool in Kali Linux. (2021, November 25). GeeksforGeeks; GeeksforGeeks. https://www.geeksforgeeks.org/blackeye-phishing-tool-in-kali-linux/

Huang Z., Zhang Y., Duan R., & Wang R., (2021). "Research on Malicious URL Identification and Analysis for Network Security," 2021 7th IEEE International Conference on Network

Mythilipriya, C., Priyadharshini, S., Karan, S., & Sugantha Priyadharshini, P. (2021). Fake Website Prediction Using Random Forest. Proceedings of the 2nd International Conference on Electronics & Sustainable Communication Systems, ICESC 2021, 1924–1932. https://doi.org/10.1109/ICESC51422.2021.9532770