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

Review on Phishing Attack Detection using Recurrent Neural Network

Vaibhav Handge[1], Shubham Pokale[2], Saurabh Lavhate[3], Shubham Nalkol[4], Prof G. B. Kote[5]
Students, Department of Computer Engineering[1,2,3,4]
Guide, Department of Computer Engineering[5]
Pravara Rural Engineering College, Loni, Maharashtra, India

Abstract: *Phishing is a crime that involves the theft of personal information from users. Individuals, corporations, cloud storage, and government websites are all targets for the phishing websites. Anti-phishing technologies based on hardware are commonly utilised, while software-based options are preferred due to cost and operational considerations. Current phishing detection systems have no solution for problems like zero-day phishing assaults. To address these issues, a three-phase attack detection system called the Phishing Attack Detector based on Web Crawler was suggested, which uses a recurrent neural network to precisely detect phishing incidents. Based on the classification of phishing and non-phishing pages, it covers the input features Web traffic, web content, and Uniform Resource Locator (URL).*

Keywords: Attack detection, Recurrent Neural Network, Deep Learning.

I. INTRODUCTION

Phishing is a type of cybercrime in which a person impersonating a legitimate organisation contacts a victim or target via email, phone, or text message to entice them to provide personal information, banking and credit card information, and passwords. Phishing is a serious offence. The new term 'fishing' refers to an attacker's invitation to visit a fake site by imitating a website's appearance in order to obtain personal information from users such as usernames, passwords, financial information, account details, national security identifiers, and so on. Phishing is a new phrase coined from the word 'fishing.' The data gathered is utilised for prospective target advertisements or potentially identity theft and attacks (such as money transfers from one's account). Sending e-mails, messages that can lead to data theft or personal information, is a common attack strategy. Account on a social networking site Upgrades to their websites are provided by passwords, credit cards, or attackers, who encourage you to comply with your personal information and alter it via a false website. If you provide personal information, the attackers will be able to successfully capture it on your server, allowing them to carry out the following step with your information and utilise it for their malevolent goals.

Phishing is defined as a reverberation of a notable company's website that captures personal information from customers, such as usernames, passwords, and structured savings numbers. Mail spammers can be classified based on who they are trying to reach. Some telemarketers are spammers who send a few hundred or a big number of spontaneous e-mail messages to customers. Spammers are classified as follows: they continue to send messages at random but aren't really enthusiastic. They frequently spam or push resources that are irrelevant to the issue. Sees, knowledgeable news, and words regarding meetings are some of the examples. Phishing is not a new concept, but criminals, or phishers, have increasingly utilised it in recent years to steal personal information and commit economic and social crimes. In the last four to five years, the number of phishing assaults has increased dramatically. Phishing is a common practise that is simple to carry out at your destination. Phishing typically use social engineering to entice a victim into clicking on a spoof link to a bogus website. The faked connection might be located on public websites or emailed to the victim. A false website is created in the same way as a legitimate website. As a result, instead of directing the victim's request to the proper web server, it is forwarded to the attacker's site.

II. RELATED WORK

In this paper [1], We conducted a thorough investigation of the security flaws caused by mobile phishing assaults, which included web page phishing attacks, among other things. The author proposes MobiFish, a revolutionary automated lightweight anti-phishing strategy for mobile platforms that is both automated and lightweight. Web pages, programmes,

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

and permanent accounts are all checked for legitimacy using MobiFish, which compares the actual Identity to the claimed Identity in real time. Web phishing assaults on PCs are already being addressed with existing schemes, however these do not properly combat the many types of phishing attempts on mobile devices.

In order[2] to trick an online user into disclosing personal information, In this review, the primary goal is to conduct a literature survey on social engineering attacks, namely phishing attacks and detection mechanisms for these attacks. There are different sorts of Phishing attacks, such as tab-napping, faking emails, Trojan horses and hacking, and the paper explains the best ways to avoid them. To protect confidential information from this type of social engineering assault, every company has security concerns that have been of considerable concern to users, site developers, and security experts for a long time.

Financial institutions of all sizes are being targeted by clever, well-organized, and well-funded cyber criminals who are targeting commercial and retail account [3] holders. All account holders are automatically protected against all sorts of fraud attacks with minimal disruption to legal online banking activity thanks to the availability of anomaly detection technologies that can be implemented rapidly and immediately. In addition to meeting FFIEC expectations, implementing anomaly detection will lower the total cost of fraud while increasing consumer loyalty and trust, according to the FFIEC.

This study [4] provides an in-depth examination of phishing, including an explanation of what it is, the technologies and security flaws that it exploits, and the threats it poses to end users. The concepts and technology of phishing will be explained in this research, which will demonstrate that the threat is much more than an annoyance or a fleeting trend, and examine how organised crime groups are utilising these frauds to gain a significant amount of money. A growing number of cyber-thieves are taking advantage of these same technologies to deceive us and steal our personal information, which is unfortunate for us.

The authors of this paper[6] propose a strategy termed optimal RT-PFL for distinguishing harmful URLs identified on websites from non-malicious URLs, which they describe as follows: In order to generate feature components, the data set should be encoded as both lexical and host functions for the URL in order to construct feature components. The function extraction method is responsible for extracting certain characteristics. The proposed selection technique, which is based on the Rough Set Theory algorithm and the Gray Wolf Optimizer, is used to find the best URL functions for a given URL. As a result of the extremely effective data collection, the attributes of the suggested algorithm will be reduced to a bare minimum, which will improve the efficiency of classification systems. The URL of the permitted URL should be inserted into the classifier in order to determine whether the URL is legitimate or malicious. The classification of URLs is based on a newly developed fuzzy logical technique to particle filtering, which is based on fuzzy logic. In addition to the detection of an unusually large number of suspicious URLs from malicious pages, the following categories have been strengthened:

Using data from 1529,433 malicious URLs in the last two years, this research [7] gives a complete empirical investigation of the problem. The author examines the tactical behaviours of attackers in relation to URLs in order to identify common capabilities. After that, the author divides it into three useful pools, from which the compromise levels of unknown URLs can be determined. The author employs a similarity matching technique to increase the speed of detection. The author makes the assumption that the attackers' regular URL alteration activities will classify any new URLs that they encounter. This approach can be used to attack a large variety of malicious URLs using a limited amount of functions. When it comes to precision, the proposed method is logical (it can achieve up to 70% accuracy), and it simply necessitates an analysis of the features of URLs. As a web filter or a risk scaler, this model can be used during preprocessing to determine whether or not input URLs are friendly, or to estimate whether or not an input URL is harmful.

The [8] objective of this study is repeated twice. First and foremost, the author will discuss the history of phishing assaults as well as the motivations of those who perpetrate them. The many types of phishing assaults are then classified into taxonomies. Second, in order to protect users from phishing attacks that are based on the attacks discovered in our fiscalonomics, our services will provide taxonomies of various remedies that have been proposed in the literature, which will be available through our services. In addition, we discussed the consequences of phishing assaults on the Internet of Things (IoTs). We conclude our study by discussing a number of literary topics and concerns that are still relevant in the fight against phishing attempts.

In this study [9], the authors propose a new strategy for defending against phishing attacks that involves automatically updating a white list of legitimate websites that the user has already visited. The detection rate of our proposed approach is high, and the access time is low. When a user attempts to view a page that is not included in the white list, the browser warns them not to divulge any personally identifiable information. Aside from that, we check the legitimacy of a website through

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

the use of hyperlinks. By extracting hyperlinks from your website source code and employing the proposed phishing detection method, you can prevent phishing attacks from occurring. As demonstrated by our testing data, the proposed solution to phishing has a true positive rate of 86.02 percent while having a false negative rate of less than 1.48 percent, indicating that it is extremely successful.

Sr No	Paper Title	Paper Concept	Advantage	Disadvantage
1	LongfeiWu et al.., "Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms," IEEE 2016, pp. 6678-6691.	In this work, the author conducted a thorough investigation into the security vulnerabilities created by mobile phishing assaults, which included included web page phishing attacks, and published his findings.	The author proposes MobiFish, a revolutionary automated lightweight anti-phishing strategy for mobile platforms that is both automated and lightweight. Web pages, programmes, and permanent accounts are all checked for legitimacy using MobiFish, which compares the actual Identity to the claimed Identity in real time.	Web phishing assaults on PCs are already being addressed with existing schemes, however these do not properly combat the many types of phishing attempts on mobile devices.
2	Surbhi Gupta et al., ''A Literature Survey on Social Engineering Attacks: Phishing Attack,'' in International Conference on Computing, Communication and Automation. (ICCCA2016), 2016, pp. 537-540.	In order to trick an online user into disclosing personal information, In this review, the primary goal is to conduct a literature survey on social engineering attacks, namely phishing attacks and detection mechanisms for these attacks.	There are different sorts of Phishing attacks, such as tab-napping, faking emails, Trojan horses and hacking, and the paper explains the best ways to avoid them.	To protect confidential information from this type of social engineering assault, every company has security concerns that have been of considerable concern to users, site developers, and security experts for a long time.
3	Guardian Analytics. "A Practical Guide to Anomaly Detection Implications of meeting new FFIEC minimum expectations for layered security". [Accessed: 08 Jan 2015].	The commercial and retail account holders of financial institutions of all sizes are being targeted by cyber criminals who are clever, organised, and well-funded in their attacks.	All account holders are automatically protected against all sorts of fraud attacks with minimal disruption to legal online banking activity thanks to the availability of anomaly detection technologies that can be implemented rapidly and immediately.	In addition to meeting FFIEC expectations, implementing anomaly detection will lower the total cost of fraud while increasing consumer loyalty and trust, according to the FFIEC.
4	SANS Institute, "Phishing: An Analysis of a Growing Problem", 2007. 1417 [Accessed: 23 May 2017]	This article provides an in-depth examination of phishing, including an explanation of what it is, the technologies and security flaws that it exploits, and the threats it brings to end users.	Throughout this analysis, the author explains the concepts and technology behind phishing, demonstrating that the threat is much more than an annoyance or a passing trend, and discussing how organised crime groups are utilising these schemes to make a significant amount of money.	A growing number of cyber-thieves are taking advantage of these same technologies to deceive us and steal our personal information, which is unfortunate for us.

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

III. Open Issues

Because of its widespread use and applications, a great deal of research has been done in this sector. It is discussed in this section how many techniques to achieving the same goal have been adopted in the past. When compared to strategies for Phishing systems, these studies are primarily distinguishable.

The primary premise underlying the construction of such a system is to ensure that a customer's financial information is secure, and as a result, banks and other financial institutions implement a variety of security measures to reduce the danger of unauthorised access to their online account. Nowadays, online banking is totally reliant on online transactions carried out through a variety of applications, making it critical that this online banking activity is protected.

IV. Conclusion

Phishing is one of the most devastating types of web security risks available today. According to our research, we have developed a prediction model for the identification of Phishing websites, which is based on an analysis of the attributes of the attack. The deep recurrent neural network's deep-seated learning model outperforms other machine learning models in terms of prediction and achieves the highest level of precision.

References

[1]. Surbhi Gupta et al., "A Literature Survey on Social Engineering Attacks: Phishing Attack," in International Conference on Computing, Communi- cation and Automation (ICCCA2016), 2017, pp. 537-540.

[2]. Jian Mao, Wenqian Tian, Pei Li, Tao Wei, Zhenkai Liang, "Phishing- Alarm: Robust and Efficient Phishing Detection via Page Component Similarity".

[3]. Zou Futai, Gang Yuxiang, Pei Bei, Pan Li, Li Linsen, "Web Phishing De- tection Based on Graph Mining", Guardian Analytics,"A Practical Guide to Anomaly Detection Implications of meeting new FFIEC minimum expectations for layered security". Accessed: 08 Jan 2018.

[4]. Ibrahim Waziri Jr., "Website Forgery: Understanding Phishing Attacks Nontechnical Countermeasures," in IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2015,IEEE.

[5]. LongfeiWu et al,"Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms," IEEE 2016, pp. 6678-6691.

[6]. K. Rajitha and D. Vijayalakshmi, "Suspicious urls filtering using optimal rt-pfl: A novel feature selection based web url detection," in Smart Computing and Informatics, S. C. Satapathy, V. Bhateja, and S. Das, Eds. Singapore: Springer Singapore, 2018, pp. 227–235.

[7]. S. Kim, J. Kim, and B. B. Kang, "Malicious url protection based on attackers' habitual behavioral analysis," Computers Security, vol. 77, pp. 790 – 806, 2018.

[8]. B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," Telecommunication Systems, vol. 67, no. 2, pp. 247–267, Feb 2018.

[9]. A. K. Jain and B. B. Gupta, "A novel approach to protect against phishing attacks at client side using auto-updated white-list," EURASIP Journal on Information Security, vol. 2016, no. 1, p. 9, May 2016.