LITERATURE SURVEY ON WEB PHISHING DETECTION

Abstract:

- This article surveys the literature on the detection of phishing attacks. Phishing attacks target vulnerabilities that exist in systems due to the human factor.
- Many cyber attacks are spread via mechanisms that exploit weaknesses found in end-users, which makes users the weakest element in the security chain.
- A high-level overview of various categories of phishing mitigation techniques is also presented, such as: detection, offensive defense, correction, and prevention, which we belief is critical to present where the phishing detection techniques fit in the overall mitigation process.

Literature survey

- This paper explores detailed literature available in prominent journals, conferences, and chapters. This paper explores relevant articles from Springer, IEEE, Elsevier, Wiley, Taylor & Francis, and other well-known publishers. This literature review is formulated after an exhaustive search on the existing literature published in the last 10 years.
- A phishing attack is one of the most serious threats for any organization and in this section, we present the work done on phishing attacks in more depth along with its different types.
- Initially, the phishing attacks were performed on telephone networks also known as Phone Phreaking

which is the reason the term “fishing” was replaced with the term “Phishing”

- Previous work on phishing attack detection has focused on one or more techniques to improve accuracy however, accuracy can be further improved by feature reduction and by using an ensemble model.
- Existing work done for phishing attack detection can be placed in four categories:
- Deep learning for phishing attack detection
- Machine learning for phishing attack detection
- Scenario-based phishing attack detection
- Hybrid learning based Phishing attack detection

Discussion

- Phishing is a deceitful attempt to obtain sensitive data using social networking approaches, for example, usernames and passwords in an endeavor to deceive website users and getting their sensitive credentials.
- Nowadays phishing attacks defense is probably considered a hard job by system security experts. With low false positives, a feasible detection system should be there to identify phishing attacks.
- The defense approaches talked about so far are based on machine learning and deep learning algorithms. Besides having high computational costs, these methods have high false-positive rates; however, better at distinguishing phishing attacks.
- To mitigate the risks of falling victim to phishing tricks, organizations should try to keep employees away from

their inherent core processes and make them develop a mindset that will abstain from clicking suspicious links and webpages.

Current practices and future challenges

- A phishing attack is still considered a fascinating form of attack to lure a novice internet user to pass his/her private confidential data to the attackers.
- There are different measures available, yet at whatever point a solution is proposed to overcome these attacks, attackers consider the vulnerabilities of that solution to continue with their attacks. Several solutions to control phishing attacks have been proposed in past.
- Fake websites with phishing appear to be original but it is hard to identify as attackers imitate the appearance and functionality of real websites. Prevention is better than cure so there is a need for anti-phishing frameworks or plug-ins with web browsers.
- An automated reporting feature can be added that can report phishing attacks to the organization from the user’s end such as a bank, government organization, etc. The time lost on remediation after a phishing attack can have a damaging impact on the productivity and profitability of businesses.
- In the future, an all-inclusive phishing attack detection solution can be designed to identify, report, and block malicious web websites without the user’s involvement.
- If a website is asking for login credentials or sensitive information, a framework or smart web plug-in solution should be responsible to ensure the website is legitimate and inform the owner (organization,

business, etc.) beforehand.

- Web pages health checking during user browsing has become a need of the time and a scalable, as well as a robust solution, is needed.

Conclusion

- This survey enables researchers to comprehend the various methods, challenges, and trends for phishing attack detection. Nowadays, prevention from phishing attacks is considered a tough job in the system security domain.