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.

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.