LITERATURE SURVEY

WEB PHISHING DETECTION

Jason Hong (2009) Phishing attacks are a significant security threat to users of the Internet, causing tremendous economic loss every year. Past work in academia has not been adopted by industry in part due to concerns about liability over false positives. However, blacklist-based methods heavily used in industry are slow in responding to new phish attacks, and tend to be easily overwhelmed by phishing techniques. Phishing has become a substantial threat for internet users and a major cause of financial losses. In these attacks the cybercriminals carry out user credential information and users can fall victim. The current solution against phishing attacks are not sufficient to detect and work against novel phishes. This paper presents a systematic review of the previous and current research waves done on Internet.

Hussain Ahmed, et.al (2007) Malicious URLs are harmful to every aspect of computer users. Detecting of the malicious URL is very important. Currently, detection of malicious web pages techniques includes blacklist and white-list methodology and machine learning classification algorithms are used. However, the blacklist and white-list technology is useless if a particular URL is not in list. In This paper, we propose a multi-layer model for detecting malicious URL.

JunHoHuh (2013) We propose a new phishing detection heuristic based on the search results returned from popular web search engines such as Google, Bing and Yahoo. The full URL of a website a user intends to access is used as the search string, and the number of results returned and ranking of the website are used for classification.

Dr. Gunikhan Sonowal (2017) Phishing remains a basic security issue in cyberspace. In phishing, assailants steal sensitive information from victims by providing a fake site which looks like the visual clone of a legitimate site. Phishing shall be handled using various approaches. It is established that single filter methods would be insufficient to detect different categories of phishing attempts.

Rami Mustafa (2007) Phishing is described as the art of emulating a website of a creditable firm intending to grab user's private information such as usernames, passwords and social security number. Phishing websites comprise a variety of cues within its content-parts as well as browser-based security indicators. Several solutions have been proposed to tackle phishing.

Shubhangi Wankhede (2004) Detecting any Phishing site is extremely an intricate and dynamic issue including numerous variables and criteria. Due to the ambiguities associated with phishing

location, fluffy information mining procedures can be a viable instrument in detecting phishing websites. In this paper, we propose a strategy which consolidates fluffy rationale alongside information digging algorithms for detecting phishing websites.

Ankit singh (2007) Phishing emails are more dynamic and cause high risk of significant data, brand and financial loss to average computer user and organizations. To address this problem, we propose a hybrid feature selection approach based on combination of content-based and behaviour-based. Our proposed hybrid features selections can achieve 93% accuracy rate as compared to other approaches. In addition, we successfully tested the quality of our proposed behaviour-based feature using the Information Gain, Gain Ratio and Symmetrical Uncertainty.

Adwan Yaseen (2014) Phishing attacks are one of the trending cyber-attacks that apply socially engineered messages that are communicated to people from professional hackers aiming at fooling users to reveal their sensitive information, the most popular communication channel to those messages is through users' emails. This paper presents an intelligent classification model for detecting phishing emails using knowledge discovery, data mining.

Andrew H. Sung (2010) Phishing has become an important cybersecurity problem. The centralized blacklist approach used by most web browsers usually fails to detect zero-day attacks, leaving the ordinary users vulnerable to new phishing schemes; therefore, learning machine-based approaches have been implemented for phishing detection. Many existing techniques in phishing website detection seem to include as many features as can be conceived, while identifying a relevant and representative subset of features to construct an accurate classifier remains an interesting issue in this particular application of machine learning.

Hiba Zuhair (2007) Web services motivate phishers to evolve more deceptive websites as their never-ending threats to users. This intricate challenge enforces researchers to develop more proficient phishing detection approaches that incorporate hybrid features, machine learning classifiers, and feature selection methods. However, these detection approaches remain incompetent in classification performance over the vast web. This is attributed to the limited selection of the best features from the massive number of hybrid ones, and to the variant outcomes of applied feature selection methods in the realistic condition. In this topic, this paper surveys prominent researches, highlights their limitations, and emphasises on how they could be improved to escalate detection performance. This survey restates additional peculiarities to promote certain facets of the current research trend with the hope to help researchers on how to develop detection approaches and obtain the best quality outcomes of feature selection.

References

[1] Dr. Gunikhan Sonowal: ‘Phishing Scams Cost American Businesses Half A Billion Dollars a Year’. Forbes, 5 May 2017. Accessed Jan 2018.

[2] Hiba Zuhair
‘Phishing and Pharming – The Deadly Duo’. SANS Institute, 2007. Accessed Jan 2018.

[3] Hussain Ahmed, Riaz Khan . ‘Online frauds in banks with phishing’. The Journal of Internet Banking and Commerce, vol.12, no.2, pp.1–27, 2007.

[4] Hong, J. ‘The Current State of Phishing Attacks’. Communication of the ACM, vol.55, no.1, pp.74– 81, 2012.

[5] Adwan Yaseen ‘Classification of Phishing Email Using Random Forest Machine Learning Technique’. Journal of Applied Mathematics, vol.2014, pp.1–7, Apr 2014.

[6] JunHo Huh, ‘Spear-phishing: how to spot and mitigate the menace’. Computer Fraud &Security, Jan 2013, pp.11–16. Accessed Jan 2018.

[7] Rami Mustafa ‘Social Phishing’. In Communications of the ACM 50, no.10 (2007): 94–100.

[8] Shubhangi Wankhede: Protecting (even) naive web users from spoofing and phishing attacks’. Bar Ilan University Technical Report, 2004.