WEB PHISHING DETECTION

LITERATURE SURVEY

Team ID : PNT2022TMID34650

Team Leader : Lancy Bathsebha N

Team Members : Merjina J M

Jershini J

Rehna H

1. 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.

2. 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.

3. 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 behavior-based. Our proposed hybrid features selections are able to achieve, 93% accuracy rate as compared to other approaches. In addition, we successfully tested the quality of our proposed behavior-

based feature using the Information Gain, Gain Ratio and Symmetrical Uncertainty.

4. Husain 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.

5. 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.

6. Andrew H. Sung (2010)

Phising has become an important cyber security problem. The centralized black list 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.

7. Jun Ho Huh (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.

8. 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 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.

References

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

2. Rami Mustafa 'Social Phishing'. In Communications of the ACM 50, no. 10(2007): 94–100.

3. Akit Singh: 'Protecting People from Phishing: the design and evaluation of an embedded training email system'.In Proceedings of the SIGCHI conference on Human Factors in Computing Systems, pp.905–914. ACM, 2007.

4. 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.

5. Hong, J. 'The Current State of Phishing Attacks'. Communication of the ACM, vol.55, no.1, pp.74– 81, 2012.

6. Andrew H. Sung ‘Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions’. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp.373–382. ACM, 2010.

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

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