Literature Survey – Web Phishing Detection

1, Paper Name: A Methodical Overview on Detection, Identification and Proactive Prevention of Phishing Websites

Author Name: Bhagwat M. D., Dr. Patil P. H., Dr. T. S. Vishwanath

Journal Name: Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021). IEEE Xplore Part Number: CFP21ONG-ART; 978-0-7381-1183-4

LS Content:

Bhagwat M. D., Dr. Patil P. H. and Dr. T. S. Vishwanath suggest a new approach to detect phished websites. They selected a range of features that differentiate phished websites from genuine websites and arranged these websites according to their priority by machine learning algorithms. They evaluated the features of a URL based on fuzzy rule systems. Their prototype allowed the users to enter the genuine website but if it is a phished website then this prototype sends a notification about the phished website to the corresponding host server administrator and host server administrator blocks that phished website.

2, Paper Name: Chawathe, Sudarshan. (2018). Improving Email Security with Fuzzy Rules.

Author Name: Sudarshan

Journal Name: Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021). IEEE Xplore Part Number: CFP21ONG-ART; 978-0-7381-1183-4

LS Content:

The more extreme security risks are phishing and other malicious email messages. Automated or semi-automated malicious email detection is an effective tool for combating such email threats. For such purposes, Sudarshan reviews work on using fuzzy rules to identify communications. Experimental review of the usefulness of a fuzzy rule-based classification for other classifiers like those that rely on crisp rules and decision trees, real data set and an output comparison.

3, Paper Name: Demonstrating Different Phishing Attacks Using Fuzzy Logic.

Author Name: Ms. S. D. Shweta Dasharath Shirsat

Journal Name: Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 2018, pp. 57-61, Doi: 10.1109/ICICCT.2018.8473309

LS Content:

Phishers create fake websites that look close to legitimate websites and enable the consumer to visit the malicious website. Therefore, to secure their confidential data, users must be aware of malicious websites. But, particularly fornon-technical users, it is very hard to differentiate among legitimate and fake websites. Phishing sites, in addition, are increasing rapidly. The Ms. Shweta Dasharath Shirsat's goal is to use fuzzy logic to demonstrate phishing detection and interpret results using distinct de-fuzzification methods.

4, Paper Name: Intelligent phishing detect ion system for e-banking using fuzzy data mining.

Author Name: Aburrous, Maher & Hossain, Mohammed & Dahal, Keshav & Thabtah, Fadi.

Journal Name: Expert Systems with Applications.37. 7913-7921. 10.1016/j.eswa.2010.04.044.

LS Content:

In evaluating the e-banking phishing website, Maher Aburrous introduced a new technique for fixing 'fuzziness' and proposed a smart, resilient, successful e-banking phishing website detection model. Their model is a mixture of flippant logic and data mining techniques to define the features of the phishing e- banking website, to analyze its techniques by categorizing phishing forms, and to define various parameters for attacking the structured e-banking phishing layer.

5, Paper Name: A Method for The Automated Detection of Phishing Websites Through Both Site Characteristics and Image Analysis

Author Name: White, Joshua & Matthews, Jeanna & Stacy, John.

Journal Name: The International Society for Optical Engineering. 8408. 84080B 84080B.10.1117/12.918956.

LS Content:

Joshua S. White introduces a technique for rapid automated website detection and analysis of phishing. Our methodology relies on the aggregation and review of URLs posted on social media sites in near real-time. They fetch the pages that each URL points to and describe each page with a set of values that are easily measured, such as the number of images and links. As a form of visual comparison, they also take a screen shot of the rendered page image, compute a hashof the image and use the Hamming distance between these image hashes.

6, Paper Name: Detection of Phishing Websites and Secure Transactions Detection of Phishing Websites and Secure Transactions.

Author Name: Dhanalakshmi, R & Prabhu, C & Chellapan, C.

Journal Name: International Journal Communication & Network Security (IJCNS). 1.

LS Content:

The use of a mixture of techniques of social engineering and criminals spoofing the website is an automated extortion of an online identity to trick auser to disclose sensitive data. It gathers personal identification details and financial credentials from the user. Most phishing attacks appear as spoofed e-mails that make users trust and reveal them by clicking on the links given in the e-mail. The spoofed mails appear as legitimate ones. To describe the website, the claimed title is combined with human experts and domain features. A variety of legal websites link to domain recognition services, while phishing generally covers domain names and suspicious domain names (fake identities). In addition to blacklists, in the state-of-the-art schemes, white lists, heuristics, and classifications used; R. Dhanalakshmi is proposing to consider the identity statements of websites. With MD5 hashing algorithms, password hashing has been done to allow secure transactions, which strengthens authentication of web passwords. Often it is, it has been shown that

getting the actual password from the hashed form is not an easy task due to adding the salt meaning. Get a session key through a mobile if the user is legitimate, from which further access can be done.

7, Paper Name: Phish net: predictive blacklisting to detect phishing attacks.

Author Name: Pawan Prakash, Manish Kumar, Ramana Rao Kompella, and Minaxi Gupta.

Journal Name: International Journal Communication & Network Security (IJCNS). 1.

LS Content:

Phish Net is a predictive blacklisting scheme to detect phishing attacks. Traditional blacklist approaches (i.e., exact match with the blacklisted entries) are easy for attackers to evade. Instead, Phish Net uses five heuristics (i.e., top-level domains, IP address, directory structure, query string, brand name) to compute simple combinations of blacklisted sites to discover new phishing sites. Also, it proposes an approximate matching algorithm to determine whether a given URL is a phishing site or not. Phish Net consists of two major components, namely, component I: predicting malicious URLs and component II: approximate matching.

8, Paper Name: Large-scale automatic classification of phishing pages.

Author Name: Colin Whittaker, Brian Ryner, and Marria Nazif.

Journal Name: In NDSS, volume 10, 2010.

LS Content:

Whittaker et. al. uses a logistic regression classifier to maintain Google's phishing blacklist automatically by examining the URL and the contents of a page. The proposed scheme correctly classifies more than 90% of phishing pages several weeks after training concludes. Marchal et. al. develops a phishing detection system that requires very little training data, which is language independent, resilient to adaptive attacks and implemented entirely on client-side. The proposed target identification algorithm is faster than previous works and can help reduce false positives. The proposed scheme achieves 0.5% false positive rate and 99% true positive rate.