LITERATURE SURVEY

WEB PHISHING DETECTION

Author Name : Jason Hong

Year of Publishing : 2009

Description :

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 cyber criminals 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.

Author Name : Hussain ahmed, et.al

Year of Publishing : 2007

Description :

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.

Author Name : JunHo Huh

Year of Publishing : 2013

Description :

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.

Author Name : Dr. Gunikhan Sonowal

Year of Publishing : 2017

Description :

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.

Author Name : Rami Mustafa

Year of Publishing : 2007

Description :

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.

Author Name : Shubhangi Wankhede

Year of Publishing : 2004

Description :

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.

Author Name : Ankit singh

Year of Publishing : 2007

Description :

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.

Author Name : Adwan Yaseen

Year of Publishing : 2014

Description :

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.

Author Name : Andrew H. Sung

Year of Publishing : 2010

Description :

Phishing has become an important cyber security 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.

Author Name : Hiba Zuhair

Year of Publishing : 2007

Description :

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.

Author Name : Mahmoud Khonji , Youssef Iraqi and Andrew Jone

Year of Publishing : 2013

Description :

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. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques. 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.

Author Name : Ankit Kumar Jain and B. B. Gupta

Year of Publishing : 2017

Description :

Phishing is one of the major problems faced by cyber-world and leads to financial losses for both industries and individuals. Detection of phishing attack with high accuracy has always been a challenging issue. At present, visual similarities based techniques are very useful for detecting phishing websites efficiently. Phishing website looks very similar in appearance to its corresponding legitimate website to deceive users into believing that they are browsing the correct website. Visual similarity based phishing detection techniques utilise the feature set like text content, text format, HTML tags, Cascading Style Sheet (CSS), image, and so forth, to make the decision. These approaches compare the suspicious website with the corresponding legitimate website by using various features and if the similarity is greater than the predefined threshold value then it is declared phishing. This paper presents a comprehensive current solution space, analysis of phishing attacks, their exploitation, some of the recent visual similarity based approaches for phishing detection, and its comparative study. Our survey provides a better understanding of the problem, and scope of future research to deal with phishing attacks efficiently using visual similarity based approaches.

Author Name : M. Vijayalakshmi, S. Mercy Shalinie, Ming Hour Yang, Raja Meenakshi U

Year of Publishing : 2020

Description :

Internet dragged more than half of the world's population into the cyber world. Unfortunately, with the increase in internet transactions, cyber crimes also increase rapidly. With the anonymous structure of the internet, attackers attempt to deceive the end-users through different forms namely phishing, malware, SQL injection, man-in-the-middle, domain name system tunnelling, ransomware, web trojan, and so on. Amongst them, phishing is the most deceiving attack, which exploits the vulnerabilities in the end-users. Phishing is often done through emails and malicious websites to lure the user by posing themselves as a trusted entity. Security experts have been proposing many anti-phishing techniques. Till today there is no single solution that is capable of mitigating all the vulnerabilities. A systematic review of current trends in web phishing detection techniques is carried out and a taxonomy of automated web phishing detection is presented. The objective of this study is to acknowledge the status of current research in automated web

phishing detection and evaluate their performance. This study also discusses the research avenues for future investigation.

Author Name : Ashit Kumar Dutta

Year of Publishing : 2021

Description :

In recent years, advancements in Internet and cloud technologies have led to a significant increase in electronic trading in which consumers make online purchases and transactions. This growth leads to unauthorized access to user's sensitive information and damages the resources of an enterprise. Phishing is one of the familiar attacks that trick users to access malicious content and gain their information. In terms of website interface and uniform resource locator (URL), most phishing web pages look identical to the actual web pages. Various strategies for detecting phishing websites, such as blacklist, heuristic, Etc., have been suggested. However, due to inefficient security technologies, there is an exponential increase in the number of victims. The anonymous and uncontrollable framework of the Internet is more vulnerable to phishing attacks. Existing research works show that the performance of the phishing detection system is limited. There is a demand for an intelligent technique

to protect users from the cyber- attacks. In this study, the author proposed a URL detection technique based on machine learning approaches. A recurrent neural network method is employed to detect phishing URL. Researcher evaluated the proposed method with 7900 malicious and 5800 legitimate sites, respectively. The experiments' outcome shows that the proposed method's performance is better than the recent approaches in malicious URL detection.

Author Name : Pratik Patil and Prof. P.R. Devale

Year of Publishing : 2016

Description :

It is a crime to practice phishing by employing technical tricks and social engineering to exploit the innocence of unaware users. This methodology usually covers up a trustworthy entity so as to influence a consumer to execute an action if asked by the imitated entity. Most of the times, phishing attacks are being noticed by the practiced users but security is a main motive for the basic users as they are not aware of such circumstances. However, some methodologies are limited to look after the phishing attacks only and the delay in detection is mandatory. In this paper we emphasize the various techniques used for the

detection of phishing attacks. We have also discovered various techniques for detection and prevention of phishing. Apart from that, we have introduced a new model for detection and prevention of phishing attacks.

Author Name : Ayesha Arshad and Muhammad Azeem

Year of Publishing : 2021

Description :

Phishing is the number one threat in the world of internet. Phishing attacks are from decades and with each passing year it is becoming a major problem for internet users as attackers are coming with unique and creative ideas to breach the security. In this paper, different types of phishing and anti-phishing techniques are presented. For this purpose, the Systematic Literature Review(SLR) approach is followed to critically define the proposed research questions. At first 80 articles were extracted from different repositories. These articles were then filtered out using Tollgate Approach to find out different types of phishing and anti-phishing techniques. Research study evaluated that spear phishing, Email Spoofing, Email Manipulation and phone phishing are the most commonly used phishing techniques. On the other hand, according to the

SLR, machine learning approaches have the highest accuracy of preventing and detecting phishing attacks among all other anti-phishing approaches.