International Journal of Engineering Research and Reviews ISSN 2348-697X (Online)
Vol. 2, Issue 4, pp: (110-112), Month: October - December 2014, Available at: www.researchpublish.com

Bait Alarm: Anti-Phishing Using Visual Similarities

[1]Anuja Salve, [2]Manisha Salgar, [3]Akshata Sarode, [4]Trushali Sardal,
[5]Prof. Archana Said

[1, 2,3,4,5] Department of Computer Engineering, AISSMS-IOIT, PUNE, INDIA

Abstract: **Phishing is the combination of social engineering and technical exploits designed to convince a victim to provide personal information, usually for the economic gain of the attacker. Phishing emails contains messages to attract victims into performing certain actions, such as checking the a URL where a phishing website is hosted and executing a malware code for future use. Phishing has become the most popular practice among the criminals of the Web. Phishing is a continual threat that keeps growing to this day. URL and textual content analysis of email will results in a highly accurate anti phishing email classifier and prevention of them. We will propose a technique where we consider the advantages of blacklist, white list and combination of both that means heuristic technique for increasing accuracy and reducing false positive rate as well as true negative rate. In heuristic technique we are using textual analysis and URL analysis of e-mail and domine analysis.. Since most of the phishing mails have similar contents, our proposed method Bait Alarm will increase the performance by analysing textual contents of email and lexical contains of URL analysis. It will detect phishing mail if DNS is present in black list and If DNS is present in white list then it is considered as authorized DNS. If it is not present in white list as well as blacklist then it is analyzed by using pattern matching with existing phishing DNS test and contents found in email and analysis of actual URL analysis. With the help white list and black list we are avoiding detection time for phishing and authorized email. At the same time we are decreasing false positive rate by combining features of DNS, pattern matching, textual content analysis of email and URL analysis.**

Keyword: **Anti-phishing, Network Security, Hyperlink, iFrame, Phishing, URLObfus-cation**.

I. INTRODUCTION

Phishing is typically carried out by email, and it mis-guide the users to enter details at a fake website which is almost identical to the legitimate one. Even using server authentication, it still requires skill to detect that the website is malicious. Phishing is an example of social engineering techniques used to mislead users, and utilize the poor usability of current web security technologies.

Phishing is the process of fooling a consumer into divulging personal information, such as credit card numbers or passwords, usually by sending an email carefully constructed to appear as if it's from a bank or other trusted entity, such as PayPal. As people increasingly rely on the Internet for business, banking, personal finance and investment, Internet fraud becomes a greater issuse in todays world.

Phishing is a criminal scheme to steal the user's personal data and other credential information. It is a fraud that acquires victims confidential information such as bank account detail as well as credit card number, financial username and password etc. and later it can be misuse by attacker by hacking, We will propose a novel solution, Bait Alarm ,to efficiently detect phishing web pages through the Cascading Style Sheet (CSS). we will develop an algorithm to detect similarities in key element related CSS like the URL of trusted site, the domine of the site, the title of the site.

II. LITERATURE SURVEY

Phishing is a form of social engineering attack in which an attacker mimics electronic communications to lure users to provide their confidential information. Such communications trick users to visit phishing web sites, which collect users

private information, such as passwords, banking details credit card numbers, and social security numbers. The basic aim of this project is to detect and prevent users from phishing website attack. There are two other kinds of existing phishing detection approaches that are based on the similarity of web pages: based on page text and based on rendered page image. Text-content-based methods detect the phishing pages according to the frequency of web pages keywords, some sensitive words or the matching ratio between the suspicious page and the target page.

Drawback of Existing System:

(1) These solutions have their limitations. attackers may replace the text contents by an image with the same content. In this way, the phishing page displays the same content as the original one but anti-phishing tools cannot get the useful text content of the phishing pages for comparison and detection.

(2) Attackers may also embed noise contents with the pages background color to be invisible to users.

(3) These methods can bypass text-content comparison without losing the visual similarity to the target page.

(4) Rendered-page-based methods decide the similarity between two pages by comparing the pixel of their rendered pages. This approach has high overhead incurred by image parsing.

we will present a new solution, Bait Alarm, to detect phishing attack using features like CSS and DNS.. The suspicion of our approach is that phishing pages need to preserve the visual appearance the target pages. We will present an algorithm to the suspicious ratings of web pages based on similarity of visual appearance between the web pages. Since CSS and DNS are the standard technique to specify page layout as well as domine analysis, our solution uses the CSS as the basis for detecting visual similarities among web pages and DNS for domine information test. We prototyped our approach as a Google Chrome extension , may in future scope we will use another search engine and used it to rate the suspiciousness of web pages. The prototype shows the accuracy and correctness of our approach with a relatively high performance overhead quantify.

III. OBJECTIVES

(1) To detect phishing web pages & to avoid phishing attacks.

(2) To secure user's credential information.

IV. WORKFLOW

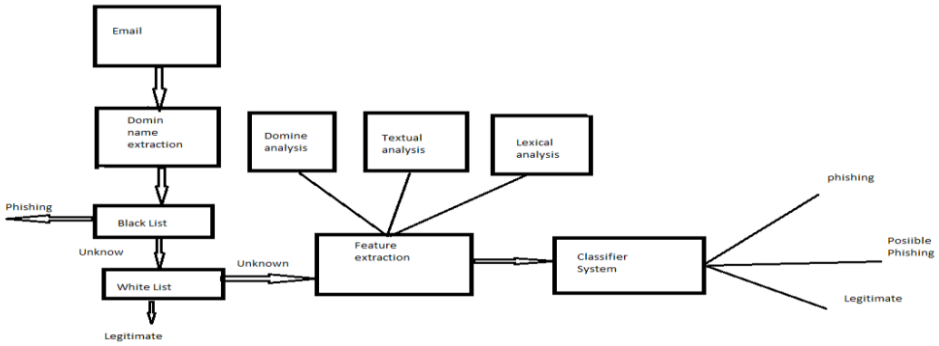

Fig. 1 workflow of algorithm

V. METHODOLOGY

1. We have implemented ObURL Detection Algorithm to detect the URL Obfuscation Phishing Attacks by hackers. ObURL Detection Algorithm stands for Obfuscated URL Detection Algorithm.

2. The ObURL detection algorithm provides the multiple type of security. Because of the use of internet service is continuously increasing day by day, the phishing attacks are also increasing. As we explaining how creating the phishing site and spoofed email is send to users. So, the ObURL detection algorithm will secure the data against the phishing attacks over the internet.

3. As we know, the attacker uses the number of methods to obfuscate the URL and domine of site. So, it is complex to detect all that attacks but the ObURL detection algorithm can detect the maximum number of URL obfuscation phishing attacks because following test cases are perform for checking the phishing site emails.

a) DNS Test

b) IP Address Test

c) URL Encode Test

d) Shorten URL Test

e) White List Test

f) Black List Test

g) Pattern Matching Test

And it also checks the iFrame, source URL of iFrame, content of iFrame's source URL, input form in email.

VI. EXPECTED OUTPUT

To get prioritize results by detecting phishing web pages.

VII. CONCLUSION

Thus in our paper we are providing prioritized and personalized results to the user using CSS detection Algorithm. We introduces a novel anti-phishing approach, Bait Alarm, which is based on efficient similarity comparison between the suspicious page and the target page. In particular, Bait Alarm uses CSS and related elements to represent visual features of a web page. Our evaluation using a large number of phishing pages supports the key idea of our approach. In the future work, we will work on improving Bait Alarms resilience to evasion attacks.

VIII. FUTURE SCOPE

We are designing this software currently only for chrome extension further This software can be extended Firefox.

REFERENCES

[1] APWG, Investigation report, http://www.antiphishing.org/ reports/apwg trends report h2 2011.pdf, 2011.

[2] APWG, Investigation report, http://www.antiphishing.org/ reports/apwg trends report h2 2011.pdf, 2011.

[3] C.Inc., Could mark toolbar, http://www.cloudmark.com/ desktop/ie-toolbar. [4] T. Ronda, S. Saroiu, and A. Wolman, itrustpage: A userassisted anti-phishing tool, in Proceedings of Eurosys08.ACM, April 2008.

[4] iTrustPage,http://www.cs.toronto.edu/ronda/itrustpage/.

[5] .I. Fette, N. Sadeh, and A. Tomasic, Learning to detect phishing emails, in Proceedings of the International World Wide Web Conference (WWW), May 2007.

[6] Y. Zhang, J. Hong, and L. Cranor, Cantina: A content-based approach to detecting phishing web sites, in Proceedings of the International World Wide Web Conference (WWW), May 2007.

[7] .A. Nourian, S. Ishtiaq, and M. Maheswaran, Castle: A scocial framework for collaborative anti-phishing databases, ACM Transactions on Internet Technology, 2009.