International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 6 – MAY 2018.

A SOLUTION FOR FAKE WEBSITE DETECTION AND DOS PREVENTION

R. Iswarya [#1] and B. Prakash [*2]

[#] M.E - II Year,Dept of CSE, Adhiparasakthi Engineering College, Melmaruvathur.India
[*] Assistant Professor/CSE, Adhiparasakthi Engineering College, Melmaruvathur.India

***Abstract*— Phishing is the third cyber-security threat globally and the first cyber-security threat in China. Phishing attacks were highly concentrated in targeting at a few major Websites. In this project, the machine learning based phishing detection using only lexical and domain features, which are available even when the phishing Web Pages are inaccessible. We then select an optimal set of features in our phishing detector, which has achieved a detection rate better than 98%, with a false positive rate of 0.64% or less. The detector is still effective when the distribution of phishing URLs changes.**

***Index Terms*—About four key words or phrases in alphabetical order, separated by commas.**

I. Introduction

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic. Unlike other kinds of cyberattacks, DDoS assaults don't attempt to breach your security perimeter. Rather, they aim to make your website and servers unavailable to legitimate users. DDoS can also be used as a smokescreen for other malicious activities and to take down security appliances, breaching the target's security perimeter. A successful DDoS attack is a highly noticeable event impacting an entire online user base. This makes it a popular weapon of choice for hacktivists, cyber vandals, extortionists and anyone else looking to make a point or champion a cause. DDoS assaults often last for days, weeks and even months at a time, making them extremely destructive to any online organization. Amongst other things, DDoS attacks can lead to loss of revenues, erode consumer trust, force businesses to spend fortunes in compensations and cause long-term reputation damage.

II. EXISTING SYSTEM

The present system is having the one which can secure the data against phishing at one of the levels and it don't have a highly secure system to detect Phishing URL's. The main drawback is Analysis method is very complicated. Furthermore, Machine Learning method can detect unknown URLs, but results may contain many false positives and false negatives. It is only able to filter phishing pages using some algorithms randomly.

III. PROPOSED SYSTEM

In this project, trying to propose a new system model which will guarantee a system where the attacker couldn't hack the user's data. The techniques implemented in this system are too simple and strong for the user and hard for the hacker to break. This project trying to address some of the huge issues like, Title Based Crawler to crawl all the URLs matching with the Title name, Implementing URLs Scanning Method using Different types of Scan Engine Like AVG, Norton's, McAfee to Detect the Phishing URLs.

So that its possible to prevent the system from all type of Phishing Attacks. It can block the Malicious/Phished URL's to enter into the system.

In Scanning Method we can find all type of URL's like Clean URL's , Gray URL's Red/Yellow URL's In this method we can filter all the Phishing URL's Easily.

IV. SYSTEM ARCHITECTURE

The architecture involves the validation of user by user name and pass word. By getting the Domain name it starts to analyse the filter, if it founds to be malicious request then it block the IP address of the system. Else it request the domain name and verify its IP address , crawl the URL. Then it finds the domain and scan it . Finally the proposed system gives the result of detection.

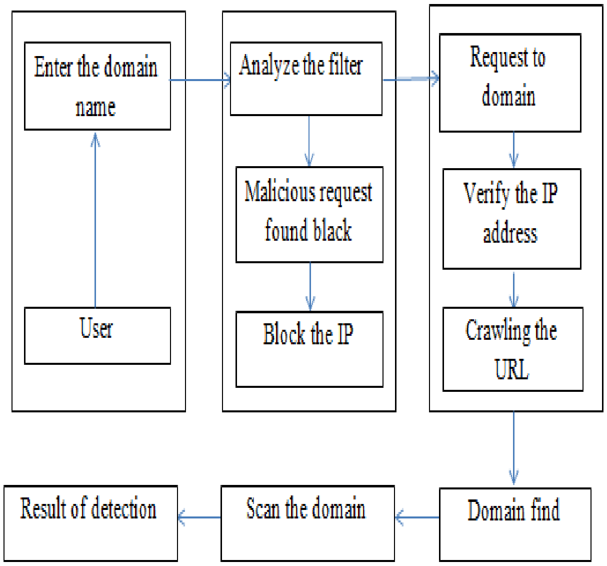

Figure 1. Architecture Diagram

V. SYSTEM MODULESS

A. Title Detection

Title detection is a prefix or suffix words are to be watched and scan the link of whole URL whether it's belonging to original link or not

B. Search Engine Crawling

A crawler is a program that visits Web sites and reads their pages and other information in order to create entries for a search engine index.

C. False Positive & False Negative Detection

Here it'll search whole of the website including the crawling link and scan domain name and ip address. It used to find out the given links are phished page or not.

D. Proxy Finder

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. Here we are checking IP address because every domain having the ip address it was registered when they were launching the website. Proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems.

E. IP verified

Analyze the IP request to server. In computer networks, a proxy server is a server (a computer system or anapplication) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems

F. IP Filtering

IP address blocking prevents the connection between a server or website and certain IP addresses or ranges of addresses. IP address blocking effectively bans undesired connections from hosts using affected addresses to a website, mail server, or other Internet server. IP address blocking is commonly used to protect against brute force attacks. Here proposed system are blocking the request if more than 7 continuous request from the client side to server then that IP users can't access the original page of the server. So it can stop the DDOS attack happened.

VI. CONCLUSION

This paper proposed a phishing detection approach that classifies the webpage security by checking the webpage source code, and checked the webpage source code, if it find a phishing character by analyzing the IP address and domain name, and it will verify the subdomain URL'S also and it will verify decrease from the initial secure weight. Finally calculated the security percentage based on the final weight, the high percentage indicates secure website and others indicates the website is most likely to be a phishing website. This paper checked two webpage source codes for legitimate and phishing websites and compare the security percentages between them, and it found the phishing website is less security percentage than the legitimate website. It is crucial to detect the Vampire flooding attacks at their early launching stage before widespread damages done to legitimate applications on the victim system. Here the paper have discussed about how it can block an IP but if the user changes their IP then the attack must not happen, so it must make use of cookies or the session id along with the IP to block a node.

REFERENCES

[1] Identity thieves take advantage of voip. http://www.icbtollfree.com/article_free.cfm?articleId=5926.

[2] Internet explorer 8 features - safer: domain highlighting. http://windows.microsoft.com/en-US/internet-explorer/products/ie8/feat%ures/safer?tab=ie8dom.

[3] Opendns' phishtank.com and anti-phishing working group to share data. http://www.opendns.com/about/announcements/19/.

[4] Phishing - word spy. http://www.wordspy.com/words/phishing.asp.

[5] Phishing- consumer laws. http://consumerprotection.uslegal.com/phishing/.