A NEW ANTI-PHISHING TECHNIQUE

Nishu Bansal
Assistant Professor, Ajay Kumar Garg Engineering College, Ghaziabad, U.P India
bansalnishu@akgec.ac.in

***Abstract*—There are many types of hacking and breaching threats to our data stored on the databases that can be accessed using internet. One of the major threats is phishing. This threat has various means through which the phisher can take your valuable data available in the form of digital money or confidential data. Reports say people can be easily lurked to extract data from them. This article provides a technique which is capable of solving the frauds conducted using phishing.**

***Index Terms*—Phishing, network security, Anti-phishing.**

I. INTRODUCTION

Now a dayswe see a lot of frauds going on in the world where people are not looting bank or people directly using physical means. But very cleverly using internet as a medium various kind of breaches can be launched.One of them is phishing. In this, the fraudster will make the person visit their fake site where they will be asked to enter their personal details such as passwords of social sites, email accountsand bank details. After collecting these details. The fraudster can fetch the money from the bank or can impersonate as that person and launch various other security breaches which can sometimes be beyond imagination.

Recently the fake sites launched are based upon the internet surfing behaviour of the users. People are easily trapped to watch sites related to health, weight loss, websites offering free offers. Some of the reels on Instagram and Facebook, videos on the YouTube ask people to click on the following link and take them their fake websites to fetch information from them.

The rest of the paper is organized as follows:

- Section II introduces the reader to existing anti-phishing techniques.
- In Section III, Functional Challenges.
- Section IV provides new system.
- Section V is measures to avoid phishing.
- Section VI is future work
- Section VII is conclusion
- In Section VIIthe various references are given.

II. EXISTING ANTI_PHISHING TECHNIQUES

As fraudsters are using different ways to launch phishing attack. To combat these new techniques are required from time to time which can address new issues and provide solution to them. Earlier the attack is launched by sending emails and messages to the target audience but now people are forced to visit a website for example telling them they are in this video and visit the website to see your popularity. The techniques are either detection systems or prevention systems. Thedetection-basedsystem [1,2,3,4,5] detect the fraud websiteearly. The prevention system become active if you are asked to submit some personal details to your website and the system will prompt you before you submit the details[6].Most of the current anti-phishing structures warn customers about capacity-threatening operations. However, those excessive false positives and / or false negatives undermine customer confidence in the structure. As a result, customers usually forget the warning

Maintain their operation. On the other hand, simply blocking a suspicious internet website is generally unacceptable unless you are really certain that the website is a phishing website.

III. FUNCTIONAL CHALLENGES

In the design of anti-phisher systems, it is important to consider that a legitimate website is not classified as fake website.

Sometimes the similar name website can be considered as not reliable. Then computational time taken by the system at the server detecting the fraud is an additional overhead and the data maintained along with it is also and overhead. Over a period of time this data also increases. So, the entire system can delay the process.So, memory and computational requirement of the system need to be carefully monitored.

IV. NEW ANTI-PHISHING SYSTEM

A new system called combphish is proposed that can make a separate list of fake websites fromreliable ones.

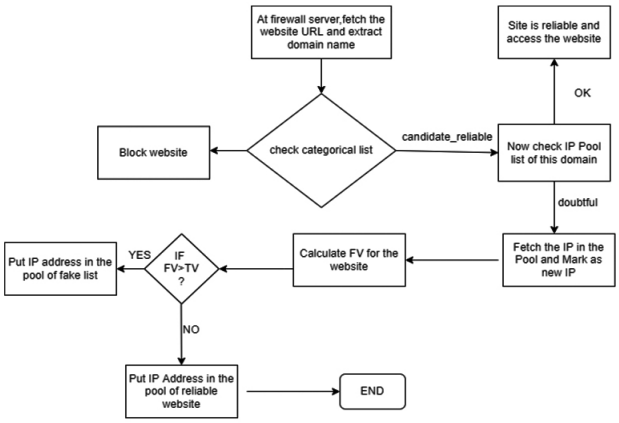

Figure 1: combphish An Anti-phishing System

In this system the user would enter the URL of the website. These are the steps:

1) During this step, the entered URL by the user is by the firewall serv er and it would extract the domain name. The important capability of the imperative server is to keep a database of black and white lists of net web sites. Phishing web sites do now no longer closing for a protracted time, typically from some hours to three days; therefore, the database, particularly the black list, wishes to be up to date regularly. The server plays this replace of the database via the subsequent means.
2) Then the domain name is checked against a categorical list maintained by the server. If the DNS is fake then the website is blocked otherwise candidate _reliable.
3) Now the system would check the IP pool of the list of this domain. If the IP is reliable then allow access to the website.
4) Otherwise mark the IP as new IP and Calculate the FV(Fake Value) of the website.

Here we take TV(Threshold Value)=1
FV(Fake Value)=2 if The domain name has wrong spelling or spelling similar to(popular website or reliable website).
FV=3 if IP is from forbidden country.
FV=4 if IP is similar to the unreliable tagged IP.
FV=0 if IP is OK.

5) IF FV>TV then put IP address in the pool of fake list. Otherwise put IP address in the pool of reliable list.
6) End the algorithm and allow access.

V. MEASURES TO AVOID TRAPPING

Many housewives and youngsters are accessing the internet for earning money or business purpose. Also, many elderly people and children use internet for time pass. They are soft targets that they drop their information here and there. They also do random clicks. So, they need to be very careful while navigating the websites and videos. Avoid leaving your personal details on mobile phones. If websites are asking for logging in using Gmail or yahoo or social networking sites then make sure you trust that site.

Email refers to the process of eradicating harmful emails via mail servers before any reach users' mailboxes, if they are spam, phishing efforts, or the propagation of a new virus. But since majority of current phishing scams utilise disseminated email (spam) to deceive people into entering a phishing website, this approach helps to fight phishing now at email level. Numerous phishing emails can be averted with an inbox filter. However phishers have become more skilled. As an indication, they may indeed gather users' personal information from repositories, also including company or university websites, after masquerading as the users' friends and writing them. These emails appear to be from well-known email addresses and will not be blocked.

Currently, there are about 12 toolbars. B. From Earthlink, eBay, Trust Watch, Google, and IE7 designed to detect phishing attacks. Most of them are mainly based on the white and black list. Others use heuristics to determine if a URL is similar to a known URL based on information about the domain name or IP address block where the website is hosted. The white and black list relies on timely reports from phishing sites. Unless the phishing site is reported, phishers can steal personal information from visitors to the site.

This method is to visually differentiate phishing webweb sites from the spoofed valid webweb sites. Dynamic Security Skins proposes to apply a randomly generated visible hash to customise the browser window or net shape factors to suggest the effectively authenticated webweb sites.

It provides interplay strategies to save you spoofing. First, its browser extension offers a depended on window withinside the browser devoted to username and password access. It makes use of a photographic picture to create a depended on route among the person and its window to save you spoofing of the window and of the textual content access fields. Second, it permits a far-flung server to generate a completely unique summary picture for every person and every transaction. This picture creates a "skin" that routinely customizes the browser window or the person interface factors withinside the content material of a far-flung net page.

VI. FUTURE WORK

Though the model proposed is very basic. In future we can incorporate the following features:

1) Machine learning is gaining popularity day by day. So, we can optimize the algorithm further using it.
2) The data we have collected can be converted into data-

set of fake and reliable sites and then we can set better accuracy of our system using deep learning model.

3)For the calculation of FV we can include more parameters such as look of the website, what kind of information the website is asking, cookies and the content of the website.

4)We can the connect the combphish with the bank also that we have given our details to this website. In case if any fraud is about to happen we get a prior approval message for deduction of money and any mishappening can be avoided.

VII. CONCLUSIONS

The system that we proposed would be very efficient for detecting and avoiding phishing. The FV is a measure that can be stored and computationally easy to find by applying very less efforts. So, if implemented into the firewall then would prevent many people from falling in the trap.

The system utilizes a client side proxy that has been installed as a browser plug-in and validates the legitimacy of a website using only a variety of white checklist, black checklist, and rules. The suspicious site is notified to a central server, which computes an aggregated spoof value of the suspicious website and take adequate action on the basis, if the client server proxy misses the sufficient information to make a solid verdict.

In our system, the client quantifies a bogus value for a dubious site employing heuristics when it reaches it. The central server is then sent both the URL and the phony value. Based on, the central server delivers an aggregated impostor value.

If the overall spoof value surpasses, the problematic site is restricted. We point you that the aggregated score is equivalent to individual impostor values and the cumulative number of reports within a specified timescale. This strategy is suitable given that the vast majority of malicious scams are fleeting, target credible websites, and have high surges of visitor.

The central server's and client proxy's threshold values computation and setting processes are vital in determining how effectively and successfully the method performs.

REFERENCES

[1] H. Tout, W. Hafner "Phishpin: An identity-based anti-phishing approach" in proceedings of international conference on computational science and engineering, Vancouver, BC, pages 347- 352, 2009.

[2] http://security.yahoo.com/article.html?aid=2006102507 Madhuresh Mishra et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4248 – 4250.

[3] M. Aburrous, M.A. Hossain, K. Dahal, F. Thabtah "Prediction phishing websites using classification mining techniques with experimental case studies" in proceedings of Seventh International Conference on Information Technology, Las Vegas, NV, pages 176-181, 2010.

[4] Michael Atighetchi, Partha Pal "Attribute-based prevention of phishing attacks" Eighth IEEE international symposium on network computing and application, 2009.

[5] V.Shreeram, M.Suban, P.Shanthi, K.Manjula "Anti-phishing detection of phishing attacks using genetic algorithm" in proceedings of Communication control and computing technology(ICCCCT),IEEE international conference, Ramanathapuram , pages 447-450, 2010.

[6] T. O. Ayodele, "Introduction to machine learning," in *New Advances inMachine Learning*. Rijeka, Croatia: InTech, 2013.

About The Author

Ms. Nishu Bansal got her B. Tech degree from UP Technical University in 2005.She has done her M.Tech from Guru Gobind Singh Indraprastha University, New Delhi, India. She has around 17 years of teaching experience. She is an Assistant Professor in the Department of Computer Science and Engineering of AKGEC, Ghaziabad affiliated to Uttar Pradesh Technical University. Her areas of interest include programming languages, Swarm Intelligence and Adhoc Networks.