IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 4, April 2016.
www.ijiset.com
ISSN 2348 – 7968

Anti-Phishing Framework Based On Phishing Target Discovery

Madhuri Manmode, Dipika Dagwar, Dipali Baharghare , Mohsin Khan, prof pooja.B.Aher
(CSE, PJLCOE/RTMNU,India)

Abstract: Phishing attacks are one of the attacks which have become popular in recent times. A phishing attack attempts to acquire confidential and personal information of person or a fir m. The most targeted domain of these phishing attacks to be known is financial domain, gene rally phishing attack attempts to obtain private information which can be exploited to gain ac cess to bank account of the individual. Many a times number of people become victim of this phishing.

Many solutions have been proposed ever since the phishing came into existence some validates the URL of the page to be visited to predict whether the page is legitimate or not wh ile some recent practices in predicting the legitimacy of a pages different domains have been exploited such as visual cryptography. With increase in number of naive users of internet the chances of getting trapped in such attacks is quite a possible thing.

So, it is necessary to provide some effective solution to this attack of phishing. This paper ex plains the details of various techniques used by phishing attacks to acquire sensitive informati on, it also provide advantages and disadvantages of the various anti-phishing technologies av ailable at this moment to counter the phishing attacks.

Keywords: Phishing, target, sensitive information, legitimate, suspicious, security.

I. INTRODUCTION

Internet Phishing attack has become the fastest growing scam on the Internet. To convince vis itors that a phishing page is legitimate, phishers typically use considerable information about targets to make their pages look as similar as possible to those targets. In this sense, phishing web pages aren’t isolated but are often associated with their targets. Phishing website is a mo ck website that looks similar in appearance but different in destination. Phishers use lot of tec hniques to lure the unsuspected web user. They send generic greetings to the customers to che ck their account immediately.

In general, phishing attacks are performed with the following four steps:

1) A fake web site which looks exactly like the genuine web site which is set up by phisher .

2) Phisher then send link to the fake web site in large amount of spoofed e-mails to target use rs in the name of legitimate companies and organizations, trying to convince the potential vict ims to visit their web sites.

3) Victims visit the fake web site by clicking on the link and input its useful information there .

4) Phishers then steal the personal information and perform their fraud such as transferring m oney from the victims' account.

ISSN 2348 – 7968

II. LITERATURE REVIEW

1) Separate set of test data are then supplied to the models, and the predicted class of the dat a instance is compared to the actual to the class of the data to compute the accuracy of the cla ssification models(Ram Basnet and Tenzin Doleck 2015).
2) A hybrid (supervised/unsupervised) learning approach may also take the merit of both fuz zy logic and machine learning, while considering the level of uniformity between features of phishing emails (Ammar et al 2014).
3) The email inbox is undoubtedly a dangerous place. But using the pattern recognition tools it may be convenient to filter a major portion of the elements that would damage the end user s (Sebastin 2013).

III. K-NEAREST NEIGHBOUR ALGORITHM

The K-nearest-neighbor (KNN) algorithm measures the distance between a query scenario an d a set of scenarios in the data set.

Suppose we have a data set of 14 scenarios, each containing 4 features and one result as displ ayed in Table.

Scenario	Outlook	Temperatur e	Humidity	Wind	Play tennis
Day1	Sunny	Hot	High	Weak	No
Day2	Sunny	Hot	High	Strong	No
Day3	Overcast	Hot	High	Weak	Yes
Day4	Rain	Mild	High	Weak	Yes
Day5	Rain	Cool	Normal	Weak	Yes
Day6	Rain	Cool	Normal	Strong	No
Day7	Overcast	Cool	Normal	Strong	Yes
Day8	Sunny	Mild	High	Weak	No
Day9	Sunny	Cool	Normal	Weak	Yes
Day10	Rain	Mild	Normal	Weak	No

Distances

We can compute the distance between two scenarios using some distance function d(x,y), where are scenarios composed of N features, such that $x=\{x_1,....,x_N\}$, $y=\{y_1,.....y_N,\}$.
Two distance functions are discussed in this summary:

- Absolute distance measuring:

$$d_A(x,y) = {}_i\text{-}y_i|$$

IV. CONCLUSION

ISSN 2348 – 7968

In the above study we can conclude that most of the anti-phishing techniques focus on conten ts of webpage, URL and email. Attribute based approach consider almost all major areas vul nerable to phishing so it can be best anti-phishing approach that can detect known as well as unknown phishing attack. Identity based anti-phishing approach may fails if phisher gets phy sical access to client's computer. This technique also enhanced the classification of phishing and legitimate websites, and finding the phishing target for preventing the phishing.
User education or training is an attempt to increase the technical awareness level of users to r educe their susceptibility to phishing attacks.

V. REFERENCES:

[1] Global Phishing Survey: Trends and Domain Name Use in 1H2011, tech. report, Antiphishing Working Group, published on 2011.
[2] "Discovering Phishing Target Based on Semantic Link Network," Future Generation Com puter Systems, vol. 26, no. 3, published on 2010.
[3] "Boom Time for Cybercrime," Consumer Reports, June 2009
[4] "Beyond Blacklists: Learning to Detect Malicious Websites from Suspicious URLs," Proc . 15th ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining, ACM Press, publis hed on 2009.
[5] "There is No Free Phish: An Analysis of 'Free' and Live Phishing Kits," Proc. 2nd Useni x Workshop Offensive Technologies, published on 2008.
[6] "An Antiphishing Strategy Based on Visual Similarity Assessment," IEEE Internet Comp uting, vol. 10, no. 2, published on 2006.
[7] "Efficient Identification of Web Communities," Proc. 6th ACM SIGKDD Int'l Conf. Kno wledge Discovery and Data Mining, ACM Press, published on 2000.