International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - TeLMISR 2015, ISSN : 2348-2273
Available Online at www.ijeecse.com

Phishing and Counter Measures: A Survey

Tripti Mishra
Delhi Institute of Advanced Studies, Delhi
mishratripti2007@gmail.com

Abstract: Phishing has been an ever prevalent challenge forthe internet security. Unlike hacking where expert programmer breaks the authentication code, criminals' phish for gullible victims and trick them into revealing their identity and their after using it for fraudulent activities. Many strategies have been developed to counter phishing, each with its own advantages and limitations. In this paper, a survey of phishing and countermeasures for phishing is presented and future research directions are explored.

I. INTRODUCTION

Acquiringpersonal information by making internet users believe that the attacker is a trustworthy email or website is called phishing. [4]

Phishing attacks exploit consumer psyche of greed, fear, or trust , who respond to fraudulent e-mail, or website that look almost similar to a legitimate email and website they have already used and these emails,web sites give a warning , special offers or huge some of money.Under all these circumstances the consumer gets tricked and tends to reveal his identity to the criminals by filling a form or get redirected to a new site .The criminals later use the identity in many ways , for monetary gain.No firewall, encryption or any security measure is there which can stop this security breach as the victim willingly reveals his identity.

According to [9], as the sale during thanksgiving period increased, there was a sharp increase in online offers and hence phishing attacks also increased during that period as shown below

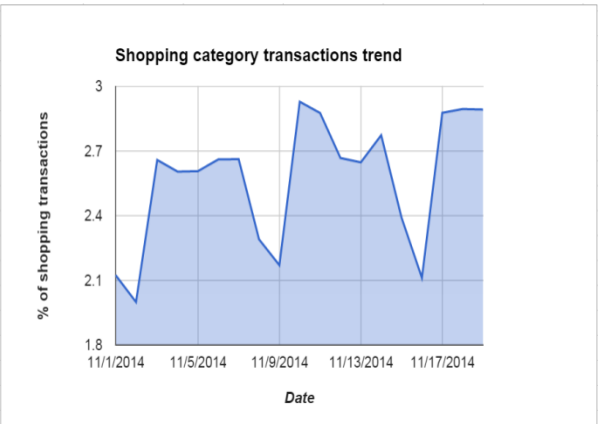

Figure 1. Shopping Pattern

Earlier phishing concentrated on identity theft and monetary gain , but later more serious crimes like Intellectual property theft, Security information and Corporate secrets theft became the motives of phishing.[6]

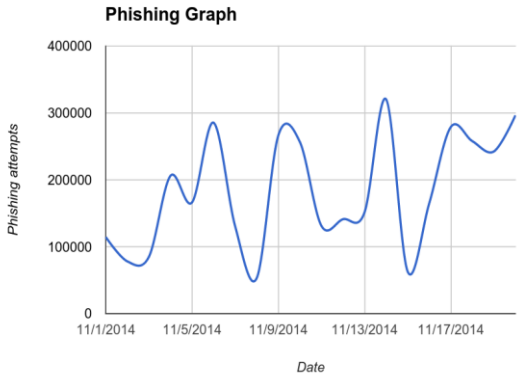

Figure 2. Phishing Pattern

Phishing attacks are much more complex and damaging than Spam and cause from monetary damage to intellectual property theft and threat to national security.

Phishing has evolved from its days of sending mass emails to get just any victim to specific spear-phishing attacks which involves knowledge about the victim and sending customized email to increase the trust rating. NowSMS.VOIP,telephones all are used for phishing a victim and getting his identity.

Phishing Attack Framework: The basic frameworkof phishing attack consists of following steps :

1. Phishers perform the research on the vulnerability of the customers and map it.
2. Information about target email list, fraud web page template as well as consumer domain is gathered.
3. The Computers are exploited through Trojans, security holes
4. Scam pages are hosted on compromised hosts
5. Mass mailing is done thus performing the phishing attack
6. The credentials of the customers are collected
7. The credentials collected can be en-cashed in many ways.

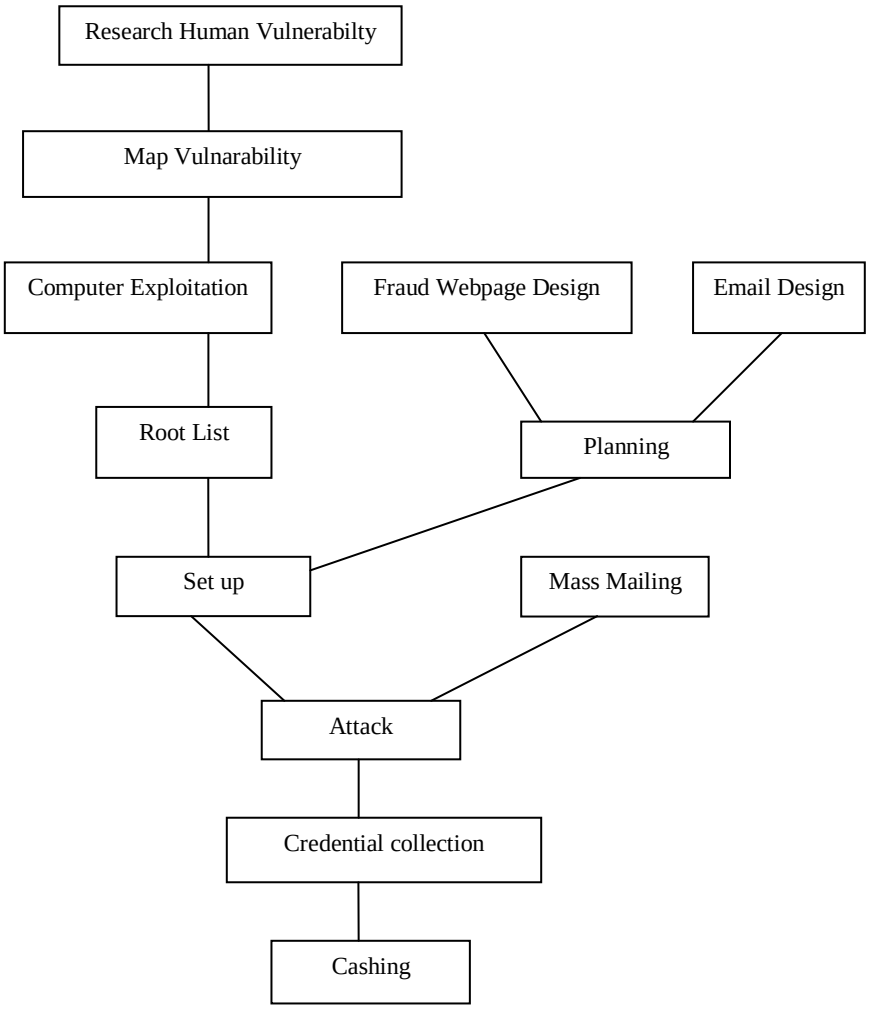

Fig.3 Phishing Attack Framework

II. EVOLUTION OF ANTI PHISHING TECHNIQUES

This paper studies the advantages disadvantages of various existing antiphishing techniques. Identifying an unsolicited mail i.e spam is much easier than identifying a phishing attack and the onus lies with the victim than the service provider.

From user point of view following strategies are used:

1. Stop phishing attack from reaching the customer
2. Make a better user interface
3. Train end users.

Phishing attacks can be stopped from reaching the customer by:

Filtering phishing email: Spam filtering is common, however detecting a phishing email is far difficult a task First email phishing filter was given byFette et [3]. They identified specific features of phishing mails like URLS that was later improved through the use of machine learning techniques like Bayesian filter, rule based ranking etc. can be applied. Some protocols have been proposed by the verify the sender[10].However the filtering techniques have not been very successful. These categories, however, must be predefined and therefore it is infeasible to use content-based filtering as a mechanism for identifying specific organizations being targeted. A content-based filter's efficiency in identifying phishing messages can be significantly lower when the user also receives legitimate mail from the target organization, making it more difficult for the filter to tell the difference

between the two, nevertheless the results are usually acceptable.

Blocking phishing sites: The phishing websites can be blocked by classifying sites after examining URLS and HTMl or server characteristics, i.e.by heuristic way or by maintaining manually verified blacklist.Garer in [5] looks for patterns in URLs , AbuNimesh in [1] searched for words in web pages while XiangG in [13] searches for the brand name, in the scam web page that the page claims to be.These techniques correctly identify the phishing sites by 90% and incorrectly labeling a legitimate site as phish approximately 1% or less.Google,Microsoft and Phishtank maintain blacklist successfully to identify phish.

Blacklist method predominates the industry with middle true positives but no false positives. However, blacklists do not generalize well , can be slow to respond to zero-hour attacks, and are easily overwhelmed by automatically generated URLs, a tactic fisherhad already adopted.

Taking down phishing sites: Many organizations prefer to take down the phishing web site by showing "page not found" message when end .A better option is showing a page which, trains theclientsdifferent methods to safeguard against phishing.

Better interfaces: A better interface can protect a client in a better way. The interfaces are good when they provide warnings that can not be ignored by the user.A passive indicator gives warning without ensuring users action in response to it,whereas an active indicator will interrupt to the point that they take notice of the warning.An analysis of warning science byEgelman et al.in [2], found that passive warnings is ineffective in protecting people from phishing scams, as they are easily missed by users the same is supported by the studies of Wu et al.in [12]. Improving authentication while signing in a website is an alternate method for example two factor authentication further strengthen the identity security.

Train the Users: Educating the users about phishing and methods to safeguard them selves can be effective through complete participation from the user. However, it remains athe least popular and least utilized technique. Kumaraguru et al in [7][8] describe how training material is useful in helping people identify fake Web sites and why emailing anti-phishing material was ineffective.

Nowadays micro games are introduced to teach people about phish. Micro games are a popular format for games played for short periods of time.. Anti-Phishing Phil game developed by Sheng et al [11] includes learning scince concepts to teach about address bar, domain names and phishing pages and also tests the learning.Thellearning ability about phishing increased by 61% through this method.

Many anti-phishing schemes have recently been proposed in literature. Despite all those efforts, the threat of phishing attacks is not mitigated. One of the main reasons is that phishing attackers have the adaptability to change their tactics with little cost. Although many anti-phishing schemes have been proposed, none of them effectively solves the authentication challenge.

III. PREVENTIVE MEASURES

A systematic study of various phishing techniques indicates that by following these simple precautions a target can safeguarditself against the attack.

- Users should be extra careful with those e-mails requiring personal information specially bank related.
- Instead of clicking on such URL type it in the browser window. If there is any chance of differentiatingbetweenURL, then it getsnoticed by typing it.
- The user must use the browser with latest security against phishing
- Fantastic offer: don't believe such offers that are not easy to believe check for all the necessary details of the web site and ask too many questions before us

IV. CONCLUSIONS

A comprehensive analysis and comparison of these detection techniques have also been provided in this paper. After analyzing these methods and their corresponding application scenarios, listing the merits and the demerits of these methods, we conclude that there is no algorithm which can be considered as the best in the phishing detection failed. Different methods focus on their specific targets. That is, the performance of the different anti-phishing mechanisms is closely related to their target and the application scenarios. Thus, design and implementation of an effective anti-phishing mechanism is really a challenging task.

V. REFERENCES

[1] Abu-Nimeh, S., Nappa, D., Wang, X., and Nair, S. A comparison of machine learning techniques for phishing detection. In Proceedings of The Anti-Phishing Working Group's Second Annual eCrime Researchers Summit (Pittsburgh, PA, Oct. 4–5, 2007), 60–69.

[2] Egelman, S., Cranor, L.F., and Hong, J.I. You've been warned: An empirical study of the effectiveness of Web browser phishing warnings. In Proceedings of the CHI Conference on Human Factors in Computing Systems (Florence, Italy, Apr. 5–10). ACM Press, New York, 2008, 1065–1074.

[3] Fette, I., Sadeh, N., and Tomasic, A. Learning to detect phishing emails. In Proceedings of the 16th International World Wide Web Conference (Banff, Canada, May 8–12, 2007), 649–656.

[4] Financial Services Technology Consortium, "Understanding and Countering the Phishing Threat," at http://fstc.org/projects/counter-phishing-phase-1/, last accessed 10th January 2015.

[5] Garera, S., Provos, N., Chew, M., and Rubin, A.D. A framework for detection and measurement of phishing attacks. In Proceedings of the WORM Workshop on Rapid Malcode (Alexandria, VA, Nov. 2). ACM Press, New York, 2007; http://portal.acm.org/citation.cfm?id=1314391 Last accessed 12th January 2015

[6] Herley, C. and Florencio, D. A Profitless endeavor: Phishing as a tragedy of the commons. In Proceedings of the New Security Paradigms Workshop (Lake Tahoe, CA, Sept. 22–25, 2008).

[7] Kumaraguru, P., Rhee, Y., Sheng, S. et al. Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In Proceedings of the Anti-Phishing Working Group's Second Annual eCrime Researchers Summit (Pittsburgh, Oct. 3–5, 2007), 70–81.

[8] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., and Hong, J.I. Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology 10, 2 (2010), 1–31.

[9] Rubin Azad, UdayPratap Singh, Beware of Phishing Attacks and Other Scams during the Thanksgiving Shopping Season http://research.zscaler.com/2014/11/beware-of-phishing-attacks-and-other.html

[10] Sender Policy Framework Specifications (RFC 4408). http://www.openspf.org/Specifications.

[11] Sheng, S., Magnien, B., Kumaraguru, P. et al. Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In Proceedings of the Third Symposium on Usable Privacy and Security (Pittsburgh, July 18–20). ACM Press, New York, 2007, 88–99.

[12] Wu , M., Miller, R.C., and Garfinkel, S. Do security toolbars actually prevent phishing attacks? In Proceedings of the CHI Conference on Human Factors in Computing Systems (Montréal, Apr. 24–27). ACM Press, New York, 2006, 601–610.

[13] Xiang, G. and Hong, J.I. A hybrid phish detection approach by identity discovery and keywords retrieval. In Proceedings of the International World Wide Web Conference (Madrid, Apr. 20–24, 2009), 571–580.