ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/299577684

Recent survey of various defense mechanisms against phishing attacks

Article *in* Journal of Information Privacy and Security · January 2016

DOI: 10.1080/15536548.2016.1139423

CITATIONS
51

READS
1,406

3 authors, including:

Aakanksha Tewari
National Institute of Technology Kurukshetra
12 PUBLICATIONS **1,260** CITATIONS

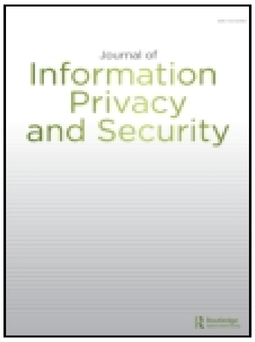
Ankit kumar Jain
National Institute of Technology Kurukshetra
104 PUBLICATIONS **4,214** CITATIONS

SEE PROFILE

SEE PROFILE

All content following this page was uploaded by Ankit kumar Jain on 11 December 2017.

The user has requested enhancement of the downloaded file.



Journal of Information Privacy and Security

Routledge
Taylor & Francis Group

Journal of Information Privacy and Security

ISSN: 1553-6548 (Print) 2333-696X (Online) Journal homepage: http://www.tandfonline.com/loi/uips20

Recent survey of various defense mechanisms against phishing attacks

Aakanksha Tewari, A. K. Jain & B. B. Gupta

To cite this article: Aakanksha Tewari, A. K. Jain & B. B. Gupta (2016) Recent survey of various defense mechanisms against phishing attacks, Journal of Information Privacy and Security, 12:1, 3-13, DOI: 10.1080/15536548.2016.1139423

To link to this article: http://dx.doi.org/10.1080/15536548.2016.1139423

Published online: 25 Feb 2016.

Submit your article to this journal

Article views: 41

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
http://www.tandfonline.com/action/journalInformation?journalCode=uips20

Download by: [115.254.77.21] **Date:** 10 May 2016, At: 23:36

JOURNAL OF INFORMATION PRIVACY AND SECURITY
2016, VOL. 12, NO. 1, 3–13
http://dx.doi.org/10.1080/15536548.2016.1139423

Routledge
Taylor & Francis Group

ARTICLE

Recent survey of various defense mechanisms against phishing attacks

Aakanksha Tewari, A. K. Jain, and B. B. Gupta

National Institute of Technology Kurukshetra

ABSTRACT

In the recent years, the phishing attack has become one of the most serious threats faced by Internet users, organizations, and service providers. In a phishing attack, the attacker tries to defraud Internet users and steal their personal information either by using spoofed emails or by using fake websites or both. Several approaches have been proposed in the literature for the detection and filtering of phishing attacks; however, the Internet community is still looking for a complete solution to secure the Internet from these attacks. This article discusses recent developments and protection mechanisms (i.e., detection and filtering) against a variety of phishing attacks (e.g., email phishing, website phishing, zero-day attacks). In addition, the strengths and weaknesses of these approaches is discussed. This article provides a better understanding of the phishing attack problem in the current solution space and also addresses the scope of future research to deal with such attacks efficiently.

Downloaded by [115.254.77.21] at 23:36 10 May 2016

Introduction

Phishing can be defined as an identity theft that takes advantage of developed technologies and system vulnerabilities due to human nature. Phishing attacks start with the phisher sending an email to the victim that appears to be from a legitimate organization, which contains links for which clicking on may either lead the victim to some false webpage where the user is asked to give his or her credentials or to install some spyware on the machine. The motive of the attacker behind such scams may be identity theft, financial gain, or notoriety (i.e., to gain recognition) as noted by Almomani et al. (2013), Tripathi et al. (2013), Gupta et al. (2015), Alomari et al. (2014), Abbasi et al. (2015); Sodiya et al. (2011); Mejias and Balthazard (2014). Statistics given in a 2013 report from the Anti-Phishing Working Group (APWG), have shown that one-third of all the phishing attempts in 2013 were intended towards stealing bank accounts details or other financial information. Since 2012, financial phishing attacks were increased by 8.5%, which is the highest increment in such attack cases (APWG, 2012). Most of these attacks pretend to be a well-known organization as it will increase the chances of user falling for the bait, organization names such as MasterCard, Visa, or PayPal are have been used for these purposes, subjecting harm to the reputation of these brands names. In addition, other bigger brands such as Apple, E-Bay, and Amazon are also targeted in most phishing attacks to fool the user (Lininger & Vines, 2005). Average costs of cybercrime in selected countries as of June 2014 and the number of brands and legitimate entities hijacked by phishing attacks from January 2009 to June 2014 [18] are shown in Figure 1 and 2, respectively.

Deception also known as social engineering aims to obtain information from the users by making them fool, which can be used over the Internet (through emails) to initiate phishing attacks. This type of attack is very easy to perform by the attacker as it is a very simple task for an attacker to copy

CONTACT B. B. Gupta ✉ gupta.brij@gmail.com 🖃 Computer Engineering Department, NIT Kurukshetra-136119, Haryana, India.

© 2016 Aakanksha Tewari, A. K. Jain, and B. B. Gupta

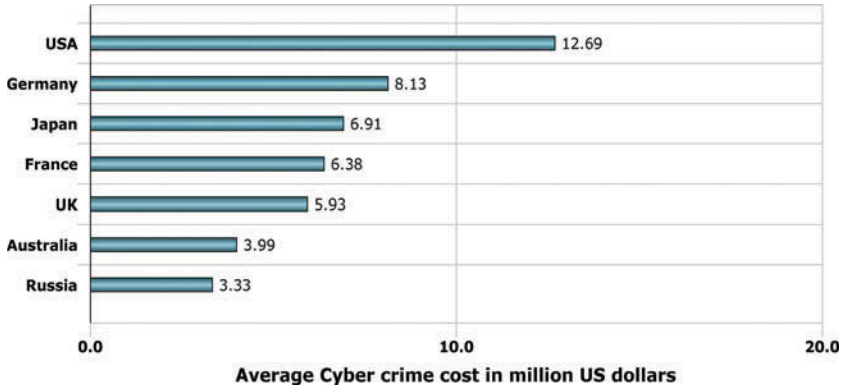


Figure 1. Average costs of cybercrime in select countries as of June 2014 (in million U.S. dollars). © 2014 Statista: The Statistics Portal. Reproduced by permission of Statista: The Statistics Portal.

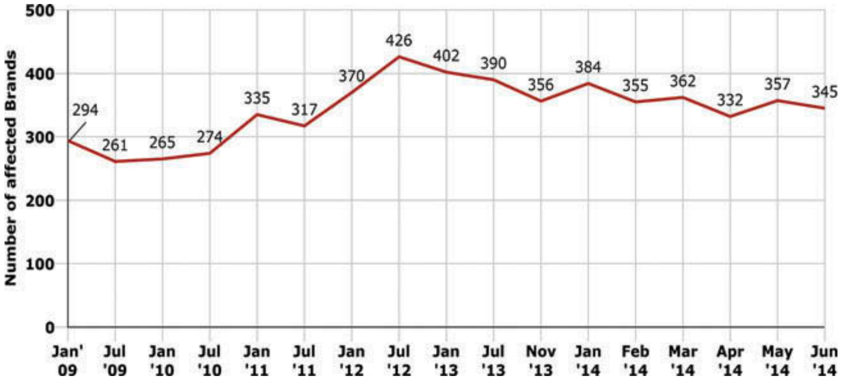


Figure 2. Number of brands and legitimate entities hijacked by phishing attacks from January 2009 to June 2014. © 2014 Statista: The Statistics Portal. Reproduced by permission of Statista: The Statistics Portal.

Downloaded by [115.254.77.21] at 23:36 10 May 2016

any legitimate website whereas detection of phishing attacks is not as easy as it seems. phishing attacks are initiated when the users receive spoofed emails from a sender that appears to be legitimate, these messages may have some malicious links embedded in them, asking to update their account information (Almomani et al., 2013; Mishra & Gupta, 2014).

This article discusses some of the recent approaches to detect phishing emails and webpages. In addition the strength and weaknesses of these approaches are presented. The discussion is organized as follows: Section 2 describes current trends and motives of the attackers behind phishing attacks. In Section 3, a comparative study of ability of machine and human in phishing detection is discussed. In Section 4, the detection techniques for phishing attacks is presented. Section 5 describes the open issues and challenges in dealing with variety of phishing attacks. Finally, Section 6 concludes the discussion.

Phishing attacks: Emerging trends and attacker's motivation

Emerging trends

Gupta and Kumarguru (2014) performed a study on the landing page created by APWG and Carnegie Mellon Cylab's Supporting Trust Decisions project, which was translated into 20 languages. They performed a comparative analysis using two datasets that were collected from the log files of the landing

Downloaded by [115.254.77.21] at 23:36 10 May 2016

page. The page was quite successful in training users. Approximately 46% of the users were able to protect themselves from these attacks. But the phishers are also continuously changing their attack techniques; they create URLs that appear fairly legitimate and purchase several domains for their campaign. Even after strict monitoring, phishers are successfully exploiting the Internet Corporation for Assigned Names and Numbers (ICANN) to carry out their campaign. The study also shows that phishing emails have considerably changed from the year 2008 to 2014.

In addition, they also observed that existing blacklists in the browser are not an effective measure to diagnose the phishing URLs today. Browsers such as Mozilla Firefox and Internet Explorer have many toolbars and plug-ins to detect such pages but are also not successful in preventing malicious web pages. Attackers today have shifted their attention from advertisement websites and blogs to social media to spread their phishing links. Phishers are now using advanced tricks such as sending promotional and monetary e-mails to attract the Internet users.

Motives of the attacker

Yu et al. (2008) described the motivations behind phishing attacks from the point of view of an attacker, including:

- *Financial benefits*: The attackers can misuse the sensitive information they steal from the victims for financial gain.
- *Identity concealing*: The attackers do not use the identities stolen themselves; instead they sell these identities to other adversaries or criminals to hide their original identity.
- *Fame and notoriety*: Novice attackers may carry out phishing campaigns for peer recognition.

Comparing human versus a machine's ability to detect phishing emails

Park et al. (2014) performed an experiment to check and compare the abilities of machines and human beings to detect phishing emails. Their goal was to understand how the capacities of human and machines could be maximized in a collaborative effort against such campaigns. They compared the performance of human subjects and supervised machine learning systems on a dataset that contained both legitimate emails from the Enron dataset and phishing emails from the Nazario's public dataset. They modified a part of emails in two different ways: 1) *synonym substitution*, which was in favor of human subjects, and 2) *similar rank word substitution*, which was in favor of machines. The results were not unexpected; the humans were able to classify the emails that were originally misclassified compared to the machines. The machines could not classify some emails even when they were marked as phishing. According to their study, in the collaboration of efforts from both human and machine, it is the human who would benefit.

Recent approaches to phishing detection

String matching algorithm for phishing detection

Abraham and Raj (2014) proposed a string matching approach for detecting phishing campaigns, which is based on the degree of similarity of a URL with the blacklisted URLs; depending on the text-based characteristics of a URL it can be classified as legitimate or phishing. In this method, instead of performing complete URL matching, the URL is broken into tokens and the degree of similarity is checked with the blacklisted URLs tokens as shown in Figure 3.

The scores are calculated based on the number of the occurrence of each token in the blacklist. The final score is calculated as:

Downloaded by [115.254.77.21] at 23:36 10 May 2016

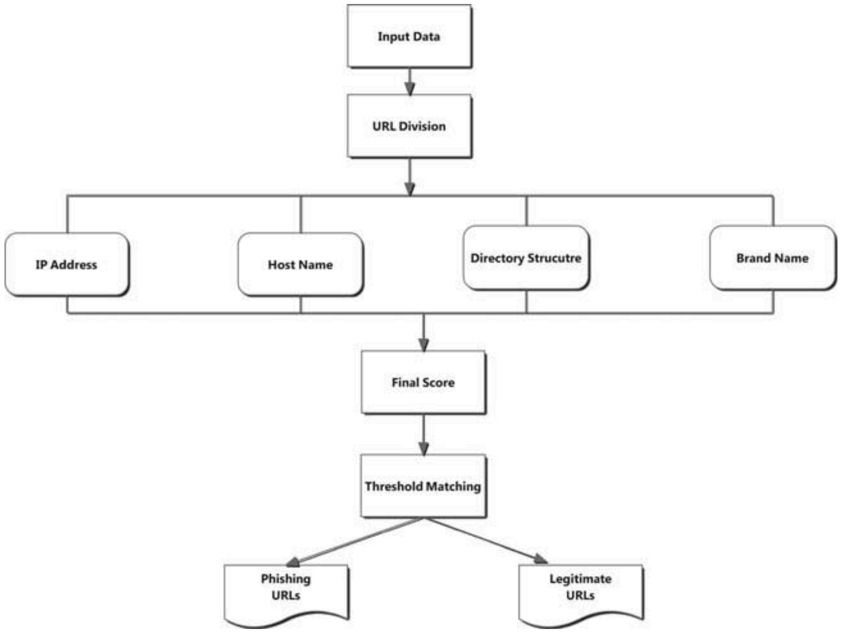


Figure 3. String matching procedure.

$$socore = \sum_{i=1}^{4} wi \times ci \quad \text{(EQ1)}$$

where w is the weight and c is the individual token score.

This approach turned out to be very effective in detecting phishing attacks with very low false negatives and false positives. These tokens are used for approximate matching and are identified from the lexical structure of a URL. Two string-matching algorithms—longest common subsequence (LCS) and edit distance—are used in the hostname comparison. The accuracy rate obtained for LCS is 99.1% and for edit distance it is 99.5%.

Phishing detection, adversarial learning, and semi supervised learning

Some of the challenges faced while developing a phishing detection models are difficulty in acquiring annotated data, increased computational complexity for robust detection methods, and variations and errors in the data distribution. These issues are addressed in a study by Debarr (2013), as supervised learning approach such as active learning that utilizes the annotated data efficiently, using only 10% of the annotated data. By making use of reputation features from the social network analysis for the evaluation of input and output paths enhance the rate of detection by 70%.

Data-centric phishing detection based on transparent virtualization technologies

Beiddermann, Ruppenthal, and Katzenbeisser (2014), proposed a novel phishing detection architecture based on transparent virtualization technologies and isolation of the own components. This architecture can be utilized as a security add-on for virtual machines (VMs) working in the cloud. To obtain, filter and normalize a color-based fingerprint of a web page, this architecture makes use of fine-grained VM introspection (VMI). The fingerprints are managed by a browser from the VM's memory. The proposed architecture is able to detect two kinds of phishing attacks: 1) based on redirection to spoofed web pages; and 2) "man-in-the-browser" (MitB) attacks. The architecture runs on a VM which is isolated and has access to the hypervisor layer and extracts information of a user's

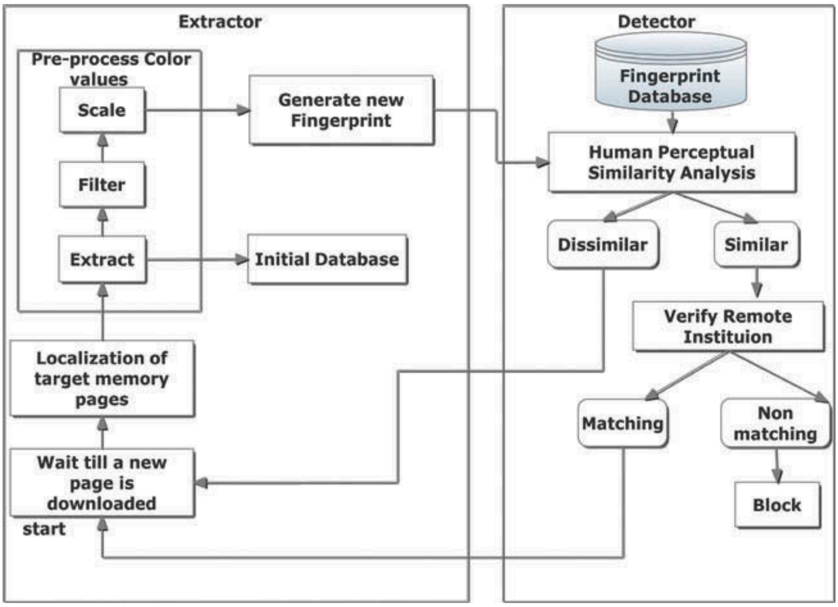


Figure 4. Extractor and detector flow graph.

browser by directly observing its used memory pages via VMI. It has two major components, shown in Figure 4 and listed here:

- The *extractor*, which detects, retrieves and pre-processes the important information from the memory.
- The *detector*, which performs human perceptual similarity analysis and intervenes once an ongoing phishing attack has been detected.

This architecture runs in isolation thus cannot be fooled by malware and it can be provided according to the paradigm of “security-as-a-service”. In addition, it can easily be enabled by an ordinary cloud user since no additional software has to be installed on the user’s VM and every browser in every version running in every operating system is generically supported.

Favicon: A clue to phishing site detection

In the favicon approach as noted by Geng, Lee, and Tseng (2013), a small but strong visual element known as a *favicon* (favorite icon) a short or bookmark icon for a website, which is extensively used by phishers but ignored by anti-phishing researchers is used. This approach analyzes the characteristics of favicon in phishing sites. Favicon detects the suspicious brand sites, including legitimate and fake brands sites, and then PageRank and DNS filtering algorithm discriminates the sites with branding rights from fake brands sites. The flow diagram of phishing detection using favicon is shown in Figure 5.

To justify the effectiveness of this method, two different experiments were carried out. One is collecting a diverse spectrum of corpora containing 3642 phishing cases (containing favicons) from PhishTank, and 19585 legitimate Web pages from DMOZ and Google. The experimental evaluations on the data set show that the proposed method achieved a greater than 99.50% true positive rate and 0.15% false positive rate. The other validated the proposed method in the real web query environment; a total of 517 unique phishing URLs were found

Downloaded by [115.254.77.21] at 23:36 10 May 2016

Downloaded by [115.254.77.21] at 23:36 10 May 2016

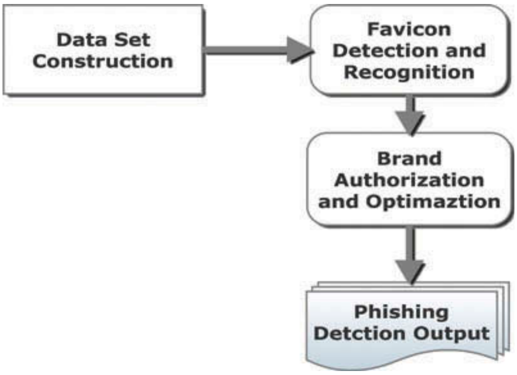

Data Set Construction
Favicon Detection and Recognition
Brand Authorization and Optimaztion
Phishing Detction Output

Figure 5. Phishing detection using favicon.

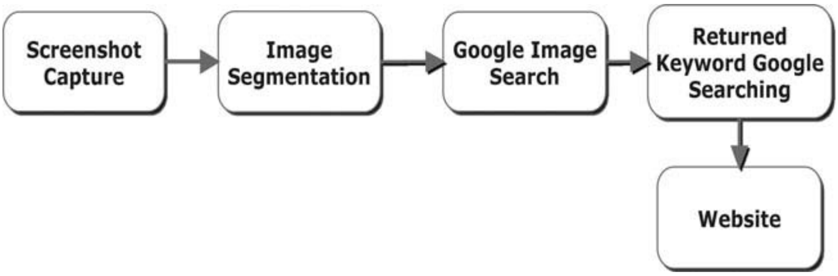


Figure 6. Website identification flow diagram.

and reported to the Anti-Phishing Alliance of China in 1 month. The experimental results demonstrate the competitive performances of favicon detection and recognition method for anti-phishing in practice.

Phishing detection via identification of website identity

Chung et al. (2013) proposed an approach to detect phishing website by logo segmentation and website identity determination. The approach first obtains a screenshot of a webpage and focuses on the region of interest (i.e., the area containing the logo). The next step is identification (as shown in Figure 6), in which the image is retrieved using a content-based mechanism provided in the Google Image search engine to find similar logos. The results show the real identity of the website. With this identity, phishing webpage can be differentiated from a legitimate one by evaluating the domain name of the query website.

Phishing detection using PSOAANN-based one-class classifier

In this approach (Pandey and Ravi, 2013), phishing websites and emails are detected using associated artificial neural networks, which is trained on particle swarm optimization. This approach used a one-class classifier. The feature selection was done on the basis of the weights from the input nodes to the hidden nodes. Then, the ranking of all the input nodes is calculated, and nodes with higher rankings are noted as having significant features. The network is trained only on the negative data. The objective function used here is to minimize the normalized root mean square error. A threshold value is used for classifying a pattern as negative or positive. The classification rate is calculated as:

$$Classification\ rate = \frac{No.\ of\ patterns\ classified\ as\ phishing}{Total\ no.\ of\ mails\ in\ test\ data} \times 100 \qquad \text{(EQ2)}$$

The evaluation results show that the feature selection method performed best and having the accuracy of 99.6% with 12 features and seven hidden nodes for phishing emails. For the phishing websites the accuracy achieved was 100% using eight features and number of nodes varying from three to six.

PhiGARo

Husak and Cegan (2013) proposed an automatic phishing detection and incident response framework that finds the users who respond to phishing attacks and prevents access of phishing sites from the secured network. This approach addresses three issues: 1) effectively dealing with phishing incidents to protect the users; 2) automation of phishing detection and incident handling; and 3) luring the attackers towards phishing detectors.

This approach depends on the users reporting the phishing incidents. They also make use of honeypots in order to remove the dependence on the user input. The honeypots are used to capture emails and detect phishing email out of them and send them to PhiGARo for incident processing. They propagate email addresses of honeypots so that the more phishing emails can be captured by honeypots. The honey-tokens (i.e., email addresses) are propagated by both active and passive ways.

Phishing detection and impersonated entity discovery using conditional random field and latent dirichlet allocation

Ramanthan and Wechsler (2013) proposed a novel approach for the detection of phishing attacks and the brands that are being impersonated. This technique deploys natural language processing and machine learning. The first step is to find out *named entities* (i.e., names of people, organizations, and locations), and *hidden entities*, using conditional random field (CRF) and latent dirichlet allocation (LDA) for both positive and negative data. Using named and hidden entities as features, Adaboost is used in the next step to classify each message as phishing or legitimate. The messages classified as phishing are sent to the last stage to detect the attacked brand by the help of CRF as shown in Figure 7.

The evaluation results reveal that when the ratio of phishing emails is less than 20%, there is no misclassification (i.e., the obtained F-measure was 100%). The detection rate of the impersonated brand is 88.1%. This approach helps to take down the phishing site protecting the user from the attacks.

Downloaded by [115.254.77.21] at 23:36 10 May 2016

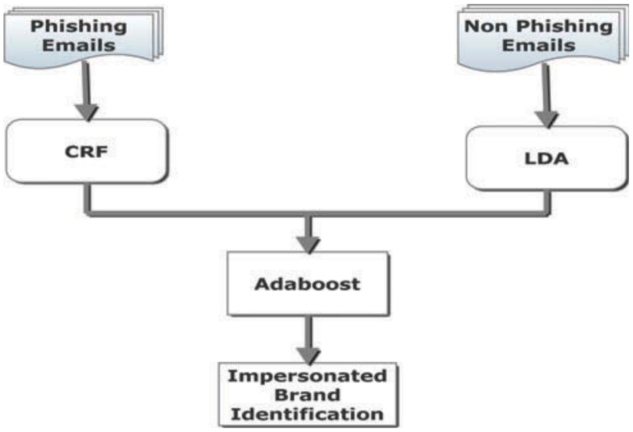


Figure 7. Stages in phishing detection and brand identification using conditional random field (CRF).

Mobifish: A lightweight anti-phishing scheme for mobile phones

Wu, Du, and Wu (2014) presented a novel automated lightweight anti-phishing scheme for mobile platforms called MobiFish. It checks the authenticity of web pages and applications by comparing the original identity to the claimed identity. This approach is implemented on the Nexus 4 smartphone running the Android 4.2 operating system. The performance was evaluated using 100 phishing and their corresponding legitimate URLs, as well as fraud Facebook Applications. The results show that MobiFish is able to detect phishing attacks on mobile phones efficiently. As the heuristic-based solutions depend on the HTML code of the page, this issue is resolved by MobiFish by using OCR, which extracts text from the mobile screenshot of a webpage so that the verification becomes easy. This technique works without any aid from search engines or machine learning.

Poster

Lee et. al. (2014) proposed an approach that uses the available blacklists to detect suspicious URLs used in the phishing campaigns in real time. They presented an approach that employs tracking of webpage redirections and forms for updating the phishing blacklists. First, DNS lookup mechanism finds out uncategorized URLs. The next step is the establishment of a connection that requests the content in the webpages of the URLs. The HTTP status code thus returned is used to check if the content is accessible or not. The accessible content is examined for the following details: If the content includes phrases like “account suspended,” “temporary unavailable,” and “access restrictions”, the URLs is assumed to be suspicious (i.e., may be phishing). The proposed architecture includes two components to anticipate potentially phishing URLs:

- *Redirection tracking*: gathers redirection URLs retrieved from the source to refine the quality of the available blacklists.
- *Form tracking*: Malicious webpages contain forms to collect sensitive information from the user. In this component, fake input credentials are used to track triggered URLs.

The proposed blacklist updating mechanism is proactive and efficient and able to detect suspicious URLs in less time.

Open issues and challenges

This article discusses the recently proposed techniques for protection against phishing attacks. The strengths and shortcomings of these methods are given in Table 1. Although these techniques are recent and are able to detect phishing attacks efficiently, some depend on the type of the input provided (Chung et al., 2013; Ramanthan & Wechsler, 2013). POSTER (Lee at al., 2014) is able to detect zero-hour attacks to a certain extent but if the environment is frequently changing it is difficult to keep up with it. The machine learning approaches give comparatively better results but are complex in design. PSOAANN (Pandey & Ravi, 2013) uses a novel feature selection approach based on weights from input to hidden nodes in the ANN which gives accuracy of 99.8% on average, and it can be used to detect both emails and webpages. However, the system architecture is somewhat complex and different for both email and web page detection. Heuristics-based approaches are highly depend on the HTML code of the webpage; this problem is addressed by MobiFish (Wu, Du, & Wu, J. (2014) which uses OCR to extract text from a page.

Although continuous research is going in this area, many issues and challenges still need to be addressed to protect against phishing attacks efficiently. One of the most important challenges faced is the detection of zero-hour attacks that is difficult to detect. Another novel type of phishing attacks are advanced persistent threats, which use wide range of techniques and are becoming highly

Downloaded by [115.254.77.21] at 23:36 10 May 2016

Table 1. Comparison of recent phishing detection and filtering techniques.

Phishing Detection Techniques	Strengths	Weaknesses
String-matching algorithm (Abraham & Raj, 2014)	● High detection rate (~99.5%) ● Low false-positives (2%) and false-negatives (1%)	● Testing details collected over a very short time span ● Not effective to detect zero-hour attacks
Random projection, adversial learning and semi-supervised learning (Debarr, 2013)	● Efficient use of annotated data ● Able to withstand changes in data distribution	● Complex algorithms, high computational cost
Data-centric technique (Beidermann, Ruppenthal, & Katzenbeisser, 2014)	● No additional software required to be installed ● Cannot be compromised as it runs in isolation	● Fast typing users can be avoided only by use of Linux HTTP
Favicon (Geng Lee, & Tseng 2013)	● Simple approach ● Language-independent	● Not all Phishing sites have fake favicons ● Does not consider logo and copyright notice
Identification of website identity (Chung et. al., 2013)	● Low complexity	● Input-dependent ● Difficult to determine the right identity from multiple logos
PSOANN (Pandey & Ravi, 2013)	● Weight-based features selection yields high accuracy ~99.8%	● Complex system design, high computational cost ● Accuracy is input-dependent
PhiGaro (Husak & Cegan, 2014)	● Modular and extensible	● Depends on the reporting of phishing attacks from users
Conditional random field (CRF) and latent dirichlet allocation (LDA) (Ramanathan & Wechsler, 2013)	● Phishing discovery rate is 88.1%	● Efficiency decreases with increase in phishing email percentage in the dataset
MobiFish (Wu, Du, & Wu, 2014)	● Very lightweight scheme for mobile phones ● Does not use any external sources ● Accurate text extraction using OCR	● Not directly compatible with android ● OS changes are required
POSTER (Lee et al., 2014)	● Proactive blacklisting approach ● Detects URLs in real time	● Difficult to keep up with changing phishing threat environments

successful in breaching security of big and reputed organizations. The attackers are always one step ahead and attempt to use techniques that are very difficult to detect or prevent.

Conclusion

Every year, increasing numbers of attacks are launched to make the Internet users trust that they are interacting with a legitimate party, which persuades them to give away their sensitive information. Recent reports show that in April 2014 phishing led to a loss of about $448 million to the corporate sector. The attackers are always one step ahead of the defense techniques developed by the

Downloaded by [115.254.77.21] at 23:36 10 May 2016

researchers. The aim of this article was to discuss some recent approaches to defend against phishing campaigns in the current scenario. In addition, this article presented some of the emerging trends of phishing attacks and the motivation of the attacker behind carrying out these campaigns. Also discussed was that the ability of users and machines can be combined to detect phishing attacks in a better way. This article will help the researchers obtain good insight of the current phishing attack scenarios and the possibilities of future research and development in this area.

References

Abbasi, A., Zahedi, F. M., Zeng, D., Chen, Y., Chen, H., & Nunamaker, J. F. Jr. (2015). Enhancing predictive analytics for anti-phishing by exploiting website genre information. *Journal of Management Information Systems*, 31(4), 109–157.

Abraham, D., & Raj, N. S. (2014, September). Approximate string matching algorithm for phishing detection. In *Proceeding of International Conference on Advances in Computing, Communications and Informatics* (ICACCI) New Delhi, India: IEEE, 2285–2290.

Alomari, E., Manickam, S., Gupta, B. B., Singh, P., Anbar, M. (2014). Design, deployment and use of HTTP–based botnet (HBB) testbed. In *Proceedings of 16th International conference on Advance Communication Technology* (ICACT–2014), 250 Phoenix Park, PyeongChang, South Korea, February 16–19, 2014.

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., and Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE Communications Surveys & Tutorials*, 15(4), 2070–2090.

Almomani, A., Gupta, B. B., Wan, T. C., Altaher, A., & Manickam, S. (2013). Phishing dynamic evolving neural fuzzy framework for online detection "zero–day" phishing email. *Indian Journal of Science and Technology*, 6(1), 3960–3964,

Anti-Phishing Working Group (APWG). (2012). Phishing activity trends report—fourth quarter 2012. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_Q4_2012.pdf

Anti-Phishing Working Group (APWG). (2013). Phishing activity trends report—first quarter 2013. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf

Beidermann, S., Ruppenthal, T., & Katzenbeisser, S. (2014, July). Data centric phishing detection based on transparent virtualization technologies. In *Proceedings of the 12th Annual Conference on Privacy, Security and Trust* (PST). Toronto, Canada: IEEE, 215–223.

Chung, E. H., Chiew, K. L. Sze, S. N., & Tiong, W. K. (2013, December). Phishing detection via identification of website identity. In *Proceedings of IT Convergence and Security* (ICITCS) *International Conference*. Macao,PRC: IEEE, 1–10.

Debarr, D. (2013). Spam, phishing and fraud detection using random projection, adversial learning and semi-supervised learning [Doctoral Dissertation]. Fairfax, VA: George Mason University.

Geng, G., Lee, X., & Tseng, S. (2013, September). Favicon—A clue to phishing detection sites. In *Proceeding of the eCrime Researchers Summit*. IEEE,San Francisco, CA: IEEE, 1–10.

Gupta, B. B. Gupta, S., Gangwar, S., Kumar, M., Meena, P.K. (2015). Cross-site scripting (XSS) abuse and defense: Exploitation on several testing bed environments and its defense. *Journal of Information Privacy and Security*, 11(2), 118–126.

Gupta, S., & Kumarguru, P. (2014, September). Emerging phishing trends and effectiveness of the anti-phishing landing page. In *Proceedings of the APWG Symposium on eCrime Summit*. Birmingham, AL: Anti-Phishing Working Group (APWG), 36–47.

Husak, M., & Cegan, J. (2014, September). PhiGARo: Automatic phishing detection and incident response framework. In *Proceedings of 9th International Conference on Availability, Reliability and Security*, Fribourg, Germany: IEEE, 295–302.

Lee, L. H., Lee, K. C., Chen, H. H., & Tseng, Y. H. (2014, November). POSTER: Proactive blacklist update for anti-phishing. In *Proceedings of ACM SIGSAC Conference on Computer and Communications Security* (pp. 1448–1450). New York, NY: AMC.

Lininger, R., & Vines, R.D. (2005). *Phishing: Cutting the identity theft line*. Indianapolis, IN: Wiley Publishing.

Mejias, R. J., & Balthazard, P. A. (2014). A model of information security awareness for assessing information security risk for emerging technologies. *Journal of Information Privacy and Security*, 10(4), 160–185.

Mishra, A., & Gupta, B. B. (2014, August). Hybrid solution to detect and filter zero-day phishing attacks. In *Proceedings of the Second International Conference on Emerging Research in Computing, Information, Communication and Applications* (ERCICA-14), Elsevier, Bangalore, India, 373–379.

Pandey, M., & Ravi, V. (2013, December). Phishing detection using PSOAANN based one-class classifier. In *Proceedings of 6th International Conference on Emerging Trends in Engineering and Technology*. Nagpur,India: IEEE, 148–153.

Downloaded by [115.254.77.21] at 23:36 10 May 2016

Park, G. Stuart, L.M., Taylor, J.M., & Raskin, V. (2014, October). Comparing machine and human ability to detect phishing emails. In *Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*. San Diego, CA: *IEEE*, 2322–2327.

Ramanthan, V., & Wechsler, H. (2013). Phishing detection and impersonated entity discovery using conditional random field and latent dirichlet allocation. *Computers & Security*, *34*, 123–139

Sodiya, A. S., Folorunso, O., Komolafe, P. B., & Ogunderu, O. P. (2011) Preventing authentication systems from keylogging attack. *Journal of Information Privacy and Security*, 7(2), 3–27.

Statista: The Statistics Portal. (2014). *Statistics and market data on cyber crime*. Retrieved from http://www.statista.com/markets/424/topic/1065/cyber-crime/

Tripathi, S., Gupta, B. B., Almomani, A., Mishra, A., & Veluru, S. (2013). Hadoop-based defence solution to handle distributed denial of service (DDoS) attacks. *Journal of Information Security* (JIS), *Scientific Research*, 4(3), 150–164.

Wu, L., Du, X., & Wu, J. (2014, August). MobiFish: A lightweight anti-phishing scheme for mobile phones. In *Proceedings of the 23rd International Conference Computer Communication and Networks* (ICCCN). Shanghai, China: IEEE, 1–8.

Yu, W. D., Nargundkar, S., and Tiruthani, N. (2008, July). A phishing vulnerability analysis of web based systems. In *Proceedings of the 13th IEEE Symposium on Computers and Communications* (ISCC 2008). Marrakech,Morocco: IEEE, 326–331.

Downloaded by [115.254.77.21] at 23:36 10 May 2016

View publication stats