This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2017 conference.

Spear Phishing: Diagnosing Attack Paradigm

Deepali N. Pande[1] and Preeti S. Voditel[2]
Department of Computer Application, Shri Ramdeobaba College of Engineering and Management, Nagpur, M.S., India
Email: [1]pandedn@rknec.edu [2]voditelps2@rknec.edu

***Abstract*—Internet is a rich source of web media and social networking applications. A cluster of users interconnect using those forming mutligroups. But the usage of web resources imprudently is causing doors to phishing, pharming and targeted phishing attacks. Careless use of social networking applications like LinkedIn, pinterest, whatsapp, face book and twitter barely from smart phones have become extrinsic sources for phishing and pharming attacks. Hence, it is essential to understand the pinholes of these attacks and their relationship with variants of user-agents on distributed platform. In this paper, we direct our survey in finding extrinsic porches influential to nasty invasions as attack entry point analysis. Also, we incline our detection considering recursive NM cache poisoning as the source of spear-phish attack. We present a detail analysis to determine spear-phishing. We evaluate and compare the spear phish feature detection attributes with PhishTank, a benchmark dataset.**

***Index Terms*—Phishing, spear-phishing, pattern mining, classification.**

I. Introduction

Phishing is a crime which involves ethical and technical artifices in stealing consumers' personal data for malevolent practices. The intruders misuse social engineering schemes ethically in disguising the users to practice phishing attacks. Phishing attack thrives on persuading the users to acquire information from them. It is usually implemented after learning various semantics from the users' interaction. Some of the most common phishing techniques include implanting crimewares to steal credentials, intercepting through the websites, hijacking the consumers' computer to compensate for locked data and many more. IT sector have been providing server side solutions for the phishing problem through schemes and soft ware's like anti-spams, anti-malwares, anti-virus update patches for dual layer security and many more [1–5].

In this paper, we focus in diagnosing the characteristics of spear phishing attack. Our purpose is to differentiate spear phishing attack versus phishing attack. Many research techniques use same features to diagnose spear phishing attack as used for phishing. We present an experimental set-up to learn the characteristics of spear phishing and formulate association rules for feature extraction of spear phish attack, right at the attack launching phase.

The paper is organized into seven sections in which we describe the preliminary process of induction of spear phish attack. Section II, presents motivation, Section III is a descriptive survey of how spear phish attacks occur. In Section IV, we present the methodology of identifying spear phishing and henceforth portray the typical features of spear phishing. In Section V, we describe the algorithmic approach used for feature extraction. Section VI highlights the problem statement describing how spear phish attacks have a different identity then phishing attacks. Section VII presents, detailed analysis of pattern mining for spear phish attacks through our empirical experimental setup. Lastly, in Section VIII, the results of spear phish attack outcomes are evaluated and illustrated using analysis tools. Section IX concludes the work.

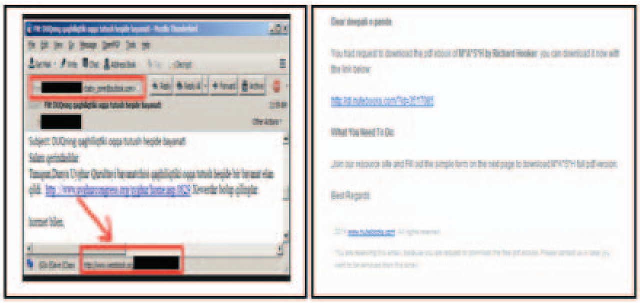
II. Motivation

All internet using organizations have firewalls as a mandatory security measures utilized with. It is an essential component designed to inspect the security issues like packet inspection, data authentication, integrity and confidentiality of the internal network. Most systems have security holes for patch updating yet spear phishing being a semantic attack cannot be restricted. The principal information most likely the username and passwords have proven to be back doors for creeping into security holes when these have been learnt by the spearphishers. A spear phishing attack can be as good as a knock towards intrusion in the system. Moreover, it has been learnt from the survey that phishing attacks can be controlled through security soft ware's, transport layer security updates, anti-viruses and patches for boosting security in operating systems but spear phishing which is a kind of known party attack cannot be controlled using them. A wide group of systems implant a honey spot for curbing phishing attempts but intra-network spear phishing has no solution in such measures. Hence, after learning that spear phishing is a non-generic ideology, merely depending on goal-specific honey spot to curb it, can never be a good solution.

III. Literature Survey

The APWG keeps a record on various strategies targeted for phishing the sites. A recent report highlights website intrinsic phishing activities. It states that a website may have thousands of URLs targeting a brand per domain. An email is sent to multiple users which direct them to a specific phishing website. A target website may have plenty of URLs all directed to a common attack destination. A negotiable remedy to such strategy can be complete browser blocking or sometimes email blocking, both being unsuccessful. The difficulty complying it is requirement of full URL to block. Though plenty of researches to thwart phishing had been changing the scenario for phishers, still it has not yet fully put to an end. APWG reported a rogue steering in the on cast of phishing activity strengthening brand/domain pairs. URLs in big amount are being hosted to target a specific brand reporting to one more

978-1-5090-4442-9/17/$31.00 ©2017 IEEE



FW: DUQning qaghiliqtiki oqqa tutush heqide bayanat - Mozilla Thunderbird

[redacted] [illegible]@outlook.com

FW: DUQning qaghiliqtiki oqqa tutush heqide bayanat

[redacted]

Subject: DUQning qaghiliqtiki oqqa tutush heqide bayanat

Salam qerindashlar

[illegible]

http://www.uyghurcongress.org/uy/ghur/home.asp?1829 [illegible]

hormet bilen,

http://www.[illegible] [redacted]

Dear deepali s panda

You had request to download the pdf ebook of M*A*S*H by Richard Hooker. you can download it now with the link below:

[illegible]

What You Need To Do:

Join our resource site and Fill out the simple form on the next page to download M*A*S*H full pdf version.

Best Regards

[illegible]

Picture 1. Snapshot of spear phish attempt redirecting to authentication demand link. The hyperlink traversed in through a book purchase email.

type in the taxonomy of phishing pronounced as spear phishing scoring a success count of 91% round the web. Another approach to gain control of personal information includes data sharing which usually seems to be legitimated and trustworthy yet risky for the victim. The phishers obfuscate the victim through usage of altered links to direct him to fake page for stealing details [1–5]. This report is notified in the phishing activity trends report, second quarter 2014.

A. Analyzing Spear Phishing Attack

The time duration between the sender and the receiver is considered the major factor in deciding vulnerabilities of the spear phishing attack. The compromise can captured when the payload of the email is delivered and is executed. This proves the indication of chances in being spear phished. Also, the ratio of emails left into the inbox undetected as spear phish from past history gives a likelihood in detection of spear phishing. Analyzing in this direction lessens the problem of reporting benign emails being flagged as malicious. Picture 1 illustrates a pinpointing spear phishing attack targeted after triggering malicious emails.

IV. Methodology

To study the source of phishing, we laid an experimental set-up for detail examination of phishing attacks henceforth identifying spear-phishing from them. In doing so, we collected bag-of-features of DNS spoofing activity records. A dataset tryfreedo.myd was featured after pattern mining using existing machine learning algorithms. The process of pattern mining is described in Fig. 2. We take into assessment, the behaviour patterns of various hyperlinks from malicious email sources. These patterns are formed after categorization of benign and malicious emails. We extract features from both, the database of malicious as well as benign records. To distinguish the benign records from malicious ones, we compute signatures from the threshold parameter as evaluated from the n-grams processing of pattern categorization phase. The information gain based feature selection on behaviour patterns is used to design the classifier using the concept of naive bayes classification. N-grams processing yields information gain in one class and its absence in other class. We take into consideration the sequences extracted from repetitive words, domain registry data, and system call records from program codes. These n-gram information gain chunks are then used to generate signatures for benign records.

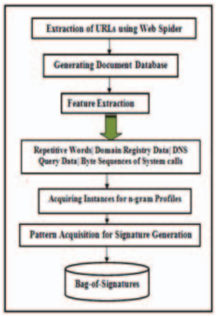

Extraction of URLs using Web Spider
Generating Document Database
Feature Extraction
Repetitive Words| Domain Registry Data| DNS Query Data| Byte Sequences of System calls
Acquiring Instances for n-gram Profiles
Pattern Acquisition for Signature Generation
Bag-of-Signatures

Fig. 2. Pattern mining.

V. Feature Mining

A spear-phish attack to target a dummy domain website, www.tryfreedo.com was designed for attack behavior modeling. In the experimental set-up, studying various characteristics of phishing were the objectives to exemplify. During pre-attack scenario, the query section and the identifier of responses have a corresponding one-to one homomorphic match. Also, in the post attack scenario, during attack monitoring, we analyzed that the spearphishers typically originating from recursive Name Server exploitability, has a premature delivery response. We also experimented that the spear phish attack is easy to launch during the name resolution process because once and all the specification details are handed over to the DNS client, then to capture the dll files really becomes a bot-attack. Also, the spear phishing attack launching requires a malicious Name resolver which silently takes over the target system by modifying the 'resolve.conf' during DNS name resolution. We therefore, target the spear phish attack scenario as redirection of name server record to other domain to steal the authentication details, which is commonly known as DNS redirection.

VI. Problem Statement

Hypothesis: We aim our attack detection hypothesis emphasizing that the spy-bot installers are causal for spear phishing. Hence lay an experimental set-up to detect the invasion of spear phishing through extrinsic porches.

We begin the spear phish attack analysis by first identifying whether query block is present in the transmission packet. If it is present, our target is to diagnose the type of query namely recursive query, iterative query or inverse query. If the type is 'recursive query' then we treat it as a source of spear phish attack and judge it using attack-parameter analysis. We describe various parameters for analyzing spear phish as a part of features of spear phish attack in the section described above.

A recursive query is mostly used for information collection during spear-phishing since the DNS server which receives this query has to fetch the answer and return back the needful information. During a typical browsing session, the 'resolve.conf' puts complaint DNS servers' addresses in it, which diverts all queries to these addresses. Only some of the DNS servers from the list in 'resolve.conf' may be recursive query based. The plausible attack paradigms used for spear phishing include session hijacking and DNS address replacement and is usually mounted by conquering the 'resolve.conf'. The victim node is fully unaware of these paradigms. A weaker point in spear phish attack mounting is that the root servers fully work on iterative query system. A major significance of iterative query system is that the DNS server sends a referral to another DNS server which may have an answer for the query. Exploiting this property, the early identification of spear phish attack launch is possible. The querying property of DNS name servers provided in the 'resolve.conf' can be monitored and shielded. In the experimental phase, we examined that if all the DNS servers use iterative query system then the chain of dependency in spear phishing is destroyed and henceforth causes early identification of attackers in the chain.

VII. Experimental Setup for Attack Detection

We laid an experimental set-up of zabbix tool to find the causal vulnerabilities for spear phish attack. We configured zabbix as a network server to keep track of multiple instances and one as a client. Our target was to monitor phishing activities on agent-based and agent-less platforms. A website sniffer tool version 1.5 was used to monitor www.tryfreedo.com for an examination period of 99 days. We used DNS function exploit kits freely available for estimating the probability of a phishing attack by the intruder targeting externals ports as the source for attacks to enter.

The workstation holding the tryfreedo.com was configured under SNMP as managed server agent to record the activity under MySQL database tryfreedo.myd. The records were analyzed using pattern mining described in Fig. 3. The PhishTank database and tryfreedo, where used to generate patterns for stylometric feature vectors on spams. As a part of pre-processing, the hyperlinks were parsed and URLs for images and links to other pages were retrieved from the tryfreedo.myd. The DNS query sniffer generated a record consisting of descriptions like hostname, port number, response time, duration and content into a dnsquery.csv file. The hostnames and port numbers were used as a testament for similarity assessment of the records obtained in the tryfreedo.myd. We used the formula described below to identify the scores of legitimate versus phished URLs on well known machine learning algorithms like bayesian classifier and nearest neighbor classifier.

$$\text{Scorematch} = \frac{\text{Number of Patterns matched}}{\text{Total Patterns Extracted}}.$$

Doing this, a list of ports proving frequency of intrusions were recorded as a memoir from the DNS activity monitoring kits used in the experiment, as shown in the Table I.

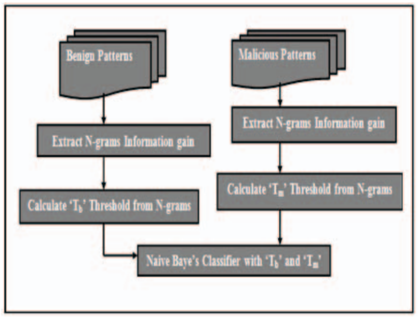

Benign Patterns
Malicious Patterns
Extract N-grams Information gain
Extract N-grams Information gain
Calculate 'T_b' Threshold from N-grams
Calculate 'T_m' Threshold from N-grams
Naive Baye's Classifier with 'T_b' and 'T_m'

Fig. 3. Spear-phishing profile detection.

TABLE I
List of Memoirs Collected During the Experimental Phase.

Service	Renderers
File transfer protocol-port 21	Like HTTP web server Microsoft SQL server Windows file sharing probe Gnutella peer to peer file sharing tool
Simple mail transfer protocol port 25	Like HTTP web server Microsoft SQL server Windows file sharing probe Gnutella peer to peer file sharing tool
Domain name system service port 53	Like HTTP web server Microsoft SQL server Windows file sharing probe Gnutella peer to peer file sharing tool
Hypertext transfer protocol port 80	Like HTTP web server Microsoft SQL server Windows file sharing probe Gnutella peer to peer file sharing tool

VIII. Evaluation and Analysis

As, a part of experiment, the default internet explorer browser was installed. The spam filter properties were disabled for period of 99 days in tuning with the zabbix activity monitor. During the activity, we collected 570 phishing URLs in which mostly are diversion links, stegano-images, dll installers. The machine learning algorithms developed using java were tested using tryfreedo.myd and phishtank, available under APWG site. Table II, shows illustrations of phishing attachments and diversal links and executables found on a prominent frequency.

During the analysis, it was found that spear-phishing can be promisingly identified from link diversion attacks. We

TABLE II
List of Top 7 Most Frequently Occuring Attachments. The Attachment Names Appear as Genuine Names.

Spear-phishing attachment source	Spear-phishing attachment name
page-jjjj9.war	109-WX-AZ-PA4-2 certified.exe
apr-123.jar	/var/directory0/attach_dominician.exe
urns.dll	111_dx_oooo_fpqw.html
img049897.scr	/attach/ui40064_2013_Article_296.exe
20uiu.rar	/ybhjoumal.pone.0130968.t001.exe
scriptforyou.au3	/var/cdr/fvmgHZXfRz5fhytx-croppedCjB1H.exe
qrtyui.rar	/nygvxspl_lk9_stylesheet.exe

TABLE III
ANALYSIS OF PHISHING/LEGITIMATE LINKS.

Datasets	Machine learning algorithms			
	Bayesian classifier		Nearest neighbour classifier	
	% Match		% Match	
	Legitimate	Phished	Legitimate	Phished
Tryfreedo	82 TPR/8 FPR	92 TPR/8 FPR	88 TPR/5 FPR	93 TPR/4 FPR
Phishtank	84 TPR 4 FPR	96 TPR/7 FPR	81 TPR/7 FPR	85 TPR/6 FPR

used a computer system with minimalist configuration core i3, 2.4 GHz processor versus a smartphone with iOS and mutli-client web-applictions for reverse analysis. The Table III, shows the results of computation of legitimate versus phished websites detection on well known classifiers namely the bayesian classifier and the nearest neighbour classifier.

The distribution of classification parameters was not uniform in tryfreedo. The discrimative attributes used for comparative analysis in similarity assessment of tryfreedo and phistank had varied values. The precision-recall exhibit informative results under variant scenarios.

We installed web scanner software to analyze whether the attacks focus spear phishing or phishing attacks. Some of existing soft-wares like arachni web scanner was used to acquire features from the user-agent used at all the terminals in the complete experiment process. The arachni is complaint to distributed architecture, in that multiple clients can be remotely scanned. A set of two smart phones with iOS and two Windows based 64 bit clients were treated with arachni webscan. The user agents iCab, dolphin, internet explorer and mozilla firefox were dynamically scanned and informative features like IP address, hostname, Proxy IP, referrer page, and whether java & dot net enabled were monitored and stored as binaries. The runtime activity of the top-10 attachments were scrutinized using compliant application servers and web containers. We used eclipse-neon 64-bit level compatibility to assess the targeted activity of the pin-pointing attachments. The contents revealed usage of JOnAS with EJB container for typical attachments of web codes and extension as '.war', also Jetty with java servlet container revealed hidden activity. The executables exhibit deception of social-net links.

A. The TryFreeDo Dataset

The dataset acquired in manner described above, was focused to record total 11 attributes which converge towards phishing attacks. It has total 912 records from which 570 regarded cleanly as phishing. The tryfreedo.myd was compared for similarity with benchmark dataset phishtank freely available under UCI machine learning repository. The percentage of recall over precision show significant retrieval rate. The records evaluated as phishing were further used for discrimination of spearphishing. We computed information gain index on 570 dataframes after setting feature learning

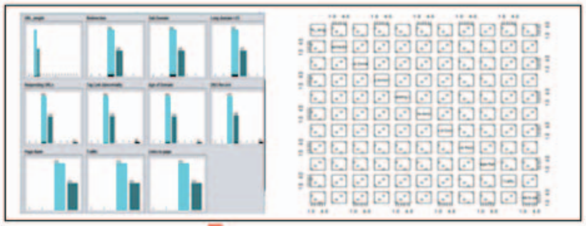
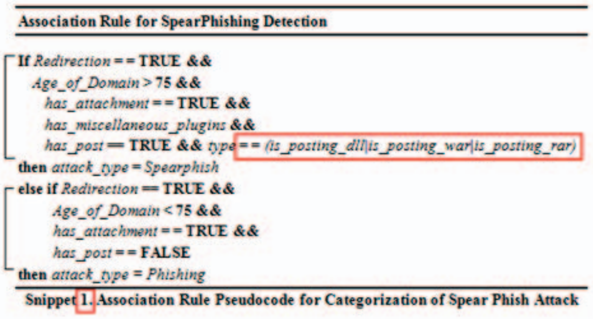


Fig. 4. Density graph of tryfreedo dataset.

association rules using pinpointing features describing type of attack as spearphishing. The top-9 informative features directing towards spearphishing detection with a hitting information gain index is illustrated in Table V. We discriminate the spearphishing from phishing using association rule minning on the pinpointing attributes as described below.



Association Rule for SpearPhishing Detection

```
If Redirection == TRUE &&
  Age_of_Domain > 75 &&
    has_attachment == TRUE &&
    has_miscellaneous_plugins &&
    has_post == TRUE && type == (is_posting_dll|is_posting_war|is_posting_rar)
then attack_type = Spearphish
else if Redirection == TRUE &&
      Age_of_Domain < 75 &&
      has_attachment == TRUE &&
      has_post == FALSE
then attack_type = Phishing
```

Snippet 1. Association Rule Pseudocode for Categorization of Spear Phish Attack

The Fig. 4 highlights the density of information captured and refined for spearphish analysis. The machine learning tasks was evaluated using Java on eclipse neon purely using algorithmic approach. We also used Ri386 for dataframe calibration and various data preprocessing tasks mining inbuilt packages. We illustrate our pseudocode used for categorization of spear phishing attacks from pharming attacks and spamming attacks in snippet-1. The hypothesis that a spear phish can be launched only through intrusion, is proven and analysed in experiment. We demonstrate the clarity of the proposed hypothesis in Table IV showing inclination on features attributes pinpointing the targetted attack.

We used different combinations of cross-fold validation on tryfreedo under same testing conditions. On a generic score of 10 fold cross validation, different variants of classifer algorithms bayesian classifier, bayesNet, OneR, ZeroR, RandomForest, j48 were used to compare the results of classification. The results of classification on tryfreedo in comparison of PhishTank show an initial score of ROC with 0.9881 and 0.996. The ROC curve plots, shown in Fig. 5, specify accuracy of detection.

IX. DISCUSSION AND CONCLUSION

In the experimental evaluation we used DNS function exploiters on 3-way server-client; client-client; server-server configuration to identify and evaluate the source of spearphish attacks. We developed a website www.tryfreedo.com to record the scrupulous activity as the agent. In the pro-

TABLE IV
ACCURACY OF FEATURE RETRIEVAL USING PRECISION AND RECALL. THE RECALL PERCENTAGE SHOWS SIGNIFICANT RETRIEVAL AS COMPARED TO BENCHMARK PHISHTANK. RESULTS SHOW BALANCED AUC RELATIONSHIP.

Feature attributes	URL length >60	Redirection	Sub-domain	Long domain >25	Requesting URLs	URL anchor	Tag link abnormality	Age of domain	DNS record	Page rank	Traffic	Multiple links
PhishTank												
Precision (%)	97.66	94.12	97.14	88.22	87.89	91.17	89.23	81.15	91.10	93.21	95.37	95.16
Recall (%)	97.45	94.36	97.16	82.17	86.71	90.13	88.24	80.02	92.18	94.43	96.12	96.89
Tryfreedo												
Precision (%)	94.01	90.55	99.01	89.76	82.45	99.89	78.90	77.98	90.17	74.16	91.11	92.22
Recall (%)	91.99	93.47	98.19	87.61	80.90	91.22	81.23	80.01	92.18	62.23	80.18	98.15

TABLE V
INFORMATION GAIN INDEX OF TOP 9 DISTINGUISHED FEATURES PINPOINTING THE SPEAR PHISHING ATTACK.

Pinpointing features	Information gain ratio
has_redirection	0.041
age_of_domain	0.012
has_attachment	0.017
has_miscellaneous_plugins	0.087
has_posting	0.019
type_posting_is_dll	0.871
type_posting_is_war	0.912
type_posting_is_jar	0.964
type_posting_is_rar	0.926

cess, two smatphones with webapps like facebook, linkedin, pinterest,instagram,twitter and shareit were exploited to send intrusion activities on tryfreedo by flaunting the website www.catchfreedo.com on bare internet explorer as a browser providing it only a minimal set of security,with spam filters disabled permanently. Also, in the trial period, we disabled the hotlink protection and leech protection features. It was examined that the attachments, fetched in the experimental phase are floated on the internet through webomedias. These attachments have dll files, war files, and self-installable plug-ins which target any users through sniffing activity. We have listed some of these malicious attachments in the Table II. The outcome exhibits, smartapps can be used for link reversals from the iOS smartphones. We calculated the true positives and the false negatives on the records obtained in the process. The results show, on an average a 83% correct identification of legimate websites whereas a 94% correct identification of phishing URLs. As a part of the future work, we are targetting to reduce the false negative rate in identification of phished URLs. Also, we aim to identify cross-site script link-reversals as a stylometric feature in the feature collection phase of our proposed system of spear-phish detection.

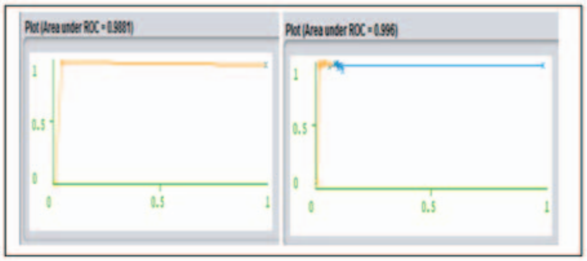


Fig. 5. Area under ROC of tryfreedo in comparison to PhishTank. The ROC values exhibit accuracy in detection.

REFERENCES

[1] A. Martino and X. Perramon, “Phishing secrets: History, effects, and countermeasure,” *International Journal of Network Security*, vol. 12, no. 1, pp. 37–45, Jan. 2011.

[2] F. Aloul, “The need for effective information security awareness,” *Journal of Advances in Information Technology (JAIT)*, vol. 3, no. 3, pp. 176–183, 2012.

[3] M. Cova, C. Krueger, and G. Vigna, “There is no free phish: an analysis of “Free” and live phishing kits,” in *Proc. of the 2nd USENIX Workshop on Offensive Technologies*, 2008.

[4] R. Dhamija, J. Tygar, and M. Hearst. “Why phishing works,” in *Proc. of the Conference on Human Factors in Computing Systems (CHI)*, 2006, pp. 581–590.

[5] Y. Zhang, S. Egelman, L. Cranor, and J. Hong, “Phishing phish: evaluating anti-phishing tools,” in *Proc. of the 14th Annual Network & Distributed System Security Symposium (NDSS)*, Feb. 2007.

[6] M. Wu, R. Miller, and S. Garfinkel, “Do security toolbars actually prevent phishing attacks?,” in *Proc. of the Conference on Human Computer Interaction (CHI)*, New York, pp. 601–610, 2006.

[7] S. Egelman, L. Cranor, and J. Hong, “You’ve been warned: an empirical study of the effectiveness of web browser phishing warnings,” in *Proc. of the Conference on Human-Computer Interaction (CHI)*, Florence, Italy, 2008, pp. 1065–1074.

[8] G. Ollmann, “The pharming guide: understanding and preventing DNS-related attacks by phishers,” NGS Secure, 2005. Available at: www.infosecwriters.com/text_resources/pdf/ThePharmingGuide.pdf.

[9] L. Shujun and R. Schmitz, “A novel anti-phishing framework based on honeypots,” in *Proc. of the eCrime Researchers Summit*, pp. 1–13, Sep 2009.

[10] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs, “Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions,” in *Proc. of the Conference on Human Computer Interaction (CHI)*, Atlanta, Georgia, 2010.

[11] T. Jagatic, N. Johnson, M. Jacobson, and F. Menczer, “Social phishing,” *Proc. of the Communications of ACM*, vol. 50, no. 10, pp. 94–100, Oct. 2007.

[12] R. Dodge, E. Rovira, R. Zachary, and S. Joseph, “Phishing awareness exercise,” in *Proc. of the 15th Colloquium for Information Systems Security Education*, Fairborn, Ohio, June 13–15, 2011.

[13] https://archive.ics.uci.edu/ml/datasets/Phishing+Websites, UCI Machine Learning Repository.