POSTER: Proactive Blacklist Update for Anti-Phishing

Lung-Hao Lee[1,2], Kuei-Ching Lee[1,2], Hsin-Hsi Chen[1] and Yuen-Hsien Tseng[2]
[1]Department of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan
[2]Information Technology Center, National Taiwan Normal University, Taipei, Taiwan
{d01922005, p00922002, hhchen}@ntu.edu.tw, samtseng@ntnu.edu.tw

ABSTRACT
This study explores the existing blacklists to discover suspected URLs that refer to on-the-fly phishing threats in real time. We propose a PhishTrack framework that includes redirection tracking and form tracking components to update the phishing blacklists. It actively finds phishing URLs as early as possible. Experimental results show that our proactive phishing update method is an effective and efficient approach for improving the coverage of the blacklists. In practice, our solution is complementary to the existing anti-phishing techniques for providing secured web surfing.

Categories and Subject Descriptors
H.3.3 [**Information Search and Retrieval**]: *Information filtering.*

General Terms
Experimentation, Human Factors, Security.

Keywords
Phishing threat detection; cyber crime; web security

1. INTRODUCTION
Phishing is a cyber crime employing both social engineering and fraudulent techniques to steal users' personal identity data and financial account credentials. Phishing attacks are pervasive and sophisticated. They can be spread through spoofed emails, instant messaging, social networking sites, and massively multiplayers games [6]. Criminals usually create phishing websites by exactly copying the legitimate ones or slightly modifying their page content. Content-based features have been extracted to detect phishing URLs using online learning [3]. A feature-rich framework has been proposed to detect phishing websites [12]. Lexical and host-based features have been learned from suspicious URLs to distinguish phishing web pages [9]. An image-based scheme has been presented for anti-phishing [4]. The effectiveness of several machine-learning techniques on phishing detection has been compared [2]. Different from formulating the discriminative patterns between legitimate and phishing web pages, users' behavioral response to phishing risk has also been surveyed [5]. The access contexts in which users fall into phishing situations have been explored from behavioral perspective [7]. Users' browsing behaviors that confront phishing dangers are studied for context-aware phishing detection [8].

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author. Copyright is held by the owner/author(s)

CCS'14, November 3-7, 2014, Scottsdale, AZ, USA
ACM 978-1-4503-2957-6/14/11.
http://dx.doi.org/10.1145/2660267.2662362

Phishing URLs tend to look like the original legitimate ones. For example, the domain name "www.paypalsicher.eu" was verified as a phishing website of www.paypal.com. The URL-blocking mechanism rejects any requests to URLs in a blacklist and accepts requests to URLs that are not blacklisted. Blacklisting has the advantage of consuming fewer computational resources for filtering dangerous accesses. Nevertheless, the dynamic characteristics of the changing web require such blacklists to be constantly updated for sustainable blocking performance. A large scale of phishing pages has been verified empirically for investigating their life spans. Phishing URLs usually survive within a very short time period [1]. How to find suspected phishing threats as early as possible is a challenging issue. Different from previous work that develops automatic methods to detect phishing pages, we focus on updating a given blacklist actively to discover on-the-fly phishing URLs in real time for providing secured web surfing.

2. PROACTIVE BLACKLIST UPDATE
Phishing blacklists are usually generated in combination of procedures that involve automatic detection mechanism and human intervention. Although blacklists provide the simplicity in design and implementation by browsers, the coverage of a blacklist plays an important role in keeping up with the changing trails of phishing treats. Phishing criminals employ many sophisticated techniques to evade blacklisting. It is inherently difficult to predict the suspected URLs to be included in the blacklists exhaustively. The research problem in this study is formulated as follows. We focus on actively improving the resilience and efficiency of an existing blacklist by discovering on-the-fly phishing URLs as early as possible for fighting the phishing crimes.

Criminals usually create many temporary URLs to host fraudulent page content for their phishing purposes. These URLs are invalid in a rapidly changing fashion. We adopt a process to eliminate unsuitable URLs in the current blacklists and retain the remaining ones as seed URLs to reflect the on-the-fly web environment. A DNS lookup is conducted firstly to filter out non-resolved URLs. Then, a connection is established to request page content of resolved URLs. We check the returned HTTP status code to verify whether their content can be successfully accessed. Those URLs referring to inaccessible content are also removed. Finally, we further examine the accessible content. In our observations, the page content contains text descriptions such as "account suspended," "temporary unavailable," and "access restrictions" may be phishing URLs that have been reported and blocked. We also discard those URLs that do not have threats at the access time. Only the remaining URLs that pass the above examinations will be regarded as seed URLs for blacklist update. We propose the architecture of PhishTrack, which consists of the following two major components to predict possible phishing URLs.

(1) **Redirection Tracking**: URL redirection techniques are often adopted for referring to phishing web content, *e.g.*, the location field in HTTP return header, the refresh attribute of HTML <meta> tag, and the values of windows.location or location.href designed in JavaScript language. PhishTrack collects the redirection URLs extracted from the phishing seeds to improve the incompleteness of an existing blacklist.

(2) **Form Tracking**: Phishing pages always provide forms for gathering users' valuable data. In PhishTrack, we input fake data to pass validation examination for tracking triggered URLs that are described in action attribute of HTML <form> tag. We follow the phishing forms iteratively for discovering newborn phishing URLs.

3. PERFORMANCE EVALUATION

The phishing data came from the PhishTank [10], a free community website where everyone can submit, verify and track the phishing URLs. The phishing data released on 6th April 2014 was downloaded as our original blacklist for discovering suspected phishing URLs. We took the PayPal, the top-1 identified brand that was fraudulently represented as phishing pages in terms of popularity, as a target to measure the effectiveness of our method. In total, 3,916 phishing URLs that masquerade as official PayPal were collected in our seed data.

The following two phishing blacklist update approaches were compared to demonstrate their performance.

(1) **PhishNet** [11]: This approach adopts 5 heuristics, *i.e.*, replacing TLDs (H1), IP address equivalence (H2), directory structure similarity (H3), query string substitution (H4), and brand name equivalence (H5), to enumerate combinations of known phishing sites for predicting new phishing URLs. Typical URLs in the blacklist have the structure: http://domain.TLDs/directory/filename?query_string. These heuristics involve interchanging the field values lexically observed from the collected URLs. We had collected phishing URLs from PhishTank within a time period of a week starting from 30th March to 5th April 2014 for observing possible substitution strings. After generating the suspected URLs, a DNS lookup was conducted to remove those that cannot be resolved. Finally, a publicly available detection tool (http://www.webconfs.com) was used to analyze content similarity between original seeds and URL candidates. If the candidates' content has sharp resemblance above 90%, the candidates' URLs were added to enhance the coverage of the original blacklist.

(2) **PhishTrack**: This is the approach proposed in this paper. It is composed of redirection tracking (T1) and form tracking (T2) for phishing blacklist update.

We submitted newly found URLs to PhishTank for category verification. Volunteers participate in voting suspected URLs as a phish or benign by examining the page content manually. Each submission needs enough votes to be confirmed or denied as phish. The platform moderators labeled those URLs that do not have final category decision, but could not be accessed permanently for any reasons, as unavailable. We adopt three metrics for performance evaluation. The numbers of phishing and non-phishing URLs are denoted as #Phish and #NotPhish, respectively. The number of unavailable cases, denoting as #N.A., shows how many URLs are offline before category assurance.

Table 1 shows the results. The performance difference between the two approaches was statistically significant (p<0.01), no matter which metric was adopted. In PhishNet approach, the heuristic H5, which treats the masqueraded brand as an equivalence class for lexical substitution, did not have any effects. The possible reason is that phishing criminals did not have the same URL structure for all popular targets to avoid being found easily. Besides, there are many unavailable cases generated by the other four heuristics (H1~H4). It took about 51 hours to enumerate all possible combinations, in a computing environment with an Intel Core I7 processor and 24 GB of memory. This shows that the time-consuming operations cannot keep up with the changing web, especially for those phishing websites. The page content of the suspected URLs may be removed and labeled as unavailable without obtaining an assured category. In our PhishTrack approach, the two proposed components T1 and T2 came the similar numbers regardless of which metrics are concerned. There were 91.97% (*i.e.*, 2165/2354) of found phishing URLs are newly discovered. In other words, they had not been collected in the blacklist released by PhishTank. We further analyzed the errors of our proposed approach. We found that most of false positive cases are related to some specific hosting services. The phishing websites had been removed and returned to legitimate homepage of hosting providers. These errors can be avoided with an exception list, which contains well-known legitimate domain names. In addition, there are few unavailable instances, because our method took about only 10 hours given the same data in the same computing environment.

In summary, the experimental results indicated that the PhishTrack approach obviously discovered more phishing URLs and predicted fewer incorrect URLs than the PhishNet approach. In addition, comparing PhishNet with PhishTrack, the former needs certain amount of collected phishing URLs for observing specific heuristic patterns, while the latter can work using individual phishing URL by tracking criminals' behavioral trails. The former also expends large amounts of execution time. These findings show that our approach is effective and efficient for proactive blacklist update. Intrinsically, the proposed PhishTrack approach is more proper to block the phishing accesses actively for avoiding threats to be propagated unlimitedly.

Table 1. Performance evaluation on phishing update

Methods		#Phish	#NotPhish	#N.A.
PhishNet	H1	32	26	10
	H2	780	3	747
	H3	129	0	38
	H4	22	0	80
	H5	0	0	0
	All	**963**	**29**	**875**
PhishTrack	T1	1,140	11	168
	T2	1,214	15	194
	All	**2,354**	**26**	**362**

According to most recent Anti-Phishing Working Group (APWG) industry advisory [1], the average life span of phishing attacks in 2H2013 was 28 hours and 43 minutes, in which half of all phishing attacks live for less than 8 hours. These findings reveal that time is a critical factor for curbing phishing crimes. In response, PhishTank releases the recent phishing blacklists every hour for anti-phishing. We hourly downloaded the brand-new blacklist containing phishing URLs belonging to PayPal target on

6th July 2014. Each blacklist is regarded as a seed for updating blacklist actively using our proposed PhishTrack approach. Figure 1 compares the URL differences between the original blacklists and our updated ones. The numbers of URL entries in the original blacklists were marked in purple color. The numbers of unsuitable URLs at the experimental time is denoted in blue color. The numbers of retained URLs and newly discovered ones are represented in red and green color, respectively. The average number of URL entries in the original PhishTank's blacklists is 2081.67. There are no significant differences among the original blacklists, because about 99% of URLs were kept in the continuous 6 hours. Empirical analysis indicated that our approach found 578.83 new URLs and removed 1101.67 ineffective ones on average. The average number of URLs included in our updated blacklists is 1558.83. This shows that our update method can actively find suspected URLs and remove the out-of-update ones to form the on-the–fly phishing blacklist for reflecting the real web situation. Besides, our model spent less than 20 minutes to finish the update process performed in a parallel computing framework. It is significantly less than average 78.9 hours consumed by PhishTank for phishing verification.

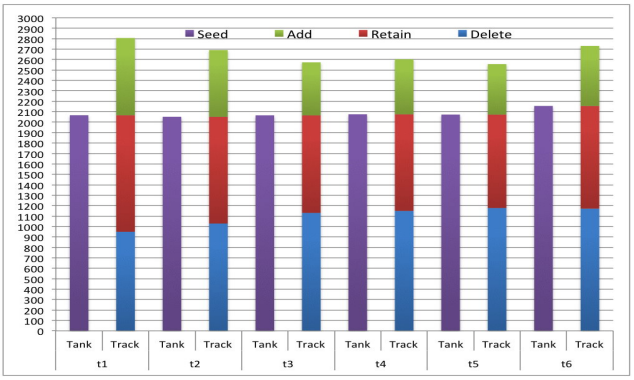

Figure 1. URL differences between the original and updated blacklists

In summary, the PhishTank provides a crowd-sourcing platform in which volunteers can submit and verify the suspected URLs manually. If nobody submits the phishing URLs in real time, it is impossible to include them in the released blacklists. In addition, if a submitted URL wastes much time for waiting the voting result, it may be unavailable even the true category belongs to phishing threat and the criminals have achieved their phishing purpose. Different from PhishTank mechanism, our PhishTrack approach automatically updates the existing blacklists to find on-the-fly phishing URLs actively. Intuitively, our solution is more suitable to the rapidly changing web.

4. CONCLUSIONS AND FUTURE WORK

This work demonstrates the feasibility of exploring the existing blacklists for discovering the on-the-fly phishing URLs in real time. A proactive blacklist update mechanism that consists of redirection tracking and form tracking is proposed to find suspected URLs as early as possible. Experimental results show that PhishTrack is an effective and efficient method that yields promising performance. In practice, it needs to be complemented by other phishing detection schemes for enhancing blacklisting. How to keep up with the changing trails of phishing threats within very short time periods is a really challenging research problem. A more aggressive strategy will be investigated in the future to achieve more satisfactory blocking performance for anti-phishing.

5. ACKNOWLEDGEMENTS

This research was partially supported by Ministry of Science and Technology, Taiwan under grant MOST 102-2221-E-002-103-MY3, MOST 103-2221-E-003-013-MY3 and the "Aim for the Top University Project" of National Taiwan Normal University, sponsored by the Ministry of Education, Taiwan. We are also grateful to volunteers for their participation of phish voting provided by the PhishTank platform.

6. REFERENCES

[1] Aaron, G., Rasmussen, R., and Routt, A. 2014. Global phishing survey: trends and domain name use in 2H2013. *An APWG Industry Advisory*, available online at http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf

[2] Abu-Nimeh, S., Nappa, D., Wang, X., and Nair, S. 2007. A comparison of machine learning techniques for phishing detection. In *Proceedings of the 2nd Anti-Phishing Working Group Annual eCrime Researchers Summit* (Pittsburgh, Pennsylvania, USA, October 4-5, 2007). eCrime'07, 60-69.

[3] Blum, A., Wardman, B., Solorio, T., and Warner, G. 2010. Lexical feature based phishing URL detection using online learning. In *Proceedings of 3rd CCS Workshop on Security and Artificial Intelligence* (Chicago, Illinois, USA, October 8, 2010). AISec'10. 54-60.

[4] Chen, K.-T., Chen, J.-Y., Huang, C.-R., and Chen, C.-S. 2009. Fighting phishing with discriminative keypoint features. *IEEE Internet Computing*, 13, 3 (May/June 2009), 56-63.

[5] Downs, J. S., Holbrook, M., and Cranor L. F. 2007. Behavioral response to phishing risk. In *Proceedings of the 2nd Anti-Phishing Working Group Annual eCrime Researchers Summit* (Pittsburgh, Pennsylvania, USA, October 4-5, 2007). eCrime'07, 37-44

[6] Hong, J. 2012. The state of phishing attacks. *Commun. ACM*, 55, 1 (January 2012), 74-81.

[7] Lee, L.-H., Juan, Y.-C., Lee, K.-C., Tseng, W.-L., Chen, H.-H., and Tseng, Y.-H. 2012. Context-aware web security threat prevention. In *Proceedings of the 19th ACM Conference on Computer and Communications Security* (Raleigh, NC, USA, October 16-18, 2012). CCS'12. 992-994.

[8] Lee, L.-H., Lee, K.-C., Juan, Y.-C., Chen, H.-H., and Tseng, Y.-H. 2014. Users' behavioral prediction for phishing detection. In *Proceedings of the 23rd International World Wide Web Conference* (Seoul, Korea, April 7-11, 2014). WWW'14. 337-338.

[9] Ma, J., Saul, L. K., Savage, S., and Voelker, G. M. 2011. Learning to detect malicious URLs. *ACM Trans. Intell. Syst.* Technol. 2, 3 (April 2011), Article 30.

[10] PhishTank, available online at http://www.phishtank.com.

[11] Prakash, P., Kumar, M., Kompella, R. R., and Gupta, M. 2010. PhishNet: predictive blacklisting to detect phishing attacks. In *Proceedings of the 29th IEEE Conference on Computer Communications* (San Diego, CA, USA, March 15-19, 2010). INFOCOM'10, 1-5.

[12] Xiang, G., Hong, J., Rose, C. P., and Cranor, L. F. 2011. CANTINA+: a feature-rich machine learning framework for detecting phishing web sites. *ACM Trans. Inform. Syst. Se.* 14, 2 (September. 2011), Article 21.