Shielding Against Web Application Attacks

Hari karan.S[1], Naresh.K[2], Mrs.Shanthi[3]
[1, 2, 3] Dept of Information and Technology
[1, 2, 3] Sri Muthukumaran Institute of Technology

Abstract- *Today search engines are tightly coupled with social networks, and present users with a double-edged sword: they are able to acquire information interesting to users but are also capable of spreading viruses introduced by hackers. It is challenging to characterize how a search engine spreads viruses, since the search engine serves as a virtual virus pool and creates propagation paths over the underlying network structure. In this paper, we quantitatively analyze virus propagation effects and the stability of the virus propagation process in the presence of a search engine in social networks. First, although social networks have a community structure that impedes virus propagation, we find that a search engine generates a propagation wormhole. Second, we propose an epidemic feedback model and quantitatively analyze propagation effects employing four metrics: infection density, the propagation wormhole effect, the epidemic threshold, and the basic reproduction number. Third, we verify our analyses on four real-world data sets and two simulated data sets. Moreover, we prove that the proposed model has the property of partial stability. Evaluation results show that, comp black with to a case without a search engine present; virus propagation with the search engine has a higher infection density, shorter network diameter, greater propagation velocity, lower epidemic threshold, and larger basic reproduction number.*

Keywords- Phishing

I. INTRODUCTION

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information .An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft. Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced perishment (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

II. OBJECTIVE

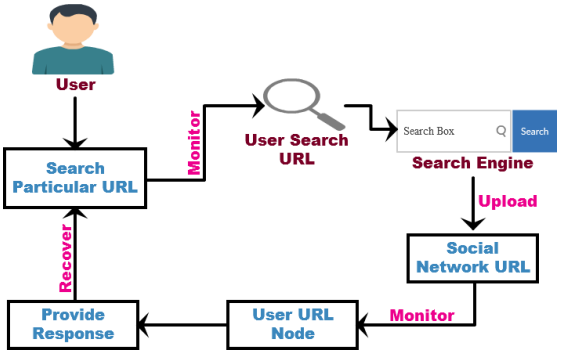
Search engines supply a highly effective means of information retrieving way. But the search engine is also a platform for spreading information. Because of these features, the propagators of malicious code have kept in step with search engines, building a hidden relationship within them. In recent years, so-called worms have utilized the search engine to spread themselves across the Web. A search engine is a quick and easy vehicle for malicious code to locate new targets. But it also has some down sides. The search engine can cause a single point of failure. Operators can choose not to return results for the malicious code's query or even purge the search engine database of web pages that match the query if they discover they are being used for malicious purposes. Moreover, the search engine poisoning (SEP) was applied by malicious software's that published some vicious and fake pages to push the page ranking higher and attract more accesses

III. LITERATURESURVEY

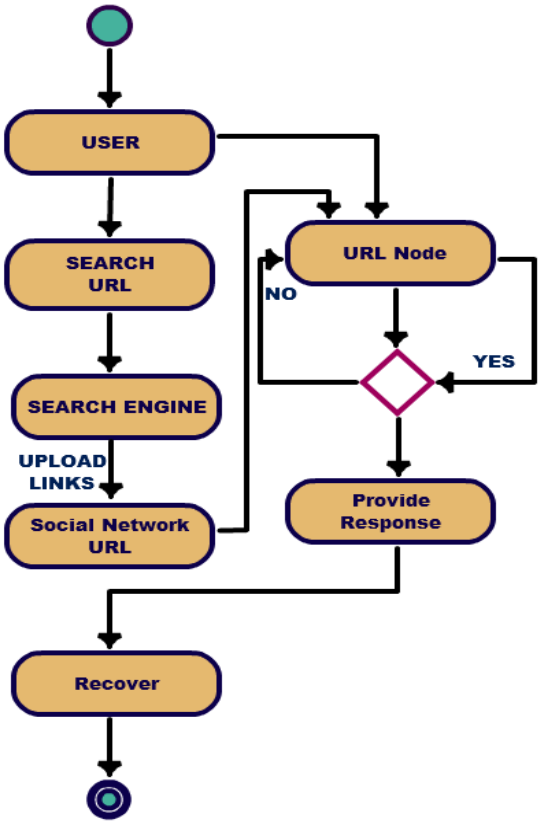
Phishing is a form of cyber-attacks that leverages social engineering approaches and other sophisticated techniques to harvest personal information from users of websites. The average annual growth rate of the number of unique phishing websites detected by Anti Phishing Working Group (APWG) is 36.29% for the past six years and 97.36% for the past two years. In this paper, we provide a systematic study of existing phishing detection works from different perspectives. We first describe the background knowledge about the phishing ecosystem and the state-of-the-art phishing statistics. Then we present a systematic review of the automatic phishing detection schemes. Specifically, we provide taxonomy of the phishing detection schemes, discuss the datasets used in training and evaluating various detection approaches, discuss the features used by various detection

schemes, and discuss the underlying detection algorithms and the commonly used evaluation metrics.

IV. ARCHITECTURE DIAGRAM



V. ACTIVITYDIAGRAM



VI. ADVANTAGES

- We discover that a search engine generates a propagation wormhole effect by delivering virtual virus sources to each community.
- The search engine gathers viruses from a global domain and serves as a virtual virus pool, and the propagation wormhole spreads those viruses across the whole network.
- We theoretically analyze the positive feedback epidemic model with and without the presence of a search engine.
- We find that virus propagation with the search engine has partial stability.

VII. DISADVANTAGES

- Which were utilized by the attacker? Search engines put illegal searching results before legal searching results.
- Search engines had no strict control ver advertisements and search results which were utilized by the attacker.
- This manipulated search results to increase advertising revenue, while allowing attackers to spread malicious codes.
- This caused many identities to be exposed.

VIII. CONCLUSION

With the proliferation of social networks and their ever increasing use, viruses have become much more prevalent. We investigate the propagation effect of search engines, and characterize the positive feedback effect and the propagation worm hole effect. The virtual virus pool and virtual infection paths that are formed by a search engine make propagation take place much more quickly. We show that propagation velocity is quicker, infection density is larger, the epidemic threshold is lower and the basic reproduction number is greater in the presence of a search engine. Finally, we conduct experiments that verify the propagation effect in terms of both infection density and virus propagation velocity. Results show the significant influence of a search engine particularly its ability to accelerate virus propagation in social networks.

REFERENCES

[1] Burton-Jones A, Straub D W.2006.“Reconceptualizig system usage: An approach and empirical test,” Information Systems Research (17:3), pp. 228- 246.

[2] Changsheng Hu, Zhiwen Guan, Liping Chen. 2008. “The impact of efficiency and satisfaction of staff on hospital information management, ” Medical Information (21:5), pp. 597-599.

[3] Chunan Wang. 2011. “The experience on nursing work in the condition of hospital information management, ” Nursing Practice and Research (8:14), pp.97-98

[4] He, C., Jin, X., Zhao, Z., & Xiang, T. (2010, October). A cloud computing solution for hospital information system. In Intelligent Computing and Intelligent Systems(ICIS),

[5] 2010 IEEE International Conference on (Vol. 2, pp. 517-520). IEEE

[6] Jiqing Yin, Min Wang, Huling Wang. 2006. "The effect of hospital information system in modern management of hospital, " Chinese Journal of Hospital Statistics (13:2), pp.170-171.