The Evolution of Phishing Scam

Student's name

Institution

Abstract

Phishing is a type of social engineering through which phishers execute attempts to retrieve users' credentials fraudulently. To achieve the goal, the attackers mimic electronic communication from a known public organization. The history of phishing scam starts in the year 1995. That time criminals were using emails to "fish" for essential data such as passwords among other identifiable information. Today, as technology advances financial institutions and banks as well as gaming sites and social media are the primary targets for attackers. There are different types of phishing that goes beyond the use of emails including SMS, VOIP, and social networking. Such kind of phishing includes clone phishing where criminals create a cloned email. Since its invention, phishing is a force to reckon with as no appropriate security measure that has proven to be effective in terms of detection and prevention.

Keywords: phishing, scam, security, attack.

Introduction

Today we are living in a swiftly changing world powered by technological advancement through innovation. Technological advancement is an essential element in our lives today for both social and economic development. However, despite the numerous benefits of technology it has its related shortcomings, such includes phishing scam. However, this sort of scam has not been a force to fight rights from the beginning. By definition, phishing is a sort of social engineering attack through which criminals utilizes spooned emails as a way of tricking targeted victims in sharing sensitive information such as personally identifiable information (Bergholz, De Beer, Glahn, Moens, Paaß, & Strobel, 2010). Besides, attackers can also install malware on the victims' computers. On the other hand most victims are tricked to believe that the emails are from a trusted brand but in reality, the emails were the work of criminals. Unlike another form of cybercrime which targets the system that people use, phishing scam targets the users of the system. Today, phishing scam have cleverly circumvented a considerable number of firms' security measures. This type of cyber violation is an issue of concern as it is difficult to counter. Because it doesn't matter the number of encryption software or security firewall the organization has as long as the person behind the keyboard falls a victim the attack materializes.

History of phishing

The origin of the concept and the term phishing has its origin in the mid-1990s via AOL (America Online). During this time America online was the best provider of internet access then (Ones, 1998). As of such millions of were in need of the services and they logged on for the services the platform offered each day. As there was no any legitimate competitor, it brands monopolized. And due to its popularity by default, it becomes a natural choice. Since the invention, malicious people and hackers used the platform for communication. As of such, they

formed an association known as warez community. Those were the people who made the first attempt to execute a phishing attack. One of the methods used was defining algorithms that would create credit card number randomly. Besides, they could steal sensitive information from users such as passwords (McCall, 2007). These criminals could strike jackpot most often to cause considerable damage. The random credit card number that the hacker could generate was used to open an account with AOL. The created account could then be used for wide range activities such as spamming other users. The specific program such as AOHell was used to simplify the process. The company didn't take long before stabling security measures to halt the use of randomly created credit card numbers to create fake accounts.

Phishing scams evaluation

In the year 2001 phishers focused their attention to a different kind of attack targeting the online payment systems. The first victim of this type of attack was E-Gold. However, it was not successful though this was a clear indication of security threat. At the end of 2003 phishers had registered several domains with false appearance (Deeb Al-Mo, Wan, Al-Saedi, Altaher, Ramadass, Manasrah, & Anbar, 2011). Some of the sites appeared as legitimate sites such as PayPal and eBay. Hackers used worm programs to root out spoofed emails to target customers who used PayPal. As a result, customers were being directed to spoofed sites where they could be tricked to update credit card information alongside with other personal information. Early 2004 phishers had attained a significant success rate as they had managed to penetrate banks sites as well as their customers.

Phishing example

With time phishing has evolved to have different subcategories and methods. However, regardless of the various techniques and category, the primary objective of a phisher is to fool people to give up their personally identifiable information. One of the primary tools the phishers use to trade is the mail to target busy and stressed workers of successful organizations who might be easily tricked to click before thinking. Despite the presence of numerous technology and software of protecting organizations, information hackers are always up-to-date with emerging technology to exploit any weakness within the systems. An example of phishing scam is the "breach of the retail giant's network" (Jarvis, Milletary, & Unit, 2014). This cyber breach was executed in the year 2014, and as a result of a phishing attack, a total of one hundred and ten million credit card were compromised (Khonji, Jones, & Iraqi, 2011). The phishing scam was executed on an air conditioning company; the company had maintained retailer's Pennsylvania outlets. Besides, had access to target victim vendor database. A worker of Fazio Mechanical intentionally or unintentionally clicked an active malicious link unbeknownst that his PC was hacked. As a result, his credentials were compromised, and from them, they were able to access the target, and in four-month time they were able to execute the attack. Even though the victim managed to recover from the damage caused several other victims have not been lucky.

Conclusion

Even though numerous preventive methods and techniques have been fronted to counter phishing, it is still of paramount importance to consider the use of artificial intelligence as part of the remedy to the problem of a phishing scam. Blending phishing preventive security measures with artificial intelligence will contribute to a long-lasting solution. Such security measure will provide the capacity to detect or predict phishing mail while in online mode. When integrated

with other technologies such as ECosk (Evolving connectionist system) (Kasabov, & Song, 2002). It will be much easier to gather knowledge in regards to neural networks. And thus enabling the security to monitor phishing scams continuously and in time to adapt their functionality and structure through continuous relation with other systems as well as the environment. The framework uses hybrid unsupervised or supervised learning and hence incorporating the concepts of fuzzy logic and machine learning regarding the level of similarity between phishing mails features.

References

Almomani, A., Wan, T. C., Altaher, A., Manasrah, A., ALmomani, E., Anbar, M., ... & Ramadass, S. (2012). Evolving fuzzy neural network for phishing emails detection. Journal of Computer Science, 8(7), 1099.

Bergholz, A., De Beer, J., Glahn, S., Moens, M. F., Paaß, G., & Strobel, S. (2010). New filtering approaches for a phishing email. Journal of computer security, 18(1), 7-35.

Deeb Al-Mo, A. A., Wan, T. C., Al-Saedi, K., Altaher, A., Ramadass, S., Manasrah, A., ... & Anbar, M. (2011). An online model for evolving phishing e-mail detection and classification method. Journal of Applied Sciences, 11, 3301-3307.

Fette, I., Sadeh, N., & Tomasic, A. (2007, May). Learning to detect phishing emails. In Proceedings of the 16th international conference on World Wide Web (pp. 649-656). ACM.

Jarvis, K., Milletary, J., & Unit, D. S. C. T. (2014). Inside a targeted point-of-sale data breach. Last accessed August, 20.

Kasabov, N. K., & Song, Q. (2002). DENFIS: dynamic evolving neural-fuzzy inference system and its application for time-series prediction. IEEE Transactions on fuzzy systems, 10(2), 144-154.

Khonji, M., Jones, A., & Iraqi, Y. (2011, February). A novel Phishing classification based on URL features. In GCC Conference and Exhibition (GCC), 2011 IEEE (pp. 221-224). IEEE.

McCall, T. (2007). Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks. Stephane GALLAND.

Ones, C. (1998). Third and Fourth Genders in Native North America. New York: Saint Martin's.

Saberi, A., Vahidi, M., & Bidgoli, B. M. (2007, November). Learn to detect phishing scams using learning and ensemble? methods. In Proceedings of the 2007 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology-Workshops (pp. 311-314). IEEE Computer Society.