Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International journal of advanced research in computer science
CASE STUDY
Available online at www.ijarcs.info

Defending Against Phishing: Case Studies

Shweta Sankhwar and Dhirendra Pandey
Department of Information Technology
Babasaheb Bhimrao Ambedkar University,
Lucknow (U.P.) India

Abstract: Phishing is characterized as a strategic and well execute engineering approach that use fraudulent means to acquire confidential and sensitive information from an unsuspecting online user. A phishing attacker is motivated by the need to acquire important login credentials and other sensitive data such as banking details, credit card number, and social security number among others. Phishing attacks are normally perpetrated using enticing email messages and fake URLs. Phishing attackers exploit the ignorance and the low level of awareness among online users concerning the online usage behavior. When perfectly executed, a phishing attack leads to serious cases of fraud and huge financial losses. An attacker has managed to execute the attack by exploiting an already established level of trust with online users. Nevertheless, a phishing attack can be avoided by ensuring that online users are equipped with the necessary knowledge about browsing behavior. Additionally, the implementation of a variety of anti-phishing software greatly helps to detect and eliminate possible cases of phishing attack. This paper discusses five cases of phishing attack with a focus on how they were perpetrated and the parties involved in the attacks. A detailed discussion of the consequences and the methods used to detect and prevent a phishing attack are also discussed.

Keywords: Phishing, E-mail phishing, Information security, vulnerabilities, web security.

1. INTRODUCTION

Phishing is similar to fishing in a lake, but instead of trying to capture a fish, a phishing attacker attempt to steal personal information. Phishing attacks are perpetrated using luring email messages, website forgery, redirection of traffic, and evading filters among others. The attackers send out e-mails that appear to come from legitimate websites such as eBay, PayPal, or other online and e-commerce organizations. The e-mails prompt the user to provide the login details, notably the username and password with the aim of updating personal information. Some e-mails will ask the user to provide even more information, such as full name, address, phone number, social security number, and credit card number. However, upon visiting the false website and just entering the username and password, the phishing attacker may be able to gain access to personal information by just logging into the account. Phishing attacks are strategically and well executed such that victim is unaware of the attack. According to a 2016 security report prepared by Verizon, organized crime groups perpetrate almost 90% of phishing attacks [1]. The majority of phishing attacks culminate in the disclosure of private personal information whereby the attack is conducted within a matter of minutes. Nowadays there are so many cases of phishing attacks, which happens because the majority of online users are unaware and do not have adequate on how to use various online platforms and websites.

The purpose of this paper is to provide a descriptive and research based case study of five phishing attack cases with a focus on how the attack was perpetrated and the consequences of the attack.

Case 1:

Phishers craft the replica of legitimate website and lure the naïve user to steal their confidential information. As shown in Figure.1 a website that has been the subject of a phishing attack, whereby the majority of the website contents have been tampered with.

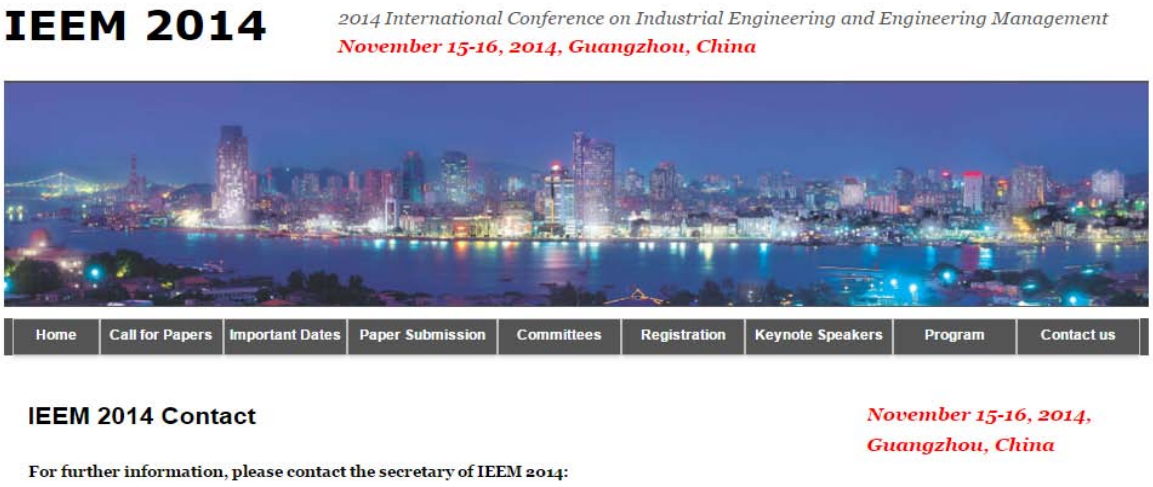

Figure 1: Snapshot of the phished/fake webpage of legitimate Conference series

This compromised webpage shown in Fiure.1 was the replica of reputed conference website. Phishers targeted the research students interested to submit their research work on that repute conference website by spreading link of replica website or by redirecting them to fake website. Phishers charged publication fees of submitted articles and fooled innocent students. Many Students faced money, time and efforts loss by this phishing attack. The attacker has managed to JavaScript code to the website the consequently has altered the address bar. The phishing attack has been implemented through a piece of code that has managed to disable the flash and multimedia content on the web page. It is highly likely that the attacker's intention was to get into the backend of the website and retrieve important personal information. According to Dede, the phishing attack was most likely perpetrated through website lures whereby the unsuspecting user was enticed to click on a link with malicious malware [2]. A careful examination of the phishing attack indicates that the attacker used the pharming technique to perpetrate the attack. The pharming technique involves the user hijacking the domain name and injecting poison into the domain name system [3]. The intention is to redirect the users to a specific website, which in this case is a Chinese based URL.

Case:-2

Most phishing attacks start with a spoof email that appears to come from a legitimate organization and thus the user is unable to find any difference because of its appearance. There was a case registered in which a 3rd-party cloud service notably Dropbox was targeted by attackers to accomplish the intended action. It is an innovative tactic developed by hackers to deliver malicious content through the network

DropBox is a file hosting service that allows users to create a special folder on their computers. The data stored in that folder can be accessed from the Dropbox site and mobile app anytime. This service is free up to a limited storage size. In DropBox, the attacker sends emails that link to a supposed invoice on Dropbox. The Dropbox link itself was legitimate, only it led to a .zip file containing a source file, not an invoice. Dropbox after detecting this type of false data can shut down this type of abuse, but it is proven to be a great method for attackers to get past spam filters. Dropbox use is so trustworthy that most organizations will not block its links.

Case: -3

This is the 21st century whereby people spend more and more time on social networking sites, which means they are busy in virtual life rather than real life. People interact with the online friends and they trust them a lot without confirming their real identity. Here it becomes a strong point for the attacker to perpetrate an attack. Hackers could harm the system and could acquire sensitive information for several misuses. The pertinent question that arises, how the attack is perpetrated? The following is a detailed explanation.

There are so many social networking sites on the internet like Facebook, Twitter, LinkedIn, Instagram, SnapChat, and WhatsApp among others.

Now attacker copies the source code of the login page of social networking site and creates a fake login web page of that networking site. The attacker then hosts that fake login page, which looks exactly like the original page of the social networking site with few changes or spelling mistake. A good example is -www.facedook.com whereas the original URL is www.facebook.com. There are many more sites, which are hosted with some changes in original page domain name and a normal user does not easily detect this change. After hosting of that page

I. The attacker creates a shortcut on a desktop in a computer used in a public place like a cyber café that is frequented by many users come on a daily basis. The attacker creates the name of shortcut to mimic the name of a web browser so that when the user opens that it directly opens the fake page created by an attacker. When the user provides the login details, notably the username and password these details are received in the attacker's inbox.

   The attacker creates an email spoof with messages that read like

- You have a new friend request.
- Your account needs some updating.
- You are tagged in a new photo. "To like the photo, click on above link."

Upon clicking on the luring message or link, the user is prompted to provide the login details, which are eventually revealed to the attacker.

Case: -4

Today, there are many cases of phishing attacks not only on social networking sites, but also in the majority of online financial and e-commerce platforms. The majority of financial institutions has migrated their operations to online platforms, thereby increasing the probability of being attacked by hackers and phishing attackers. In an online banking platform, the attacker is able to create email spoofs and send them to bank customers asking for login credentials for accessing their bank accounts. The e-mail looks so genuine that it entices users to click on the URL given in the spoofed mail, which lead to a fake web page that closely resembles the official site. Upon providing the requested login credentials, the attacker is able to fetch confidential information about the banking details of the unsuspecting customer. In one particular case, a big fraud was discovered when unsuspecting clients were sent fake emails that ended up enticing them to reveal confidential information. The information security manager discovered the fraud after analyzing the emails to ascertain that they did not originate from within the bank.

Case: -5

The rate at which technological innovations are advancing is very high and so does the level of expertise of fraudsters and hackers. Modern phishing attackers are now using sophisticated tools to implement their attacking endeavors. Attackers are able to infiltrate an organization and establish a high level of trust with the people working there. In one particular case, the attacker used the name of RBI and created an email spoof. In an email, the attacker attached an MS Word file that appeared like it came from RBI with a genuine RBI logo. The file had an enticing message that reads;

"The Foreign Exchange Transfer Department (RBI) hereby bring to your attention of the payment of your deposited funds here in the RBI, you were listed as a beneficiary in the recent schedule for payment of the past edition email/SMS award incurred by the BRITISH GOVERNMENT, which is yet unclaimed up-till date due to some circumstance". In the message, the amount was expressed in the form of 4 crores 48 lacs rupee. At the end of the message, the attacker was asking customers to provide their bank account number, personal

details, and email address. This way the attacker was able to obtain important information from the customers and consequently used to perpetrate a fraud.

2. CONSEQUENCES

The editor in chief at Help Net Security classifies identity of theft as one of the most serious consequences of phishing [4]. In the case described in Figure 1 the attacker has managed to take control of the DNS subsequently assuming the identity of the legitimate owner of the website. The intention is to retrieve personal information about the schedule of the technical program. Goes on to add that the intention of a phishing attacker is to steal confidential data, such as personal emails and credit card numbers. The phishing attack has also culminated in the denial of service because users are unable to visit various parts of the website. In this context, the attacker has injected malware code that has concealed all the multimedia content in the website. The ultimate result creates confusion among users and loss of loyalty. From a business perspective, a phishing attack has the potential of damaging the reputations from the side of the customers. [5]

3. PREVENTION AND REMOVAL

Even though there are a wide variety of tools and techniques used for removing malicious software in a phishing attack, the best strategy is to ensure that the phishing attack does not take place in the first place. In other words, the best strategy towards the prevention of a phishing attack is to implement a comprehensive and strong security mechanism for the entire web framework. [4] Places more emphasis on the need to educate employees rather than implementing technical controls. Website users need to be sensitized to how to approach potential phishing cases by handle luring messages with the best care possible. Additionally, users need to be taught how to read and interpret the URLs and luring links in a website.

Technique anti-phishing approaches require the installation of anti-phishing software to help in the identification and elimination of phishing attempts. Strong security mechanisms, both on the server and browser side are essential for thwarting the majority of phishing attacks. Securing a website with SSL and PKI cryptographic mechanisms will also help in the prevention of phishing attacks [1]. Also recommends the installation of a monitoring tool that will assist in the identification of malicious software in a web page. Continuous monitoring of a web page core structure helps to understand the file organization mechanism thus is in a position to identify any anomalies. An additional measure involves the implementation of regular sessions of integrity checks of the entire file directory system. [1] Maintains that an integrity check assists in the identification of files and folders that have been added to the website directory. Nevertheless, the most important element to note is that the use of technical tools to prevent phishing attacks is not entirely enough. Phishing attackers exploit the weakness in human capacity and thus web users should be given continuous education and awareness on how to avoid phishing cases. Anti-phishing software such as Kaspersky will provide the user with the necessary security level for alerting and stopping potential phishing attacks.

4. CONCLUSION

A phishing attack has the potential of not only rendering a website inoperable but also creating a massive fraud and loss of personal data among unsuspecting users. The five cases described in this paper show the extent in which phishing attackers were able to access confidential information and perpetrate fraud. The cases illustrate that majority of phishing attacks is perpetrated due to ignorance and lack of knowledge among the users. The majority of phishing attacks is initiated using email spoofs and luring messages on web platforms and social media sites. Users are required to be extra careful and advised to desist from clicking on luring messages and links that appear to be suspicious. Additionally, information security personnel in financial institutions are advised to conduct regular monitoring and audit of a web directory to identify potential cases of fraud. The implementation of anti-phishing tools is also an important measure that helps in the detection and removal of phishing threats and malicious software. A comprehensive monitoring and reporting mechanism also helps information security personnel to keep track of potential cases of phishing attacks within the organization. Most importantly, online users are supposed to be equipped with the necessary knowledge that can help them to detect and evade phishing attacks.

REFERENCES

1. Dede, D. (2014, November 21). Website Malware Removal: Phishing. Retrieved from https://blog.sucuri.net/2014/11/website-malware-removal-phishing.html
2. Bisson, D. (2016b, June 5). 6 Common Phishing Attacks and How to Protect Against Them. Retrieved from https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/
3. Bisson, D(2016a, April 28). Takeaways from the 2016 Verizon Data Breach Investigations Report. Retrieved from https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/takeaways-from-the-2016-verizon-data-breach-investigations- report/
4. Zorz, M. (2012, December 24). Phishing techniques, consequences and protection tips. Help Net Security. Retrieved from https://www.helpnetsecurity.com/2012/12/24/phishing-techniques-consequences-and-protection-tips/
5. D Pandey, V Agarwal," E-commerce Transactions: An Empirical Study" International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 3, March 2014 ISSN: 2277 128X

