Magnum Opus Of Phishing Techniques

Ronnie T Baby, V. Ebenezer, N. Karthik

Abstract: As time evolved, the definition of phishing has taken drastic meanings supported by various subsections or type of phishing technique available around the internet and used commonly by spammers and black hat hackers. Phishing has found its roots long back from the starting of the internet and was actively used to target incautious users and continues to be used even now in various forms. In this paper, we review types the various phishing techniques available online and suggest preventive measure against them.

Index Terms: Web Security, Privacy, Phishing Detection, Phishing Methodology, Random Forest Algorithm

1. INTRODUCTION

HACKERS derived phishing from the term 'fishing' which typically meant as hackers were trying to 'fish' out the username and password of victims [1]. A phishing attack usually comes in the form of a declaration intended to persuade you to:

1. Access a document
2. Click on a link
3. Install software upon your device
4. Enter your username and password into a website that's made to seem valid.

Phishing is an apt example among many social engineering techniques being used to deceive online users. The first phishing technique was introduced around the 1980s and the term "phishing" was coined in and around the 1990s. The first recorded phishing attack was AOL phishing where; once the victim had revealed the password, the attacker could access and use the victim's account to commit covert transactions.

2 TYPES OF PHISHING TECHNIQUES

There are a certain variety of phishing techniques evolved over time. But most of them can be classified under two basic categories-

1. Deceptive Based Phishing Techniques
2. Malware Based phishing techniques

Deceptive Based Phishing mostly depends upon social engineering schemes, which depend on forged

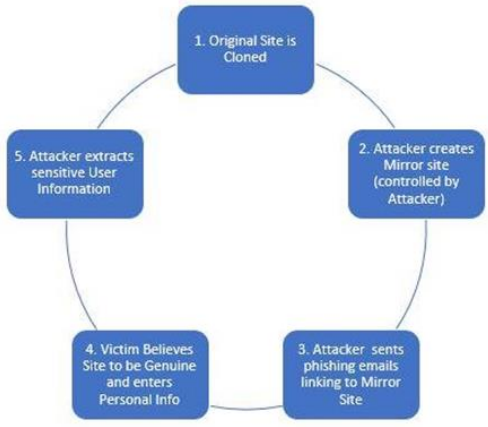

***Fig. 1**. Representation of a Sample Phishing Methodology*

1. Subsequently, such mails seem to convince the victim about the genuity of the message and pass on a link. The link may seem genuine to the victim, but in actual, the attacker would redirect the victim to malicious sites to harvest his credentials or steal user tokens (OTP, Nonce values) etc [2].

The second technique revolves around making the victim click on malicious code via embedded links and may also try to exploit the security loopholes in the system (in case of sudden 0-days). The code can run in a case by case basis and may be done with or without the user click on a link [3]. Sometimes, the attacker may trick the user to a legitimate site but it will be over a proxy controlled by the attacker; simply allowing the attacker to read the data passing through the network.

- *Ronnie T Baby, IV B. Tech CSE, Karunya Institute of Technology and Sciences, India, E-mail: ronnietbaby.work@gmail.com*
- *V. Ebenezer, Assistant Professor, Karunya Institute of Technology and Sciences, India,. E-mail: ebenezerv@karunya.edu*
- *N. Karthik, Assistant Professor, Karunya Institute of Technology and Sciences, India, E-mail: karthik@karunya.edu*

3 VARIOUS TYPES OF PHISHING ATTACKS

Now we will look at the different types of phishing attacks along with the methods which have evolved over time along with a study of a particular attack know as "Fullscreen API" attack and how it can be actively used to deceive Facebook users via Facebook mobile app's inbuilt browser.

3.1 Email Phishing

It is the bare minimum type of phishing example, which was employed heavily during the early 2000s but it still finds mention even today as it's used as a starting bait to any victim. A seemingly genuine email is sent to a victim to convince to click on an attacker-controlled link or give out sensitive details via fake websites [4]. Spear phishing is one of the types of email phishing where an attacker might send emails to thousands of people and motivate them to visit and click on fraudulent sites.

3.2 Domain Phishing

Hackers started buying out domain names which spelled similarly to well-known domain names. After registering the domain names, they can use send it via emails and convince the user to visit the site and leak user credentials. For example, the phisher may register the site name as thegoodsite.org instead of the genuine site name thegoodsite.com just by changing the domain extension. Most MNC's like Google and Facebook have prevented this type of attack by a great extent by already registering similar-sounding sites in their name. Also in case if the phisher manages to register such a domain name, ICANN recommends contacting Anti-Phishing Working Group (APWG) as it doesn't directly involve and is tasked only to deal with the registering of the domain name [5]. Another similar domain related issue is "Subdomain Takeover" where hackers may take control of the vacant subdomain which may have been forgotten by the website. Once the phisher takeover a subdomain, he can easily host his content on the subdomain within the genuine domain of the company. The best way to resolve subdomain takeover is to either, close the subdomain or drop the subdomain from the DNS entry of the site.

3.3 IDN Homograph Attack

This spoofing attack is also known as script spoofing and revolves around tricking visitors to believe they are in the original site via replacing domain URL via Unicode, Latin, Cyrillic and similar such characters which seem to replicate with the original URL of the site [6]. Internationalized domain name is exploited with the fact that many different characters look alike and they are homographs of each other. The recent example of active attacks via IDN homograph attacks was when hackers set up a fake site adoḅe[.]com and used this to spread Beta Bot which firsts disables security software and then executes malicious functions [7]. Major browsers like Chrome, Firefox, and Opera have homograph protection mechanism enabled to warn users; which immediately show the original fake site URL instead of deception. A simple way to limit the damage from bugs such as this is to always use a password manager.

3.4 Voice Phishing

Voice phishing has effectively become more sophisticated in the past years. With improvements in automation and voice recognition, hackers can now robot generated voices and human callers to more imitate well-known brands and easily convince victims to believe that the call came from genuine sources. There are several voice changing applications available online which allows easy manipulation of the voice.

3.5 Whaling

Whaling is a similar technique which involves sending emails, but only to "whales of the company" like CFO, CEO, Co-Founder, etc to harvest quick and accurate information [8]. Most companies have policies in place to restrict such attempts but phishes have been successful on occasions and have extracted sensitive information from big corporate companies.

3.6 In-Session Phishing

In-session phishing involves around launching a pop-up window that pretends to have been opened from the targeted session but might be generated from the third party site. If the victim interacts with the popup window, the user session may be sent to the attacker. Continuous browser updates have made in session phishing methods near impossible to carry out but we can never say when an attack revives again.

3.7 Inception Bar Phishing Attack

We believe it is a derived variant of the fullscreen API attack (discussed below). When a user visits a site and then scrolls down via mobile, the attacker may screenshot any other site's URL and then using some web designing makes it feel, that the user is on a genuine page. It can definitely be argued that such attacks rely on the level of attention of the user and possibilities of carrying out the perfect covert operation, while the victim never gets wind that they are on a different site [9]. Such attacks mostly depend from browser to browser and it becomes the responsibility of the browser to fix and not of the site.

3.8 Fullscreen API Attack

Fullscreen API Attack takes help of fullscreen application programming interface in HTML5 in order to carry out advanced phishing attacks [10] . The Fullscreen API allows web developers to show content that fills up the user's screen completely [10]. Using this method, an attacker can deceive a user to click on any button or any link and then trigger fullscreen mode viaelementToMakeFullscreen.requestFullScreen();

Since the restrictions for fullscreen API is such that it can be triggered only via a click or keypress. So the attacker can go to fullscreen mode and use fake browser and OS UI and fool the victim. Same as in the case of Inception Bar Phishing Attack, the also is a browser issue and not of a site responsibility. Browsers have started to ask the user permission before going to fullscreen mode or apply an intermittent gap or animation before going fullscreen to prevent such attacks. Even though many users may get warned about it, there is still a small percentage of users who can easily fall victim to such attacks. A similar finding using the fullscreen API phishing method was reported to the Facebook security team, via its bug bounty program recently. The Facebook Android app has an inbuilt browser. The browser didn't employ any animation or warning when the user was

made to go in "FULLSCREEN MODE". This made it possible to mimic the UI of facebook's inbuilt browser and trick facebook users to give out sensitive info. Facebook rejected the finding claiming for the attack to work, the user must first click on a link a third party site which is totally true. But it is recommended to at least show some warning before going to fullscreen mode as all major browsers at least show some animation of or message that the user is in fullscreen mode.

4 PREVENTING PHISHING ATTACKS

According to the latest second-quarter report by APWG, the numbers have substantially increased from 2018 and most of the business email compromise (BEC) attacks were based on the gift card requests [11]. Webmail services and SaaS (Software-as-a-ServicePhishing and webmail services continued to be the biggest favourite among phishers.

Some recommendations to prevent phishing attacks are-

1. Deploy a SPAM filter that detects viruses or block emails originating from compromised sites . Gmail has inbuilt [3] spam detection mechanism which cautions the user if it believes the mail to be a part of spear phishing [12].
   Also, ensure that not to click on any links which come via untrusted sources. Keep an eye on shortened links and try to decode it before clicking. We can also deploy a web filter to block malicious websites .
2. Always be updated with the latest security patches and updates. Even in case if you fall victim to malware-based phishing, it may be prevented as the systems are all up-to-date. But in the case of deceptive phishing methods, it is not possible to prevent as mostly takes into factor the intelligence of the victim as to whether the message has come from a genuine source or not.
3. Keep an eye on the URL Bar. The URL (Uniform Resource Locator) is the single best way to ensure whether we are on an original site [13]. Ensure that the site has SSL enabled along with running on top of https and the certificates have not expired. Web admins can install free certificate authority like 'Lets's Encrypt' to enable transport Layer Security encryption at no charge.
4. Enable two-factor Authentication. Assume that in some cases, we fell for the phishing campaign and gave out our credentials to the attacker. Even under such case, the account may be secure, if we have enabled two-factor authentication. This will send an OTP to a user-controlled device which may prevent the phisher to log into the account as he can't predict the OTP.
5. Encrypt all sensitive company information using SDN. In case the company's employees get compromised via whaling or emailing phishing, the phisher can't decode the credentials as they are stored in an encrypted format [14]. So the attacker may only be able to obtain the hashed passwords. In case the attacker succeeds in cracking the hash value over time; by that time, the company can easily reset the password.
6. Implement machine learning techniques to detect phishing attacks. We may use the Random Forest 'Machine Learning Technique' to classify between genuine and fake emails [15]. We can train them via mock deceptive emails and it can evolve itself over time along with the sophisticated increase of the phishing methods.
7. Train employees. Conduct training sessions for all professionals having computer access with mock phishing scenarios and give clear SOP (Standard Operation Procedure) while opening and replying to any email from third party sources [16] .

5 CONCLUSION

In the paper, we have analyzed the different variety of phishing methods and some recommended methods to prevent them from being actively exploited. Even though a major amount of phishing attempts can be stopped via spam filters and employing machine learning techniques [17] ; still a few sophisticated phishing campaigns continue to be in-boxed to unsuspecting victims, and the onus is on them to finally decide whether to trust the sender or not.

REFERENCES

[1] Marc a. Rader and syed (shawon) m. Rahman, "exploring historical and emerging phishing techniques and mitigating the associated security risks", international journal of network security & its applications (ijnsa), vol.5, no.4, july 2013

[2] Minal chawla, siddarth singh chouhan "a survey of phishing attack techniques" international journal of computer applications (0975 – 8887) volume 93 – no 3, may 2014

[3] Claes adam wendelin "malware detection in secured systems" seminar future internet ss2017 lehrstuhl netzarchitekturen und netzdienste, doi: 10.2313/net-2017-09-1_11

[4] L. Joy singh "a survey on phishing and anti-phishing techniques" international journal of computer science trends and technology (ijcst) – volume 6 issue 2, mar - apr 2018

[5] Icann (https://www.icann.org/resources/pages/phishing-2013-05-03-en)

[6] Evgeniy gabrilovich, alex gontmakher "the homograph attack" communications of the acm 45(2):128 doi: 10.1145/503124.503156

[7] Betabot ((https://threatpost.com/idn-homograph-attack-spreading-betabot-backdoor/127839/)

[8] A. Mahalakshmi, n. Swapna goud, dr. G. Vishnu murthy "a survey on phishing and it's detection techniques based on support vector method (svm) and software defined networking(sdn)" international journal of engineering and advanced technology (ijeat) issn: 2249 – 8958, volume-8, issue-2s, december 2018

[9] James fisher, " the inception bar: a new phishing method " (https://jameshfisher.com/2019/04/27/the-inception-bar-a-new-phishing-method/)

[10] Feross aboukhadijeh, using the html5 fullscreen api for phishing attacks https://feross.org/html5-fullscreen-api-attack/

[11] Second quarter report, anti-phishing workingroup, https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf

[12] J. Vijaya chandra ; narasimham challa ; sai kiran pasupuleti, "a practical approach to e-mail spam filters to protect data from advanced persistent threat"

international conference on circuit, power and computing technologies (iccpct) doi: 10.1109/iccpct.2016.7530239

[13] Mohammed nazim feroz ; susan mengel ,“phishing url detection using url ranking” 2015 ieee international congress on big data doi: 10.1109/bigdatacongress.2015.97

[14] Tommy chin, jr., kaiqi xiong, chengbin hu “phishlimiter: a phishing detection and mitigation approach using software-defined networking” ieee access doi 10.1109/access.2018.2837889

[15] E. G. Dada and s. B. Joseph “random forests machine learning technique for email spam filtering” university of maiduguri faculty of engineering seminar series volume 9 number 1, july 2018

[16] Bolkas pavlos panagiotis “a survey about attack and defence phishing techniques” doi: 10.13140/rg.2.2.32605.31204

[17] Ram basnet, srinivas mukkamala, andrew h. Sung, “detection of phishing attacks: a machine learning approach” studies in fuzziness and soft computing 226:373-383 doi: 10.1007/978-3-540-77465-5_19