Journal of Engineering Sciences
Vol 11, Issue 6,June/2020
ISSN NO:0377-9254

PHISHING

Dhruti Sanghani[1], Monika Shah[2], Pooja Jain[3] and Vivek Dave[4]

[1]*Student of MCA Department, Parul University, India*

[2]*Student of MCA Department, Parul University, India*

[3]*Student of MCA Department, Parul University, India*

[4]*Prof. of MCA Department, Parul University, India*

***Abstract*— This Phishing is a form of social engineering or website forgery whereby attackers mimic a trusted website or public organization or sending in an automated manner in order to steal sensitive information or credentials of online users. Many anti-phishing schemes are there but Phishers still find their ways for breaking the existing techniques.**

***Keywords*— Put Phishing, steal sensitive information, online users, anti-phishing, break existing technique.**

1. INTRODUCTION

The term phishing is a general term used for criminals of e-mails and websites – designed to look like they come from well-known, trusted businesses, financial institutions and government agencies.

These criminals use Internet users into disclosing their bank information or other personal data such as usernames and passwords, or into unwittingly downloading malicious computer code onto their computers that can allow the criminals subsequent access to those computers or the user's financial accounts.

1.1 TYPES OF PHISHING

1.1. 1 Email Spoofing – Name Impersonation

In e-mail spoofing as soon as the user click on the link attached in the e-mail user's data is spoofed by the phisher (individual attack).

1.1.2. Mass Target – Brand Impersonation

Mass phishing attacks are the emails sent to a group of people with some common interest and choices. In mass phishing attacks, by single email sent to potential victims are clones of transactional emails 1ike receipts, payment reminders, or gift cards.

1.1.3. URL Phishing

In URL phishing attacks, scammers use the phishing page's URL to steal the target information.

- **Hidden link**

One way to target a person with phishing attack is by using a hidden link. We all receive emails with the action phrase "CLICK HERE" or "DOWNLOAD NOW" or "SUBSCRIBE."

- **Tiny URL**

Other way to hide phishing links is by using link-shortening tools like Tiny URL to shorten the URL and make it look authentic and trusted.

- **Misspelled URL**

Instead of tiny URLs, Phishers may also use misspelled URLs. Hackers buy domains which sound similar to popular websites. Then, phisher phish users by creating an identical website, where they ask users to log in by submitting personal information.

- **Homograph attack**

In the example of the Amazon, when you click on the link, instead of 'amazon.com,' you will be redirected to 'a**rn**azon.com' – which belongs to the attacker. Once you open the attacker's site, the fake page will prompt you to enter login credentials or financial data like credit card information or other personally identifiable information.

1.1. 4. Subdomain Attack

These types of phishing scams mostly target at non-technical people. Scammer's open up the lack of understanding about the difference between a domain and a subdomain to release phishing attack.

1.1.5. Pop-Up Messages: In-Session Phishing

Pop-up messages are the easiest way to run a successful phishing attack. With the help of pop-up messages, attackers get a window to steal the login details by redirecting them to a fake website.

1.1.6. Search Engine Attack

The link is set through the search engines. If we search anything from that particular search engine on which the Phishers have targeted our information is steeled.

Phishers create unauthorized websites with "Exclusive offers" which look too good to be true! When users open upon these fake sites, they are fooled by sharing their information.

1.1.7. Website Spoofing

Website spoofing is similar to e-mail spoofing, though it needs the attacker to put in a lot more effort.

1.1.8. Scripting

Scripting (XSS) uses malicious scripts deployed on the user's computer or phone using emails as the medium.

1.1.9. Man-in-the-Middle Attack

In Man-in-the-Middle attack– MITM, MiTM, MiM, or MIM – attack, a malicious actor intercepts online interaction between two parties. Hackers also impersonate themselves by both sides to access confidential information like transactions, conversations, or other data.

1.1.10. Clone Phishing

In clone phishing attack, a previously-sent email containing any link or attachment is used as a true copy to create almost identical or cloned email.

1.1.11. Image Phishing

In this type of phishing, linking the image directly to the URL and sending it to the targeted victim's in a group or mass.

1.1.12. Voice Phishing Attack

In voice phishing or vishing attack, the message is orally communicated to the targeted victim.

This is one of the trickiest types of phishing – you have nothing to confirm or verify about what is said over the phone!

2. LITERATURE REVIEW

Email based attack where phisher masquerade emails to appear as a legitimate request for personal and sensitive information is known as phishing. Now a day's phishing attacks are known as "spear phishing," are a type of highly targeted email attack to organizations and it appears genuine to employees within the organization. Spear phishing emails have mostly similar features as early generations of phishing scams, but are more contexts specific. It seems to have originated from an organization, for creating more relevance in the sender entity. Many spear phishing emails uses text-based messages rather than the more elaborate visual messages normally encountered in financial phishing instances. Therefore, the tactics employed to persuade recipients to give information and cues that signal the nature of deception remain similar as those for earlier generations. This type of phishing adds context to the attack and, becomes an effective tool for scammers.

3. APPLICATION AREAS

3.1 SOCIAL NETWORKING ON MOBILE

Due to the rise in the number of users accessing the Internet through smart phones, social networking websites have expanded their services on smart phones, including messaging, chatting, photo viewing, etc.

3.2 LIVE CHAT

In November, Symantec observed that five percent of the targeted applications were on live chat and among them adult sex chat was the most common target.

3.3 BLOGGING

Phishing websites that attacked blogging in social networking comprised 23 percent of all targeted applications.

3.4 GAMING

In 2009, gaming has become an increasingly popular aspect of social networking.

Symantec evaluated gaming and found that it comprised 13 percent of the targeted applications.

4. METHODOLOGIES

4.1 EMAIL AND SPAM

Mostly the phishing attacks are done through email.

Phishers can send emails to valid email addresses by using the techniques and tools by spammers

4.2 WEB-BASED DELIVERY

In this type of attack, it is carried out by targeting the customers through the third party website.

4.3 IRC AND INSTANT MESSAGING

IRC and IM clients are allowing for embedded dynamic content. The attackers send the fake links to the users through IRC and IM.

4.4 TROJANED HOSTS

Trojan is a program that gives complete access to host computer to Phishers after being installed on the host computer.

Phishers will make the user to install the Trojaned software which helps in email propagating and hosting fraud websites.

5. TECHNIQUES

5.1 LINK MANIPULATION

Link manipulation is a phishing attack done mainly to miss-lead the user to a fake website or a "look-a-like" of some renowned site. The main trick used in this type of phishing is use of sub-domains.

5.2 FILTER EVASION

Phishers have used anti-phishing filters to detect text commonly used in phishing emails.

5.3 WEBSITE FORGERY

If a victim visits the Phishing website deception is not over. Some Phishers uses java scripts commands in order to alter the address bar.

5.4 PHONE PHISHING

phishing is a form of criminal phone, using social media over the telephone system to get the access to personal and financial information.

6. CONCLUSION

This data has helped me to understand how Phishers actually behave and some of the methods they employ to lure and trick their victims. We have learned that phishing attacks can occur very fast, with limited time between the initial system intrusion and a phishing web site going online with supporting spam messages to advertise the website, and this speed can make such attacks hard to recognize and prevent. IP address blocks host or small business DSL addresses appear to be particularly popular for phishing attacks, because the systems are less well managed and not always up to date with current security patches. Also because the attackers are less likely to be traced than when targeted major corporate systems. Simultaneously attacking many smaller organizations also makes incident response harder. We have observed that end users regularly access phishing content, presumably through receiving spam messages, and a surprisingly large number appear to be at risk from becoming victims of such attacks

REFERENCES

WEBSITE

[1] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-rprt-phshng/archive-rprt-phshng-eng.pdf

[2] https://blog.syscloud.com/types-of-phishing/

[3] https://www.slideshare.net/defquon/phishing-4909625

[4] https://www.symantec.com/connect/blogs/phishing-applications-social-networking-websites

[5] www.slideshare.net/kranthi0987/phishing-ppt

BOOK

[6] Phishing for Pools: The Economics of Manipulation and Deception By George A.Akerlof, Robert J.Shiller

[7] Phishing cutting the identity theft line By Rachael Liniger, Russell Dean vines