IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

A Study on Various Phishing Techniques and Recent Phishing Attacks

Bhagya Bajanthri[1] and Mr. Sayeesh[2]
Student, Department of Computer Science and Engineering[1]
Assistant Professor, Department of Computer Science and Engineering[2]
Alva's Institute of Engineering and Technology, Mangalore, India

Abstract: *Now-a-days internet has become a very unsafe space to deal with. Hackers are constantly trying to gain the user's personal information, and detailed credentials. So many websites on the internet, even though safe, this safety cannot be assured by all websites. These rule breakers avoid abiding by rules, and try to employ methods like trickery and hacking to gain illegal access to private information. To be able to overcome this problem, we need to first understand the intricacies of how the virus is designed. This paper mainly deals with the different phishing techniques and recent phishing attacks that took place during COVID 19. like Link Manipulation, Filter Evasion, Website Forgery, Phone Phishing and Website Forgery. We have also studied a subtle method to perform phishing attacks that makes links appear legitimate, but actually redirect a victim to an attackers website called Convert Redirect. In this paper, we present some phishing examples like Paypal phishing which involves sending an email that fraudulently claims to be from a well known company and Rapidshare Phishing where in the spoofed web page, phishers attempt to confuse their victims just enough to entice them to enter their login name and password. To perform these types of phishing the Phishers uses so many phishing techniques like Link Manipulation, Filter Evasion, Website Forgery, Phone Phishing and Website Forgery. Phishing techniques include the domain of email messages. Phishing emails have hosted such a phishing website, where a click on the URL or the malware code as executing some actions to perform is socially engineered messages. Lexically analyzing the URLs can enhance the performance and help to differentiate between the original email and the phishing URL. As assessed in this study, in addition to textual analysis of phishing URL, email classification is successful and results in a highly precise anti phishing. From the thorough analysis of the research paper, we have understood how phishing attacks work and the different methods employed to carry out the attack. Also, we have studied some of the most recent phishing attacks and measures taken by the authorities to overcome and prevent any such attacks in future.*

Keywords: Phishing Attacks.

I. INTRODUCTION

Phishing is a term to refer to the cyber-attack which involves an attacker trying to acquire their victims' sensitive or confidential information through electronic communication by pretending to be a trusted party. Most phishing attacks start with sending fraudulent messages claiming to be from a trusted organization and are often made to seem similar to the legitimate one, causing it hard to be distinguished by the users. Phishing is often used to learn someone's password or credit card information. With the help of email prepared as if coming from a bank or official institution, computer users arc directed to fake sites. In general, the information that is stolen by a phishing attack is as follows:

- User account number
- User passwords and username
- Credit card information
- Internet banking information

In the field of computer security, Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is a fraudulent email that attempts to get you to divulge personal data that can then be used for

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

illegitimate purposes. There are many variations on this scheme. It is possible to Phish for other information in addition to usernames and passwords such as credit card numbers, bank account numbers, social security numbers and mothers' maiden names. Phishing presents direct risks through the use of stolen credentials and indirect risk to institutions that conduct business online through erosion of customer confidence. The damage caused by Phishing ranges from denial of access to email to substantial financial loss.

This report is also concerned with Phishing techniques. There are several different techniques to combat Phishing, including the information about the recent phishing attacks. No single technology will completely stop Phishing. However, a combination of good organization and practice, proper application of current technologies and improvements in security technology has the potential to drastically reduce the prevalence of Phishing and the losses suffered from it. software and computer programs are designed to prevent the occurrence of Phishing and trespassing on confidential information. Phishing software is designed to track websites and monitor activity; any suspicious behavior can be automatically reported and even reviewed as a report after a period of time. This also includes detecting Phishing attacks, how to prevent and avoid being scammed, how to react when you suspect or reveal a Phishing attack and what you can do to help stop Phisher. The simplified flow of information in a Phishing attack is:

1. A deceptive message is sent from the Phishcrs to the user.
2. A user provides confidential information to a Phishing server (normally after some interaction with the server).
3. The Phishers obtain confidential information from the server.
4. The confidential information is used to impersonate the user.
5. The Phishers obtain illicit monetary gain.

Steps 3 and 5 are of interest primarily to law enforcement personnel to identify and prosecute Phishers. The discussion of technology countermeasures will center on ways to disrupt steps 1, 2 and 4, as well as related technologies outside the information flow proper.

II. PHISHING TECHNIQUES

Phishers use a wide variety of techniques, with one common thread. Some of the techniques are explained in detail

2.1 Link Manipulation

Most methods of Phishing use some form of technical deception designed to make a link in an email appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains arc common tricks used by Phishers. In the following example, http://www.yourbank.example.com/, it appears as though the URL will take you to the example section of your bank website; actually this URL points to "your bank" (i.e. Phishing) section of the example website. An old method of spoofing used links containing the '@' symbol, originally intended as a way to include a username and password. For example, http://www.google.com@members. tripod, com/ might deceive a casual observer into believing that it will open a page on www.google.com, whereas it actually directs the browser to a page on mcmbcrs.tripod.com, using a username of www.google.com: the page opens normally, regardless of the username supplied.

2.2. Filter Evasion

Phishers have used images instead of text to make it harder for anti-Phishing filters lo detect text commonly used in Phishing emails.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

2.3 Ebsite Forgery

Once a victim visits the Phishing website the deception is not over. Some Phishing scams use JavaScript commands in order to alter the address bar. This is done cither by www.studymafia.org placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

2.4 Phone Phishing

Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number {owned by the Phishers) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice Phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

2.5 Website Forgery

Some phishing scams use JavaScript commands in order to alter the address bar of the Website. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL. An attacker can also potentially use flaws in a trusted website's own scripts against the victim. These types of attacks, known as cross-site scripting (XSS) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult lo spot without specialist knowledge. Such a flaw was used in 2006 against PayPal.

III. Convert Redirect

Covert redirect is a subtle method to perform phishing attacks that makes links appear legitimate, but actually redirect a victim to an attacker's website. The flaw is usually masqueraded under a log-in popup based on an affected site's domain. It can a fleet OAuth 2.0 and OpenID based on well-known exploit parameters as well. This often makes use of open redirect and XSS vulnerabilities in the third-party application websites. Users may also be redirected to phishing websites covertly through malicious browser extensions.

Normal phishing attempts can be easy to spot because the malicious page's URL will usually be different from the real site link. For covert redirection, an attacker could use a real website instead by corrupting the site with a malicious login popup dialogue box. This makes covert redirects different from others.

For example, suppose a victim clicks a malicious phishing link beginning with Facebook. A popup window from Facebook will ask whether the victim would like to authorize the app. If the victim chooses to authorize the app, a "token" will be sent to the attacker and the victim's personal sensitive information could be exposed. This information may include the email address, birth date, contacts, and work history. In case the "token" has greater privilege, the attacker could obtain more sensitive information including the mailbox, online presence, and friends list. Worse still, the attacker may possibly control and operate the user's account. Even if the victim does not choose to authorize the app, he or she will still get redirected to a website controlled by the attacker. This could potentially further compromise the victim.

This vulnerability was discovered by Wang Jing, a Mathematics Ph.D. student at School of Physical and Mathematical Sciences in Nanyang Technological University in Singapore. Covert redirect is a notable security flaw, though it is not a threat to the Internet worth significant attention.

IV. Phishing Examples

4.1 Paypal Phishing

In an example PayPal phish, spelling mistakes in the e-mail and the presence of an IP address in the link are both clues that this is a Phishing attempt. Another giveaway is the lack of a personal greeting, although the presence of personal details would not be a guarantee of legitimacy. A legitimate Paypal communication will always greet the user with his or her real name, not just with a generic greeting like, "Dear Account Holder." Other signs that the message is a fraud are misspellings of simple words, bad grammar and the threat of consequences such as account suspension if the recipient fails to comply with the message's requests. Note that many Phishing emails will include, as a real email from PayPal would, large warnings about never giving out your password in case of a Phishing attack. Warning users of the possibility of Phishing attacks, as

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

well as providing links to sites explaining how to avoid or spot such attacks arc part of what makes the Phishing email so deceptive. In this example, the Phishing email warns the user that emails from PayPal will never ask for sensitive information. True to its word, it instead invites the user to follow a link to "Verify" their account; this will take them to a further Phishing website, engineered to look like PayPal's website, and will ask for their sensitive information.

4.2 Rapidshare Phishing

On the Rapid Share web host, Phishing is common in order to get a premium account, which removes speed caps on downloads, auto-removal of uploads, waits on downloads, and cool down times between downloads, www.studymafia.org Phishers will obtain premium accounts for Rapid Share by posting at warez sites with links to files on RapidSharc. However, using link aliases like Tiny URL, they can disguise the real page's URL, which is hosted somewhere else, and is a look-a-like of Rapid Share's "free user or premium user" page. If the victim selects a free user, the Phishers just pass them along to the real RapidShare site. But if they select premium, then the Phishing site records their login before passing them to the download. Thus, the Phishers have lifted the premium account information from the victim.

Examples of Phishing Emails

Phishing e-mail messages take a number of forms. They might appear to come from your bank or financial institution, a company you regularly do business with, such as Microsoft, or from your social networking site. The main thing Phishing e-mail messages have in common is that they ask for personal data, or direct you to Web sites or phone numbers to call where they ask you to provide personal data. The following is an example of what a Phishing scam in an e-mail message might look like.

Example of a Phishing email message, which includes a deceptive Web address that links to a scam Website. To make these Phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Website, but actually takes you to a phony scam site or possibly a pop-up window that looks exactly like the official site. Phishing links that you are urged to click in e-mail messages, on Web sites, or even in instant messages may contain all or part of a real company's name and are usually masked, meaning that the link you see does not take you to that address but somewhere different, usually an illegitimate Website.

Notice in the following example that resting (but not clicking) the mouse pointer on the link reveals the real Web ad ress, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's Web address, which is a suspicious sign.

V. Recent Phishing Attacks

There are a lot of phishing activities taking place all over the world. The Attacks, more focused and efficient in making a mistake and talented and more sophisticated social engineering techniques to trick users. During this pandemic situation

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

there has been a large scale of phishing attacks taking place which is out of the government site and let us view some of the examples of recent phishing attacks and how it is affecting the people around the world.

1. Govt warns against large-scale phishing attacks using COVID-19 as bait

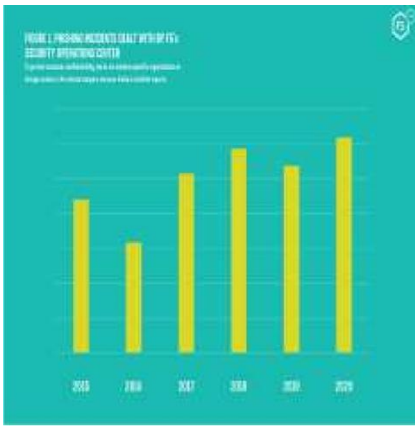
The government has warned against a large-scale attack against individuals and businesses, where attackers may use COVID-19 as a bait to steal personal and financial information. India's cybersecurity nodal agency, CERT-In has issued an advisory warning that the potential phishing attacks could impersonate government agencies, departments and trade bodies that have been tasked to oversee disbursement of government fiscal aid.

The attackers are expected to send malicious emails under the pretext of local authorities that are in charge of dispensing government-funded COV1D-19 support initiatives.

"Such emails are designed to drive recipients towards fake websites where they are deceived into downloading malicious files or entering personal and financial information," Indian Computer Emergency Response Team (CERT-In) said in its latest advisory dated June 19. The advisory noted that the "malicious actors" arc claiming to have 2 million individual/citizen email IDs and are planning to send email with the subject line: free COV1D-19 testing for all residents of Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad in a bid to coax users to disclose personal information.

"It has been reported that these malicious actors arc planning to spoof or create fake email IDs impersonating various authorities," it cautioned. CERT-In, in its advisory, outlined a list of steps for users to protect themselves, including not opening attachments in unsolicited emails even if it comes from people in the contact list.

It has asked users to encrypt and protect their sensitive document to avoid potential leakage. It also urged people to use anti-virus tools, firewalls and filtering services and asked them to report any unusual activity or attack immediately to CERT-In.



2. Attacks on industrial enterprises using RMS and TeamViewer: new data

In summer 2019, Kaspersky ICS CERT identified a new wave of phishing emails containing various malicious attachments. The emails target companies and organizations from different sectors of the economy that are associated with industrial production in one way or another.

We reported these attacks in 2018 in an article entitled "Attacks on industrial enterprises using RMS and TeamVicwcr". but recent data shows that the attackers have modified their attack techniques and that the number of enterprises facing the threat of infection is growing.

Before publishing this report, we waited for the vendor of the RMS software to make changes to its services to ensure that the results of this research could not be used to exploit vulnerabilities.

This report in a nutshell:

- From 2018 to at least the early fall of 2020, attackers sent phishing emails laced with malware.
- The attacks make use of social engineering techniques and legitimate documents, such as memos and documents detailing equipment settings or other in ustrial process information, which have apparently been stolen from the company under attack or its business partners.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

- The attacks still use remote administration utilities. The graphical user interface of these utilities is hidden by the malware, enabling the attackers to control infected systems without their users' knowledge.
- In the new version of the malware, the attackers changed the notification channel used after infecting a new system: instead of malware command-and-control servers, they use the web interface of the RMS remote administration utility's cloud infrastructure.
- Stealing money from the organization under attack remains the main objective of the attackers.
- During an ongoing attack, the cybercriminals use spyware and the Mimi katz utility to steal authentication credentials that are subsequently used to infect other systems on the enterprise network.

3. Dyer malware reboots for holiday phishing attacks

Shortly after online banking customers in the UK were warned of a major phishing campaign using the notorious Dy re malware designed to steal financial data, the malware has resurfaced in a new iteration for the holiday season.

Customers of Barclays, Sanlander and Lloyds TSB were being targeted by the trojan malware. Nearly 20,000 malicious emails were sent containing infectious .exe files posing as an email from a tax consultant. The file acts as a downloader that fetches and executes the Dyre banking trojan when opened. Follow up emails then urge victims to attach financial documentation and verify its authenticity. The malware has also been found in the US and Germany. Customers of Bank of America, Deutsche Bank and PayPal are all thought to have been affected by the most recent attack.

Shortly after online banking customers in the UK were warned of a major phishing campaign using the notorious Dyer malware designed to steal financial data, the malware has resurfaced in a new iteration for the holiday season. Customers of Barclays, Santander and Lloyds

TSB were being targeted by the trojan malware. Nearly 20,000 malicious emails were sent containing infectious .exe files posing as an email from a tax consultant. The file acts as a downloader that fetches and executes the Dyre banking trojan when opened.

Follow up emails then urge victims to attach financial documentation and verify iis authenticity. The malware has also been found in the US and Germany. Customers of Bank of America, Deutsche Bank and PayPal are all thought to have been affected by the most recent attack.

VI. DYRE MALWARE

However, as Europeans head to the beaches of Spain this summer, the cybercriminals behind the highly successful Dyre malware arc not taking a break. In fact, they are turning up the heat and have set their sights on 17 Spanish banks, and several European banks' Spain-based subsidiaries.

IBM Security X-Force researchers were able to analyze a new Dyre Trojan configuration file that followed the release of a new Dyre build. This is the first configuration that targets such a large number of Spanish banks. Previous versions only included three or five Spain-based banks on the victim roster, likely as a way to test the waters before moving to a more aggressive phase.

The analysis reveals that Dyre's developers have expanded the capabilities and reach of the malware by updating its web injections to match the new banks they are targeting in Spain. On top of its targets the Dyre gang sees opportunities in other Spain speaking countries beyond Spain attacking Chile, Colombia and Venezuela. This is hardly surprising give that Spanish is the second most spoken language in the world.

Dyre is not new in Europe. It already targets banks all over the European continent, unsurprisingly leaving out only Russia and the former Soviet Union region. Within Euro Dyre infection rates in Spain are ranked third after the UK and France. IBM has appropriately shared the new Dyre information to help prepare and protect targeted banks against the heightened security risk.

VII. DROPBOX PHISHING

Has provided attackers with an interesting new method to deliver nasly stuff through your network. In a round of email that served as the precursor to Dyre, we received phishing emails that linked to a supposed invoice on Dropbox. The Dropbox link itself was legitimate, only it led to a .zip file containing a .scr, not an invoice. Dropbox has been quick to shut down

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

this type of abuse, but it's proven to be a great method for attackers to get past spam filters. Dropbox use is so pervasive that most organizations won't block its links. A few weeks later we would see Dropbox links abused in targeted attacks against the Taiwanese government.

VIII. CONCLUSION

Phishing is constantly evolving to adopt new forms and techniques. Phishing is a technique to gather sensitive information about the target using malicious links and emails. It is one of the most dangerous cyber-attacks that occurs in organizations, personal devices, etc. Phishing is the core concept of hacking. There arc a number of attacks present which break the user's privacy. It is often difficult to distinguish between genuine emails and phishing emails. There arc several methods that can be used to avoid this attack. This study provides an in-sight to phishing, the mechanism of the phishing attack, and various forms it can occur.

REFERENCES

[1] For phishing email," J.Comput. Secur., vol. 18, pp. 7-35, January 2010. [Online]. Available:http://portal.acm. org/citation.cfm?id=17 34234.1734239
[2] http://www.hackersonlineclub.com/tab-nappinu
[3] krebsonsccurity.com
[4] www.tripwirc.com/
[5] http:/ /en. wikipedia.org/
[6] http://webopedia.com/
[7] http://computcrworld.com/
[8] A.-P. W. G. (APWG), "Phishing activity trends report", 2009, [online] Available: http://wwwantiphishing.org/ reports/apwgreport Q32009.pdf.
[9] S. Sheng, B. Wardman, G. Warner, L. F. Cranor, J. Hong and C. Zhang, "An empirical analysis of phishing blacklists", 2009, [online] Available: http://ceas.cc/2009/papers/ceas2009-paper-32
[10] Fette, N. Sadeh and A. Tomasic, "Learning to detect phishing emails", Proceedings of the 16th international conference on World Wide Web ser. WWW '07, pp. 649-656, 2007.
[11] A Bergholz, J. De Beer, S. Glahn, M.-F. Moens, G. Paafi and S. Strobel, "New filtering approaches for phishing email", J. Comput. Secur., vol. 18, pp. 7-35, January 2010.
[12] "International Journal Of Scientific & Technology Research", 90 ijstr©2012, vol. 1, no. 6, July 2012, ISSN 2277-8616.