International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 8, Issue 09, ISSN No. 2455-2143, Pages 68-72
Published Online January 2024 in IJEAST (http://www.ijeast.com)

A SUMMARY OF RECENT ATTACKS AND VARIOUS PHISHING ATTACKS

Rithik R M
Department of CSE
Alva's Institute of Engineering and Technology,
Mijar, D.K-574227

Abstract: **The internet has evolved into a really dangerous place to be these days. Hackers are always attempting to obtain comprehensive credentials and personal information about users. Despite being safe, not all websites on the internet can guarantee your safety. These rule-breakers try not to follow the rules and instead use deceit and hacking to obtain unauthorized access to personal data. We must first comprehend the complexities of the virus's architecture in order to be able to solve this issue. The primary topics of this essay are the various phishing strategies and the most current phishing assaults that occurred during COVID 19. Such as Phone Phishing, Link Manipulation, Filter Evasion, and Website Forgery. We have also researched a deceptive technique for conducting phishing attacks, known as Convert Redirect, which poses as a genuine link and sends the victim to the attacker's website. In this paper, we demonstrate a few phishing examples, such as Paypal Phishing, which is sending an email pretending to be from a reputable company, and Rapid share Phishing, where phishers try to fool their victims into entering their login credentials by creating a spoof website that looks real. Phishers use a wide range of phishing techniques, including phone phishing, website spoofing, filter evasion, and link manipulation, to carry out these kinds of attacks. Email messages are one of the domains used in phishing strategies. Such a phishing website has been made possible via phishing emails, wherein a click on the URL or malware code prompts the execution of socially engineered messages. The performance can be improved and the phishing URL and original email can be distinguished with the use of lexical analysis of the URLs. According to the findings of this study, email classification is effective and produces a highly accurate anti-phishing system in addition to textual analysis of phishing URLs.**

I. INTRODUCTION

Phishing is the word used to describe a cyberattack in which the attacker poses as a reliable source in an attempt to obtain the sensitive or private information of their target through electronic communication. The majority of phishing attacks begin by sending phony emails purporting to be from reputable companies. These messages are frequently designed to look identical to the real ones, making it difficult for consumers to tell them apart.

Phishing is frequently used to obtain credit card numbers or passwords. Computer users are driven to phony websites through emails that are designed to look like they are from banks or other official institutions. The following details are typically taken advantage of by phishing attacks:

•Account number of the user
•Credit card details
•Online banking details

Within the realm of computer security, Phishing refers to the illicit and unlawful act of purporting to get confidential data, including credit card numbers, usernames, and passwords, on the pretense of seeming as a reliable source in an electronic correspondence. Phishing is the term for a bogus email that aims to obtain personal information from you for use in illegal ways. There are numerous versions of this plan. In addition to usernames and passwords, other types of information can be obtained through Phishing, including credit card numbers, bank account numbers, social security numbers, and maiden names of mothers. Phishing poses two types of hazards to internet businesses: direct risk, which involves using credentials that have been stolen, and indirect risk, which involves eroding client confidence. [14]

Phishing can result in harm that varies from denial of email access to significant loss of money. Phishing tactics are also included in this study[1]. The knowledge of the most recent phishing assaults is one of the strategies to counteract phishing. Phishing cannot be totally eliminated by any one technology. However, the frequency of phishing attacks and the losses they cause can be significantly decreased with the right setup and use of modern technologies, along with advancements in security technology. Computer applications and software are made to stop phishing attacks and unauthorized access to private data [3]. Phishing software is made to follow websites and keep an eye on activity. It can automatically report any suspicious activity and, after a while, review the report. This covers spotting phishing attempts, preventing and avoiding scams, responding to a suspected or

International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 8, Issue 09, ISSN No. 2455-2143, Pages 68-72
Published Online January 2024 in IJEAST (http://www.ijeast.com)

confirmed phishing attempt, and taking action to stop phishers.

In a phishing attempt, the information flow is simplified to:
1.The user receives a misleading message from the Phishers.
2.A user gives a phishing server access to private information (usually following some contact with the server).
3.The server provides sensitive data to the phishers.
4.The user is impersonated using the private information. [13]
5.The Phishers make money they shouldn't. Law enforcement officials are mainly interested in steps 3 and 5 because they help them identify and prosecute Phishers. The focus of the technical counter measures discussion will be on how to interfere with stages 1, 2, and 4, as well as related technologies that are not directly related to the information flow.

PHISHING METHODS
Phishers employ many different strategies, but they all share one thing in common. A few of the methods include detailed explanations.

LINK DEFORMATION
The majority of phishing techniques use some kind of technological trickery intended to make a link in an email seem to be from the company being faked. One popular tactic employed by phishers is the use of subdomains or misspelled URLs [12]. In the instance that follows, While the URL http://www.yourbank.example.com/ seems to direct you to the example area of your bank's website, it actually directs you to the "your bank" (i.e., Phishing) section of the example website. Links with the '@' symbol included in them were once used as a means of encrypting a login and password. As an illustration, A casual observer may be led to believe that http://www.google.com@members.tripod.com will open a page on www.google.com, but in reality, it points the browser to a page on members.tripod.com using a username from www.google.com. Regardless of the username entered, the page opens as intended. [2]

1.EVASION OF FILTER
To make it more difficult for anti-phishing filters to identify text often used in phishing emails, scammers have started using graphics in place of text. [4]

2.PHOTOCOPYING
The trickery continues even after the victim accesses the phishing page. Certain Phishing schemes modify the address bar using JavaScript commands. This is accomplished by either closing the current address bar and establishing a new one with the valid URL, or by having an image of a real URL placed over the address. [7]

3.Phishing on phones
Users received messages posing as bank communications instructing them to call a number if they were having issues with their bank accounts[8]. Users were prompted to input their PIN and account information after dialing the Phishers' phone number. Sometimes, caller- ID spoofing, or "voice phishing," creates the impression that calls are coming from a reputable company[9].

2. FORGERY OF WEBSITES
Certain phishing scams modify the website's address bar with the use of JavaScript instructions. One way to accomplish this is to either overlay the address bar with an image of a valid URL or to close the current bar and open a new one with the valid URL[11]. Potential vulnerabilities in the scripts of a reliable website might also be used by an attacker against the target. Because they force the user to sign in at their bank's or service's own website, where everything from the web address to the security certificates seems proper, these assaults, also known as cross-site scripting (XSS) attacks, are very dangerous. Actually, the website URL is designed to initiate the assault, which makes it exceedingly challenging to identify without specialized understanding. A similar weakness was exploited against PayPal in 2006.

TRANSFORM REDIRECT
A stealthy technique for carrying out phishing attacks is known as "covert redirect," which seems as genuine links but really takes the victim to the attacker's website[1]. Usually, the vulnerability appears as a log-in prompt depending on the domain of the impacted website. Additionally, depending on well-known attack settings, it may impact OpenID and OAuth 2.0. This frequently exploits XSS and open redirect vulnerabilities found on the websites of third-party applications. Malicious browser extensions can also secretly divert users to phishing websites.
A typical phishing effort may be easily identified since the URL of the malicious page would often differ from the link to the legitimate website. An attacker might utilize a legitimate website in place of a covert redirection by infecting it with a malicious login popup dialogue box. This distinguishes covert redirection from other methods[2].
Let's say, for instance, that a victim clicks on a malicious phishing link that starts with Facebook. Facebook will prompt the victim to activate the app through a popup window. A "token" will be supplied to the attacker and the victim's private, sensitive information may be revealed if they decide to approve the app. The email address, birthdate, contacts, and employment history are a few examples of this data[4]. An attacker may be able to access more private data, such as the buddy list, online identity, and email, if the "token" has additional privileges. Even worse, the attacker could be able to take command of and manage For example, suppose that a victim clicks on a fraudulent Facebook-based phishing link. Through a popup window, Facebook will ask the victim to

enable the app. Should the victim choose to authorize the app, they would receive a "token" and potentially expose their private and sensitive data.
Among the information are the email address, birthday, contacts, and work history[3]. If the "token" has higher rights, an attacker could be able to access more personal information, such the friend list, online identity, and email. Worse worse, the attacker could be able to seize control and oversee

EXAMPLE of PHISHING
1.PAYPAL PHISHING
Spelling errors in the email and the existence of an IP address in the link, for instance, are indicators that this is a phishing effort using PayPal[6]. The absence of a personal welcome is another telltale sign, yet having personal information would not imply authenticity. A genuine Paypal correspondence will always address the recipient by name, not only by using a formulaic salutation such as "Dear Account Holder." Misspellings of basic phrases, poor language, and threats of account suspension if the receiver disobeys the message's instructions are further indicators that the communication is fraudulent[8].
Be aware that a lot of phishing emails contain strong cautions not to divulge your password in the event of a phishing assault, just like an authentic email from PayPal would. Part of what makes the Phishing email so misleading is because it alerts users to the potential for Phishing attacks and includes links to websites that describe how to prevent or recognize them. The Phishing email in this instance alerts the recipient that critical information is never requested in emails from PayPal[5]. As promised, it asks the user to click on a link to "Verify" their account, which, when clicked, will direct them to another phishing website that imitates PayPal's design and requests sensitive personal data.

2.PHISHING RAPIDSHARES
Phishing is a popular way to obtain a premium membership on the Rapid Share web host, which eliminates download speed limits, automatically removes uploaded content, delays downloads, and cools down intervals between downloads. scholarlymafia.org Phishers will be able to get premium Rapid Share accounts by providing links to files on RapidShare on warez websites. But, by utilizing link aliases such as Tiny URL, They can hide the true URL of the page, which is a spoof of Rapid Share's "free user or premium user" page and is hosted someplace else. When the victim chooses a free user, the phishers simply direct them to the legitimate RapidShare website. Nevertheless, if they choose premium, the phishing website logs their login information before directing users to the download. As a result, the victim's premium account information has been stolen by the scammers.

Phishing email examples
Phishing emails can come in a variety of formats. They might look to be from your social networking site, your bank or other financial institution, or a company you frequently do business with like Microsoft. The primary characteristic of phishing emails is that they either request personal information from you or refer you to websites or phone lines where they do the same. An illustration of a phishing scheme in an email message is shown below[7].
An illustration of a phishing email message, complete with a fake website link that takes the recipient to a fraudulent website. In order to add even more legitimacy to these phishing emails, the con artists may include a link that seems like it leads to the official website, but in reality it leads to a fake scam website or even a pop-up window that mimics the genuine website. Phishing links that you may see in emails, websites, or instant messaging may include all or part of a legal company's name. They are often disguised, so clicking on the link will send you to a different website, usually one that is not official. Notice that in the following example, the genuine Web URL is displayed in the box with the yellow background while the mouse cursor is rested (not clicked) on the link. It's strange that the string of obscure digits doesn't resemble the business's website address.

RECENT ATTACKS BY PHISHERS
1.Phishing is a widespread activity that happens worldwide. The attacks, which employ skillful and more advanced social engineering approaches to deceive users, are more concentrated, efficient, and capable of making mistakes. Let's look at some examples of current phishing assaults and how they are affecting people worldwide during this epidemic. Phishing attacks have been occurring on a big scale, even outside of official websites[9].
2.The government issues a warning about widespread phishing scams that use COVID- 19 as a lure.The authorities have issued a warning about a widespread assault on people and companies, claiming that the perpetrators may exploit COVID-19 as a lure to get financial and personal data[13]. The alert warning from CERT-In, India's cybersecurity nodal body, states that possible phishing attacks may pose as government departments, agencies, or trade associations that are in charge of monitoring government funding disbursements. Financial assistance.

It is expected that the perpetrators would distribute malicious emails posing as local government agencies in charge of distributing government-funded COVID-19 assistance programs.
The Indian Computer Emergency Response Team (CERT-In) stated in its most recent advice dated June 19 that "such emails are designed to drive recipients towards fake websites where they are deceived into downloading malicious files or entering personal and financial information." The advisory stated that in an attempt to trick users into disclosing personal information, the "malicious actors" are claiming to have 2 million individual/citizen email IDs and are preparing to send emails with the subject line: free COVID-19 testing for all

residents of Delhi, Mumbai, Hyderabad, Chennai, and Ahmedabad[10].
"It has been reported that these malicious actors are planning to spoof or create fake email IDs impersonating various authorities," said the agency. In its alert, CERT- In listed many precautions users could take to keep themselves safe, such as refusing to accept attachments in unsolicited emails, even if they are from contacts
Users are requested to safeguard and encrypt their confidential documents to prevent any possible disclosure. Additionally, it invited users to report any strange behavior or attack to CERT-In right once and encouraged them to utilize firewalls, filtering services, and anti-virus software.

3.New information on attacks on industrial businesses with RMS and TeamViewer
Kaspersky ICS CERT discovered a fresh wave of phishing emails with numerous malicious attachments in the summer of 2019. The emails are directed towards businesses and institutions from various economic sectors that are somehow connected to industrial output.
In 2018, we documented similar assaults in an article titled "Attacks on industrial enterprises using RMS and TeamViewer." However, new information indicates that the attackers have changed the way they attack, and an increasing number of enterprises are at risk of infection.
In order to guarantee that the findings of our investigation could not be utilized to exploit vulnerabilities, we waited for the RMS software provider to make modifications to its services before releasing this report.

The summary of this report is:
●Phishing emails containing malware were delivered by attackers between 2018 until at least the first autumn of 2020.
●The assaults employ documents specifying equipment settings and other valid materials, as well as social engineering tactics.Industrial process data, which appear to have been taken from the targeted organization or its suppliers.
● Remote administration tools are still utilized in the assaults.

Because the virus conceals these programs' graphical user interface, it allows attackers to take control of compromised PCs without the victims' awareness.
After infecting a new machine, the attackers modified the notification channel in the new malware version by using the web interface of the cloud-based RMS remote administration application rather than malware command-and-control servers[14]. The primary goal of the attackers is still to steal money from the targeted firm. Cybercriminals employ spyware and the Mimi Katz tool to collect login credentials during an attack, which they then use to infect additional systems on the enterprise network.

4.To prepare for holiday phishing assaults, the infamous Dyre virus, which is used in large-scale phishing campaigns to steal financial data, has reappeared in a new version just in time for the holiday season, alerting UK online banking clients to the potential danger.
The trojan software was aimed against customers of Lloyds TSB, Santander, and Barclays. Under the pretense of being emails from tax consultants, about 20,000 fraudulent emails with infectious.exe files were sent. When opened, the file serves as a downloader, obtaining and launching the Dyre banking trojan[1].
Subsequent correspondence thereafter request that victims affix financial records and confirm their legitimacy. Germany and the US have also reported encounters with the spyware. It is believed that customers of PayPal, Deutsche Bank, and Bank of America were impacted by the most recent hack.
The infamous Dyer virus, which was used in a large- scale phishing attempt to steal financial data, was discovered again in a new version just in time for the holiday season, alerting UK online banking clients to the threat.
The trojan software was aimed against customers of Lloyds TSB, Santander, and Barclays. Under the pretense of being emails from tax consultants, about 20,000 fraudulent emails with infectious.exe files were sent. When opened, the file serves as a downloader, obtaining and launching the Dyre banking trojan.
Subsequent correspondence thereafter request that victims affix financial records and confirm their legitimacy. Germany and the US have also reported encounters with the spyware. It is believed that customers of PayPal, Deutsche Bank, and Bank of America were impacted by the most recent hack.

DYRE VIRUSES
But the hackers responsible for the extremely popular Dyre virus are not taking a vacation as Europeans flock to Spain's beaches this summer. In reality, they are stepping up their efforts and focusing on 17 Spanish banks as well as the Spain-based subsidiaries of other European banks.
After a new Dyre build was released, researchers from IBM Security X-Force were able to examine a fresh configuration file for the Dyre Trojan. This is the first setup that aims to target so many banks in Spain. Earlier iterations of the victim roster only contained three or five banks with headquarters in Spain, most likely as a test run before a more active phase.
According to the research, Dyre's creators updated the malware's web injections to match the new Spanish banks they are targeting, therefore increasing the malware's functionality and reach. In addition to its primary objectives, the Dyre gang perceives chances in other Spanish-speaking nations, such as Chile, Colombia, and Venezuela. Considering that Spanish is the second most spoken language in the world, this is not unexpected.
In Europe, dyre is nothing new. It now targets banks throughout Europe, naturally excluding only Russia and the former Soviet Union. Spain has the third-highest rate of Euro Dyre infection, behind the UK and France[6].

In order to assist in preparing and shielding the targeted institutions from the increased security risk, IBM has duly disclosed the new Dyre information.

Phishing via DropBox

The popularity of third-party cloud services, such as Dropbox, has given hackers a novel and intriguing way to spread malware throughout your network[12]. We received phishing emails that linked to a fictitious invoice on Dropbox during an email campaign that was the forerunner to Dyre. The Dropbox link was authentic; nevertheless, it sent users to a.zip file that contained a.scr file instead of an invoice. Although Dropbox has responded swiftly to stop this kind of misuse, attackers have found that it's an excellent way to get past spam filters. Because Dropbox is so widely used, most companies won't ban its links. A few weeks later, Dropbox connections will be used in deliberate strikes against the government of Taiwan.

II. CONCLUSION

Phishing is always changing, taking on new shapes and methods. Phishing is a tactic used to get private information about a target by sending out fraudulent emails and links. It is among the most hazardous cyberattacks that target gadgets, businesses, and other targets. The fundamental idea behind hacking is phishing. Numerous attacks exist that compromise the privacy of the user. It might be challenging to tell the difference between phishing and legitimate emails. To prevent this assault, a few strategies can be employed. This research offers an understanding of phishing, its process, and its possible manifestations.

III. REFERENCE

[1]. Sophos, "The State of Ransomware 2022," [sophos.com]
[2]. MITRE, "Understanding and Mitigating Supply Chain Attacks," [mitre.org]
[3]. Symantec, "Zero-Day Vulnerabilities: A 2022 Perspective," [symantec.com]
[4]. APWG, "2022 Phishing Trends and Intelligence Report," [apwg.org]
[5]. FBI, "BEC in 2022: Tactics, Techniques, and Procedures," [fbi.gov]
[6]. Akamai, "Credential Stuffing Attacks and How to Defend Against Them," [akamai.com]
[7]. Nexusguard, "Global DDoS Threat Landscape Report," [nexusguard.com]
[8]. FireEye, "APTs in 2022: Tactics and Mitigation Strategies," [fireeye.com]
[9]. Kaspersky, "Social Engineering Attacks: A Comprehensive Overview," [kaspersky.com]
[10]. Trend Micro, "IoT Security Report 2022," [trendmicro.com]
[11]. CrowdStrike, "Global Threat Report 2022," [crowdstrike.com]
[12]. Lookout, "Mobile Security Threats and Solutions," [lookout.com]
[13]. OWASP, "Web Application Security: Current Threat Landscape," [owasp.org]
[14]. CSA, "Cloud Security Threats and Best Practices," [cloudsecurityalliance.org]