Second National Conference on Internet of Things : Solution for Societal Needs
In association with International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Phishing Attacks in Cyber Security

Prof. Pradip Sitaram Ingle[1], Ms. Pranita Shivkumar Murkar[2], Ms. Shital Prabhu Gadkari[2]

[1]Assistant Professor, Department of Information Technology, Anuradha Engineering College Chikhli, Maharashtra, India

[2]Student, Information Technology Department, Anuradha Engineering College, Chikhli, Maharashtra, India

ABSTRACT

In using various techniques of social engineering, the criminels font des ravages sur Internet et escroquent de nombreuses personnes de different manières. Cela met diverses communautes organizations, en danger. Therefore, it is important that people in those communities learn to protect themselves when active in cyberspace or when confronted with cyberspace-related technologies. In fact, training can play an important role in this regard and, consequently, help alter the unsafe behavior of many people. The goal of this research article is to determine whether simulating phishing attacks in conjunction with built-in training can help cultivate user resistance to "phishing attacks."

I. INTRODUCTION

In Phishing (pronounced as fishing), the social engineer tries to get the targeted individual to reveal personal information such as usernames, account numbers, and passwords. This is often done through the use of authentic-looking but fake emails from corporations, banks, and customer service personnel. Other forms of phishing try to get users to click on fake hyperlinks that will allow malicious code to be installed on the target computer without their knowledge. This malware will be used to delete data from the computer or use the computer to attack others Phishing is the act of attempting to acquire information such as username, password, and credit card details as a trusted entity in electronic communication. Phishing attacks have become more and more sophisticated and often mirror the target site transparently, allowing the attacker to observe everything while the victim is browsing the site and cross any limits above victim security. [1] As of 2020, phishing is by far the most common attack carried out by cybercriminals, with the FBI's Internet Crime Complaints Center recording more than twice as many phishing incidents as any other type of computer crime. [2] Attempts to prevent or mitigate the impact of phishing incidents include legislation, user training, public awareness, and technical security measures. [3]

Communications purporting to be from popular social web sites, auction sites, online payment process or IT administrators are commonly used to lure the unsuspecting public.

II. WHAT IS PHISHING?

On day to day base every one that used internet used a web application we can be used a web application through your apps on your smartphone or some application on your desktop or you mid be using a web application. Now you can consider the keys where we using a web browser and you have to shop something online. Now you search for the product and you came cost in different websites and you like the products on to different website. So, one of this website is a very famous, very popular, very trusty ecommerce website and there is another website which is selling your product for the same price and may be for amore discount price, but it is not popular, you never heard that ecommerce website before. Now you chose to pay for a product online and for that you mid have to enter your credit card or debit card details. Now the question is which website would you trust more with your personal details with sensitive details that is a credit card details. Obviously you would deal less habitat well your entering the credit card details on the e-commerce website that is trustworthy and would be more hassidden would be worried while entering this details on to the website that your here in the name for the first site. This is because you don't trust the new website the other website the popular website you hear the name before you used before and you have trust factor with that website so psychology is what hacker take advantage of in phishing attacks, so hacker take advantage of this trust factor and they fake them cells as a trustworthy entity. To sale you are sensitive data and your personal data. So phishing is a attack of gathering sensitive information of a target such as username password email ID or other sensitive information maybe bank details your credit card, your debit card details etc, buy discussing as a trustworthy entity. So as a told you previously if you are entering any sensitive information maybe a card details on to a trustworthy website. You wouldn’t be hesitate. So, if phishing attack hacker disguises him self as a trustworthy entity. Them his make you tricks you enter your sensitive information into that a fake web application. So, this is phishing.

2.1 How phishing works

Like you told you phishing is a web base applications and this is mainly used to cradiation . So we need a web application that is using a web server. Now every web application as connected to web server. When we have using a web application , what happened is there is some data and the packets, the information i.e. being send from your web application to the web server, and from the web server on the web application. Now, this is has an communication between web application and the web server happens. So, what happened the phishing attack is , the hacker disguises him self as this web server, so you think that your communication with the genuine with the actual web server but you reality you just communicating with the fake web server on the fake web application that the hacker has beld . And when you enter sensitive information on to this web server or this web application. The hacker used your prediction. This is how phishing work.

2.2 Step for phishing attack

1. Hacker creates a fake website.
2. F ake website is sent to the victim.
3. Victim enter credentials .
4. Hacker gets the credentials.

Step 1 : Hacker creates a fake website because, like I told you a phishing is a attack where a hacker disguises himself as a trustworthy entity. So, first he has to create a fake website, a fake of genuine website at to trick the victim to enter the credentials.

Step 2 : The next step is to send this fake website to the victim now, suppose a victim is trying to access a Facebook for example, if it goes yo the web application by him it's self may be he enter the URL of the websites on search engine and then used the link go to that website. Than he does that he goes to the actual the genuine website and not to the fake website. So the second step is hacker has to send this fake website to the victim where, the victim enters the credentials.

Step 3 : The third step that happened is the victim he used that this fake website is a trustworthy website and enter credentials.

Step 4 : And finally the hacker gets the credentials.

2.3 Types of phishing

The attack can be carried out in several ways. drive for all types are similar. The only difference between Types are the number of targets and the mechanism used get data.

The different types of phishing attacks are [4]

- **Deceptive phishing :-**
  It reflective attached by we front emphases altimetry company. Once use of click the link off word credentials user personal information or login credentials are stolen. A fake email from a bank asking you to click a link and verify your account details is ones such a example.
- **Spear phishing :-**
  It target integer specific kind of profile. Attach a the social media and other websites. Forester customized attack email with target specific information that includes is name his position, his company to trick the recipient into believe in the mail her he gone into the confidential information. Take secret and even famashial gain.
- **Whaling :-**
  Her target is high post parson in an organization such as CFO, CEO. etc The high designating person more information, and Hence could be more damage into the organization this is the also known as CEO fraud.
- **Pharming :-**
  This is a form of online fraud where in bad actor relevant the clone or duplicate website to still information. Bad actor may used BNS redirection or occasionally MITM attack to execute it successfully.
- **Clone phishing :-**
  In this attack target are presented with a copy of ligament massage that they have regular earlier. But with a specific changes that the attacker are made in an attempt trap the target this change could be related to the malicious attachment invalid URL ext. Because communication was the part of the earlier communication this kind of attack are more successful or effective.
- **SMS Phishing :-**
  It is the combination of SMS and phishing. It is an act of commentating at text message fraud try to lure the victim into revolution account information or installing a software. The presenting to be limit emptily.
- **Voice phishing :-**
  That is voice phishing and vising. Her people are treat into giving money or veiling personal information vising frequently in was a criminal patent into the pre- presentative of bank or organization. It is a fondle on impact is, of existing sensitive information over the phone. Here, the hacker uses the VUIP technology so have to prove the caller ID, so that it's look like the call come from the authentic source.
- **Baiting :-**
  It realizes an quercetin or grid of the victim. Better offer users free download an using long in credential also and infected storage media like CD ROM or USB flash drive line unattended are used to live of the victim. Once the parson insert this drive into the computer there computer get infected with tandoors and backdoor emprise created in the victim computer.

- **Search Engine Based Phishing :-**
  Same phishing camsondboll search engine whether uses are directed to product are its. Its may offer low cost product or services. When the user try to by the product by entering the credit card details there collected by the phishing side. There are many fake bank websites of reacting credit card or loans to user at a low rate but actually they are phishing site

2.4 Phishing Technique

- Link Manipulation
- Filter Evasion
- Website Forgery
- Phone Phishing

2.5 Effect of Phishing

- Internet fraud
- Identity theft
- Financial loss to the original institutions
- Difficulties in law enforcement investigations
- Erosion of public trust in the internet

2.6 Defend against phishing attack

- Preventing a phishing attack before it begins
- Detecting a phishing attack
- Preventing the delivery of phishing messages.
- Preventing deception in phishing messages and sites.
- Counter measures

Interfering with the use of compromised information.

III. ANTI-PHISHING TECHNIQUES

In [5], the authors used text mining to extract distinct features of emails. Emails can be fraudulent or real emails To better detect the attack. The strategy used was Initial conversion of email to vector representation Followed by feature selection techniques for classification. The evaluation was performed using accumulated data sets From the Ham Corpus of Spam Assassin project (legal email) and publicly available Phishing Corpus E-mail).

The study carried out in [6] used a unique technique from Natural Language Processing (NLP) to determine if mail has been malicious or not. In this article, they extracted and compared common features using NLP tools. PhishNet-NLP used natural language techniques with all information present in an e-mail, namely the header, links and text in the body. PhishSnag used information from e-mail to detect phishing. Phish-Sem used NLP and statistical analysis on the body to label the mail as phishing or not phishing.

The authors talk about reusable components for anti-phishing component layer in [7]. These reusable components are used to convert web pages to feature vectors using heuristic methods and external repositories. The finished line the vectors which provide input to these vector machines cause the support vector machine. Thanks to the training provided by these inputs, the classified and determined support vector machine various web pages as legitimate or a phishing web page. This has been experimented with the mixture of heuristics to identify a phishing web page. A more advanced filtering and classification technique has been used in [8]. In this article, the authors tested URLs and checked whether it was malicious or not. They used a automated approach to detect phishing. He had two phases- Pre-filtering and classification phase. In pre-filtering phase, the URL was matched against a blacklist using the domain part of the URL. If the

URL was present in this list then it was classified as malicious and would not be move on to the classification phase. In the next phase, two the main characteristics were checked for consistency- the RU and the Position of thedomain. Based on the result of the classification phase, the URL was classified as malicious or non-malicious.

In [9], the anti-phishing technique was developed with the help of the advanced heuristic approach. In this technique, when suspicious site was encountered, it was immediately updated in the blacklist. If a legitimate website is found, it updates the same in the whitelist. Therefore, when the user open a website, it was first checked if the website was a phishing or non-phishing website and, accordingly, provided access to the same. This technique uses the PHP programming language with a database to maintain the two lists.

The method used in [10] is slightly different from the others technical. In [8], they classify emails as unwanted or non-unwanted based on spam filter. When an email arrives at mailbox, Spam filtering is performed on the basis of the reputation of the URL present in the to post. If the URL looks dangerous or suspicious, the filter marks the mail as "junk". URLs in mail are disabled and the mail is then moved to junk mail. If the mail is genuine, the mail is moved to the inbox for the user to open without issue.

The method of extraction and classification was further developed in [11]. In this article, the vulnerabilities have been differentiated into three categories according to the structure of the email. The three categories were the content of the page vulnerability, domain vulnerability and code script vulnerability. The evaluation model used was Anti-Phishing Effectiveness evaluation model (APEE model) that is used analyze the effectiveness of anti-phishing mechanisms that have been implemented. The reputation of vulnerabilities in all three categories are tested, which helps to determine whether the email is a phishing email or not.

Example:

1. Petya Ransomware Attack Date : 27-28 June 2017

Victims: Ukraine (80%) ,Germany (9%), Russia ,Italy, France, UK ,Poland ,US

Attack Type: Cyber Attack - Ransom ware

Attacker: Russia (according to Ukrainian authorities and the CIA)

Intention: Politically motivated attack against Ukraine

Results: More than 80 companies (Several Ukrainian ministries, banks and metro systems) including national bank of Ukraine

Description:

On 27 june 2017 a major cyber attack occurs on Ukraine and it was a ransomware name "petya". Same cyber attack reported from Germany , Russia US .

The main target of this cyberattack is Ukraine. More than 80% companies in Ukraine were affected with petya.

80% infections were reported on Ukraine and 9% infections were reported on Germany.

There was enough evidence that Russia is responsible for this and it was done out of political motivation against Ukraine.

This ransomware target on companies power grid s, bus stations, gas stations, airports, and banks.

This attack were originated from an update of Ukrainian tax accounting package called MeDoc (M.E.Doc) developed by Intellect Service.

MeDoc is common among the Ukrainian accountants. The impact occurs on around 400,000 customers and 1 million computers across Ukraine.

What is petya & How does it work

Petya is an encrypting ransomware that is first discovered in 2016.

This targets Microsoft Windows based systems infected on the master boot record (MBR).

Then execute a payload that encrypt the file systems of hard drive and prevent Windows booting.
To regain the access to file system user needs to pay a ransom with Bit coin to the attacker.
Used for performing a cyder attack on Ukraine

There are four steps in petya.

1. Prepare - Attack begins with compromising the MeDoc application when an organisation updated the application the Petya code will be inserted.
2. Enter - When customers update MeDoc software Petya code runs on an enterprise host and spread over the enterprise network.
3. Traverse - There are two path malware traverse.
   *Exploitation - Exploiting the vulnerability SMBv1 (MS17_010).
   *Credential theft - Impersonate any account that currently logged in to the account.
   *Petya only compromised accounts witch has an active session (credentials loaded into LSASS memory)
4. Execute - Petya then reboot and start the encryption process. Then user can display screen text that is a ransomware.

Impact:

During the attack, radiation monitoring system at Ukraine's Chernobyl Neclear Power Plant went offline.
Inflected to Serveral Ukrainian ministries, banks,metro systems and state-owned enterprises (Boryspil International Airport, Ukrtelecam, Ukraine's electricity company's computers also went offline (But Company continued to fully operate without using computer). Inflected computer data were overwritten and permanently damaged.
The total estimated damage was more than $10 billion

Mitigation:

Patch Management: lmplement an emergency patch program and ensure that all Windows systems are receiving security patches from Microsoft and other vendors on a frequent basis. This patch relevant to fixing the Eternalblue vulnerability is MS17-010.
Host Based Firewalls: Consider applying firewall rules at the host level (Windows firewall) which prevent unnecessary system to system communication (making it more difficult for Worms to propagate).
Network Segmentation: Properly segment networks and apply routing and firewall rules which create security zones within your network, limiting the attack surface of malware was introduced. Use Supported Operating System: Ensure all operating systems currently being ran by the vendor (Windows XP and Server 2003 are no longer supported or receiving security updates).
Properly Manage Backups: Verify that backups are not stored within network attached directories that might be susceptible to being infected by a Worm (End up being encrypted as part of the ransomware attack).

Cognizant

One of the worst largest provide sophisticate services sad they become ogecting of a ransomware attack. Then thus maze ransomware attack. That has goes description of yields client. Company realized a official statement on its website and its states. Cognizant conform there security incident involving our internal system and cozing services disruption for some of our clients. It the result of a maze ransomware attack. They also said cognizant conform that it is taking spoke of the incident and already started communicating with all there client on this maze ransomware attack. The reported maze attack on cognizant is horizon as it is not like a typical ransomware other than encrypting data it is also to spread accrosed network infecting and increasing every computer on its swag and it can also oxidation data of the attackers.

“The Maze attack reported on Cognizant is worrying, as it does not look like typical ransomware. Besides data encryption, it is capable of propagating over a network, infecting and encrypting every computer in its path, and it can also exfiltrate data to attackers,”said Saket Modi, CEO of Lucideus, a corporate cybersecurity platform company.” [12]

“Although Maze operators denied the attack, it was always classified as Maze because indicators of compromise listed included the IP addresses of servers and file hashes, which are known to be used in previous attacks by the. Maze actors.”[12]

At a time when more than 90% of IT service company employees around the world work from home, such an attack indicates a worrying trend. While there has been a significant increase in phishing attacks in the form of Covid-19-themed websites, the ransomware attack appears to be the most serious form of such attempts at this point. [12]

IV. CONCLUSION

Phishing is a technique to collect confidential information about the target via malicious links and emails. It is one of the most dangerous cyberattacks that occur in organizations, personal devices, etc. It is often difficult to distinguish between genuine emails and phishing emails. exist various methods that can be used to avoid this attack. Regular updating of anti-phishing tools and platforms can prove to be very powerful. This study provides a perspective of phishing, the mechanism of the attack, various ways it can occur and possible solutions to overcome them.

V. REFERENCES

[1]. Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark; Stavroulakis, Peter (eds.). Handbook of Information and Communication Security. Springer. ISBN 978-3-642-04117-4.

[2]. "Internet Crime Report 2020" (PDF). FBI Internet Crime Complaint Centre. U.S. Federal Bureau of Investigation. Retrieved 21 March 2021. "Internet Crime Report 2020" (PDF). FBI Internet Crime Complaint Centre. U.S. Federal Bureau of Investigation. Retrieved 21 March 2021.

[3]. Jøsang, Audun; et al. (2007). "Security Usability Principles for Vulnerability Analysis and Risk Assessment". Proceedings of the Annual Computer Security Applications Conference 2007 (ACSAC'07). Archived from the original on 2021-03-21. Retrieved 2020-11-11.

[4]. Gaurav, Madhuresh Mishra, Anurag Jain - Anti-Phishing Techniques: A Review, International Journal of Engineering Research and Applications (IJERA), vol. 2, pp. 350- 355, April – 2012.

[5]. Masoumeh Zareapoor, K.R. Seeja, Text Mining for Phishing E-mail Detection, Intelligent Computing, Communication and Devices: Advances in Intelli-gent Systems and Computing, vol. 308, pp. 65-71, August 2016.

[6]. Rakesh Verma, Narasimha Karpoor, Nabil Hossain and Nirmala Rai - Automatic Phishing Email De-tection based on Natural Language Processing Techniques, Research Gate, 2016.

[7]. Anna L. Buczak, Erhan Guven - A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Communica-tons Surveys & Tutorials, vol. 18, pp. 1153-1176, June – 2016.

[8]. Yi-Shin Chen, Huei-Sin Liu, Yi-Hsuan Yu and Pang-Chieh Wang, Detect Phishing by Checking Content Consistency, IEEE, 2017.

[9]. Okunoye, O.B, Azeez, N.A, Ilurimi F.A - A Web Enabled Anti-Phishing Solution Using Enhanced Heuristic Based Technique, FUTA Journal of Research in Sciences, vol. 13 (2), pp. 304-321, Octo-ber – 2017.

[10]. Xavier Joseph, Mitchell Aime M, Tsang Brian J, Herbert, George A, Savastano, Hernan I, Khandel-wal Lubdha, Pengelly Robert C. J, Novitskey Robert, Grant Stanley - Anti-phishing protection, United States Patent 10,069,865 B2, Sept 4th, 2018 Sankhwar S., Pandey D., Khan R.A - A Novel Anti-phishing Effectiveness Evaluator Model, Smart Innovation, Systems and Technologies, Springer, vol 84, Cham, 2018.

[11]. "PM Narendra Modi pushes for use of technology in the 'era of Covid-19'"