Intelligent Tool to Detect Social Engineering Attacks Using Rule-Based Expert Systems

S.Priyadharsini
Department of Computer Science and Engineering
Velammal Engineering College, Chennai
Email: subipriya2@gmail.com
S.Revathy
Department of Computer Science and Engineering
Velammal Engineering College, Chennai
Email: revathy.selvaraj98@gmail.com
S.**Lydia**
Department of Computer Science and Engineering
Velammal Engineering College, Chennai
Email: princylydi16@gmail.com

ABSTRACT

Social engineering is the art of manipulating users of a computing system into revealing confidential information that can be used to gain unauthorized access to a computer system. The types of information these criminals are seeking may vary. Phishing is one of the most common social engineering techniques and one such fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication. This technique uses trickery and deceit to obtain private data from users. Spear phishing is a variation on phishing in which hackers send emails to groups of people with specific common characteristics or other identifiers. It is a targeted attempt done through email or electronic communication to steal sensitive information such as account credentials or financial information from a specific victim, organization or business often for malicious reasons. In this paper, a comparative study about the various features of phishing and spear phishing is made. The techniques used by the attackers to perform phishing is discussed in detail. The proposed system introduces a unique methodology to develop an intelligent tool to detect phishing and spear phishing attacks performed by social engineers and cybercriminals. Also other technical solutions to prevent such social engineering attacks are addressed.

I. INTRODUCTION

The rise of 21st century marked the transition phase of the most global businesses towards a paperless office environment, where the focus shifted the manual to the computerized form of work culture. But at the same time, change brought a number of threats and menace in terms of one of the biggest issues of the current businesses, the social engineering used among the hackers for cracking techniques that rely more on human weaknesses rather than technology itself. The aim or motive of such attacks was getting access to passwords or other relevant information by tricking people for carrying out illegal or criminal activities.

Phishing is one such fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication. It is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Such Phishing emails will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and will capture and steal any information the user enters on the page.

Spear phishing is a variation on phishing in which hackers send emails to groups of people with specific common characteristics or other identifiers. It is a targeted attempt done through email or electronic communication to steal sensitive information such as account credentials or financial information from a specific victim, organization or business often for malicious reasons.

II. TECHNIQUES

2.1. Difference between Regular Phishing and Spear Phishing

Regular phishing attacks usually come from a large, well-known company that the recipient is associated with or is a member such as an Internet, telephone, or electrical company. The email will usually state that there is some sort of problem with the user's account and ask the user to confirm some personal information to proceed with the resolution of the error. The email may seem valid, but most people have become wise to how these attacks work, and they are not nearly as effective as they were in the beginning. Most corporate users who utilize email every day have become savvy about giving out personal information and clicking on links contained in emails. Spear phishing is more targeted, more believable and is usually harder to discern that there is malicious intent because they appear to come from a known, trusted source.

2.2. Link manipulation

Internationalized domain names can be exploited via IDN spoofing or homograph attacks, to create web addresses visually identical to a legitimate site, that lead instead to malicious version. Phishers have taken advantage of a similar risk, using open URL redirectors on the websites of trusted organizations to disguise malicious URLs with a trusted domain. Even digital certificates do not solve this problem because it is quite possible for a phisher to purchase a valid certificate and subsequently change content to spoof a genuine website, or, to host the phish site without SSL at all.

2.3. *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. These types of attacks 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.

2.4. Covert 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. For covert redirect, an attacker could use a real website instead by corrupting the site with a malicious login popup dialogue box. This makes covert redirect different from others.

2.5. Voice phishing

Messages that claimed to be from a organization told users to dial a phone number regarding problems with their organization . Once the phone number 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.

2.6. Filter evasion

Phishers have sometimes used images instead of text to make it harder for anti-phishing filters to detect the text commonly used in phishing emails. In response, more sophisticated anti-phishing filters are able to recover hidden text in images using OCR (optical character recognition).

III. CHARACTERISTICS OF PHISHING EMAIL

It normally appears as an important notice, urgent update or alert with a deceptive subject line to entice the recipient to believe that the email has come from a trust source and then open it.

- It contains messages that sound attractive rather than threatening e.g. promising the recipients a prize or a reward.
- It normally uses forged sender's address or spoofed identity of the organisation, making the email appear as if it comes from the organisation it claimed to be.
- It usually copies contents such as texts, logos, images and styles used on legitimate website to make it look genuine. It uses similar wordings or tone as that of the legitimate website. Some emails may even have links to the actual web pages of the legitimate website to gain the recipient's confidence.
- It usually contains hyperlinks that will take the recipient to a fraudulent website instead of the genuine links that are displayed.
- It may contain a form for the recipient to fill in personal/financial information and let recipient submit it. This normally involves the execution of scripts to send the information to databases or temporary storage areas where the fraudsters can collect it later.

IV. CHARACTERISTICS OF PHISHING WEBSITES

A typical phishing website will have the following characteristics:

- It uses genuine looking content such as images, texts, logos or even mirrors the legitimate website to entice visitors to enter their accounts or financial information.
- It may contain actual links to web contents of the legitimate website such as contact us, privacy or disclaimer to trick the visitors.
- It may use a similar domain name or sub-domain name as that of the legitimate website.
- It may use forms to collect visitors' information where these forms are similar to that in the legitimate website.
- It may in form of pop-up window that is opened in the foreground with the genuine web page in the background to mislead and confuse the visitor thinking that he/she is still visiting the legitimate website.
- The body of the email message is an image.

V. FEATURES

To protect yourself from phishing attacks, look out for emails and messages that have these characteristics:

- Requests to click on links or open attachments
- Sense of Urgency
- Appeal to Human Greed and Fear
- Requesting Sensitive Data

5.1. Requests to click on links or open attachments

The basic method for cyber criminals is to send out a mass e-mail containing an attachment or a hyperlink. The attachment is malware and any hyperlink will to be a website masquerading as something legitimate. The goal is to trick the e-mail recipient into downloading the

attachment (exposing their PC to the malware), or clicking the link to a website that may be infected with malware, or asks for confidential data such as credit card numbers to be entered.

The scarier version of phishing is known as "Spear phishing". This is where things get personal and the criminal attacks an individual using information they've collected about them

5.2. Sense of Urgency

A new study shows that phishing emails are most effective when they create a sense of urgency. When people feel a sense of urgency they're more prone towards rash decisions.

Such Emails usually contain words like 'expires' , 'immediately,' 'notification'… They're all designed to get that sense of urgency.

- Your Password Expires in Less Than 24 Hours
- Change of Password Required Immediately

5.3. Appeal to Human Greed and Fear

It's important for IT professionals to understand the ways in which social engineers take advantage of human emotion in order to carry out their attacks.

Notify you that you're a 'winner.' Maybe the email claims to be from a lottery, or a dead relative, or the millionth person to click on their site, etc. In order to give you your 'winnings' you have to provide information about your bank details. These are the 'greed phishes' where even if the story pretext is thin, people want what is offered and fall for it by giving away their information, then having their bank account emptied, and identity stolen.

5.4. *Requesting Sensitive Data*

You receive an email asking for details such as:

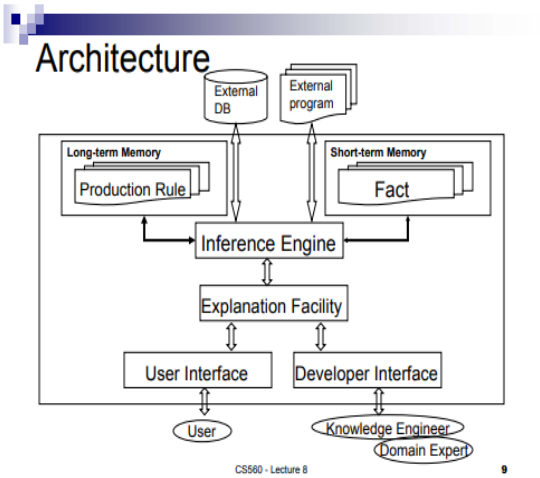
- Your name and address
- The password or PIN for your account
- Your bank account number
- Your credit card/debit card number
- Your card validation code (known as a CVC or CVV)

Most banks and organisations will never ask for such details through an email.

VI. RULE BASED EXPERT SYSTEM

6.1. Introduction

Rule based system or knowledge based systems are specialized software that encapsulate 'Human Intelligence' like knowledge there by making intelligent decisions quickly and in repeatable form. The definitions of rule-based system depend almost entirely on expert systems, which are system that mimic the reasoning of human expert in solving a knowledge intensive problem. Instead of representing knowledge in a declarative, static way as a set of things which are true, rule-based system represent knowledge in terms of a set of rules that tells what to do or what to conclude in different situations. A rule-based system can be simply created by using a set of assertions and a set of rules that specify how to act on the assertion set. The problem is stated naturally by a lay person and the way it needs to be coded as a program in a computer is also stated by the lay person.



6.2. Notations

Rules are expressed as a set of "if-then" statements. Like a Rule, hence the name rule based system. Easy for human beings to understand. Computer can create other computers Rule engines, Logic Engines and Inference Engines, Logical Knowledge.

6.3. Rules

- IF the webpage contains promising keywords [rewards , cash prize] THEN the webpage is likely phishing.
- IF a webpage URL is IP based[hex-based, decimal-based] THEN the webpage is likely phishing.
- IF a webpage used forged sender's address or spoofed identity of organisation THEN the webpage is likely phishing.
- IF a webpage copies content such as logo ,text ,images AND similar wording THEN the webpage is likely phishing.

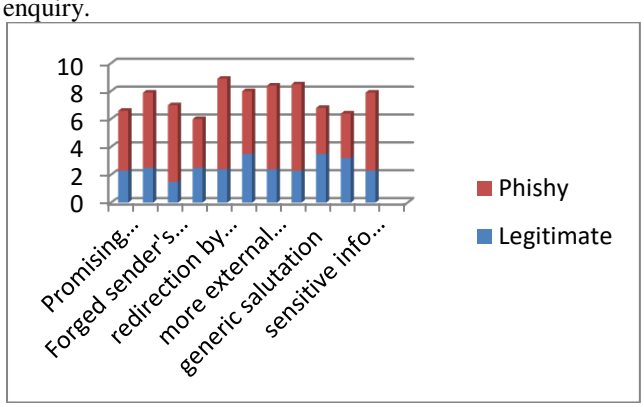
- IF a webpage is redirected by server AND the page contains password field the webpage is likely phishing.
- IF a webpage contains tempting keywords [Hurry up, Change of password required immediately] THEN the webpage is likely phishing.
- IF a webpage contains password field AND more external links than internal links THEN the webpage is likely phishing.
- IF a webpage contains generic salutations[Dear customer] the webpage is likely phishing.
- IF the body of email is an image THEN the webpage is likely phishing.
- IF the email asks for sensitive details [name,address,password,pin,bank account number,credit/debit card number,cvv number] THEN the webpage is likely phishing.

6.4. Inference

From the above set of rules, Many works related to software engineering rely upon formal models, e.g., to perform model-checking or automatic test case generation. Nonetheless, producing such models is usually tedious and error-prone. Model inference is a research field helping in producing models by generating partial models from documentation or execution traces (observed action sequences).

This paper presents a new model generation method combining model inference and expert systems. It appears that an engineer is able to recognise the functional behaviours of an application from its traces by applying deduction rules.

A bar graph is used as an inference model to analyze the legitimacy and phishing nature of an email or a website. Bar graph is plotted for various factors like Promising keywords, sender's forged address, Redirection by server, external links, generic salutation, sensitive information by enquiry.



VII. SOLUTION

7.1. Can Spear Phishing Attacks be Prevented?

The answer is no, but there are ways to help reduce their occurrence and efficacy. One way is through the use of artificial intelligence and machine learning. Spear phishing takes advantage of a lack of awareness on the user's part. The best defense is a tool that utilizes artificial intelligence and machine learning to proactively prevent spear phishing attacks by examining every email for suspicious links or URLs.

7.2. Sanitize Email Attachments

As a precautionary measure, it is highly recommended to change the format of incoming email attachments in order to remove any possible embedded threats that may go undetected by antivirus engines. Many spear phishing emails include malicious Word or PDF attachments. By changing the format of a Word document to PDF and vice versa, scripts and other possible threats are automatically removed.

- Scan for specified document properties, active content, embedded content, URLs, or hyperlinks.

If a rule is triggered, the Gateway:

- Attempts to sanitize the content appropriately and applies the What To Do? actions.
- Each content rule applies a different set of What To Do? actions for the following conditions:
- On successful sanitization - for example, Perform no action (email) or Continue to the next rule (web).
- On unsuccessful sanitization - for example, Deliver the Message (email) or Block communication using the block page for the failure (web).

7.3. Rules

Sanitization is performed by the following content rules:

- Sanitize Active Content - removes active content, such as scripts and macros, from email attachments, before safely delivering or displaying.
- Sanitize Message - removes potential threats, such as embedded and active content, URLs and hyperlinks from message bodies, and attachments from an email before safely delivering.

7.4. Use Multi Anti-Malware Scanning:

Antimalware is a type of software program designed to prevent, detect and remove malicious software (malware) on IT systems, as well as individual computing devices. Antimalware software can be installed on an individual computing device, gateway server or dedicated network appliance.

7.5. Email filters:

Loud/Noisy email subject/body (i.e. "You just won $10,000!!! Click here now!")

- Embedded images (Hosted from a trusted/untrusted domain)
- Embedded hyperlinks (Linked to a trusted/untrusted domain)
- DKIM/SPF of sending domain (Additional authentication from the sending domain to the MX server.)
- Age of sending domain (i.e. A domain purchased this week vs. one that's been around for years.)

VIII. CONCLUSION

This paper presents an investigation into the social engineering issues and technical aspects of detection and protection of phishing and spear phishing. A detailed literature survey is used to provide an analysis of different context of vulnerability of the users and to demonstrate the existing state of technology. Particular attention has been

given to spear phishing as it is considered one of the most common attacks on individual vulnerability. It is clearly demonstrated that by determining the main differences between the legitimate emails and the phishing, one can reduce the risk of this type of attack. In addition, a rule based expert system has been explored to evaluate the suitability for real-time detection and protection. Different rules have been formed based on the characteristics and features to distinguish between a legitimate and a phishing website or an email. Bar graphs are inferred from the above rules illustrating the varying level of legitimacy and phishing nature according to different features.

REFERENCES

[1] https://en.wikipedia.org/wiki/Rule-based_system

[2] https://www.incapsula.com/web-application-security/social-engineering-attack.html

[3] https://searchsecurity.techtarget.com/definition/spear-phishing

[4] https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing

[5] https://www.incapsula.com/web-application-security/spear-phishing.html