Cipher Security Phishing Attack: Study for Immunizing System

Taif S. Hasan
Computer Science Department
Al-Ma'moon University College, Baghdad, Iraq Taif.s.hasan@almamonuc.edu.iq

Abstract

The highly need usage for the internet has leads to undesired attack that could be considered as dangerous for each of us. That work involves trying to get the sensitive data such as credit card info, Bank account info, personal files and others. There are many aspects for that work. One of the most affected is the phishing attack. Fishing attack involved using much strategy in order to get the sensitive data. Our attention will be devoted to study and suggest many efficient methods for preventing the attack.

Key Words: *Cipher, Security, Phishing, Attack, Vulnerability*

Introduction

Internet plays a key role in almost all application and fields. Recently It is impossible to ignore the great need for internet. Every person, researcher, child, student, business man, and awesome will be loose if worked without the use of internet. The greater need has led to undesirable aspect; all sensitive data are stored in somewhere in the internet (Facebook server, instagram server, mail server, amazon server, classroom, Google accounts, database). These great prize pulled many bad guys to word with many tools in order to get the prize, and to earn huge money.[1]

Internet Security Issues

A security issues is any unmitigated risk or vulnerability in your system that hackers can use to do damage to systems or data. This includes vulnerabilities in the servers and software connecting your business to customers, as well as your business processes and people. A vulnerability that hasn't been exploited is simply a vulnerability that hasn't been exploited yet. Web security problems should be addressed as soon as they are discovered, and effort should be put into finding them because exploit attempts are inevitable. [2]

Network Vulnerability

What Is Network Vulnerability? A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach. Nonphysical network vulnerabilities typically involve software or data.[3]

Fig(1): Vulnerability Assessment

The most common software security vulnerabilities include:

- Missing data encryption
- OS command injection
- SQL injection
- Buffer overflow
- Missing authentication for critical function
- Missing authorization
- Unrestricted upload of dangerous file types
- Reliance on untrusted inputs in a security decision
- Cross-site scripting and forgery
- Download of codes without integrity checks
- Use of broken algorithms
- URL redirection to untrusted sites

- Path traversal
- Bugs
- Weak passwords
- Software that is already infected with virus

Phishing Attack

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering. [4]

Type of Phishing Attack

Email Phishing

Most phishing attacks are sent via email. Attackers typically register fake domain names that mimic real organizations and send thousands of common requests to victims.

For fake domains, attackers may add or replace characters (e.g. my-bank.com instead of mybank.com), use subdomains (e.g. mybank.host.com) or use the trusted organization's name as the email username (e.g. mybank@host.com).

Many phishing emails use a sense of urgency, or a threat, to cause a user to comply quickly without checking the source or authenticity of the email. [5]

Email phishing messages have one of the following goals:

- Causing the user to click a link to a malicious website, in order to install malware on their device.
- Causing the user to download an infected file and using it to deploy malware
- Causing the user to click a link to a fake website and submit personal data.
- Causing the user to reply and provide personal data.

Spear Phishing

Spear phishing includes malicious emails sent to specific people. The attacker typically already has some or all of the following information about the victim:

- Name
- Place of employment
- Job title
- Email address
- Specific information about their job role
- Trusted colleagues, family members, or other contacts, and samples of their writing

This information helps increase the effectiveness of phishing emails and manipulates victims into performing tasks and activities, such as transferring money.

Whaling

Whaling attacks target senior management and other highly privileged roles. The ultimate goal of whaling is the same as other types of phishing attacks, but the technique is often very subtle. Senior employees commonly have a lot of information in the public domain, and attackers can use this information to craft highly effective attacks.

Typically, these attacks do not use tricks like malicious URLs and fake links. Instead, they leverage highly personalized messages using information they discover in their research about the victim. For example, whaling attackers commonly use bogus tax returns to discover sensitive data about the victim, and use it to craft their attack.

Smishing and Vishing

This is a phishing attack that uses a phone instead of written communication. Smishing involves sending fraudulent SMS messages, while vishing involves phone conversations.

In a typical voice phishing scam, an attacker pretends to be a scam investigator for a credit card company or bank, informing victims that their account has been breached. Criminals then ask the victim to provide payment card information, supposedly to verify their identity or transfer money to a secure account (which is really the attacker's).

Vishing scams may also involve automated phone calls pretending to be from a trusted entity, asking the victim to type personal details using their phone keypad.

Angler Phishing

These attacks use fake social media accounts belonging to well known organizations. The attacker uses an account handle that mimics a legitimate organization (e.g. "@pizzahutcustomercare") and uses the same profile picture as the real company account.

Attackers take advantage of consumers' tendency to make complaints and request assistance from brands using social media channels. However, instead of contacting the real brand, the consumer contacts the attacker's fake social account.

When attackers receive such a request, they might ask the customer to provide personal information so that they can identify the problem and respond appropriately. In other cases, the attacker provides a link to a fake customer support page, which is actually a malicious website.

Threats or a Sense of Urgency

Emails that threaten negative consequences should always be treated with skepticism. Another strategy is to use urgency to encourage or demand immediate action. Phishers hope that by reading the email in a hurry, they will not thoroughly scrutinize the content and will not discover inconsistencies. [6]

Message Style

An immediate indication of phishing is that a message is written with inappropriate language or tone. If, for example, a colleague from work sounds overly casual, or a close friend uses formal language, this should trigger suspicion. Recipients of the message should check for anything else that could indicate a phishing message.

Unusual Requests

If an email requires you to perform non-standard actions, it could indicate that the email is malicious. For example, if an email claims to be from a specific IT team and asks for software to be installed, but these activities are usually handled centrally by the IT department, the email is probably malicious.

Linguistic Errors

Misspellings and grammatical misuse are another sign of phishing emails. Most companies have set up spell checking in their email clients for outgoing emails. Therefore, emails with spelling or grammatical errors should raise suspicion, as they may not originate from the claimed source.

Inconsistencies in Web Addresses

Another easy way to identify potential phishing attacks is to look for mismatched email addresses, links, and domain names. For example, it's a good idea to check a previous communication that matches the sender's email address.

Recipients should always hover over a link in an email before clicking it, to see the actual link destination. If the email is believed to be sent by Bank of America, but the domain of the email address does not contain "bankofamerica.com", that is a sign of a phishing email.

Request for Credentials, Payment Information or Other Personal Details

In many phishing emails, attackers create fake login pages linked from emails that appear to be official. The fake login page typically has a login box or a request for financial account information. If the email is unexpected, the recipient should not enter login credentials or click the link. As a precaution, recipients should directly visit the website they think is the source of the email.

Preventing the Attack

Phishing attack protection requires steps be taken by both users and enterprises. For users, vigilance is key. A spoofed message often contains subtle mistakes that expose its true identity. These can include spelling mistakes or changes to domain names, as seen in the earlier URL example. Users should also stop and think about why they're even receiving such an email.

For enterprises, a number of steps can be taken to mitigate both phishing and spear phishing attacks [7]:

Two-Factor Authentication (2FA)

is the most effective method for countering phishing attacks, as it adds an extra verification layer when logging in to sensitive applications. 2FA relies on users having two things: something they know, such as a password and user name, and something they have, such as their smartphones. Even when employees are compromised, 2FA prevents the use of their compromised credentials, since these alone are insufficient to gain entry.

In addition to using 2FA, organizations should enforce strict password management policies. For example, employees should be required to frequently change their passwords and to not be allowed to reuse a password for multiple applications.

Educational campaigns can also help diminish the threat of phishing attacks by enforcing secure practices, such as not clicking on external email links.

Phishing Protection from Imperva

Imperva offers a combination of access management and web application security solutions to counter phishing attempts:

Imperva Login Protect lets you deploy 2FA protection for URL addresses in your website or web application. This includes addresses having URL parameters or AJAX pages, where 2FA protection is normally harder to implement. The solution can be deployed in seconds with just a few clicks of a mouse. It doesn't require any hardware or software installation and enables easy management of user roles and privileges directly from your Imperva dashboard.

Working within the cloud, Imperva Web Application Firewall (WAF) blocks malicious requests at the edge of your network. This includes preventing malware injection attempts by compromised insiders in addition to reflected XSS attacks deriving from a phishing episode.

Employee Awareness Training

It is paramount to train employees to understand phishing strategies, identify signs of phishing, and report suspicious incidents to the security team. Similarly, organizations should encourage employees to look for trust badges or stickers from well-known cyber security or antivirus companies before interacting with a website. This shows that the website is serious about security, and is probably not fake or malicious.

Deploy Email Security Solutions

Modern email filtering solutions can protect against malware and other malicious payloads in email messages. Solutions can detect emails that contain malicious links, attachments, spam content, and language that could suggest a phishing attack.

Email security solutions automatically block and quarantine suspicious emails and use sandboxing technology to "detonate" emails to check if they contain malicious code.

Make Use of Endpoint Monitoring and Protection

The increasing use of cloud services and personal devices in the workplace has introduced many new endpoints that may not be fully protected. Security teams must assume that some endpoints will be breached by endpoint attacks. it is essential to monitor endpoints for security threats and implement rapid remediation and response on compromised devices.

Conduct Phishing Attack Tests

Simulated phishing attack testing can help security teams evaluate the effectiveness of security awareness training programs, and help end users better understand attacks. Even if your employees are good at finding suspicious messages, they should be tested regularly to mimic real phishing attacks. The threat landscape continues to evolve, and cyber-attack simulations must also evolve.

Limit User Access to High-Value Systems and Data

Most phishing methods are designed to trick human operators, and privileged user accounts are attractive targets for cybercriminals. Restricting access to systems and data can help protect sensitive data from leakage. Use the principle of least privilege and only give access to users who absolutely need it.

References

1. A Review on Phishing Attacks, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 9 (2019) pp. 2171-2175, © Research India Publications.
2. Minal Chawla, Siddarth Singh Chouhan; A Survey of Phishing Attack Techniques, International Journal of Computer Applications (0975 – 8887)Volume 93 – No 3, May 2014.
3. N-ABLE RMM, Top computer security & network vulnerabilities, https://www.n-able.com/features/computer-security-vulnerabilities, 10-8-2022.
4. Imperva, Phishing attacks, https://www.imperva.com/learn/application-security/phishing-attack-scam/, 11-8-2022
5. Oluwatobi Akanbi; A Machine Learning Approach to Phishing Detection And Defense, https://www.imperva.com/learn/application-security/phishing-attack-scam/, 11-8-2022.
6. Rajeev Kumar Shah,,Md Altab Hossin, Intelligent Phishing Possibility Detector, International Journal of Computer Applications 148(7):4-8
   August 2016.
7. Vikas Sahare, Sheetalkumar Jain, Manish Bhimrao Giri, Survey:Anti-Phishing Framework Using Visual Cryptography On Cloud, DOI: 10.5120/ ijca2016911206