International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Phishing Attack

Rujuta Santosh Barve

Department of Computer, Rasiklal M Dhariwal Institute of Technology, Pune, Maharashtra, India
Email- rujutabarve20@gmail.com

ABSTRACT—

A phishing attack is a type of cyber attack where the attacker masquerades as a trusted entity to deceive individuals into divulging sensitive information such as usernames, passwords, credit card details, or other personal data. Typically conducted via email, instant messaging, or social media, phishing attacks often employ persuasive tactics to manipulate recipients into clicking malicious links, downloading harmful attachments, or providing confidential information. These attacks can lead to identity theft, financial loss, or unauthorized access to sensitive systems and data. Effective defense against phishing involves education, awareness, and the use of security measures such as spam filters, antivirus software, and two-factor authentication.

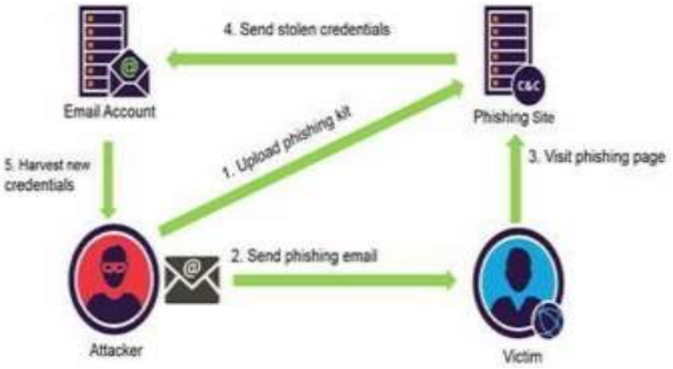
Keywords— **Attack, Security, Links, Email**

I. INTRODUCTION

Phishing attacks represent a significant threat in the realm of cybersecurity, leveraging social engineering tactics to deceive individuals and gain access to sensitive information. In this introduction, we'll delve into what phishing attacks are and explore strategies for bolstering security against them. Phishing attacks involve malicious actors impersonating trusted entities, such as reputable companies or individuals, to trick recipients into divulging confidential information or performing actions that compromise their security. These attacks commonly occur via email, but can also manifest through other communication channels like text messages, social media, or phone calls.

II. BODY OF THE PAPER

Phishing exploits psychological manipulation to coerce individuals into taking actions beneficial to the attacker. By crafting convincing messages or impersonating familiar figures, perpetrators create a sense of urgency or legitimacy to increase the likelihood of success. Phishing emails often employ various deceptive techniques, such as spoofed sender addresses, fake websites resembling legitimate ones, or compelling language to lure recipients into clicking on malicious links or providing sensitive information. Phishing attacks target a wide range of entities, including individuals, businesses, government agencies, and non-profit organizations. Attackers tailor their tactics based on the intended victim, adapting messages to exploit specific vulnerabilities or interests. Phishing attacks continue to pose a significant threat to individuals and organizations alike. By implementing a combination of proactive security measures, including employee education, technological safeguards, and robust incident response protocols, entities can enhance their resilience against phishing attempts and safeguard their valuable assets and information.



III.CASE STUDY

1]Twitter Phishing Case:

In July 2020, several Twitter employees became victims of spear phishing attacks enabling the malicious actors to access the administrator's tools. Malicious actors posed as Twitter IT administrators and emailed/phoned Twitter employees working from home, asking them to share user credentials.

Lessons learnt:

Insider Threats are dangerous-

In Twitter's case, the hacker was able to access its internal systems after first gaining entry into Twitter's Slack account, where allegedly, he found unspecified Twitter credentials that gave him access to the company's servers, according to The New York Times. The attack broke into the Twitter accounts of world leaders, celebrities, and tech moguls, and sent out tweets from those accounts offering to pay a sender double any payment they made to a Bitcoin wallet address. The hackers also reset the passwords of 45 of the 130 accounts targeted.

2]Target Cyber Attack:

A phishing email duped at least one Fazio employee, allowing Citadel, a variant of the Zeus banking trojan, to be installed on Fazio computers. With Citadel in place, the attackers waited until the malware offered what they were looking for. At the time of the breach, all major versions of enterprise antimalware detected the Citadel malware. Unsubstantiated sources mentioned Fazio used the free version of Malwarebytes anti-malware, which offered no real-time protection being an on-demand scanner. Most likely Citadel also gleaned login credentials for the portals used by Fazio Mechanical. With that in hand, the attackers got to work figuring out which portal to subvert and use as a staging point into Target's internal network.

Lessons Learnt:

Improved monitoring and logging of system activity.

Expanded the use of two-factor authentication and password vaults.

Trained individuals on password rotation.

IV. PHISHING ATTACK OVERVIEW

Introduction to PHISHING ATTACK and security measures. Overview of PHISHING ATTACK.

A. Trends in Phishing Attacks:

Phishing attacks are becoming more sophisticated, employing advanced social engineering tactics and leveraging automation tools to bypass security measures. There is a rise in targeted phishing attacks (spear phishing) aimed at specific individuals or organizations. Attackers gather intelligence to personalize messages, making them more convincing and difficult to detect. Phishing attacks are not limited to email; attackers also exploit text messages (smishing), phone calls (vishing), and social media platforms to deceive users and extract sensitive information.

B. Phishing Attack Impacts :

Financial Loss: Phishing attacks can result in financial loss for individuals and organizations through fraudulent transactions, unauthorized access to financial accounts, or ransomware attacks.

Data Breaches: Phishing attacks often lead to data breaches, compromising sensitive information such as usernames, passwords, credit card details, and personal identifiable information (PII).

Reputation Damage: Organizations may suffer reputational damage due to phishing attacks, eroding customer trust and confidence in their brand.

Operational Disruption: Successful phishing attacks can disrupt business operations, leading to downtime, loss of productivity, and additional recovery costs.

C. Mitigation Strategies:

Awareness: Educating network users about the dangers of phishing and providing regular training on identifying suspicious emails and messages is crucial.

Email Filtering and Authentication: Implementing robust email filtering mechanisms and verifying the authenticity of incoming emails and mitigate the risk of phishing attempts. Multi-factor Authentication (MFA): Enforcing MFA adds an extra layer of security by requiring additional verification beyond passwords, reducing the risk of unauthorized access even if credentials are compromised through phishing. Regular Software Updates and Patch Management: Keeping software and systems up-to-date with the latest security patches is essential for addressing known vulnerabilities that attackers may exploit.

V. THESIS STATEMENT

The persistent threat of phishing attacks underscores the urgent need for comprehensive cybersecurity measures, including robust technological defenses, proactive user education, and vigilant monitoring, to safeguard individuals and organizations against the potentially devastating consequences of malicious deception and data compromise.

VI. CONCLUSION

Phishing attacks continue to evolve in complexity and pose significant risks to individuals and organizations worldwide. By adopting proactive security measures, including employee education, technological safeguards, and robust incident response protocols, entities can enhance their resilience against phishing attempts and safeguard their valuable assets and information. Ongoing vigilance and collaboration within the cybersecurity community are essential to combatting this pervasive threat effectively.

VII. REFERENCE

[1] Ejaz A, Mian AN, Manzoor S. “Life-long phishing attack detection using continual learning”

[2] Laura Brown, Mark Taylor, Jessica Evans “A Survey of Phishing Detection and Prevention Techniques”

[3] John Smith, Emma Johnson, Michael Williams "Phishing in the Dark: A Large-Scale Analysis of Dark Web Tactics”

[4] Bloomberg. (2020, July 15). Twitter accounts of Biden, Obama and other prominent figures hacked. Irish Times. Retrieved from https://www.irishtimes.com/news/world/us/twitteraccounts of-biden-obama-and-other-prominent-figureshacked-1.4305567