BUBT
Committed to Academic Excellence

BANGLADESH UNIVERSITY OF BUSINESS AND TECHNOLOGY

Assignment

Course Code: CSE 413

Course Title: Cyber Security and Digital Forensic

Submitted to:	Submitted by:
Name: Dr. Shekh Abdullah-Al-Musa Ahmed Lecturer Dept. of CSE at Bangladesh University of Business and Technology.	Name: Syeda Nowshin Ibnat ID: 17183103020 Intake: 39 Section: 02 Program: B.Sc. in CSE Semester: Fall 21-22

Date of Submission: 17-03-2022

Why Visual-similarity-based phishing still works: User strategies for struggling on phishing attacks.

1. Abstract:

Phishing attacks, in which bogus Websites steal users' account information, have become a major problem on the Internet. The blacklist-based technique and the heuristics-based approach are the two main approaches to phishing detection. In order to detect new phishing sites that are not yet listed in blacklists, heuristic-based algorithms leverage common characteristics of phishing sites such as unusual keywords used in Web pages or URLs. However, these kinds of heuristics can be easily circumvented by phishers once their mechanism is revealed. In order to overcome this weakness, visual similarity-based detection techniques have been proposed. Because phishing sites have to mimic victim sites, visual similarity between phishing sites and their victim sites is supposed to be an inherent and not easily concealable characteristic. However, for detection, these approaches require photos of actual victim sites.

2. Keywords:

Visual-based-phishing, phishing mechanism, phishing detection, phishing attack, server-side-security, internet, information, cybercriminal.

3. Introduction:

Phishing attacks, which use a combination of faked e-mails and bogus websites to steal personal information, have increased dramatically. Phishers send e-mails to users of prominent websites, instructing them to visit a bogus site and enter their user name and password. In 2008, it was stated that over 20,000 phishing sites were created each month. There are a variety of anti-phishing tactics that may be used to prevent consumers from visiting rogue websites. PayPal, for example determines five blocking points from a phishing sequence; Reclaim email, Block phishing sites, authenticate users, Prosecute, and

Brand & Customer Recovery. For "Block phishing sites," we need to think about phishing detection. In phishing detection, there are two main approaches: blacklist-based and heuristic-based. A blacklist is a list of known phishing sites that may be compared to legitimate sites to determine if they are real or not. The blacklists are usually maintained by the software's creator. This strategy, however, cannot cover all phishing sites since the appearance and taking down cycle are too fast to keep up with. Heuristic-based detection, on the other hand, uses common phishing site features such the URL, string, and domain name information. Phishers, on the other hand, can create such traits. When heuristics-based detection employs a characteristic of a phishing site, phishers can conceal that characteristic when constructing the next phishing site.

In "Visual Similarity-based Phishing Detection without Victim Site Information" paper, they proposed a phishing detection mechanism based on visual similarity among phishing sites that mimic the same victim site.

In another paper of "Visual-Similarity-Based Phishing Detection", they presented an effective and novel approach to detect phishing attempts by comparing the visual similarity between a suspicious page and the potential, legitimate target page. The proposed approach is inspired by two previous open source anti-phishing solutions: The Anti-Phish browser plugin and its DOM Anti-Phish extension.

4. Methodology:

A phishing attacks target customers of banks and online payment services. Attackers send an e-mail to victim user, leading them to phishing sites. We must take countermeasures against these attacks. The phishing mechanism is shown in the below Figure. The fake website is the clone of targeted genuine website, and it always contains some input fields (e.g., text box). When the user submits his/her personal details, the information is transferred to the attacker. An attacker steals the credential of the innocent user by performing following steps:

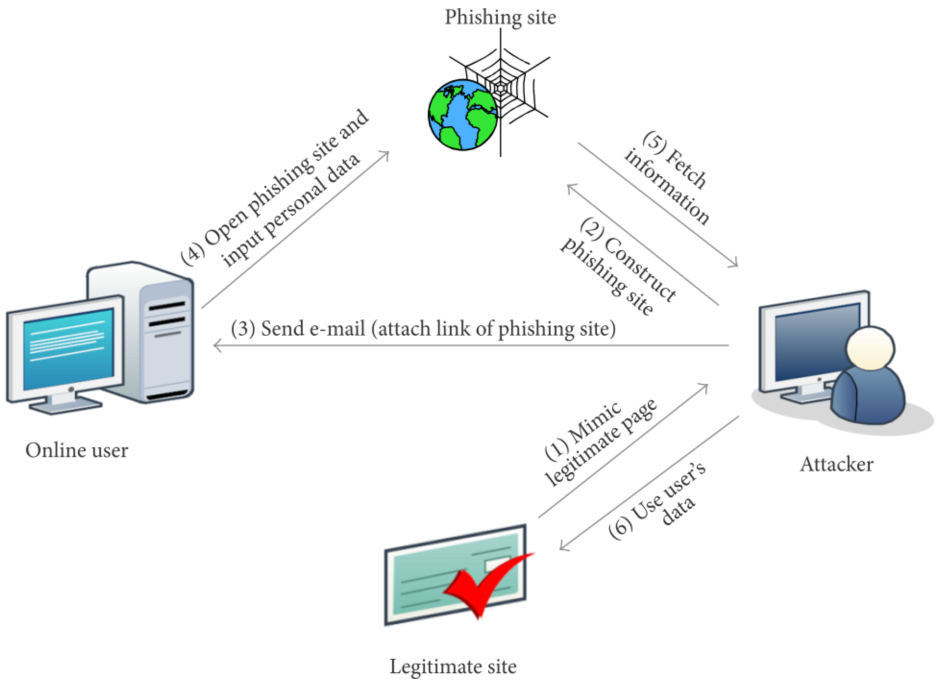
Phishing site
(5) Fetch information
(4) Open phishing site and input personal data
(2) Construct phishing site
(3) Send e-mail (attach link of phishing site)
Online user
Attacker
(1) Mimic legitimate page
(6) Use user's data
Legitimate site

Figure: Phishing Mechanism

Construction of Phishing Site. In the first step attacker identifies the target as a well-known organization. Afterward, attacker collects the detailed information about the organization by visiting their website. The attacker then uses this information to construct the fake website, URL Sending. In this step, attacker composes a bogus e-mail and sends it to the thousands of users. Attacker attached the URL of the fake website in the bogus e-mail. In the case of spear phishing attack, an attacker sends the e-mail to selected users. An attacker can also spread the link of phishing website with the help of blogs, forum, and so forth. Stealing of the Credentials. When user clicks on attached URL, consequently, fake site is opened in the web browser. The fake website contains a fake login form which is used to take the credential of an innocent user. Furthermore, attacker can access the information filled by the user. Identity Theft. Attacker uses this credential of malicious purposes. For example, attacker purchases something by using credit card details of the user.

5. **Server-Side Security:**

Server security covers the processes and tools used to protect the valuable data and assets held on an organization’s servers, as well as to protect the server’s resources. Due to the sensitive information they hold, servers are frequently targeted by cybercriminals looking to exploit weaknesses in server security for financial gain. In a computer security context, server-side vulnerabilities or attacks refer to those that occur on a server computer system, rather than on the client side, or in between the two. Cybercriminals may be getting more sophisticated, but that doesn’t mean we should make it easy for them.

The following list of common mistakes that cause server security issues:

- **Passwords:** Weak passwords can be easily hacked and poor security controls can lead to passwords being stolen and sold on the dark web. We should consider using a password manager if we’re concerned about the integrity of our passwords.
- **Old software/operating systems:** Cybercriminals are constantly identifying and exploiting weaknesses in software, which means that running an outdated version significantly increases risk of exposure.
- **Patch management**: By using a patch management service, we can ensure any changes in code are acquired, tested, and installed.
- **Open network ports:** Misconfigured servers can be easily exploited.
- **Old and unnecessary accounts:** Unused accounts offer hackers an additional way in.
- **Poor physical security:** Not all threats are virtual. Poorly secured keys can be just as dangerous.

6. **Anticipating Threats from Strengths and Weaknesses:**

With the significant growth of internet usage, people increasingly share their personal information online. As a result, an enormous amount of personal information and financial transactions become vulnerable to cybercriminals. Phishing is an example of a highly effective form of cybercrime that enables criminals to deceive users and steal important data. Phishing is a problem on two fronts. First, a hacker may gain valuable access to a single account through a successful phishing attempt. Second, if an employee is using the same password for multiple company accounts, then the hacker has now gained access to a great deal of confidential company data. Cyber-threats commonly include computer viruses and other types of malicious software (malware), unsolicited e-mail (spam), eavesdropping software (spyware), orchestrated campaigns aiming to make computer resources unavailable to the intended users (distributed denial-of-service (DDoS) attacks), social engineering, and online identity theft (phishing). Phishing, however, is a form of semantic attack and sometimes referred to as online identity theft, which aims to steal sensitive information such as username, password and online banking details from its victims. In phishing attacks, victims get directed by phishing emails to visit fake replicas (often, for example, purporting to be from the user's bank) of legitimate websites. Strengths are things that organization does particularly well, or in a way that distinguishes from the competitors. Think about the advantages your organization has over other organizations. These might be the motivation of staff, access to certain materials, or a strong set of manufacturing processes. Weaknesses, like strengths, are inherent features of organization.

7. Conclusion:

Phishing is an appalling threat in the web security domain. In this attack, the user inputs his/her personal information to a fake website which looks like a legitimate one. Many approaches are discussed in the paper "Phishing Detection: Analysis of Visual Similarity Based Approaches" for phishing detection; however most of the approaches still have limitations like accuracy, the countermeasure against new phishing websites, failing to detect embedded objects, and so forth. These approaches use various features of a webpage to detect phishing attacks, such as text similarity, font colour, font size, and images present in the webpage. Text based similarity approaches are relatively fast, but they are unable to detect phishing attack if the text is replaced with some image. Detection of phishing websites with high accuracy is still an open challenge for further research and development.

8. Reference:

[1] M. Hara, A. Yamada, and Y. Miyake, "Visual similarity-based phishing detection without victim site information," in *Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security (CICS '09)*, pp. 30–36, IEEE, Nashville, Tenn, USA, April 2009.

[2] Eric Medved, Engin Kirda, Christopher Kruegel, “Visual-SimilarityBased Phishing Detection,” 4th International Conference on Security and Privacy in Communication Networks (SecureComm 2008).

[3] K.-T. Chen, J.-Y. Chen, C.-R. Huang, and C.-S. Chen, “Fighting phishing with discriminative keypoint features,” *IEEE Internet Computing*, vol. 13, no. 3, pp. 56–63, 2009.

[4] A. Y. Fu, W. Liu, and X. Deng, “Detecting phishing web pages with visual similarity assessment based on Earth Mover's Distance (EMD),” *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 301–311, 2006.

[5] G. Weaver, A. Furr, and R. Norton, Deception of Phishing: Studying the Techniques of Social Engineering by Analyzing Modern-Day Phishing Attacks on Universities, 2016.

[6] Anti Phishing Working Group, “Phishing Activity Trends Report, Q1 2008,” Aug. 2008 http://www.antiphishing.org/reports/apwg_report_Q1_2008.pdf

[7] Visual-Similarity-Based Phishing Detection:
https://scihub.hkvisa.net/10.1145/1460877.1460905

[8] Phishing Detection: Analysis of Visual Similarity Based Approaches:
https://www.hindawi.com/journals/scn/2017/5421046/

[9] https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams

[10] https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

[11] https://www.mindtools.com/pages/article/newTMC_05.htm