DOI: https://doi.org/10.36910/6775-2524-0560-2022-47-01
UDC 004.05(075.8)
Andrushchak Igor Yevhenovich, Ph.D., Professor
https://orcid.org/0000-0002-8751-4420
Lutsk National Technical University, Lutsk, Ukraine

FEATURES OF THE MAIN DIRECTIONS, TECHNIQUES AND METHODS OF PROTECTION AGAINST FISHING ATTACKS.

Andrushchak I.Ye. Features of the main directions, techniques and methods of protection against fishing attacks. This article discusses common modern heuristic technologies used in anti-phishing tools and protection methods. An overview of different types of mobile phishing attacks is given, as well as the main methods of detecting and reducing the level of fishing attacks.
Keywords: fishing, favicon, cyber threat, vishing, smishing, mobile application, anti-phishing protection, site falsification.

Андрущак І.Є. Особливості основних напрямів, технік та методів захисту від фішингових атак. У даній статті розглядаються поширені сучасні евристичні технології, що використовуються в антифішингових засобах та методах захисту. Наведено огляд різних типів мобільних фішингових атак, а також розглянуто основні методи виявлення та зниження рівня фішингових атак.
Ключові слова: фішинг, фавікон, кіберзагроза, вішинг, смішинг, мобільний додаток, антифішинговий захист, фальсифікація сайтів.

Formulation of the problem. Currently, many services have become available via the Internet and not only. The financial sector is also no exception. Various payment systems, payment terminals, Internet wallets have appeared. The security of payments within these systems is ensured by a variety of high-tech solutions, such as security certificates, cryptographic protocols. However, all these solutions turn out to be ineffective when attackers use social engineering methods that exploit the weaknesses of the human factor.

One of the most common methods of this kind of attack today is fishing. A popular phishing technique is to create fake websites that look identical to the real ones. Fishing crimes cost billions of dollars in damages. At the same time, according to statistics, the number of fishing attacks increases by about one and a half times every year.

It is possible to stop the rapid development of such crimes by creating complex systems of protection against phishing attacks. Since the arsenal of phishers is growing at a rapid pace, it is necessary to ensure the trainability of such systems. Currently, there are no solutions of this kind, as the statistics eloquently narrates, so the creation of a comprehensive, trainable, highly effective system for protecting against fishing attacks is an interesting and relevant area. The creation of such a system involves a preliminary study of the characteristic features of fishing resources and the development on their basis of methods for assessing the degree of danger of an information resource and identifying potentially dangerous resources. This is the main focus of this work. On the basis of the obtained results, a scheme of functioning of the system of protection against fishing attacks is proposed.

Analysis of research. Currently, there is an active growth in the number of cybercriminals and cybercrimes. Fraud is the most common crime on the Internet. In this case, the victim voluntarily and knowingly provides confidential information that fraudsters can use and cause material harm. Information is often obtained through phishing, a type of Internet fraud.

Every year the number of fishing attacks is growing and their methods are being modernized. In addition, the effectiveness of fishing attacks is affected by the human factor, as scammers actively use social engineering. Therefore, there is no universal way to protect against fishing, and in order to prevent or prevent it, it is necessary to constantly study its development and methods used by attackers [1].

Since phishing resources cause the greatest damage on the first day of their existence, to ensure effective protection against them, it is necessary to continuously monitor information resources. However, it is not possible to analyze all the resources of the Internet, so you should concentrate on those that are most likely to be dangerous. When developing fishing sites, attackers are guided by the fact that the user will either make a mistake when typing a domain name, or follow a link that looks like a trusted resource. According to this, several principles for constructing domain names have been identified that represent a potential danger in relation to the given one.

Presentation of the main material and the justification of the results. Fishing is a type of fraud through which attackers obtain the user's personal information (logins, passwords, details of pay-

ment documents). Phishing can be spread through email, messaging applications (Skype, Viber, WhatsApp), social and professional networks and other web resources with high traffic (news sites, thematic forums, bulletin boards).

Fishing can be in the form of a hyperlink leading to a fake site where you need to enter the user's personal data, or in the form of a malicious application that may contain the following functionality: intercepting characters entered from the keyboard, stealing passwords from the operating system and browsers, recording audio and video, transfer of personal information and interaction with the attacker's C&C server. Fishing does the most damage to the financial sector. More than 900 bank customers fall victim to financial phishing in world every day, which is three times the daily number of victims from malware [2].

More than eight million spam and fishing attacks are recorded daily by the IBM X-Force system. This indicates that phishing attacks are an urgent threat to all areas of activity. Today, anti-fishing technologies are used based on heuristic algorithms and reputation databases (white and black lists).In the following, common heuristic techniques that are used to detect phishing links will be discussed [3].

- IP address in URL. Most legitimate web resources register a domain name. Fishers - cybercriminals who carry out phishing attacks - often save money on domain registration. As a result, on phishing sites, instead of the domain in the URL, the IP address of the malicious web server is indicated, for example, http://104.131.37.183/itau.

- Dots in URL: In a URL, dots are used to indicate a subdomain. Attackers can create third-level and higher domains to make the site address look legitimate, for example, http://settings-upgrade.000webhostapp.com/.

- Suspicious symbols. Phishers use special characters in the domain name to fool the inattentive user. Often in the URL of a fishing page you can see the special characters "@", "&", "-" and "_", for example, https://team-update-informations-account.com/.

- Slashes in URL: In URLs, slashes (slashes) indicate the presence of subfolders. As a result of a compromise of a legitimate site, a fisher can upload a phishing page to an existing subfolder (or a newly created one). As a result, the user will think that he is entering sensitive data on a legitimate site. Example: http://www.carisma.org.br/css/netflix11/.

- Availability of an SSL certificate. The certificate data indicates the use of a secure connection for the secure transmission of data between the client and the web server. SSL certificates come in entry level (DomainSSL), business level (OrganizationSSL), and extended trust level (ExtendedSSL). Acquiring ExtendedSSL is expensive for attackers. But an entry-level certificate of trust can be obtained absolutely free of charge, for example, in the Let's Encrypt certification center. Most legitimate sites have SSL certificates.

- Empty anchors or anchors leading to third-party web resources. An anchor is an HTML element that contains a link to navigate to a specific location on a given web page or to a bookmark from another web page. A fake site often has many empty anchors or anchors that lead to third-party web resources, which is rare for legitimate sites [2].

- Position of the URL and/or domain in Google, Bing and Yahoo search engines. Newly created phishing sites do not have time to be indexed by search robots, as a result of which information about them is not included in the search results.

All of the above heuristic fishing detection algorithms have both advantages and disadvantages. Let's consider some of them.

Fishing sites that use IP addresses in URLs, suspicious characters, or are located on third-level domains and above are used for mass attacks and can be easily detected by employees of companies that have received information security awareness training. The use by attackers of empty anchors or anchors leading to third-party web resources also indicates the low quality of the attack and their mass focus. The slash in URL heuristic only detects a fake page on hacked sites. Knowing the position of a domain in search engines will increase the chance of a Type 2 error if the attack comes from an infected legitimate domain, and the chance of a Type 1 error for recently registered legitimate domains [4].

The heuristic technology developed as part of the scientific work, based on the analysis of the content of a web resource, namely, on the analysis of favicons (a small image that is displayed on a browser tab to the left of the title of an open web page), is able to detect targeted phishing attacks that are carried out from again registered domains and subdomains of the third level and above, but is ineffective against fishing carried out from hacked legitimate sites. Thus, each anti-phishing technology is designed for a specific task, and only the use of all these technologies in combination with the use of machine

learning algorithms makes it possible to confirm or deny the maliciousness of a web resource with a high degree of probability.

Mobile Fishing is a growing security threat in today's world. In a mobile phishing attack, the attacker typically sends an SMS message containing links to phishing web pages or apps that ask for credentials when visiting. Attacks can also be initiated using email messages downloaded in the browser of mobile devices.

Experts come to the conclusion that the number of mobile phishing attacks has increased significantly over the past few years for various platforms on mobile devices. Compared to traditional users of desktop software, mobile app users are more vulnerable to phishing attacks. Experts agree on some common, well-known reasons for this vulnerability:

- on a small device, it is quite difficult for the user to verify the authenticity of the page, which confirms private hyperlinks, since URLs are not always displayed on mobile browsers;
- mobile users are less aware of security options to stop or prevent fishing attacks;
- Most legitimate mobile apps require users to enter their credentials with a very simple user interface, which makes it quite easy for an attacker to come up with fake apps or simple websites that mimic legitimate user interfaces [5].

The main phishing methods based on mobile device infrastructure vulnerabilities:

1. Screen size - mobile devices tend to have a small screen size. These small screens make it hard to see the full URL when users follow the link. Therefore, many users do not know when they are not on official sites when browsing the Internet. In addition, it should be noted that the small size of the on-screen keyboard can also lead to an error in typing the address.

2. Applications - the creation and deployment of malicious software (SW) does not require a high level of knowledge and special skills to persuade users in order to force them to install malware. Many mobile device owners accept offers of games, unfamiliar software, or attractive images, even if they are not at all sure about the source of the software.

3. Delays in software updates - untimely software updates allow attackers to exploit this vulnerability. First, many lower-end phones are never updated because they can't support the newer software version. Secondly, mobile device users do not install updates immediately for several reasons, for example, the update procedure takes a long time, the phone runs out of power, and the like.

4. Smishing (SMS Phishing) - Another popular phishing method uses SMS messages. This method is called "smishing". This method works in the same way as phishing, but instead of email, the victim receives a regular SMS text message. The SMS message contains a link to a phishing site. Alternatively, the user of the mobile device is asked to send confidential information in a response SMS message, for example, payment details or personal access parameters to information and payment resources on the Internet. Once the user receives such a message from a phone number, it is recommended to notify the cellular service provider.

5. Wi-Fi fishing - occurs when a user connects to the Internet through public Wi-Fi hotspots. WiFFhisher is a tool that can find WPA-secured wireless networks and disable their access points, then creates a fake WPA page that asks for password confirmation. Due to a malfunction of the access point, the user is forced to look for other available points, and without knowing it, he connects to a fake network. This allows an attacker to perform man-in-the-middle attacks and also use fake access points to intercept traffic.

6. Vishing - is one of the social engineering scams. It consists in the fact that an attacker, using telephone communication and playing a certain role, for example, a bank employee, etc., under various pretexts, entices confidential information from the payment card holder or pushes them to perform certain actions with their card account.

7. Email/Spam is the most common form of phishing. It uses the "spray and pray" approach, i.e. the same email is sent to millions of users, in the hope that the fishing attack will succeed.

8. Malware - fishing scams that involve malware that requires it to run on the user's computer. For example, ransomware is a malicious program that denies access to a device or files until some amount of money is paid. A program such as keylogger is used to identify keyboard input. The information is sent to hackers who will be able to decrypt passwords and other types of information. The trojan malware infiltrates a computer under the guise of a legitimate piece of software, but actually performs unauthorized access to the user's account. The resulting information is then passed on to cybercriminals. Malicious software is usually attached to an email sent to a user by fishers, or may also be attached to downloaded files.

9. Malvertising is malicious advertising that contains scripts designed to download malware or force inappropriate content to be placed on a user's device.

10. Spear Phishing is a more targeted attack in which scammers know which specific person or organization they are targeting. Attackers examine the target to personalize the attack and increase the chance of the victim falling into their trap.

11. Whaling is not very different from Spear Phishing, but the target group becomes more specific and limited. This method targets senior positions that are considered important figures in the information chain of any organization, commonly known as "Whale" ("Whale") in fishing terms.

12. Fishing through Search Engines - A method involving search engines where the user is directed to sites that may offer inexpensive products or services. When a user tries to buy a product, they enter their payment card or e-wallet details, which are collected by the phishing site.

13. Web Based Delivery is one of the most difficult fishing methods. Also known as "man-in-the-middle" when the hacker is between the original site and the fishing system. The phisher keeps track of the details during the transaction between the genuine website and the user without the user being aware of it.

14. Pop-Ups - Pop-ups are one of the easiest methods to successfully launch phishing attacks. They allow attackers to obtain login information by sending users pop-up messages and eventually leading them to fake websites. One type of phishing attack, also known as in-session phishing, works by displaying a pop-up window during an online banking session that looks like a message from a bank.

15. Session Hijacking is a session hijacking technique in which a phisher uses a web session control mechanism to steal information from a user.

16. Content Injection is a method in which a fisher modifies some of the content on a page of a trusted website. This is done in order to mislead the user and send him to a page outside of the genuine website, where the user is prompted to enter personal information.

17. Clone fishing is a type of phishing attack in which a legitimate and previously delivered email containing an attachment or link is used to create a nearly identical or cloned email. An attachment or link in an email is replaced with a malicious version and then sent from an email address spoofed to appear to be from the original sender. Typically, this requires either the sender or the recipient to have been previously hacked by a third party.

18. Filter evasion is a technique in which phishers use 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).

19. Link Manipulation - Using this method, the scammer sends a link to a malicious website. When a user clicks on it, they open the phisher's site instead of the one listed in the link.

Fishers can use subdomains. For example, looking at the URL www.mybank.user.com, an uninformed person will think that the link will lead him to the "user" section. In fact, the link leads to the "mybank" section, since the domain hierarchy always goes from right to left. There is a way to hide the actual URL under plain text. Instead of displaying the actual URL, fishers use offers such as "click here" or "subscribe". In fact, the URL behind the text leads to phishing sites. A more compelling email might even display an actual link, but it leads to a phishing site.

Another link manipulation method is when scammers buy domains with different spellings of a popular domain, such as: facebok.com, googlle.com, yahooo.com, etc. They then trick users into creating similar sites and asking for personal information. In the following method, the attacker misleads the user about the link by taking advantage of similar characters. For example, the Latin letters "s", "o" and "x" can be replaced with similar Cyrillic letters.

20. Website Forgery - a method in which a malicious website pretends to be genuine. Forgery is mainly carried out in two ways: cross-site scripting and site spoofing.

21. Cross-site scripting (XSS) is an attack in which a hacker injects malicious code into a web application or website. This is a very common and widely used technique in which the victim is not the direct target. Most likely, an attacker exploits a vulnerability in a web application or website that the user is visiting. Ultimately, the malicious script is delivered to the victim's browser. Another method is to create a website that looks like a legitimate site that the user actually intends to access. The fake website has a similar user interface and design, often with a similar URL [6].

Methods for detecting mobile fishing attacks. Typically, phishing detection systems for mobile devices contain a filter-based mechanism: blacklist and whitelist. Filtering mechanism: URLs are checked in this technique. Filtering can be done based on a set of rules or based on statistical differences between legitimate and fraudulent content. This method can effectively detect smishing, vishing and Wi-Fi fishing.

"Blacklist": A human-checked method that compiles a list of websites known as phishing links. This method is currently supported by various browsers that communicate with trusted servers to obtain a blacklist of URLs.

Whitelist: In this method, users specify sites they trust. The method can be used to detect an attack where multiple legitimate numbers can be provided to stop receiving unwanted SMS containing fake web addresses, such as smishing.

Methods to reduce mobile fishing attacks. While it can be difficult to identify fake mobile apps, there are several ways to mitigate phishing attacks on mobile devices:

a) Use Official Apps: Users should only download apps from official stores.

b) User education: User education is very important to prevent users from clicking on unknown links.

c) Use secure browsers: Browsers with security features eliminate malware and phishing sites to protect users.

d) App Store Control: Providers must take additional steps before allowing developers to upload apps to the public.

e) Security Solutions: Just like for regular desktop computers, security vendors offer antivirus programs for mobile devices. Such programs eliminate malicious attacks on mobile devices[7].

Conclusion and prospects for further research

The considered methods and technologies of fishing attacks demonstrate how resourceful attackers are, and the study of the analysis of diagrams confirms the relevance of the phishing problem. Effective protection against phishing is possible only with the complex specific use of various technologies.

Fishing sites use various types of technologies to prevent users from entering sensitive information. Currently, the most popular browsers are equipped with anti-phishing protection. Many companies specializing in the development of cyber threat protection systems create software that includes filters for fishing sites.

A popular type of solution to alert the user to an unsafe site is to use a database with a list of phishing site addresses. The problem is that today's phishers create and distribute phishing sites faster than the addresses of these sites can be blacklisted. In addition to list-based technology, machine learning is used, where a combination of various site characteristics determines the level of trust in it. Both the appearance of the site and its registration data are considered.

The task of determining the technologies of the level of trust in an Internet resource is difficult to formalize, and the site URL also contains a lot of information that can be extracted and used. algorithmically difficult to implement. Despite this, some algorithms can be used in combination with different methods. For example, this is how you can determine the degree of similarity between a phishing domain and a domain from the "white list" and use this feature in a multicriteria task.

References

1. Bay H., Ess A., and Tuytelaars T. SURF: Speeded Up Robust Features // Computer Vision and Image Understanding (CVIU). 2008. V. 110. No. 3. P. 346–359.
2. Devyanin P. N. Security models of computer systems. Access and information flow management. Proc. allowance for universities. M.: Hotline-Telecom, 2011.
3. Lininger R. and Vines D. Phishing: Cutting the Identity Theft Line. Wiley, 2005. 334 p.
4. Mobile Phishing Attacks and Mitigation Techniques. [Electronic resource] // Journal of Information Security. URL: http://www.scirp.org/journal/jis/
5. Patil R., Dhamdhere B.D., Dhonde K.S., Chinchwade R.G., Mehetre S.B. A hybrid model to detect phishing sites using clustering and bayesian approach // IEEE International Conference for Convergence of Technology (I2CT), 2014.
6. RamB.Basnet,TenzinDoleck.TowardsDevelopingaTooltoDetectPhishingURLs:A Machine Learning Approach // IEEE International Conference on Computational Intelligence & Communication Technology. 2015.
7. Sandhu R., Coyne E. J., Feinstein H. L., and Youman C. E. Role-Based Access Control Models // IEEE Computer (IEEE Press). 1996. V. 29. No. 2. P. 38-47.