Advances in Intelligent Systems and Computing 918

Álvaro Rocha
Carlos Ferrás
Manolo Paredes *Editors*

Information Technology and Systems

Proceedings of ICITS 2019

Springer

The Art of Phishing

Teresa Guarda[1,2,3(✉)], Maria Fernanda Augusto[1,4], and Isabel Lopes[3,5]

[1] Universidad Estatal Península de Santa Elena – UPSE, La Libertad, Ecuador
tguarda@gmail.com, mfg.augusto@gmail.com
[2] Universidad de las Fuerzas Armadas-ESPE, Sangolqui, Quito, Ecuador
[3] Algoritmi Centre, Minho University, Guimarães, Portugal
[4] BITrum-Research Group, C/San Lorenzo 2, 24007 León, Spain
[5] UNIAG (Applied Management Research Unit), Polytechnic Institute of Bragança, Bragança, Portugal
isalopes@ipb.pt

Abstract. Nowadays there are many threats that a company needs to protect itself. Everyone knows someone who has fallen for a coup by using an email, message or phone. People who pass by someone they trust, to extract data and money from the victim. These three ways are used to try convince someone to deliver accounts, credit card and document data in companies and at a particular level. According to Symantec, more than 6 hundreds of companies per day are targeted for Phishing, specifically Business E-Mail Compromise (BEC). In it, criminals pass through a central figure in the company, usually the CEO, and try to extract information or get employees to transfer money. This type of attack has generated in the last years losses of billions of dollars for the businesses affected. It is urgent that all company employees and individuals know as soon as possible what Phishing is and what steps to take.

Keywords: Phishing · Spear phishing · SMiShing · QRishing · Vishing · Threats · Security · IoT

1 Introduction

The Internet has become an integral part of our lives on a personal and professional level. With the rapid technological advancement many types of fraud have emerged seeking obtain confidential data and use them for personal profit. The main ones being Phishing, vishing, SMiShing, and QRishing.

Symantec 2018 Internet Security Threat Report (ISTR) shows that the targeted attack industry continues its expansion, including a 600% increase in IoT attacks. According to Symantec, innovation, organization and sophistication are the tools of cyber-attackers, because they work even more efficiently to discover new vulnerabilities [1].

The increase in the use of Internet services, produces that we provide personal information to different platforms, applications, sites and web portals. This is not done in a controlled way, on the contrary, every time we pay less attention, so it is expected that there are people inspired by various motivations that want to get our data.

Á. Rocha et al. (Eds.): ICITS 2019, AISC 918, pp. 683–690, 2019.
https://doi.org/10.1007/978-3-030-11890-7_64

Phishing arise from this thought of subtraction of information, and currently is considered one of the most common crimes, and unfortunately the crime in which we fall more easily [2].

Phishing is a process of obtaining confidential information illegally from users, such as usernames and passwords, for fraudulent purposes [3]; which is operationalized through the sending of emails as a bait, with the objective of capturing a potential victim, creating the necessary scenarios to make credible the whole scheme.

Lately phishing is one of the most common attacks on the Internet [4], because it is a relatively easy attack to apply and reaches multiple users at the same time. And it is enough that the user clicks on the malicious link to have their personal data stolen.

Phishing attacks are executed by performing the following steps (Fig. 1):

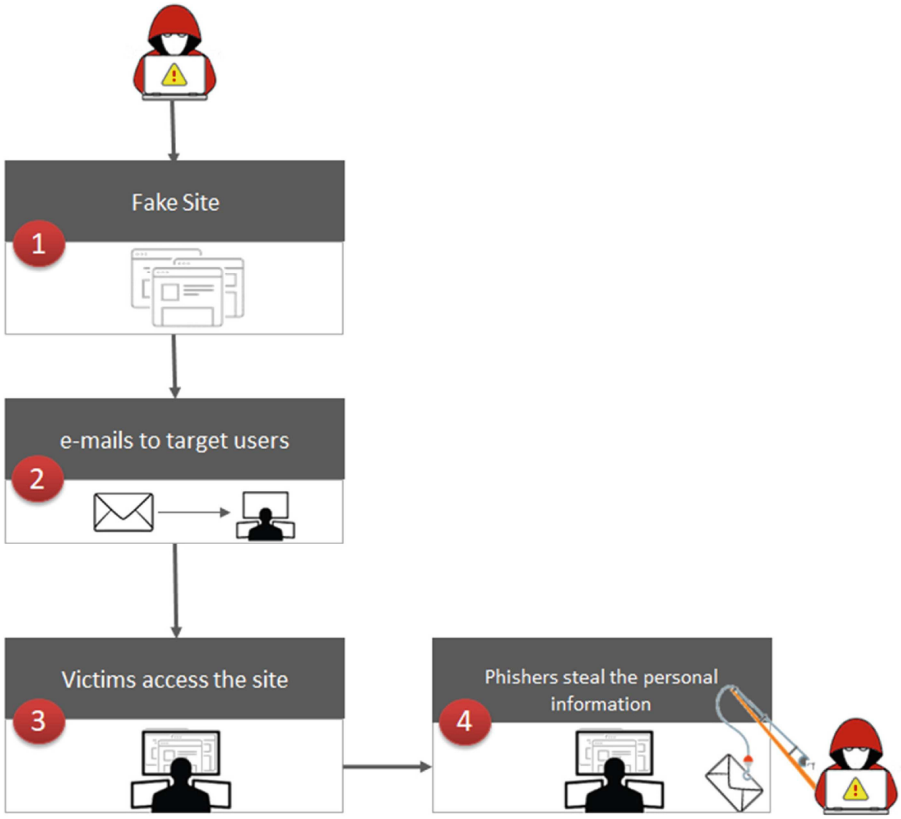

Fig. 1. Phishing attacks steps.

– In a first step the phisher creates and makes available a false site equal to the legitimate site;
– After in the second step, false emails are sent with the link from the legitimate site to the potential victim on behalf of legitimate companies and organizations, trying to convince potential victims to visit the sites;
– In the third step, victims visit the fake site by clicking on the link and entering their useful information;
– Then in the fourth step, phishers steal personal information and thus begin to perform fraud.

2 Phishing

The term Phishing comes from the English word fishing which means fishery. This threat consists of false messages sent by criminals who pass through reputable companies or people [1]. They cast the bait and often the victims are hooked. Among the most common baits we have: the most urgent email from the bank warning that your account would be blocked; and the offer of a well-known company in which it only gives you a few hours to decide [2].

Spear Phishing is a highly localized Phishing attack, preceded by a thorough study of the target by the attacker [5–7]. Spear Phishing has a ten steps cycle:

(1) The phisher defines its target within an organization, using social networks or others Internet information sources to find the company employee's with access to the data\systems;
(2) The attacker's work reveals the patience of a fisherman, he will follow the digital footprint of the potential victim (employee), identifying other people he may know;
(3) A false but recognizable email is created to impress a colleague or boss;
(4) An email is sent to the false e-mail employee, with a link or file (s) attached;
(5) The fake email skips the spam filter and arrives at the employee's inbox;
(6) The employee opens the email because he knows (he thinks he knows) the sender;
(7) The employee trusts the sender, and clicks on the link, or opens the attachment;
(8) The open website causes the credentials to be stolen, allowing malware to be installed. When opening attachment the malware is installed infecting the system \network;
(9) The attacker use the backdoor to stolen information, which if used intelligently by the attacker can guarantee him enough knowledge to assimilate the identity of someone from the organization with more power [3].

In 2017 the phishing rate in South Africa was the highest, where 1 in 785 emails was a phishing attack [1] (Fig. 2).

Rank	Country	1 in
1	South Africa	785
2	Netherlands	1,298
3	Malaysia	1,359
4	Hungary	1,569
5	Portugal	1,671
6	Austria	1,675
7	Taiwan	1,906
8	Brazil	2,117
9	Indonesia	2,380
10	Singapore	2,422

Fig. 2. Phishing rate by country (source Symantec [1]).

For Symantec "Spear phishing is the number one infection vector employed by 71% of organized groups in 2017. The use of zero days continues to fall out of favor. In fact, only 27% of the 140 targeted attack groups that Symantec tracks have been known to use zero-day vulnerabilities at any point in the past" [1]. In 2017 71% of targeted attack infection vectors were caused by spear phishing emails [1] (Fig. 3), spear phishing is the most popular.

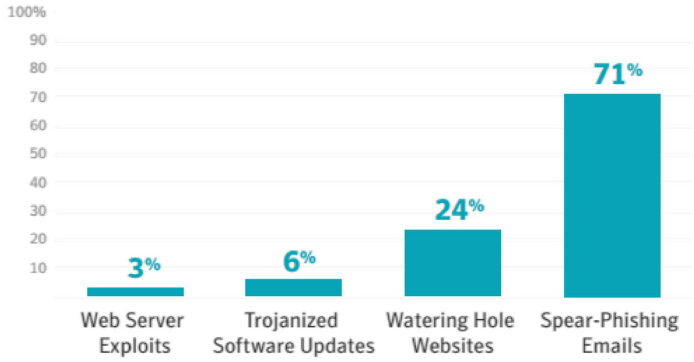

Fig. 3. Targeted attack infection vectors (source Symantec [1]).

We can consider another's forms of Phishing, like SMiShing, QRishing and Vishing; which we will describe in the following subsections (Fig. 4).

Fig. 4. Phishing forms. ❶ Phishing, ❷ SMiShing, ❸ QRishing,❹ Vishing.

2.1 SMiShing

SMiShing means Phishing by SMS. SMiShing is similar to Phishing, a text message is sent to the user of the phone instead of an email. In the text message, the user is asked to call a certain phone number or to go immediately to the website to take immediate action, and a personal information system (passwords, credit card data) is requested through an automatic response system. These messages ask to use it and click on a link and fill out a form or reply to the message. It could be for example, about a need to update registration or the opportunity to redeem a prize not to be missed. SMiShing is characterized by having two attack vectors [8]:

(1) When the attacker sends an SMS with information about changes, a purchase, changes, refunds or cancellations. The user is alarmed and is deceived, the message includes a phone number of the attacker, and thus could communicate with the attacker requesting personal information of the user or codes necessary for a micro-payment online. This form of attack is summarized by the theft of information through a telephone conversation between the victim and the attacker;
(2) Through the sending of an SMS that includes a URL that when visited by the user, a malware is installed on his phone. Then it replicates all the user information stored on the phone to the attacker's server.

2.2 QRishing

QR codes are becoming more and more present in our daily lives (shoppings, train stations, marketing promotions, touristic spots, apps that can be used to read and decipher codes and in many cases can lead directly to a website, among others). Once QR codes are used for legitimate purposes, they can also be developed or manipulated for illicit purposes and have the same effect as phishing e-mail. QRishing uses socially engineered bait to make potential victims scan the code [9].

2.3 Vishing

The Vishing attacks, abbreviated to Voice phishing, is an electronic fraud technique. Vishing is applied over phone calls rather than through messages or email. These calls are

primarily intended to obtain bank details or other important personal information from victims, usually by automatic calls or equipment that modify the voice of the fraudster [8].

When a visher creates an automatic voice system to make voice calls to telephone users requesting private information, it is called Vishing or Voice Phishing. The intent is the same as phishing by email or phishing by SMS, The voice call creates a sense of urgency for the user to take action and provide additional information [10].

3 Attack and Prevention

Company's usual security policy includes anti-virus software, firewall, e-mail protection, among others. While prevention is always the best option, a company should not rely only on best practices on the part of its users, it should make sure that all its employees are fully aware of what Phishing is and the risks to which they can expose themselves if they are not attentive.

The most common form of phishing attack is through email. Sometimes phishers use domains similar to real emails or even common domains like hotmail. If someone you know has become a victim of a phishing attack, attackers can gain access to that person's account and fire e-mails through it or him. What the attacks usually have in common is the alarming tone. Phrases like "your bank account was blocked" or "your email account will be deleted soon" are used to attract attention and make the victim act without thinking [11].

It is not enough to know what Phishing is to be free of it. You need to always be alert and instruct all your team members to be aware of this type of threat. The main tips are:

- Always check the sender's email address;
- Observe the contact information and signature of the email;
- Never write your access data and passwords on forms or pages sent by email
- Do not click on links unless you're sure the sender is trusted;
- Do not download attachments without first checking with the antivirus;
- If you receive an unusual request to transfer files or money from an acquaintance, manager or co-worker, confirm with the person if the request is true.

In the case of SMiShing when clicking or replying to the message, you can be directed to malicious sites, where, once you enter your data, they will end up in the hands of criminals. The targets are usually personal information such as address or CPF, credit card data and bank access passwords, social networks and emails. To avoid SMiShing, never click sent links and never provide your data on unknown forms or sites. Whenever you make purchases or transactions that require typing your data, make sure the URL starts with https instead of http.

With QRishing, just as it is possible to attack users, it is possible to attack the systems that will make use of the content of this QR Code. Depending on the content inserted in the QR Code and the security of the application that makes use of the scanned content it is possible to cause of the most diverse frauds. It is also possible to dominate the victim's device if the QR Code content exploits some vulnerability like Buffer Overflow in the application that interprets the QR Code. For attackers, one of the

advantages of using QR Code to trigger access to a URL is the fact that the user does not have to type the URL and often end up only holding onto the displayed content, thus becoming a victim in potential for Phishing attacks that lead to cloned-looking Web sites. Users are often the weakest link in a system, so instructing them is critical. When we're talking about targeted attacks on businesses, where curiosity drives users to risk exposures. To avoid QRishing users should only scan secure sources with a reliable scanner, and disable any kind of automatic action on the part of the reader. In the case of information systems there should be a duly updated whitelist and verify that the content size is as expected [12].

In Vishing attacks, calls can be made directly by a person or using recordings or automated voices. It is common for the fraudster to pretend that he has to confirm personal data to update the register at the bank, authorize a purchase on the credit card or give away some credit. Do not provide personal information over the phone under any circumstances. If you do have a pending purchase, you can call the central bank whose number is usually written on the card. Do not call the numbers passed by the person who called you, as they are also part of the coup.

4 Conclusions

On the Internet, attacker's try to get users to access malicious links through various tactics, including email persuasion, or by requesting confirmation of cadastral data, by false letters sent via mail taking advantage of the name of entities, by SMS and any other means that can lead the innocent user to bite the bait in this attack called Phishing. While all these means involve some kind of persuasion, none is so simpler and probably effective as the Quick Response Code (QR Code).

Today's diversity of computing devices and mobile devices allow users to download and install applications without realizing that they may not be a copy of legitimate official applications,

Attackers are using phishing as a highly profitable activity. In recent years there has been an increase in the technology, diversity and sophistication of these attacks Phishing differs from traditional scams at the level of fraud that can be achieved, being a higher level.

Online users should be informed and undertake a periodic vulnerability analysis to identify and mitigate weaknesses that can lead to a successful phishing attack.

References

1. Symantec Internet Security Threat Report. Symantec, vol. 23 (2018)
2. Alsharnouby, M., Alaca, F., Chiasson, S.: Why phishing still works: user strategies for combating phishing attacks. Int. J. Hum.-Comput. Stud. **82**, 69–82 (2015)
3. Brill, J.A., McGeehan, R., Muriello, D.G.: U.S. Patent No. 9,578,499, Washington, DC (2017)
4. Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D.: Wirel. Netw. **20**(8), 2481–2501 (2014)

5. Mohammad, R.M., Thabtah, F., McCluskey, L.: Tutorial and critical analysis of phishing websites methods. Comput. Sci. Rev. **17**, 1–24 (2015)
6. Ariu, D., Frumento, E., Fumera, G.: Social engineering 2.0: a foundational work. In: Proceedings of the Computing Frontiers Conference (2017)
7. Gascon, H., Ullrich, S., Stritter, B., Rieck, K.: Reading between the lines: content-agnostic detection of spear-phishing emails. In: International Symposium on Research in Attacks, Intrusions, and Defenses (2018)
8. Chiew, K.L., Yong, K.S.C., Tan, C.L.: A survey of phishing attacks: their types, vectors and technical approaches. Expert Syst. Appl. **106**, 1–20 (2018)
9. Rzeszut, E., Bachrach, D.: 10 don'ts on your digital devices: the non-techie's survival guide to cyber security and privacy. Apress (2014)
10. Dhiman, P., Wajid, S.A., Quraishi, F.F.: A comprehensive study of social engineering - the art of mind hacking. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. **2**(6), 543–548 (2017)
11. Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., Ebner, N.: Dissecting spear phishing emails for older vs young adults: on the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (2017)
12. Falkner, S., Kieseberg, P., Simos, D.E., Traxler, C., Weippl, E.: Usable cryptographic QR codes. In: IEEE International Conference on Industrial Technology (ICIT) (2018)