Phishing and Advanced Persistent Threats

Pedro Ramos Brandao[1]*, Henrique S Mamede[2] and Miguel Correia[3]

[1] Instituto Superior de Tecnologias Avançadas, Lisbon, Portugal

[2] INESCT TEC - Universidade Aberta, Lisbon, Portugal

[3] INESC-ID, Instituto Superior Técnico – Universidade de Lisboa, Lisbon, Portugal

ABSTRACT

The paper addresses one of the techniques mor used by Advanced Persistent Threats attacks, phishing. The paper demonstrates the complexity of the technique, explains how attacks can be carried out, and presents defense techniques, and strategies against phishing attacks. The article also presents a summary description of what an Advanced Persistent Threat attack is. This description characterizes this type of attack.

***Corresponding author**

Pedro Ramos Brandao, 1Instituto Superior de Tecnologias Avançadas, Lisbon, Portugal. E-mail: pb@pbrandao.net

Keywords: Cybersecurity, Advanced Persistent Threats, APT, Phishing.

Introduction

In recent years there has been a significant increase in Advanced Persistent Threat (APT) cyberattacks. These attacks are significantly more dangerous and complex than traditional attacks. It has also been noted that one of the techniques, among others, used in these attacks is phishing. The main purpose of this paper is to demonstrate the complexity of the phishing technique used in APT-type attacks, as well as possible defense techniques against phishing [1].

Research Background

An Advanced Persistent Threat, as the name implies, is not like a regular attack or attack performed by an ordinary hacker. APTs are usually achieved by a group of advanced attackers who are well funded by an organization or government, to obtain crucial information on their target organization or government. In some cases, they may also can serve to destroy or disable certain structures or systems [1].

APT is a military term adapted to the information security context that refers to attacks carried out by nation-states. The term APT is defined by the combination of three words, which are [2]:

- **Advanced:** APT attackers are usually well-funded and with access to the advanced tools and methods needed to carry out an APT attack. Such advanced methods include the use of various attack vectors to initiate and maintain the developing attack, where the phishing tool is included.
- **Persistent:** APT attackers are highly determined and persistent, and do not give up. Once they enter the system, they try to stay within it as long as they can. They plan to use various evasive techniques to avoid detection by their targets' intrusion detection systems. They follow the - low and slow - approach to increase the success rate, that is, they use a lateral movement approach (after gaining initial access, the attacker moves deeper into the network in search of sensitive data and other high-value assets).
- **Threat:** The threat in APT attacks is usually the loss of confidential data or hindering of mission-critical components. These are growing threats to many national entities and organizations which have advanced protection systems that protect their missions and/or data [3].

According to the National Institute of Standards and Technology (NIST), an APT attacker [4]:
(i) Pursues its goals repeatedly over a long period of time;
(ii) Adapts to the efforts of defenders to resist it; and
(iii) Is determined to maintain the level of interaction necessary for the execution of its purposes. Such purposes are to exfiltrate information or to undermine or prevent critical aspects of a mission or program through multiple attack vectors. They can also render certain systems inoperable.

To achieve the assigned aim, the attackers need to go through several attack stages in different ways, without being detected. Those multiple stages involve establishing back-up points, scanning the internal network, and moving laterally from one system to another in the network to reach the target system and perform its harmful activity. After the harmful activity, the attackers can choose:
(i) To stay on to continue their malicious activities on other systems on the network; or
(ii) Leave the system after the cleanup, depending on the requirements of the funding source. Those various stages usually involve logging into one of the systems within the network and then performing privilege escalation as necessary to reach the

target system, followed by accessing sensitive systems and sending the status/information over an Internet connection to the attackers' command and control center [2]. The second stage of the attack has seen the systematic use of, among others, the phishing technique [2].

In an article published in 2013, Mandiant, an American cybersecurity company, reported several important findings of APT attacks carried out by one of the largest APT organizations on a wide range of victims over long periods of time, starting around 2006, maintaining an extensive computer infrastructure around the world [1]. In its M-Trends 2017 report, FireEye points to the increase in the level of sophistication of financial attackers which is no longer inferior to advanced state-sponsored attacks [1]. In support of this, FireEye presented evidence showing how the attackers avoided detection by IDS/IPS by using backdoors that were loaded before the operating system was even loaded. Every year the number of reported APT attacks has been increasing [2]. All this advancement in attack methods and tools repeatedly points to the need for the implementation of strong defense methodologies by every organization looking to protect itself as well as its data. Defense methods must be employed in all phases of an APT attack, since the technology and methods used for the attack are also different in all phases and stages [1].

Phishing

Phishing is a cybersecurity attack that uses e-mails, messaging software or any other form of electronic communication to trick users into acting on behalf of others, can release confidential user data or financial data that can be used on behalf of the criminal, or he can install malware on the victims' machine to access other computers through it.

A phishing attack involves three factors: the bait, the hook, and the catch. The bait in most cases is an e-mail message that seems to come mainly from a trusted organization (e.g., the victim's company or a bank) or some other service and contains a link to the hook. The hook is a website that looks legitimate and asks users to enter their credentials to log into the application. The problem is the use of the data captured by the phisher [5]. The most common form of phishing is email phishing. Phishing is a hybrid attack that uses social engineering and technology. Phishing can also be used to get users to install malicious software on their machines, usually it is an attached downloadable file that can have any format and can be used as a keylogger that captures user credentials or as a session capture that can steal an active session and act on behalf of the phisher, for instance by sending funds to the phisher's account [5]. Another form of phishing is Search Engine Phishing, where phishers create a fake website and, with their own tools, index that site in search engines to rank high in the results.

Phishing may also use messaging applications, SMS, social media and even online games [5]. The steps of a phishing attack are the following [6]:

1. The perpetrators have created a site that at first glance appears legitimate, which may correspond to a real site, eg. banking site.
2. They send a large number of e-mails to a variety of Internet users that contain a link to their fake website and hope that the victims will take the bait.
3. When users click on the link in this e-mail. They are directed to the fake website, where they can enter their credentials for a service they believe to be legitimate, for example, e-banking username and password.
4. Now, the phisher can hijack victims' personal information and use it for an attack or a lateral movement intrusion, as is the case with APTs.

Attack Techniques

To be successful, a phishing attack must contain an attractive bait. Usually, bait is a hyperlink that is hidden within Text tag that induces clicking in an email, Narendra et al. classifies hyperlinks used as bait into the following 5 categories [6]:

Category 1: The hyperlink provided in the <a> tag is different from the anchor text, e.g.. www.cgd.pt/bank/login. Thus, the user thinks that once he clicks the link he will be sent to his bank, yet in fact, he will be redirected to another machine to a malicious web page.

Category 2: Dotted decimal address inside URI or anchor text instead of a DNS name, for instance. Log in to your Bank here

Category 3: The hyperlink is encoded by encoding letters of the address alphabet to ASCII codes or by linking the original page, but at the end of the link adding an @ character after the IP of the malicious page. for instance. Log in to your Bank here

Category 4: The hyperlink does not contain a link in the anchor text, but a phrase that engages users to click on it, for instance. Click here to login to your bank and in the URI position contains a link similar to the original link to make it look legitimate, for example. for a bank where the legitimate URI is "www.bankwebsite.pt" the phisher can create a new DNS similar to this as "www.cgd-security.pt" to make it look more realistic to the victims.

Category 5: The fifth type of bait is trickier and contains more cyber attack methods, such as CSS (Cross Site Scripting). The basic idea is to exploit a vulnerability in the legitimate website that will direct users to a fake website. for instance. <a href="http://pt.unicre.pt/track/dyredir.jsp?rDirl= http:// 200.251.251.11/.verified /"> Click here <a> the above method exploits a vulnerability of "en.unicre.co.uk" to lead users to phisher site.

According to there are two methods of phishing attacks that are quite similar to each other [7]. The first is that the phisher creates the fake website and once the user enters his credentials, the phisher redirects the user to a genuine login page, so that the phisher does not log the user into the genuine page. The second method is the same, but this time the phisher logs the user into the genuine application, so that the phisher is not affected by the security safeguards of the genuine site. Furthermore, "clone-phishing" can be used to appear more reliable to users. Clone-phishing presents a similar legitimate website address and replaces existing characters with similar ones, e.g. "1" (one) can be used to replace l (small L).

Defense Techniques

Phishing detection is divided into different categories or approaches [6]. We introduce the following 4 phishing defense approaches: email approach, browser integrated tool, web page content analysis, visual similarity.

1. The logic of the email-level approach is that a user cannot be fooled if he does not receive the email, so it consists of filters that block or blacklist suspicious emails.
2. A built-in browser tool, detects phishing by comparing the address bar value with values from a blacklist and alerts the user to prevent them from visiting the site.
3. Web page content, analyzes of every component like entry, div, form, img, text, hyperlinks etc tags, of every html page, suspecting legitimacy through anomalies, but phishers have found a way to overcome this method, by creating web pages without any html tags.
4. The idea of visual similarity is to divide into blocks, dividing according to viewing cues, each Web page and then compare them to find out if any of them are false [6].

According to, phishing detection, which is the first step in finding a phishing attack, is categorized into two categories: human detection and machine detection [5]. A Phishing attack can be recognized by checking the address bar (URL), digital certificates, content and type expressions of a website [8]. Except for users who are trained on their job, other users generally cannot tell a legitimate site from a fake one. Human detection is based on training Internet users not to be fooled; it also includes games designed to train users to avoid phishing. For machine detection, proposes a framework called PhishSnag that operates between an email transfer agent and an email user agent and processes the user's emails before they reach him, so it stops the threat before it is accessed by the target [5]. The detection rate can be set from 93% with 0.5% false positives to 99% with a higher false positive rate. Moreover, there are algorithms such as Adaline and Backpropagation that work with the support of a vector machine and detect and classify phishing attacks with a detection rate of over 99%.

Defense Strategy

Most phishing detection methods consist of whitelisting and blacklisting and content-based filtering [9]. Shahriar et. al. propose an email add-on that checks the identity of the phisher based on the link contained in the email and is also useful on known and unknown threats because it uses a character-based algorithm. The article presents the algorithm used to implement this add-on [10]. Briefly, it works as follows, it acquires anchor text and real links and if it is not the same it is considered a type 1 attack, if either of the two texts is in IP address form it is considered a type 3 attack, if either of the two texts is in encrypted form it is considered a type2 attack and finally if the complement cannot find the destination details we say it is a type4 attack, so it needs to be analyzed by a DNS analysis procedure where it will find out if that DNS name is whitelisted or blacklisted.

In some browsers such as Google Chrome there is already a built-in antiphishing system called Google Safe Browsing. It is based on URL address comparison [8]. In a survey comparing antiphishing systems in browsers Chrome proved to be the best among other popular ones such as Firefox, Safari, Internet Explorer [8]. Best practices according to avoid mobile phishing are as follows: use official applications, user education, safer browsers with security features installed, bookmarks that can prevent incorrect typing of a URL, increased control of installed applications from application stores, and security solutions such as installing antivirus software on mobile phones [5, 10]. MobiFish, which is designed for mobile platforms, and consists of two applications: WebFish which is for checking websites; and Appfish for checking applications. This software compares the real identity of web pages and applications with their claimed identity to detect phishing sites or applications [11].

Phishing in APTs

When compared to other malware, APT attacks follow a different attack script. Taking as an example the Zeus bot, which is a widespread Trojan used to steal passwords for victims' online banking activities. It provides no propagation mechanism, but victims are often lured into opening malicious attachments or clicking on a malicious link to download the malware via linked emails, i.e., phishing [12].

The malware generates a dropped, which in turn will be injected into a running process to perform predefined malicious functions, including collecting the online banking password, for instance, or opening a back door to start an APT attack, or acting as a Trojan to control the machine for a long period, or launching multiple DDoS-like attacks [13].

Generally, several C&Cs are deployed, and the malware will connect to different C&Cs. The malware or its associated configuration file at any time can be updated to generate a new version of the dropped to perform similar predefined malicious functions, and collect further data or perform more functions, all possible through the initial use of the phishing technique; entry is through human error someone clicking on a malicious link and allowing an APT attack to evolve [14].

Phishing in the APT context is used to deploy espionage malware of restricted dissemination for data exfiltration or another goal. Spear phishing emails are well crafted and consistently distributed. High pre-infection recognition is needed to mitigate this attack after the phishing malware runs. The attackers must know and understand the identity and background of the victims or their affiliations, so there is a social engineering factor here in connection with phishing applied to APT. Furthermore, attackers will typically be very actively monitoring all events that happen in the context of the victims or the victims' organization [13].

Like ZeuS bot, the APT type phishing malware generates a dropped, injected into a running process to acquire preliminary information, including email or message passwords and all file names on the hard drive. To hide from the detection mechanism, phishing-generated APT-type malware usually does not carry obvious malicious functions, for example, it rarely changes the infected system as a zombie machine to launch DDoS attacks or send spam emails. C&C is usually designed to allow attackers to monitor infected systems' status, issue commands to acquire additional payloads, and retrieve more information whenever a certain event occurs. The sole C&C can be implemented and is usually located in a country whose cybercrime laws are not effectively enforced. After collecting preliminary data, APT-type phishing malware is equipped with functions that can react to the collected data or be instructed by the attackers to download different payloads [15].

That is, phishing currently functions as one of the technological tools for one of the initial phases of APT-type attacks, only preceded by non-technological techniques such as social engineering.

Conclusion

Because phishing is one of the main tools used by APTs, it requires an understanding of how this technique works, and its success is largely related to the lack of user awareness.

Phishing has proven to be an effective and growing cybersecurity attack, but there are already tools and tactics created that counter these malicious acts. That can be achieved with software and algorithms or by training the users. Cybersecurity professionals must be able to mitigate these malicious acts, and as technology evolves, cybercriminals will find new ways to attack, so in the future, training and machine lerarning as well as artificial intelligence will play a key role in detecting phishing attacks and cybercrime in general. Therefore, it could also lead to creating greater difficulties for APT attackers.

In terms of future work, it is important to study how to automatically prevent phishing from being such an effective tool for APT-type attacks to be so effective.

References

1. D McWhorter (2013) APT1: Exposing One of China's Cyber Espionage Units, vol. 18, Mandiant, Alexandria, VA, USA. https://www.fireeye.de/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.
2. R S Ross (2011) Managing Information Security Risk: Organization, Mission, and Information System View, document SP-800-39, Nat. Inst. Stand,USA.https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.
3. E Cole (2012) "Advanced Pesistent Threat: Understanding the Danger and How to Protect Your Organization", Sygresss, Waltham. https://www.amazon.in/Advanced-Persistent-Threat-Understanding-Organization/dp/1597499498.
4. R Kissel (2013) "Glossary of key information security terms," NIST Interagency/Internal Rep., Gaithersburg, MD, USA, Rep. https://docplayer.net/4865344-Nistir-7298-revision-2-glossary-of-key-information-security-terms.html.
5. P Chen, L Desmet, C Huygens (2014) "A study on advanced persistent threats," in Proc. IFIP Int. Conf. Commun. Multimedia Security. https://hal.inria.fr/hal-01404186/document.
6. Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, Robert G. Rittenhouse (2016) "Phishing Attacks and Defences" IJSIA 10: 247-256.
7. Narendra M Shekokar, Chaitali Shah, Mrunal Mahajan, Shruti Rachh (2015) "An Ideal Approach for Detection and Prevention of Phishing Attacks" Procedia Computer Science 49: 82-91.
8. Nalin Asanka Gamagedara Arachchilage, Steve Love, Konstantin Beznosov (2016) "Phishing threat avoidance behaviour: An empirical investigation", Computers in Human Bahavior, https://www.sciencedirect.com/journal/computers-in-human-behavior/vol/60/suppl/C.
9. K Nirmal, B Janet, R Kumar (2015) "Phishing – The threat that still exists", IEEE https://ieeexplore.ieee.org/document/7292734.
10. Hossain Shahriar, Tulin Klintic, Victor ClincyK (2015) "Mobile Phishin Attacks and Mitigation Techniques" Journal of Information Security 6: 206-212.
11. J Dileep Kumar, V Srikanth, L Tejeswini (2016) "Email Phishng Attach Mitigation using Server Side Email Addon", Indian Journal of Science and Technology 9: 1-5.
12. J Andress (2021) "Advanced Persistent Threat, Attacker Sophistication Continues to Grow", ISSA Journal https://www.sciencedirect.com/topics/computer-science/advanced-persistent-threat.
13. Mandiant (2020) "M. Trends, the Advanced Persistent Threat", file:///C:/Users/Dell/Downloads/M-Trends.pdf.
14. M Brand (2021) "Malware Forensics: Discovery of the Intend Deception", Cowan University, https://commons.erau.edu/jdfsl/vol5/iss4/2/.
15. M Auty (2015) "Anatomy of an Advanced Persistent Threat", Network Security, https://www.sciencedirect.com/journal/network-security/vol/2015/issue/4.