Skyler Booth

Introduction to Cybersecurity

Duncan, J

05/05/2015

“Gone Phishing”

Throughout this class, we have been discussing many areas that deal directly with cybersecurity. I am going to focus on the Pharming and Phishing area and summarize two articles; the first article is “Phishing: A Computer Security Threat” and the second article is a “Literature Review” which discusses a variety of details involving with both Pharming and Phishing. However, this paper is going to have more of an angle on Phishing instead of Pharming, even though they are both equally important when dealing with this highly controversial topic. Phishing can be defined in a variety of ways, but all of them are expressing the same meaning.

According to Aryan Chandrapal Singh, an assistant professor at the Jaihind College of Engineering, he claims that “Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.”[1] One of the common ways that Phishing is defined is that it happens entirely over the internet by the usage of E-mailing. Phishers are attracted to this way of communication because it is easy to obtain personal data, and then reshaping it for their illegal processes. Something to keep in mind is that Phishers can be after a number of things not just a username and a password, but also more serious and important things such as: credit card numbers, social security numbers, bank account information, even as far as your mother’s maiden name. It basically comes down to any personal information that can come back and hurt you, or give another access to important things, Phishers are after. When they gain access to that kind of information the outcome could become costly and dangerous to an individual or even a family. Some accounts could be small, like being rejected from your e-mail, meaning the Phisher just wanted to have access to your personal e-mails, but it could get farther and you could have a significant amount of financial loss. [1]

Fortunately, there have been some techniques and research on how to eliminate phishing. Individual aspects can play a key role in this, for example technology is a major contributing factor to the varieties of ways to try and lessen phishing and also the use of legislature. Going closer into the technology, there have been special creations in technology dealing mainly with the idea of phishing and how to combat it. There is a down side, however, and that is that in the end there will not be one single technology that will be able to completely destroy phishing, it cannot be done. When mixing a variety of technologies together however, many combinations can be produced. For example, the prevalence of phishing can be diminished and also the losses that are being suffered by this danger. There is exact software that is directly related and which is called Anti-Phishing software and this is designed to decrease the occurrence of phishing and to keep the trespassing of information limited as well. In order for this software to be successful it has the power to track down websites and monitor the activity on them if needed. It also has the technology to be able to report any suspicious behavior automatically. [1]

One interesting contribution is that it can also detect when someone is attacking, or otherwise known as a “Phisher Attack”, once it has been identified it can explain how to prevent another one from occurring and avoid being scammed. This article took phishing attack and set it aside to explain the chain reaction events more clearing. This kind of attack is being broken down into five steps:

1. A deceptive message is sent from the Phishers to the user.
2. A user provides confidential information to a Phishing server.
3. The Phishers obtains the confidential information from the server.
4. The confidential information is used to impersonate the user.
5. The Phishers obtains illicit monetary gain. [1]

After these five steps it continues going through specific kinds of Phishing, there are a lot to explain. Some of the main ones however, would be the following: filter evasion, website forgery, phone phishing, paypal phishing, and rapid share phishing. All have their own unique qualities and definitions, but they are all parts of Phishing and the different forms an attack can take on.

To further sum up this article it goes into one of the main reasons why Phishing happens and that is Trust of Authority. Many people fall as a victim to this problem and here is why, people are becoming too eager to give out information over the internet without fully thinking the consequences through. Most people do not want to think of all the possible ways that a website could be a forgery or how many ways they can get scammed, however it is happening every day. When an email comes in with the subject line reading “High Importance” many people don’t even hesitate to open that, and that simple action is giving the Phisher all the motivation they need in order to steal personal information.

When looking at this next article it continues on the topic of Phishing and Pharming, as I mentioned earlier both of these terms can be defined a variety of ways. According to Matthew Marx, he simply defines Phishing in two ways: the first way he states, “Phishing is a form of deception in which an attacker attempts to fraudulently acquire sensitive information from a victim impersonating a trustworthy source” [2] For the second definition, he describes it as a unification between the new advances in technology and also with the variation of social engineering attacks. It then focuses on how to draw out the personal information from targeted users. In this article the main form of attack is through ‘bulk’ emailing. Attackers have been at this game for a while, however with this new combination of technology and engineering it gives them more of an advantage.

The main differences between the two articles is in this second one it briefly explains pharming and how it is also important to this topic within computer security. Marx defines pharming as attacks that look extremely similar to phishing ones, except in this concept they are more complex and are more technical than phishing attacks. It also goes into there are varieties of pharming attacks as well, but these focus mainly on controlling computer systems to create a falsified IP address. Both terms are generally used together throughout this topic, but there is a slight distinction between the two and readers should be aware of that.

Reading through this article I mainly focused on the cost that comes from a phishing attack, the numbers were extremely shocking and interesting. Matthew Marx typically concentrated in the year 2013. In this year the number of phishing attacks was about 450,000 all around the world, which resulted in costing the United States roughly $5.9 billion in compensations. This is only creating more of a threat for the United States today and further on in the future if it is not handled in a quick and efficient manner. Besides the United States the next country to be affected most by the phishing attacks would be Australia, averaging around 34,249 attacks yearly. This can also can be known as a data breach. [2]

In the midst of a data breach many things can happen regarding customers. Even after a data breach it is still negatively impacting companies. When a customer becomes aware of this problem they become extremely hesitant about continuing with that business, and this will definitely harm the industry. Some factors that can limit the cost of phishing attacks and data breaches would be, maintaining a strong security system, having a policy ready, and also establishing a concrete incident response team. A major factor in limiting the cost is duration of the phishing attack, once an attack is identified it becomes very important to get rid of it as quickly as possible. “Most of the costs are within the first 24 hours of an attack” [2]. The article then goes into two types of costs, the first being hard costs and the second being soft costs. Briefly going into detail a hard cost is anything that is measured in time, money, or effort. Whereas a soft cost is any intangible cost that an institution purchases, these are much harder to measure.

Another main point to this article is the introduction of Certificate Authorities (CA). This concept has a huge role in providing personal identity assurance between the clients and also the servers that are on the internet. Certificate Authorities have two main functions: to verify that something is what it is, and binding the public key to a specific entity. Phishers are also attacking these authorities and causing breaches within and producing fake certificates. What it comes down to is there are four main methods of violating trust within these certificate based systems. These four things are: impersonation, Registration authority, CA System Compromise, and CA signing Key compromise. Each of these four systems have the same common attack, phishers are drawn to these four ways of attacking because it provides them with trust that they did not earn, and it also ensures them that they have a primary role to steal more identities [2].

There are many kinds of phishing attacks, the first article introduced some but this article digs deeper and provides more details about certain kinds. The first one is clone phishing, this is the one that is used the most when attacking individual’s identity. In order for this to work efficiently, the phisher must have knowledge in skill and technical areas and be effective in carrying out the order. The process behind this type of attack is through email, the attacker creates an email that has been cloned from a real email and comes from the same authority figure as the original. This cloned email has all the same qualities of the original except the slightest difference is in the ‘sent from field’ box, the attacker uses a slightly impersonated code which makes it a clone and gives the attackers access to personal information [2].

Another new type of phishing attack is tabnabbing; this is when the attackers take advantage of specific features of web browsing that an individual user might do. This only works if the user does two things, the first is when the user leaves multiple tabs open and travels back and forth to them frequently and the second thing is when users leave a variety of tabs open they become unaware of what accounts are open or what pages have been signed in, this leaves the pages wide open for an attacker to gain information on you. This is a new form of phishing and that poses a serious threat to internet users, because they have no knowledge about this become careless on the internet. Individuals are not realizing that keeping many tabs open is dangerous and could allow access into your private accounts without even realizing it [2].

To conclude this article the main message is that these attacks are a constant threat to any individual who spends time on the internet these attackers are preying on the inexperience individuals who are not aware of cloning emails or tabnabbing. Some people are not even aware that their information can be stolen; this is the main danger of the internet. The main goal is to start educating users on how to identify what could be fraudulent and what is real. The most common way phishing is happening is through emails. Once we get a solid number of users educating this could become useful and could limit the amount of phishing accounts. The right steps are being taken to ensure that the problem will decrease in the future, the idea is just to keep using the advancing In technology to our advantage. This will help be able to identify what type of attack phishers are using and what attack is working, once we have this information then it will be easier to identify it quicker, saving people’s identities and also the country’s money supply.

When we discussed this topic in class, we mainly focused on the concept of SPAM emails and also the process of spear phishing. The first article identified SPAM emails as bulk emailing, both of these terms share the same concept of requesting personal information. The second article describes many varieties of phishing attacks, and this is where spear phishing is identified. Spear phishing is when a certain customer is being targeted by a specific site. For example, may phishers use wide known companies to frame, Chase Bank is very popular and is also very important to customers. When a customer or user receives an email supposedly from Chase Bank saying “Warning your account may be closed if you do not do…” People automatically jump at this email and follows the instructions that are within the email to fix their account, not even thinking twice if this email is trustworthy or not. This is one of the bigger problems, because this creates a window of opportunity for the phishers to access any personal information that could be dangerous if used. Overall, both of these articles and what we discussed in class mainly reflects on phishing and pharming as a whole and focusing on the way attacks work and how the best ways to prevent them.

References

[1] A. Singh, K. Somase, K. Tambre,*Phishing: A Computer Security Threat*, 1st Edition, Gujarat, India:

IJARCSMS Publication, Decemer 2013, p. 64-71.

[2] M. Marx, *Literature Review*, 1st Edition, : A.A.V Newsletter, March 2014, p. 1-17.