Scientific Research Publishing

Journal of Information Security, 2018, 9, 257-264
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Social Engineering Threat and Defense: A Literature Survey

Islam Abdalla Mohamed Abass[1,2]

[1]Department of Computer Science, Al Jouf University, Al-Jawf, KSA
[2]The Holy Qur'an and Islamic University, Khartoum, Sudan
Email: islamabdalla32@gmail.com

How to cite this paper: Abass, I.A.M. (2018) Social Engineering Threat and Defense: A Literature Survey. *Journal of Information Security*, **9**, 257-264.
https://doi.org/10.4236/jis.2018.94018

Received: January 18, 2018
Accepted: September 15, 2018
Published: September 18, 2018

Abstract

This article surveys the literature on social engineering. There are lots of security application and hardware in market; still there are several methods that can be used to breach the information security defenses of an organization or individual. Social engineering attacks are interested in gaining information that may be used to carry out actions such as identity theft, stealing password or gaining information for another type of attack. The threat lies with the combinations of social engineering with another type of attacks like Phishing and Watering hole attack which make it hard to defense against. This research aims to investigate the impact of modern Social Engineering on the organization or individual. It describes the categories of Social Engineering, and how the attacker takes advantage of human behavior. At the same time, I also discuss the direct and indirect attack of social engineering and the defense mechanism against this attack.

Keywords

Social Engineering, Security, Phishing, Watering Hole, Spyware

1. Introduction

Social engineering is one of the few types of attacks that can be classified as non-technical attacks in general, but at the same time it can combine with technical type of attack like spyware and Trojan more effectively. Human beings can be very easily manipulated into providing information or other details that may be useful to an attacker. "Malicious social engineers aren't necessarily very technical people but they're crafty and clever in the way they think" says chief operating officer of Social Engineer [1]. Today most business and banks are relying on technology like internet and smartphone. They are paying a lot of money for

buying security tools software and hardware, but at the same time a naive employer can give all the information the attacker need without going to the trouble of hacking the system. That is what social engineering all about use the human factor which is the weakest factor in any institute or organization. Humans are easier to hack than computer systems and networks. Most people are raised to be kind and helpful leading them to inherently trust others. The concept of bad people taking advantage of the good and honest does not sit well with most people. Social engineers are creative and clever, they use different techniques to deliver malicious software to gain personal information, commit fraud or gain access to secure systems.

2. Categories of Social Engineering

There are two main categories under which all social engineering attempts could be classified:

1) Computer or technology based deception: The technology-based approach is to deceive the user into believing that he is interacting with the real computer system and get him to provide confidential information.

2) Human based deception: This is done through deception, by taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked [2].

3. Social Engineering and Electronic Breakthroughs

Social engineering is the use of mentally manipulation to deceive the computer users to gain access to computers, certain information or database. It can be the most dangerous methods because of the following reasons:

1) Social engineering is one of the most successful compared to other technical.

2) Information security specialists as well as computer users pose little to the risk of social engineering.

3) Human habit and Nature: human beings tend to follow certain default habits and actions without thinking. A good attacker can observe these habits and use them to track people or group [2].

According to a survey done by Dimension Research (2011) on 850 IT and security professionals located in the United States, Canada, the United Kingdom, Germany, Australia, and New Zealand, 48 In April 2016, the FBI released its latest statistics on incidents and losses attributed to business email compromise. It states that:

1) 17,642 reported victims of business email compromise between Oct. 2013 and Feb, 2016.

2) 270% increase in identified victims and exposed loss since Jan, 2015.

3) $2.3 billion global fraud losses from these crimes since Oct, 2013.

To complement those numbers, here are some compelling statistics from the 2016 Social Engineering Report:

1) 60% of survey respondents say social engineering is one of the most signif-

icant threats they face today. 60% know they were or may have been victims of a social engineering attack in the past year.

2) 65% of those who were attacked say that employee's credentials were compromised as a result of these incidents [3].

4. The Stage of Social Engineering

Most of hackers use these steps to start their attack, because it provides a road map to approach the target safely without any suspicion:

1) Gathering information for social engineering:

Over the last decade, some of the biggest security threats have come from the use of social networking. The rapid growth of these technologies lets millions of users each day post on Facebook, twitter, and many other networks. That type of information they are posting may look not important but it's the ignition key for launching successful attack, like:

a) Personal information.

b) Photos.

c) Location information.

d) Friend information.

e) Business information.

f) Likes and dislike.

The danger of making this wealth of information available is that a curious attacker can piece together these sources and get a clear picture of an individual or a business. Once a message is posted it is nearly impossible to remove it completely from a social network. Especially since it might already have been forwarded to others and been reposted again. With this information in hand the attacker can use social engineering to make a convincing impersonation of that individual or gain into a business by using insider information. Also many worms spread through social networks. In most cases they have used social engineering tricks to post enticing messages on behalf of an infected user. Social networking can be fun but at the same time it can made the attacker's job much easier based on the sheer volume of data and personal information available [4] [5] [6].

2) Develop relation and trust with the victim:

Trust development can be done by using insider information, usually by presenting themselves as a more senior member of the institute. Human nature based on trusting others until they prove that they are not trustworthy. If someone tells us that they are a certain person, we usually accept that statement. Some time we fear to get in to trouble or get lazy to shout down or computer after finish our work. A skilled hacker will often try to exploit this weakness before spending time and effort on other methods to crack passwords or gain access to systems [5] [6].

3) Exploitation of relationship:

In this step the attacker is focused on maintaining the momentum of compliance that was built in step 2) without raising suspicion. He uses manipulation

tactics to get the target in a desired emotional state suited to the plan. The attacker must study the emotion state of his victim and how to use it to his benefit. Exploitation can take place through the divulging of seemingly unimportant information or access granted/transferred to the attacker. Examples of successful exploitation include:

a) Personal information the act of holding the door open or otherwise allowing the attacker inside the facilities.

b) Offering social proof by introducing the SE to other company personnel.

c) Exposing trade secrets in a discussion with a supposed "peer" [5] [7].

4) Execution:

In this step the attack start the real attack without alerting the victim that he is under attack. It's better to leave the target feeling as if they did something good for someone else that allows possible future interactions to continue [7].

5. Aspects of Social Engineering Attacks

Social engineering attack can be launched using social engineering on several levels:

1) Sensory level: The focus is on the location and the environment surrounding, including:

a) Place of work: The attacker enters as a worker, contractor, cleaning worker or maintenance worker roams the offices and tries to collect what he can collect from the passwords.

b) Phone: The most vulnerable to this type of attacks are the workers in the technical support centers, for example the attacker may contact the technical support center and ask for some technical information and gradually gets the information like passwords, and then uses this information to launch attacks on computers Enterprise.

c) Wastes: It is one of the most popular methods for attackers using social engineering because the attacker can collect much important information without attracting the attention of any one such as: passwords, corporate structure, Company telephone directory, employee names, staff meeting dates and purchase invoices.

d) The Internet: Usually the same password is used for more than one site to make it easier to remember. When an attacker can see this password, it becomes easy for him to penetrate all the applications that the original password owner handles.

2) Psychological level: This level means the psychological climate surrounding the manner in which the attack is carried out. The attacker seeks to create the appropriate psychological atmosphere to inspire the victim that he is a trusted person, and has the authority to see sensitive information of the target person or facility [2].

6. Methods of Social Engineering Attacks

There are several methods of attack using social engineering, most notably the

following:

1) The temptation to have something rare: People in general have the desire to own anything specially if it became rare. The desire to own increases when we feel that the ability to own will become limited in the future. The attacker can use this thought to push the victim to try to own what he desire no matter the cost of it even if he comet treason.

2) Show the similarities with the target: characteristics of the human soul tend to feel secure similar in the race, color, Concerns and nature. Our sense of the existence of parallels with someone makes us less cautious when dealing with him.

3) Pay back the favor: we normally desire to return the favor; this property is firmly rooted in communities tribal and family. The attacker provides service to the target, which makes the target indebted to him. This feeling make the target help the attacker by given him some information or to allow him to use his device [2].

4) The style of flattery: many employees and members of the society seek to create a good image of themselves at their superiors. Therefore, some of them will not hesitate to provide the information the attacker needed to feel good about their self. Usually attackers keep flattering the victim that has authority or is related to the owner of the authority within the company or institution to gain his trust [2].

5) Move with the flow: In most of society's a person should not take a different position from what others have believe, the attackers knowing that and will strike using this point. By using the traditional way of society attackers can get easily to a victim and make him give information or perform a certain act [2].

6) Pretexting: it's also known in the UK as blagging, is the process of creating and using an invented scenario to engage a victim in a manner that increases the chance he will divulge information or perform actions that would be unlikely in ordinary circumstances. This technique can be used to fool a business into disclosing customer information as well as by private investigators to obtain telephone records, utility records, banking records and other information directly from company service representatives. It can also be used to impersonate coworkers, police, bank, tax authorities or any other individual [8].

7) Reverse Social Engineering: It is one of the advanced ways to win the confidence of the target and then get the information. This method apply by create a position that shows the attacker in the form of administrative or technical authority, so that the target may begin to ask help and receive instructions. The attacker can achieve this by applying this process:

a) Fabricating position.

b) Introduce himself as the person with the necessary knowledge or authority to deal with the situation.

c) Given help [9].

8) Phishing: It's a technique of fraudulently obtaining private information. According to Verizons Data Breach Investigation Report for 2016 [10], phishing

was involved in 9576 data breaches 916 of them having resulted in confirmed data disclosure out of about 100,000, or roughly 10 The latest Business Continuity Institute (BCI) report (2017) say that phishing was a part of 21 Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization. SMS phishing uses cell phone text messages to induce people to divulge their personal information [11] [12] [13].

9) Spear phishing: Although similar to "phishing", spear phishing is a technique that fraudulently obtains private information by sending highly customized emails to few end users. It is the main difference between phishing attacks because phishing campaigns focus on sending out high volumes of generalized emails with the expectation that only a few people will respond. On the other hand, spear phishing emails require the attacker to perform additional research on their targets in order to "trick" end.

Users into performing requested activities. The success rate of spear-phishing attacks is considerably higher than phishing attacks with people opening roughly [14] [15].

10) Watering hole attack: The term watering hole refers to initiating an attack against targeted businesses and organizations. Attacker use social engineering strategy that capitalizes on the trust users have in websites they regularly visit. The goal of this attack is not to serve malware to as many systems possible. Instead, the attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. This makes the watering hole technique effective in delivering its intended payload. This strategy has been successfully used to gain access to some (supposedly) very secure systems [16]. The preparation to this type of attack start with information gathering to confirm that the targets visit the websites and that the system allows such visits. The attacker then tests these websites for vulnerabilities to inject code that may infect a visitor's system with malware. Once the victims visit the compromised site, the exploit takes advantage of software vulnerabilities to drop malware. The dropped malware may be in the form of a remote access Trojan which allows attackers to gain access to the secure system and get sensitive data can [8] [17].

7. Protection against Social Engineering

1) Organization can buy insurance against hacker's attacks but they must have good information access policies and procedures.

2) Don't trust any email that ask for information like username, password, and credit card number or ask you to go to specific link, because this type of information won't be asked by the genuine organization online. Unless the e-mail is digitally signed, you can't be sure it wasn't forged, because any one can mail it by any name hence when it is stating some important better to check for the full headers.

3) Constantly check your bank, credit and debit card statements to ensure that all transactions are legitimate.

4) When contacting your financial institution, use only official site which most of them use https protocol. This is good defense against phishing attacks.

5) When a social engineering attack occurs make sure you information security specialist knows how to manage such attack, as each attack has its own signature and objective [18]. Also use software protection such as anti-virus, firewalls and antispyware to protect form malware like spyware, virus, adware and Trojan.

6) Educate users and employers about social engineer is an important part of security system. The trainers must focus on different social-engineering attacks scenario and how to reacts [9] [18].

8. Conclusion

In this paper, I described the common method used for modern social engineering attacks and revealed the grown threat of this attack lately. This attack became so dangerous because it can combine with technical type of attack like spyware, Trojan and phishing; also it targets the weakest point in any system which is human. In this attack people are the weakest point, but also the best tool to defend against it. I have explained the stage of social engineering and how the attacker can approach the target and manipulate it to be in his control. The increase number of people how use social media makes the attacker job more easily, because most of them share personal and sensitive data unintentional. Also I found that Organization must ensure to educate their employer about social engineering, and make sure that their policies and procedure are executed properly to eliminate the threat of this attack.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Oriyano, S.-P. (2016) Certified Ethical Hacker. John Wiley & Sons, New York. https://doi.org/10.1002/9781119419303

[2] Gulati, R. (2003) The Threat of Social Engineering and Your Defense against It. SANS Institute, North Bethesda.

[3] Field, T. (2016) Email Security: Social Engineering Report. AGARI, Foster City.

[4] Symantec Corporation (2016) Internet Security Threat Report. Symantec Corporation, Mountain View.

[5] Mouton, F., Malan, M.M., Leenen, L. and Venter, H.S. (2014) Social Engineering Attack Framework. 2014 *Information Security for South Africa*, Johannesburg, 13-14 August 2014.

[6] Chantler, A.N. and Broadhurst, R. (2007) Social Engineering and Crime Prevention in Cyberspace.

[7] Nyirak, A. (2017) The Social Engineering Framework. https://www.social-engineer.org/framework /attack-vectors/attack-cycle/

[8] Wekipedia (2018) Socialengineering (Security). https://en.wikipedia.org/wiki/Socialengineering

[9] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2014) Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, **22**, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

[10] Wynants, F. (2017) Verizons 2016 Data Breach Investigations Report. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[11] Poremba, S.M. (2017) Dramatic Increase in Phishing Proves its Effectiveness. http://www.itbusinessedge.com/blogs/data-security/dramatic-increase-in-phishing-proves-its-effectiveness.html

[12] Jagatic, T., Johnson, N., Jakobsson, M. and Menczer, F. (2005) Social Phishing. *Communications of the ACM*, **50**, 94-100. https://doi.org/10.1145/1290958.1290968

[13] Thorp, D. and Tilley, K. (2017) BCI Cyber Resilience Report, Sungard Availability Services. Business Continuity Institute, Berkshire.

[14] FireEye, Inc. (2016) The Real Dangers of Spear-Phishing Attacks. FireEye, Inc., Milpitas.

[15] Brody, R.G., Brizzee, W.B. and Cano, L. (2012) Flying under the Radar: Social Engineering. *International Journal of Accounting and Information Management*, **20**, 335-347. https://doi.org/10.1108/18347641211272731

[16] Papazov, Y. (2016) Social Engineering, NATO-STO. Business Park Sofia.

[17] Oscar Celestino Angelo Abendanll (2013) Water hole 101. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/137/watering-hole-101

[18] Puneeth, M., Farha, J.S., Yamini, M. and Sandhya, N. (2015) Social Engineering on Social Networking Sites. *International Journal of Advanced Engineering Research and Science*, **2**, 57-60.