Fatima et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 4 Issue 1, Jan, - March 2020

A Brief Overview of Social Engineering

Muhammad Shairoze Malik
Lahore Garrison University
Shairozemalik@lgu.edu.pk

Abstract:

Right now digitization, the requirement for information protection and information security is very significant. The IT organizations today lean toward their information over everything. Not just for organizations, information security is significant for any person. Be that as it may, regardless of how secure is the organization, how best in class is the technology utilized or what amount cutting-edge their product is, there's as yet a weakness in each segment known as 'Human'. The craft of acquiring sensitive data from a person is known as Social Engineering. Technology has advanced rapidly in recent years, but the danger of Social Engineering still persists in the society. This is mostly due to lack of awareness regarding social engineering attack patterns. Social engineering is an extremely basic practice to accumulate data and touchy information using portable numbers, messages, SMS or direct methodology. Social engineering can be extremely valuable for the aggressor whenever done in an appropriate way. This paper will look into some of the basic and rudimentary techniques used by attackers to gain personal information about victims. The goal of the article is to enable others in successfully defending against social engineering attacks by having the knowledge into how these attacks are performed.

Keywords: Spear Phishing, Pretexting, Watering Hole, Phishing, SEToolkit, Baiting.

1. Introduction:

Generally, the data breaches and information theft in any organization is due to some vulnerabilities present in the organization itself. However, this vulnerability is not only in the technical department. Humans are also considered as a vulnerability as people present in different sectors can also be used to extract confidential information and here comes the word Social Engineering [1]. In digital security, social engineering alludes to the control of people so as to instigate them to complete explicit undertakings or to part with data that can be useful by an aggressor [2]. Social engineering in itself doesn't really require a lot of specialized information so as to be effective. Rather, social designing goes after normal parts of human brain research, for example, interest, politeness, artlessness, sympathy, covetousness, and so on. Social engineering has expanded radically over the most recent couple of years. As indicated by a study, Social Engineering was associated with the 95% of the assaults that occurred in most recent couple of years [3].

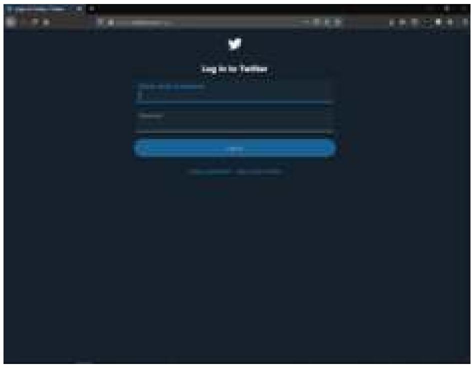
2. Social-Engineering Attacks:

There are many types of attacks are used by malicious hackers to perform social engineering which is explained below. There are basically seven types of social engineering attacks [4, 5]:

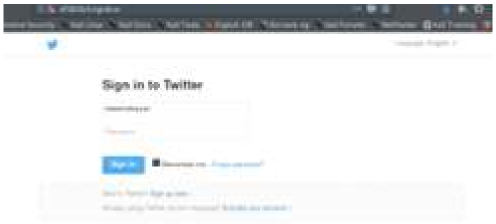
1. Phishing:

Phishing is the most widely recognized and compelling approach to accumulate data about the target [6]. Phishing is for the most part done through emails. These phishing pages generally contain links that redirect the target to some malicious website. Approximately 90% of people using internet receive phishing emails on regular basis. If the phishing has to be done on a specific person, the malicious hacker first tries to find some interest in the target so that the probability of the target clicking on the email increases. The phishing generally focuses on gathering sensitive information of target like social media accounts details, Credit card details etc.

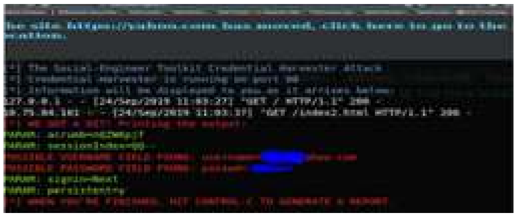
To study this process in more detail let's see the example below in which the attacker makes a fake clone of Facebook Page and when the target enters his credentials in the fake page, the attacker gets all the credentials and the personal information of the target is compromised. The practical below is done using 'Social engineering Toolkit (SEToolkit)'.



(Fig 1. Original Twitter Page)



(Fig 2. Fake Twitter Page)



```
he site https://yahoo.com has moved, click here to go to the
cation.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [24/Sep/2019 11:03:27] "GET / HTTP/1.1" 200 -
10.75.84.181 - - [24/Sep/2019 11:03:37] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: [illegible]
PARAM: sessionIndex=[illegible]
POSSIBLE USERNAME FIELD FOUND: username=[redacted]
POSSIBLE PASSWORD FIELD FOUND: password=[redacted]
PARAM: signin=Next
PARAM: persistent=y
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT
```

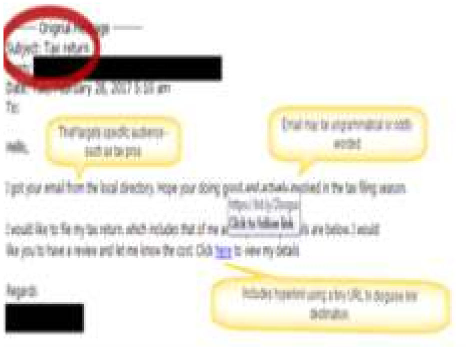
(Fig 3. Attacker got the credentials)

2. Spear Phishing:

Spear phishing is another type of phishing attack but in this instead of targeting too many people the focus is on a specific person. This method is really hard as compared to a normal phishing attack. In this, the hacker gains information about his target like his likes, dislikes, characteristics etc. It is a time consuming method, where it may take from one week to several months, depending upon the target. Spear phishing is far more effective and efficient way of social engineering as compared to other ways if done professionally. For instance, a hacker sends an email with a critical update to the employees of targeted IT company. The email contains a malicious link which redirects them to a page were hacker either ask them to update their software by downloading a file (which contains malware) or as them to change their password on the malicious page itself and the company's security is compromised [7].

3. Baiting:

Baiting is similar to the phishing attack, but in baiting the attacker promises for something in exchange. For example, the hacker promises free music, phones, prize money, etc. and to get this the target has to just log in to a page or has to share some personal information. Some hackers send infected pen drives to employees of the company as a gift and this flash drive contains malware which is used for hacking into company's network. Baiting is commonly done through emails and adds. Baiting adds are common on unsecured sites and dark web [8]. The screenshot below shows a baiting mail which promises money by clicking on link.



----- Original Message -----
Subject: Tax return
[redacted]
Date: [illegible] January 26, 2017 5:10 am
To:

Hello,

I got your email from the local directory. Hope your doing good and actively involved in the tax filing season.

I would like to file my tax return, which includes that of me a[illegible] are below. I would like you to have a review and let me know the cost. Click here to view my details

Regards

[redacted]

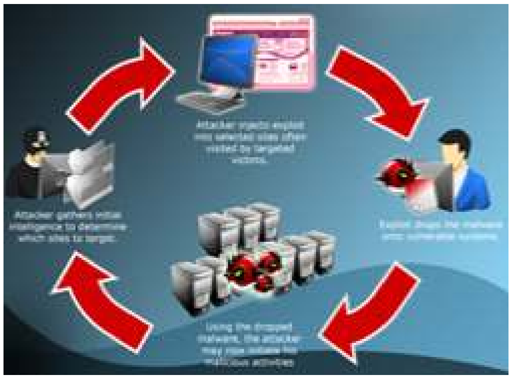
This targets specific audience- such as tax pros
Email may be ungrammatical or oddly worded
https://bit.ly/[illegible]
Click to follow link
Includes hyperlink using a tiny URL to disguise true destination

(Fig 4. Baiting Email)

4. Watering hole Attack:

The name watering hole attack is inspired by a real-life situation in which the predator lurks near the water holes so that they can attack a targeted prey. Similarly, in this attack, attacker instead of getting directly in touch with the target the attacker keeps track of every website that his prey visits frequently. Now, the attacker chooses the most frequent website that his target visits. The attacker will then find a vulnerability in this website like reflected XSS, stored XSS, host header, etc. and so that the attacker can fetch confidential data from his target. This type of attacks is really on government employees, as hacking into government sector is really difficult and risky. So, the attacker uses their target's most frequently visited sites to get their personal information like tracking details or any kind of sensitive information. Watering hole attacks are though uncommon but are really dangerous as these attacks are really difficult to detect [9, 10].

Let us assume that the attacker wants to hack into or gather information about Metro, Washington DC. The attacker first chooses a common site where his target visits frequently. The people from three other sectors also visit the same website as shown in the figure. Now the attacker will hack into this common site and the attach some malware, phishing pages, baiting pages, etc. The site is now compromised. Here, instead of attacking all four sectors the attacker will only try to get information of the person associated with Metro. This way, instead of connecting directly to the attacker, an indirect way of gathering sensitive information is attained.


Attacker injects exploit into selected sites often visited by targeted victims.
Exploit drops the malware onto vulnerable systems.
Using the dropped malware, the attacker may now initiate for malicious activities
Attacker gathers initial intelligence to determine which sites to target.

(Fig 5. Working of Watering Hole Attack)

5. Pretexting Attack:

In a pretexting attack the attacker builds up a fictitious scenario in which the possibility of target giving his sensitive information is increased. This method is generally used to trick employees of IT organization so that they give away the personal information of their client like their usernames, passwords, security questions, etc. This information can be used to build further trust relationships with other clients and then used for further social engineering. The small successful steps taken during the pretexting phase is one of the reasons for large data theft and security breaches. The strength of this type of attack totally depends on the awareness and intelligence of the target. If the target is intelligent enough to identify these attacks, then this attack can be prevented. This attack is mostly done through mobile number spoofing. Many IT firms nowadays, educate their employees about these attacks and how to prevent them.

6. Quid Pro Quo:

This attack is similar to the Pre-texting attack but in this, the attacker instead of making random calls, contact the employee of an IT firm to solve any technical issue in their system and network. The attacker first gathers information about the network and systems in the targeted organization. Then the attacker calls an employee of that organization as a technical support, security maintenance charge, etc. Most of the times the employees believe in this and give the information to the attacker [11]. This information may be the Wi-Fi password, username of or maybe they give away the username and password of his own system. This technical information helps the attacker to hack into the system or network and analyze the confidential information. This attack is a really successful attack and the data through this attack is compromised in 70% of the cases.

3. How Social Engineering Effect our lives?

Social Engineering Attacks are currently one of the most damaging attacks on any IT organization. At least 60% of the IT companies were the victim of Social Engineering attacks in 2016 and these attacks kept on increasing by 2017. The leakage of sensitive data of IT firms and their users is one of the biggest threat to social engineering. But, what would an attacker do with this information? So here's the answer, the personal information of the targets like accounts, credit card details, etc. are being sold on the dark web. At least 70% of the internet is contained in dark web. This information is sold on the dark web at really high prices and then used for illegal purposes. Below are some screenshots which tell us how our personal information is being sold on the dark web [12, 13, 14].

4. Precautions:

1. Different Passwords:
As indicated by a study roughly 60% individuals utilize same passwords for various records which makes simpler for hackers to hack into their records [15].

2. Strong Passwords:
Utilizing solid passwords is one of the essential method for preventing social-engineering attacks. A strong password key must contain a blend of alphanumeric characters.

3. Security Questions:
Using the security questions to verify identity can enhance the overall security of your account. These questions contain private information of users, which are hard to crack [16].

4. Two-Factor Authentication:
Using the two-factor authentication service provided by almost all major websites like Facebook, WhatsApp, Gmail, etc. can enhance the security of accounts.

5. Suspicious/Infected Sites:
Avoid visiting suspicious websites as the may contain infected pages or malicious code by hackers, which can then either compromise your system or steal your personal information [17].

6. Email from Unknown Source:
As most of the phishing attacks are done through emails. So users should avoid opening emails from unknown source as the may contain malicious code or these emails can be used to target users to social engineering attacks.

7. Antivirus:
Antiviruses should be installed, as they can detect the entry of malicious code or file in your system and prevent it from execution thus saving the user from potential loss of data or system compromise.

8. Log off accounts:
Always log off the accounts when they are not in use. This can prevent attackers from hijacking user's accounts and prevent from hacking attempts like session hijacking, cookie injection, etc. [18]

9. Always check the URLs:
One should always check the URL before using the website. The websites which has SSL certificate(HTTPS) installed in them are considered secured.

10. Avoid giving your laptop/smartphone to Strangers:
Preventing any third person from using your phone or laptop is one of the best methods of preventing non-technical social engineering.

11. Never install untrusted apps and software:
Most of the android devices does not have antivirus installed on them. Linux is protected from viruses but malware from there untrusted apps are still a problem.

12. Never insert any unknown flash drive:
Many people attach USB's from unknown places which contain malware and help an attacker to take full control of their system.

13. Change passwords frequently:
One must change his account's password whether it be social media accounts or bank accounts, passwords must be changed frequently.

14. Increasing awareness about Social-Engineering:
One of the best methods to prevent Social Engineering is to educate people about it and how it is affecting our life [19, 20].

5. Conclusion:
In the paper, we looked into multiple social engineering attack patterns which are often deployed by hackers to targets the victims. The effects of these attacks on an organization shows us that how much disastrous social engineering is for society as the leak of private information of individuals effects both their personal and private life. We further listed several possible precautions which can be taken by individuals to help them safeguard their sensitive information form social engineering attacks. The conclusion is that it is difficult to stop social engineering assaults as there is no fix for the human weakness. Teaching individuals about the social engineering and its unfavorable impacts can positively diminish this sort of attacks however can't be completely eliminated.

6. References:

[1] C. Hadnagy, Social engineering: The art of human hacking, Wiley, 2010.

[2] B. Blunden, "Manufactured Consent and Cyberwar," in Proc. LockDown Conference, 2010.

[3] K. D. Mitnick and W. L. Simon, the art of

deception: Controlling the human element of security, Wiley, 2001.

[4] D. P. Twitchell, "Social engineering in information assurance curricula," in Proc. The 3rd annual conference on Information security curriculum development, 2006, pp. 191-193.

[5] N. B. Ellison, "Social network sites: Definition, history, and scholarship," Journal of Computer Mediated Communication, vol. 13, pp. 210-230, 2007.

[6] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," Communications of the ACM, vol. 50, pp. 94-100, 2007.

[7] S. Abu-Nimeh, T. Chen, and O. Alzubi, "Malicious and spam posts in online social networks," Computer, vol. 44, pp. 23-28, 2011.

[8] G. M. Weiksner, B. Fogg, and X. Liu, "Six patterns for persuasion in online social networks," Persuasive Technology, 2008, pp. 151-163.

[9] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards automating social engineering using social networking sites," in Computational Science and Engineering, 2009. CSE'09. International Conference on, 2009, pp. 117-124.

[10] M. Huber, "Automated social engineering, proof of concept," Royal Institute of Technology Stockholm, 2009.

[11] S. T. Thompson, "Helping the hacker? Library information, security, and social engineering," Information Technology and Libraries, vol. 25, pp. 222-225, 2003.

[12] R. Gibson, "Who's really in your top 8: network security in the age of social networking," in Proc. The 35th annual ACM SIGUCCS fall conference, 2007, pp. 131-134.

[13] B. Fogg and D. Iizawa, "Online persuasion in Facebook and Mixi: a cross-cultural comparison," Persuasive Technology, 2008, pp. 35-46.

[14] J. Nagy and P. Pecho, Social Networks Security, pp. 321-325, 2009.

[15] G. Hogben, "Security issues and recommendations for online social networks," ENISA position paper, vol. 1, 2007.

[16] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in Proc. the 2005 ACM workshop on Privacy in the electronic society, 2005, pp. 71-80.

[17] R. G. Brody, "Flying under the radar: social engineering," International Journal of Accounting and Information Management, vol. 20, pp. 335-347, 2012.

[18] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," April 2010.

[19] T. Mataracioglu and S. Ozkan, "User Awareness Measurement Through Social Engineering," arXiv preprint arXiv:1108.2149, 2011.

[20] D. Rosenblum, "What anyone can know: The privacy risks of social networking sites," Security & Privacy, IEEE, vol. 5, pp. 40-49, 2007.