SOCIAL ENGINEERING ATTACK

(Human Hacking)

The Most Recurrent but Neglected Cybercrime

CONCEPT PAPER

Background

Today, the Internet is the most powerful tool in the world and has undoubtedly become an important element in our life. Individuals, organizations and governments are relying on the internet for a lot of activities including sharing sensitive information. However, like every single innovation in science and technology, the internet has its own advantages and disadvantages.

The risk of disclosure of sensitive information constitute the major disadvantages of using the Internet and as it is continuing to evolve, organizations and governments have a vested interest in securing sensitive information stored or shared over the internet. The protection of sensitive information and the development of countermeasures against illegal access to information are of vital importance to organizations and governments to ensure the trust of clients and citizens. Organizations and governments have been spending hundreds of thousands of dollars investing in firewalls, intrusion detection systems, encryption systems and other security technologies to prevent cyber criminals from having access to their sensitive information.

What is Social Engineering?

There is a common misconception that cyber criminals use only highly advanced tools and techniques to hack into people's computers or accounts. This is simply not true. Cyber-criminals have learnt that the easiest way to steal information, hack accounts, or infect a system is by simply tricking users into making a mistake. This is known as **social engineering or human hacking**. Some enigmatic paradox exists. Many people are sure they are rather clever or educated and will not take the crook's bait. And it's exactly these people who often fall prey to social engineering attacks. Why? Because the secret is not about intellect or education. It's all about the emotional state.

Social engineering is the term used to describe the 'art' of psychological trickery, the manipulation of behavior often through deception to influence unsuspecting users, to unwittingly divulge sensitive information which can be used to gain access to the targets computer systems and perform actions that cause harm to the confidentiality, integrity, or availability of the computer system. Being aware of this shared conviction, the attacker exploits the victim's trust without arousing suspicion. Using a variety of media, including emails, social media and phone calls, these social engineers manipulate any individual's innate desires (e.g. friendship, romance, greed) by building a trust relationship with the

target; and, then exploiting that relationship to gain access to sensitive information that should not be disclosed and shared under normal conditions. The main method is the email. The content is usually convincing enough to lure and make the victim execute the malware file or click on the poisoned link. The user become the primary target associated with the cyber-criminal's secondary target, such as the organizations computer system; which in turn may lead to a tertiary or main target such as a system control program, database, financial or telecommunication system. Cyber-criminals will try to gain this 'login information' enabling them to bypass security. This can include usernames and passwords, PIN's (**P**ersonal **I**dentification **N**umbers), tokens and credit card information. Once they have gained access to the system they are then able to erase, modify or copy the information to suit the needs of their attack.

Technology on its own is therefore not a sufficient safeguard against information theft; users are often the weak link in an information security system. Staff members can be influenced to divulge sensitive information which subsequently allow unauthorized individuals to gain access to protected systems. To prove this point, the 2015 report of a study by Vormetric shows that human error is the cause of 90% of cyber breaches. Earlier studies also show about 70% of information theft is carried out consciously or unconsciously from within the organization [2], [3], [4]. Indeed, the weakest link, in most of the cases, is unfortunately the users. Also, women have over time being at the center stage of Social Engineering (SE) either a part of crime syndicates or falling prey to the numerous schemes of hackers. An article reports that, many hacktivists females as part of their attacks owing to the fact that, women might have an edge in gaining the trust of potential targets – a key objective of any social engineer. Scientific studies have found that our tendency to find women's voices comforting may be deeply wired in our brains, and stem from our experience, before birth, hearing the sound of our own mother's voice. Most women are employed for such reasons without knowing most times what it is they have signed up for. We see the other part of the vulnerability of women in Social Engineering play out when their emotions are played on to obtain sensitive information which mostly cost them their properties, reputation and lives in the worse case. In that regard, cybersecurity experts have stated that an organization may invest hundreds of thousands of dollars in firewalls, intrusion detection systems, encryption systems and other security technologies, however, if a cyber-criminal appeals to a trustworthy person within the organization, and if the respective person consciously or unconsciously

agrees to cooperate and the cyber-criminal receives the access credentials, then all investments in the above-mentioned technologies have been wasted.

To some people, social engineering attack might seem like a fancy word for lying. To other people, they find the social engineering techniques ridiculous and think that the cyber-criminals have a low chance of them being deceived so they therefore pay little or no attention to it. Meanwhile, it is an extremely effective technique that provide cyber criminals with extremely valuable information that lead them to their target computer system.

The Session

The main objectives of this is to provide participants with a deep understanding of social engineering attack (human hacking), the types, how it works so that they can view it as any other serious attack method, and what they can do to protect themselves and their organizations. It will take the form of a lecture that will explain human hacking and a live demonstration or simulation of the manipulative techniques used by the social engineer (cyber criminals). The situation will be covered by experts from various sectors of activities in a panel discussion. Furthermore, ladies will be introduced to careers in the IT world.

References

[1] https://dtr.thalesesecurity.com/insiderthreat/2015/pdf/2015-vormetric-insider-threat-pr-v2.pdf

[2] Study on the Theft of Proprietary Information, American Society of Industrial Security, Arlington, VA: ASIS, 1996

[3] A. Katz, "Computers, The Changing Face of Criminality", Unpublished dissertation: Michigan State University, 1995

[4] T. N. Jagatic, N. A. Johnson, M. Jakobsson, F. Menczer, "Social Phishing", Communications of the ACM, Vol. 50, No. 10, Oct. 2007