Center for Cyber Security and International Relations Studies

Social engineering and human intelligence to overcome the latest generation digital protection systems

Francesca Nizzi, Samuele Foni

Nowadays, despite all the most sophisticated digital protection techniques, 43% of cyber attacks completed in 2017, exploiting a vulnerability that can not be eliminated: the human factor. In addition to technological knowledges, crackers use human psychology to carry out more sophisticated cyber attacks. The use of psychological techniques for hacking purpose is called social engineering. From this point of view, cyber insecurity is mostly a people problem, not a technology problem.

Our goal is to provide an overview of the human feelings that a social engineer relies on, which threat vectors he uses and when a cyber attacker becomes (or requests help from) a social engineer.

Introduction

"There is no patch for (human) stupidity". Kevin Mitnick[1]

Nowadays technologies are indispensable in daily life. We all have an email address, we all have a mobile phone with a 4G connection that we use to chat with friends/parents/acquaintances or to keep up to date with the VIPs (social) life.

A very important part related to technologies are the security and (user) privacy. In the cyber security area, giant steps have been taken in the research of increasingly reliable methods of defense against malicious people. The only vulnerability that can not be removed is the human being. People with emotions undermine their security and privacy.

An example of this is the following incident. *You should make a bank transfer of half-a-million Euros on this bank account. Do not call me because I'm around with the president and I can not talk.* [1] this is the text of an email sent by one (or more) cracker to a Confindustria manager at the end of September, with the president of the same organization as the sender. The unfortunate man, unconsciously, made the transfer and the money vanished in a black-hole. The cracker has, presumably, taken possession of the sender email account, forged the mail with the request and based on the

[1] Kevin David Mitnick is the most famous cracker and social engineer in the world. He is the IP spoofing technique inventor.

presumable good faith of the victim, and waited for the money transfer. This is an example of fake mail (mail spoofing) that are daily sent by malicious people with the aim of taking possession of personal data using the good faith or naivety of their victims.

Social engineering studies human personality, analyzing conscious and sub-conscious traits with the aim to obtain sensitive informations. It observes vocal cues, body language and people reaction to a particular external stimuli. As Mitnick says "social engineering uses manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker".

"Man is his own worst enemy" claimed Marcus Tullius Cicero in the first century BC and nowadays as at that time, it is always the human factor that represents the first threat to the safety of people. In the era of the Internet of Everything, social engineering is always the most successful attack vector, even in the cyber world. The social engineer is an artist of deception, a skilled persuader and trickster, who exploits any means at his disposal to get access to informations, revenues and devices normally impossible to reach. To become a good social engineer can be enough to know how to lie, but if you add also a deep technological knowledge, you will become a really skillful cracker. Fortunately, learning such skills is very difficult, but on the other hand the careless use of Internet technologies by end-users quickly fill the gap.

In this paper we will try to explain what are the human feelings on which a social engineer leverages, how he acts and what are the most important techniques used.

The psychology of social engineering

Social engineering is the set of psychological techniques, used by an attacker to convince people to reveal sensitive informations (i.e. credit card PIN). Social engineering is based on a simply concept: we all react in the same way to some basic stimuli and the attacker skill is to induce the victim to trust him or his actions. Every social engineering techniques are based on seven human emotions that can persuade the victim to perform a particular action: obedience, guilty, fear, ignorance, desire, greed, and helpfulness. In details:

- *Obedience*. It is the execution of actions given by a superior or someone with stronger "personality" than the victim. A cracker can exploit this human emotion to persuade his victim to do some particular action or to reveal reserved informations. For example the attacker can sends a fake email appearing as the boss of the victim and orders to reveal a password.

- *Guilty*. It is the deep and insuppressible discomfort, caused by, truly or hypothetical, remorse for violations to the moral or religious law. A cracker, making his victim feel guilty (persuading him to be aware of something outrageous), will push him to carry out actions that can somehow remedy to the guilty conscience.

- *Fear*. It is the disagreeable emotion caused by the proximity of a real or presumed danger. Fear is one the most commonly manipulated emotion. When we are terrified our rational faculties default and, as a consequence, it is easier to deceive ourselves. One need only think that in front of a death threat of a family member or a friend, anyone could do actions that normally would never be considered.

- *Ignorance*. It is impossible to know all the entire Internet operating principle, especially for a user without the necessary knowledge. A cracker relies on the users ignorance to create, for example, an e-mail with a polished and very technical terminology to induce the victim to execute the written actions without trying to understand the meaning of the message.
- *Desire* and *Greed*. The Desire is the achievement, or the expectation of a physical asset that we would have while the greed is an uncontrolled desire of power or wealth. The main human vulnerabilities that crackers exploit are the promise of sex and/or money in exchange for confidential informations. Major attacks [2]-[3] in the social network Facebook leverage this two human emotions.
- *Helpfulness*. It is the leaning to help others. A cracker can exploit this noble sentiment to achieve its goal. The attacker can help the victim in trouble, who, feeling safe, will be complaint to do everything.

The social engineering in the exploitation life-cycle

The 2017 Verizon DBIR[2] was recently released [4]. Among all the security incidents that have been analyzed by Verizon specialists, the 43% of the documented breaches involved social engineering attacks. This is almost half of the cyber attacks that have been made overall in the last year. This figure is quite alarming and shows that the human factor is still the Achilles' heel of digital infrastructures.

The main advantage of using social engineering as a hacking technique is to bypass virtually any physical, electronic or digital security systems. In particular, it represents an essential attack vector because it intervenes in all the phases of the exploitation life cycle [5]:

- *Reconnaissance*. In this phase, the cracker uses a variety of sources to learn as much as possible about the business and the operational processes of his target. In this context, the social engineer starts an active information gathering activity, trying to obtain what he needs through direct contact with the victims, which can be done either physically, by telephone for example, or through any other forms of messaging.
- *Scanning*. This step consists in the scanning of terminals and network devices that make up the target infrastructure in order to identify network services, operating systems and any kind of flowed configuration. From the point of view of the social engineer this phase is not different from the previous one. In fact, using the same techniques adopted during the reconnaissance phase, the social engineer is able to obtain all the necessary information in an extremely simple way. It is generally sufficient for him to ask directly to the staff who works or cooperates with the infrastructure of his target.
- *Gaining access*. In the phase in which the attacker tries to gain access to the target infrastructure, social engineering techniques give their best, and in some cases they represent the only viable way to achieve the goal. Phishing, website cloning, baiting and tailgating are just a few examples of attack vectors used to gain access to the system by a social engineer. In this context the only limitations are the imagination and the originality of the cracker.

---

[2] DBIR stands for Data Breach Investigations Report.

- *Maintaining access*. Once he has gained access to the system, the attacker must find a way to keep it reachable. In this case too, social engineering plays a privileged role, because through persuasion, using the right pretext, it is possible to convince the victim to install rootkits, backdoors or even to add exceptions among the firewall filtering rules.

- *Cleaning tracks*. A cracker must be able to cover the tracks in order to conclude an attack successfully. For a social engineer there is nothing easier, just exploit a false identity and, in the worst case, use an excuse to convince the victim to delete the system log files or to disable other security checks.

Threat vectors

Social engineering bases its foundation on human psychology and on the philosophy of deception in order to steal from the victim some confidential information. For this reason it makes use of well-known persuasion techniques, which have always been part of the intelligence processes. Added to these are digital manipulation strategies, which are those used by crackers and attackers to perform cyber crimes against a target.

Currently, the most commonly used techniques for conducting social engineering attacks are listed below:

- *Phishing*. Phishing is definitely one of the most well-known attack vectors globally and, despite being easy to avoid, it is a strategy that continues to be extremely efficient because it affects the naivety and unawareness of its victims. Phishing is a computer scam that exploits emails, SMSs and text messages in general as attack vectors. The most common scenario involves an attacker making a massive or targeted (spear-phishing) sending of well-structured fraudulent messages, in the form of a copy of authoritative or legitimate communications, within which a pretext is provided to push the user to carry out one of the following actions: enter his login credentials to a web service, send money to a specific bank account, download an attachment containing a malicious file, or click on a fictitious URL, typically similar to that used by reliable pages, which can be used to hijack the victim to a server controlled by the attacker himself.

- *Interactive Voice Response system or Vishing*. A social engineer could recreate an automatic IVR system that is practically identical-sounding compared to that used by some well-known institutional services. Even in this case, the social engineer pushes his victim to make use of the fictitious IVR system through some pretext, e.g. a message, a fake page on social networks, or a simple word of mouth too. It may seem trivial, but users tend to trust into IVR systems due to the fact that it is an unknown attack vector, and they end up revealing sensitive information without thinking too much about it.

- *Baiting*. A particularly effective social engineering attack is that of baiting, where the social engineer makes use of a person (most often a corporate employee) as a Human Trojan Horse, to install a backdoor in a trusted system, to infect it or to steal data and credentials from it. The attack strategy is particularly simple: a digital object (USB pendrive, Hard Disk, CD, DVD, etc.) containing a malicious program is given\delivered to a victim or, rather, left deliberately unattended within an organization. When someone makes the decision to check its contents, using a corporate or private target, he inadvertently sends the malicious code into execution, causing an infection in the system.

- *Quid pro quo*. This technique aims to establich an exchange of favors. Nevertheless *quid pro quo* is not one of the simplest way to get into action for a social engineer, but it is certainly one of the most effective, because it relies on people's guilt. In this context, the social engineer becomes aware (or pretends to be aware of) a damage caused by an employee within an organization. First of all, the social engineer assumes to be a person who works as a support engineer for the victim's company, so he tries to make the employee to believe that the amount of damage he caused is greater than the actual one, with the aim of encouraging his sense of guilt (Emotional Hijacking). Later, the social engineer pretends to be able to solve the problem, but in return he asks the victim to provide him some confidential information. Depending on the occasion, he can even invite the victim to install malwares\backdoors on the company system, establishing a real exchange of favors.

- *Tailgating*. All deceptive activities, which are carried out physically by the latest generation of spies, can be referred to by the term tailgating. Being the social engineer a spy in all respects or at least an expert in intelligence techniques, he often resorts to the use of such attacks. In this case the threat is not cyber-based, but merely psychological, and it makes its way through an appropriate use of the body language, the appearance of dress, the construction of a pretext and the normal reactions of individuals in the face of seemingly insignificant circumstances, common and applicants. Attacker may fake the action of presenting or knowing or owning an identity token. He looks legitimate and thus is allowed to walk behind a person with an authorized access to enter into restricted areas, e.g. to install backdoors, to disconnect cables, to clone badges, to turn off systems, etc. To be able to achieve his purpose, he is ready for anything: he carries bulky packs to get the doors open by the employees of a company, he gets dressed as a technician and goes to the construction site with a ladder or a tool bag, he offers cigarettes to get in touch with employees, and so on. In some circumstances the social engineer can choose to resort to the art of impersonation. Impersonation is the most complex form of tailgating and it provides to carry out an identity exchange, with which the attacker can achieve privileges that do not belong to him. Probably, tailgating is the most concrete example of social engineering, the one that materially makes use of a human exploit, as well as the last card to play in the world of cracking when the target system is well configured from a cybersecurity point of view.

- *Dumpster diving*. For a social engineer the garbage of a company can be a valuable source of information. By rummaging in a trash he can retrieve paper documents that contain strictly confidential information. Moreover he can take care the disposal of obsolete digital material from a company, and then calmly retrieve all the valuable information contained within the hard drives. These techniques are called dumpster diving and are mainly used in industrial espionage.

- *Shoulder surfing*. An attack of social engineering as trivial as effective is that of shoulder surfing, in which the attacker does nothing but watch and memorize the insertion of PINs, passwords, access codes and other credentials directly from behind the victim's shoulders and then use them later.

- *Google Hacking*. Google Hacking is a social engineering technique that uses Google and other search engines to find unconventional information, configuration security holes, default credentials, and private information about people. The social engineer is a skilled researcher and knows how to use properly the advanced search tips of the main web tools. Google Hacking represents a successful technique above all because social engineers know well what are the confidentiality settings of some services used internationally, which are not disabled by most people.

Conclusion

"Companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer, operate and account for computer systems that contain protected information". Kevin Mitnick

As we seen in this paper, social engineering is based on human feelings: different feelings can lead to a different perception of reality and this is the bug exploits by a cracker. Helped by well-targeted psychological techniques an attacker exploits human feelings in search of sensitive information that should never be revealed.

Everyone can be victim of an social engineering attack so a question arises instinctive: how can we defend ourself against social engineering attacks? There is no reliable answer, but what we can do is to have a simple and basic guidelines as explained in [6]: be suspicious if in conversations the speaker is interested about details not requested and do not give IDs, passwords, and personal informations via e-mail or phone. However, first of all, it is good to organize training courses on cyber security in order to increase employee awareness, especially in a corporate environment.

References

[1]. "Mr. confindustria a bruxelles truffato da un hacker: persi 500mila euro." [Online]. Available: http://www.repubblica.it/cronaca/2017/09/30/news/beffa_a_bruxelles_mister_confindustria_truffato_e_licenziato-176906111\

[2]. "Spammers are targeting facebook photo albums." [Online]. Available: https://www.markturner.net/2015/11/30/spammers-are-targeting-facebook-photo-albums/

[3]. "Nuova ondata di virus con video porno distribuiti da tag su facebook." [Online]. Available: http://www.protezioneaccount.com/2015/06/nuova-ondata-di-virus-con-video-porno.html

[4]. "Verizon's 2017 data breach investigations report. how long since you took a hard look at your cybersecurity?" [Online]. Available: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[5]. "Social engineering and manipulation." [Online]. Available: https://www.cybrary.it/course/social-engineering/

[6]. S. T. Thompson, "Helping the hacker? library information, security, and social engineering," Information Technology and Libraries, vol. 25, no. 4, p. 222, 2006.

UNIVERSITÀ DEGLI STUDI FIRENZE
DSPS DIPARTIMENTO DI SCIENZE POLITICHE E SOCIALI
DISEI DIPARTIMENTO DI SCIENZE PER L'ECONOMIA E L'IMPRESA
Centro Interdipartimentale di
Studi Strategici, Internazionali e Imprenditoriali - CSSII

Tutti gli scritti pubblicati dal CSSII sono sotto la responsabilità esclusiva dei singoli autori