SOCIAL ENGINEERING AND CYBER SECURITY

Conference Paper · March 2017

DOI: 10.21125/inted.2017.1008

CITATIONS
29

READS
35,562

3 authors, including:

Hugo Barbosa
University of Porto
19 PUBLICATIONS **66** CITATIONS
SEE PROFILE

Telmo Silva Morais
University of Porto
7 PUBLICATIONS **57** CITATIONS
SEE PROFILE

SOCIAL ENGINEERING AND CYBER SECURITY

Breda F.[1], Barbosa H.[1], Morais T.[2]

[1]*Universidade Lusófona do Porto (PORTUGAL)*
[2]*Faculdade de Engenharia do Porto (PORTUGAL)*

Abstract

As the digital era matures, cyber security evolves and software vulnerabilities diminish, people however, as individuals, are more exposed today than ever before. Presently, one of the most practiced and effective penetration attacks are social rather than technical, so efficient in fact, that these exploits play a crucial role to support the greatest majority of cyber assaults. Social Engineering is the art of exploiting the human flaws to achieve a malicious objective. In the context of information security, practitioners breach defences to access sensitive data preying particularly upon the human tendency towards trust. Cyber criminals induce their victims to break security protocol forfeiting confidential information propitious for a more targeted attack. Disastrously, in many cases, targets are manipulated to involuntarily infect and sabotage the system themselves. This paper examines recurrent social engineering techniques used by attackers, as well as revealing a basic complementary technical methodology to conduct effective exploits.

Keywords: Information security, social engineering, cyber security, cyber attack, hacking, Kali Linux, social engineer toolkit.

1 INTRODUCTION

As civilization evolves to grow increasingly connected through the inevitable ubiquity of technology, securing systems, networks and data on which we rely on has become paramount. Cybercrime is a major threat for economics, individual safety and even the public in general, as it is a primary medium for terrorism. [1] In fact, the 2016 Internet Organized Crime Threat Assessment by Europol, reports an increasing acceleration of cyber criminality to such a level, that for some EU countries, it has surpassed traditional crime. Assisting a growing range of threats, from human trafficking to terrorism. [2] Corroborating the cyber menace, on July 14 2016, the Federal Bureau of Investigation (FBI) Director, James Comey, testified before the House Committee on Homeland Security, that nearly all major threats the organization encounters are cyber facilitated: "Virtually every national security and criminal threat the FBI faces is cyber-enabled in some way. We face sophisticated cyber threats from foreign intelligence agencies, hackers for hire, organized crime syndicates, and terrorists". [3]

As the digital era thrives and the on-line universe becomes progressively indistinguishable from real life, cybercrime grows to become a part of everyone's daily lives.

Attacks towards businesses and nations have become so unrelenting that society is incapable of responding to the sheer volume and acceleration of these cyber threats. [4] According to a study by the Bank of America Merrill Lynch Global Research, cybercrime costs the global economy up to approximately 540 billion euros annually. Concluding that in a worst case "Cybergeddon" scenario, cybercrime could potentially extract a fifth of the value created by the Internet. [5] Cyber security incidents continue to grow exponentially, both in frequency and damage, unfortunately users and organizations have not yet adequately deployed defences to discourage the criminal intent to strike. [6]

In November and December 2015, ISACA[1] and RSA2[2] Conference have conducted a global survey of four hundred and sixty one cyber security managers and practitioners. The survey participants have confirmed that the number of security breaches targeting individual and organizational data continues to go unchecked, and that attack methodologies are evolving to become increasingly sophisticated. [7]

The current state of global cyber security stands chaotic, the frequency of attacks is not expected to decrease, and almost seventy five percent of respondents expect to fall prey to a cyber attack in 2016.

---

[1] An independent, nonprofit, global association formerly known by Information Systems Audit and Control Association, now ISACA goes by its acronym only.

[2] A computer and network security company. RSA was named after the initials of its co-founders, Ron Rivest, Adi Shamir and Len Adleman, after whom the RSA public key cryptography algorithm was also named.

The most prevalent attackers are astute criminals that continue to employ social engineering as their primary initial attack vector. [7] Attackers have shifted away from automated exploits and instead, have engaged on human flaws. Inducing victims to, negligently, create vulnerabilities by infecting systems, stealing credentials and transferring funds. Across all vectors, threat actors used social engineering to manipulate people into doing the work that once depended on malicious code. [8]

As a young fugitive, the world's most famous hacker, Kevin Mitnick, was incarcerated for breaching and exploiting computer networks, mostly by using his cunning and persuasion rather than his technical skills. The notorious hacker, considered to be an early master of the science of social engineering, proclaims that no matter how protected any security system is, every person involved is the greatest vulnerability. [9]

2 DEFINING SOCIAL ENGINEERING

Engebretson defines social engineering as one of the simplest methods to gather information about a target through the process of exploiting human weakness that is inherit to every organization. [6] In essence, social engineering refers to the design and application of deceitful techniques to deliberately manipulate human targets. In a cyber security context, it is primarily used to induce victims towards disclosing confidential data, or to perform actions that breach security protocols, unknowingly infecting systems or releasing classified information. [10] The basis of a social engineering attack is to avoid cyber security systems through deceit, exploiting the weakest link, the people involved. [11] Throughout the interaction, victims are unaware of the destructive nature of their actions. The social engineer exploits innocent instincts, not criminal. Explicit methods such as threats or bribery do not fall within the scope of social engineering. [10] A talented practitioner of this discipline understands and perceives social interaction patterns to manipulate the psychological aspects of the human mind. With this resolution, the attacker is capable of executing an efficient and cheap security compromise, without the need to invest in breaking technical security measures. Nevertheless, an educated social engineer on computer science may also complement technological means to the attack in order to accomplish the malicious intentions. [12]

2.1 Categories

A social engineering attack can be classified by one of two possible categories, hunting and farming.[10]

2.1.1 Hunting

This approach seeks to execute the social engineering attack through minimal interaction with the target. Once the specified objective is achieved and the security breach is established, communication is likely to be terminated. This is the most frequently used methodology to support cyber attacks and as a rule, the modus operandi involves a single encounter. [10]

2.1.2 Farming

Social engineering farming is not often practiced, nevertheless this technique may be used for situational purposes. The attacker aims to establish a relationship with the victim in order to extract information for a longer period of time. Throughout the process, the interaction can change, the target may learn the truth and the social engineer may attempt to bribe or blackmail the target, thus resorting to traditional criminal behaviour. [10]

2.2 Phases

In order to achieve a specified objective, social engineering attacks can range from a single encounter to a series of operations, possibly involving several threat actors, intended to gather fragments of related information from different sources. Attacks of this nature, even if dependent on a sole interaction, typically consist of four distinct phases: research, hook, play and exit. [10][13]

2.2.1 Research

Regularly, the operation initiates with the phase of reconnaissance, studying and gathering as much information as possible about the people and business model associated with the target. A well known sentence from Sun Tzu in The Art of War is: "Know your enemy", knowledge is power and in the context of cyber security, the investment on this stage can be invaluable to unveil possible

vulnerabilities. [14] Nevertheless, rather than executing a targeted attack, an experienced social engineering is capable of exploiting chance encounters, and thus opening further opportunities with no research prior to that point. [10]

2.2.2 Hook

In this phase, the threat actor initiates the communication with the potential victim. [13] He engages the target, spins the story, builds a level of intimacy and takes control of the interaction. [10]

2.2.3 Play

The play aims to accomplish the purpose of the attack, which can be to extract information or to manipulate the target in order to compromise the system. [10][13]

2.2.4 Exit

Lastly, the social engineering finalizes the interaction with the victim, preferably without arousing any suspicions. After this last phase, the attacker is typically very difficult to track down. [10][13]

2.3 Attack Spiral Model

This model indicates that as the process develops, the risks, although present throughout the entire operation, increase both to the target and threat actor. Consequently, so does the complexity of the attack, social engineers often have a comprehensive consideration of risk assessment throughout each phase. [15]

3 ATTACK VECTORS

An attack vector is a path or means by which the attacker can gain access to exploit system vulnerabilities, including the human element.

3.1 Social Approach

The attack vectors in social approach can be arise through different acts, tailgating, impersonating, eavesdropping, shoulder surfing, dumpster diving, reverse social engineering and others.

3.1.1 Tailgating

Tailgating is the act of following an oblivious human target with legitimate access through a secure door into a restricted space. The attacker may ask the victim to hold the door, or can simply reach for it and enter before it closes. [11][16] Considering that in the recent past, safety and health regulations prohibit smoking in company premises, this is an increasingly e effective technique as it provides opportunities for social engineering to tailgate groups of smokers. [12]

3.1.2 Impersonating

As the name implies, the threat actor assumes a false identity to gain credibility as a basis to carry out following malicious actions, like piggybacking, pretexting and quid pro quo. [13][16]

Piggybacking, similarly to tailgating, the attacker aims to gain physical entry to secured areas. In this case however, acquires permission from the person with legitimate access by impersonating business entities, like personnel that require temporary admittance. [6][13]

Pretexting, the core of this attack is the fabrication of a plausible scenario propitious to engage the targeted victim. Impersonating an authority figure or a trustworthy entity, the attacker attempts to breach security protocol and gain access to credentials and personal information. [6] This method requires a credible story to prevent arousing suspicion, and thus conducting research on the target is absolutely necessary. [11][17]

Quid pro quo, in the context of social engineering and cyber security, this attack is commonly presented to the target as a fake technical service that conveniently requires sensitive information to be successful. The attacker, impersonating as an IT[3] support technician, aims to infect a targeted system by offering assistance to a victim experiencing technical difficulties. [6]

[3] Information Technology

3.1.3 Eavesdropping

Within a company, the personnel may simply discuss classified matters out loud if expecting only authorized employees to be present. Just for being at the right place at the right time, threat actors can exploit security breaches of this nature. Nevertheless, attackers can also pro-actively listen to communicating channels such as e-mails and telephone lines. [12][13]

3.1.4 Shoulder surfing

Refers to the act of direct observation by surfing over the victim's shoulder to collect personal information, typically used for extracting authentication data. [11][12][18]

3.1.5 Dumpster diving

A classical practice for acquiring sensitive information among attackers is to simply look for it through the garbage. Often, individuals and organizations, do not adequately dispose of documents, papers and even hardware from which can be retrieved confidential data. [12][13][18]

3.1.6 Reverse social engineering

The threat actor entices the target to be the one to initiate the interaction and lies in wait, reducing the risk of arousing any suspicions. The attacker creates and plays a persona that appears to be trusted, fabricates a problem for the victim and, indirectly, presents a viable solution. [12][13][18]

3.1.7 A Recurrent Social Attack Example

In 2015, astute cyber criminals used vicious social engineering tactics to ruthlessly attack and bypass two-factor authentication systems. By exploiting the public trust in a credible entity, one attack was notably successful, the Gmail scam. [4]

A recurrent social attack example in six steps. First step, an attacker extracts the target's email address and phone number through research, often with ease. Second step, the threat actor initiates the attack by sending a message to the potential victim via SMS4[4], equivalent to: "Google has detected unusual activity on your account. Please respond with the code sent to your mobile device to stop unauthorized activity." Third step, the attacker, impersonating the victim, requests a legitimate password reset from Google. Fourth step, Google sends the password reset verification code to the actual victim. Fifth step, the victim, expecting the message from Google, follows the previous instructions and forwards the code to the attacker. Sixth step, with the code, freely given by the victim, the atacker simply resets the password and gains complete access to the account. After accomplishing the purpose of the attack, simply informs the victim of the new temporary password, terminating contact without arousing any suspicions.

3.2 Socio-Technical Approach

The social-technical approach can be arise through different situations, phishing, baiting, watering hole and others.

3.2.1 Phishing

Phishing attacks attempt to extract personal identifiable information through digital means, such as malicious emails that appear to be from legitimate sources and counterfeit websites. [19][20] More sophisticated scams of this nature tend to account for psychological vulnerabilities in order to manipulate victims, creating a sense of urgency in a way that challenges good judgment. [6] Phishing attacks target the masses striving to reach as many victims as possible. [16][17]

Spear-phishing, this technique, on the other hand, is the highly targeted counterpart. A spear-phishing attack can only be executed after initial research, and the content of the message is at least tailored to some extent for the individual target. Social networking sites can be used by cyber criminals to mine data on potential victims, extracting information to create extremely customized messages that would appear to be sent by close friends. [16][18]

[4] Short Message Service

3.2.2 *Baiting*

The attacker can use this physical attack vector by infecting a storage medium with malware, leaving it to be found by the targeted victim, who may naively plug it into the system. [17][18]

3.2.3 *Watering hole*

This is one of the most advanced social engineering attack vectors, as it requires substantial technical knowledge. After researching, the attacker identifies one or more legitimate websites regularly visited by the target. Searches for vulnerabilities, infects the most propitious website for the attack and lies in wait. [16][20]

3.2.4 *A Socio-Technical Attack Example*

This section will reveal the detailed methodology of a technical attack by describing the execution of a simple example. For this, it will be used the Social Engineer Toolkit that comes pre-installed in Kali Linux (Fig. 1).

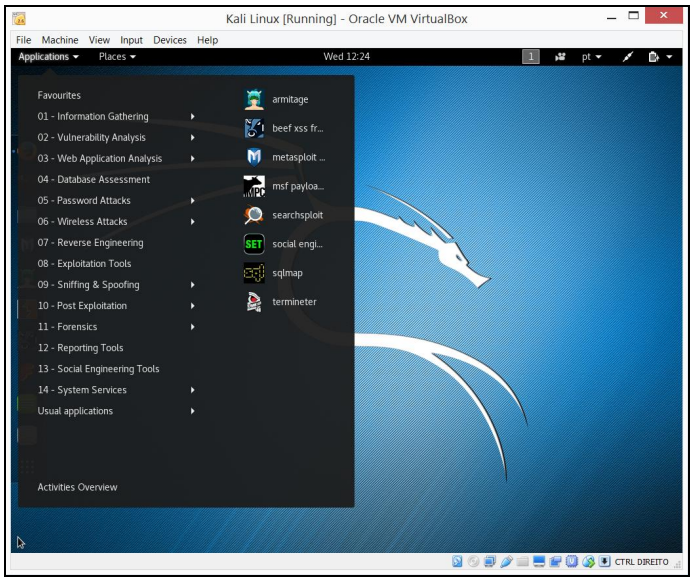

Figure 1 - A few exploitation tools including the Social-Engineer Toolkit

Kali is a Debian Linux based operating system for penetration testing purposes, providing an arsenal of tools designed for analysing and exploiting system vulnerabilities. Funded and maintained by Offensive Security, Kali Linux is a renowned open source project used by cyber security professionals and enthusiasts. [14][22]

The Social-Engineer Toolkit (SET), with over two million downloads is heavily supported within the cyber security community. Created by the founder of TrustedSec as an open source, menu driven, penetration testing tool, SET is now the standard framework for assisting advanced technological attacks in social engineering environments. To initiate the execution in Kali Linux all that is necessary, is to simply type "setoolkit" on the terminal, also accessible through the applications menu. [13][23]

Once the software executes, users are presented with a simple main menu that provides six options, and another one to exit the program (Fig.2). Given the subject of this paper, this attack demonstration is naturally focused on the first option, social engineering attacks. This attack example is a rudimentary phishing attempt of the website vector nature, and thus, in the social engineering attacks menu that follows, “Website Attack Vectors” is selected (Fig. 3).

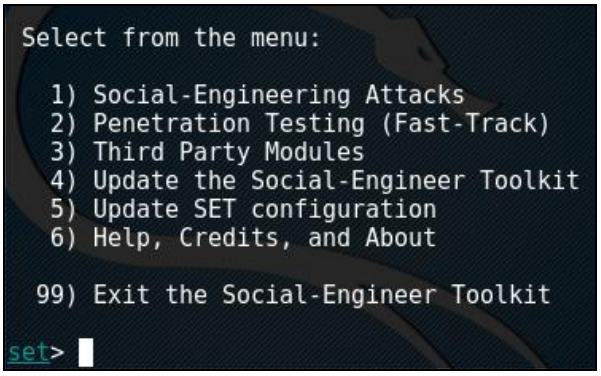

Figure 2: Social-Engineer Toolkit Menu

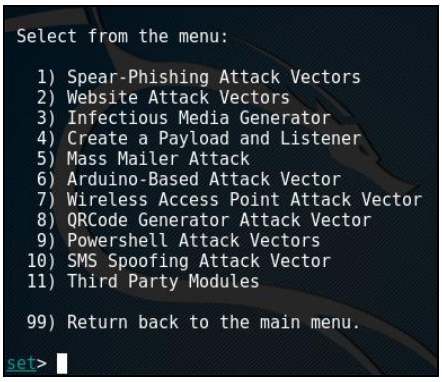

Figure 3: Social-Engineering Attacks Menu

The attacker intends to harvest credentials from a victim and to do this, simply continues to follow the instructions provided by the Social-Engineer Toolkit. In this case, by selecting from the website attack vectors menu, the third option, the “Credential Harvester Attack Method” (Fig. 4). At last, the desired exploit attempt is presented on this following menu, the procedure number two (Fig. 5).

Figure 4: Website Attack Vectors Menu

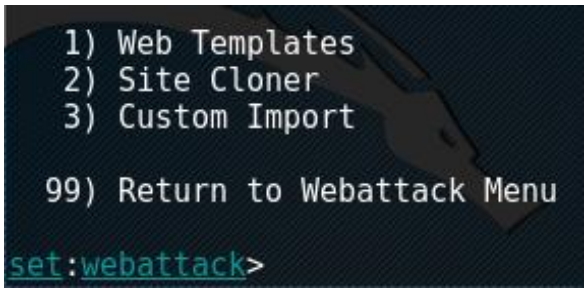

Figure 5: Credential Harvester Attack Method Menu

This attack method is capable of creating a malicious clone from a web platform, attempting to harvest credentials from a targeted victim. To execute this exploit, the attacker is required to introduce the IP5[5] address of the machine operated for the attack, in this case the Kali Linux (10.0.2.15), and the URL6[6] of the website to be cloned, which, for this demonstration, is a well known social network website, Facebook (Fig. 6).

Figure 6: Credential Harvester Attack Method Menu

[5] Internet Protocol

[6] Uniform Resource Locator

Finally, the attacker transfers to the target a fraudulent link, redirecting to the cloned web platform Fig. 7). By applying social engineering techniques, induces the victim to commit the mistake of submitting the targeted credentials. Once the victim visits the link and enters the username and password, the login credentials are redirected to the Kali Linux server (Fig. 8). [13][14]

Figure 7: Cloned Facebook page

Figure 8: Victim's credentials on the terminal

4 CONCLUSION

The Information Age is maturing, complemented by an extremely increased usage of the Internet; humanity evolves rapidly as the growth of public accessible knowledge has been greatly nurtured and facilitated. Consequently, an unmistakable dependence on the World Wide Web has been established in civilization. The digital realm, as a propitious infrastructure for a grand variety of criminal offenses, has grown with the society needs to become an increasingly protected environment. Cyber security develops to grow in sophistication but individuals however, are currently more exposed than ever before. At present, cybercrime is practiced by threat actors that do not necessarily possess a very substantial technical knowledge on information systems, they exploit the human vulnerabilities. Recent studies have shown that people are at the core of the infection chain in the greatest majority of cyber attacks. Social engineering is increasing both in sophistication and ruthless efficiency, because people, make the best exploits. As such, facts point to the conclusion that in the foreseeable future, social engineering will be the most predominant attack vector within cyber security, and thus deserve to be studied further as it evolves in order to advise good practices and measures for individuals and organizations.

REFERENCES

[1] Wenke Lee, Bo Rotoloni, “Emerging cyber threats, trends and technologies”, Technical report, Institute for Information Security and Privacy, 2016.

[2] “Internet organized crime threat assessment”, Technical report, Europol, 2016.

[3] James Comey, “Worldwide threats to the homeland: ISIS and the new wave of terror, statement before the house committee on homeland security”, FBI, July 2016.

[4] “Internet security threat report”, Technical report, vol. 21, Symantec, April 2016.

[5] Nahal Sarbjit, Ma Beijia, Tran Felix, “Global cybersecurity primer”, Technical report, Bank of America Merrill Lynch, 2015.

[6] Nabie Y Conteh, Paul J Schmick, “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks”, International Journal of Advanced Computer Research, Vol.6 pp.23-31, 2016.

[7] “State of cyber security implications for 2016”, Technical report, ISACA and RSA, 2016.

[8] “The human factor”, Technical report, Proofpoint, 2016.

[9] Kevin D Mitnick, William L Simon, “The art of deception: Controlling the human element of security”, John Wiley & Sons, 2011.

[10] “Hacking the human operating system: The role of social engineering within cybersecurity”, Technical report, Intel Security, 2015.

[11] Prashant Kumar Dey, “Prashant's algorithm for password management system”, International Journal of Engineering Science, pp.2424, 2016.

[12] Seppo Heikkinen, “Social engineering in the world of emerging communication technologies”, Proceedings of Wireless World Research Forum, pp. 1-10, 2006.

[13] Rahul Singh Patel, “Kali Linux Social Engineering”, Packt Publishing Ltd, 2013.

[14] Joseph Muniz, “Web Penetration Testing with Kali Linux”, Packt Publishing Ltd, 2013.

[15] Andrea Cullen, Lorna Armitage, “The social engineering attack spiral (seas). In Cyber Security And Protection Of Digital Services (Cyber Security)”, 2016 International Conference On, pp.1-6, IEEE, 2016.

[16] Mika Kontio et al, “Social engineering”, pp.101, 2016.

[17] “Social engineering fraud: questions and answers”, Technical report, Interpol, December 2015.

[18] Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, “Advanced social engineering attacks”, Journal of Information Security and applications, Vol.22, pp.113-122, 2015.

[19] E Rutger Leukfeldt, Edward R Kleemans, Wouter P Stol, “Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks”, British Journal of Criminology, pp. azw009, 2016.

[20] Nalin Asanka Gamagedara Arachchilage, Steve Love, Konstantin Beznosov, “Phishing threat avoidance behaviour: An empirical investigation”, Computers in Human Behavior, Vol.60, pp.185-197, 2016.

[21] Parker Graeme, Shala Vlerar, “Social engineering and risk from cyber-attacks”, Technical report, PECB, March 2016.

[22] “Kali Linux”, https://www.kali.org/. [Online; accessed on December 21 2016].

[23] “Social-engineer toolkit”, https://www.trustedsec.com/. [Online; accessed on December 21 2016].