Social Recruiting: a Next Generation Social Engineering Attack

A.H.B. Schoeman[1], B.V.W. Irwin[2]

Department of Computer Science
Rhodes University, Grahamstown, South Africa,
[1]*E-mail: adam@closehelm.com*
[2]*E-mail: b.irwin@ru.ac.za*

Abstract
Social engineering attacks initially experienced success due to the lack of understanding of the attack vector and resultant lack of remedial actions. Due to an increase in media coverage corporate bodies have begun to defend their interests from this vector. This has resulted in a new generation of social engineering attacks that have adapted to the industry response. These new forms of attack take into account the increased likelihood that they will be detected; rendering traditional defences against social engineering attacks moot. This paper highlights these attacks and will explain why traditional defences fail to address them as well as suggest new methods of incident response.

Keywords: Social-engineering, awareness training

Introduction
As the usage of computers and electronic infrastructure has moved from a fringe asset in corporations to an essential part of business profit generating processes (Black *et al*, 2001), the darker side of information technology has grown in step. The increased use of various information technology systems has equated to a decrease in operating expenses and increased productivity, but has also increased the surface area onto which malicious parties can focus attacks. Faced with this, the discipline of information security was born out of a need to protect assets that have not previously been at risk, and has been quite successful in doing so by implementing an ever-expanding toolbox of controls. But, as technical controls become stronger, devious minded groups and individuals have turned their attention toward the personnel that use the systems rather than the systems themselves, as there is often a higher probability of success associated with breaching an operator than breaching an operating system (Winkler *et al*, 1995).

Social engineering, as it has become known, focuses on the human aspect of information security, but due to its deceptive nature it relies on the ignorance of the target to be successful. This has been addressed somewhat through training and general awareness in both mainstream media and focused training, but just as the nefarious elements within information technology shifted their focus to the easier human targets when technical controls proved resilient, the opportunity now exists for that shift to happen once again. This time, social engineers could capitalise on softer targets within the human element, and, given an awareness of the training that the target may have had, the 'engineer' could avoid many of the pitfalls associated with traditional social engineering. The following section offers a brief outline of the main differences between the traditional social engineering attack and its newer evolution, the social recruiting attack.

ISSN 1445-3312 print/ISSN 1445-3347 online

Social engineering: a low-tech hack for a high tech environment

Social engineering is defined as the science of skilfully manoeuvring human beings to take action in some aspect of their lives (Hadnagy, 2010). Applied more directly to information security, and taking into consideration the actions that penetration testers use when testing the viability of social engineering against their targets, it can be seen as a collection of skills that target the human element of an organisation in an attempt to bypass technical controls. As an example, a classic social engineering attack would consist of the assailant convincing an employee to plug a flash drive into their workstation, which would then run a set of malware, attempting to exploit the workstation and bringing it under the control of the attacker (Hadnagy, 2010). The social engineering aspect of the attack is the act of convincing the target to insert the infected flash drive, which under normal technical means, would require the attacker to somehow bypass inline deep packet inspection (Ross et al, 2011). Social engineering allows the attack to instead focus their attack on a person instead of the technical controls, a method which has proven very successful for famous hackers such as detailed in Ridpath (2011) and Mitnick (2003).

Combating social engineering: knowledge is power

Social engineering relies on deception and misinformation, with the attack assuming a role that has been tailor made to suit the target and yield the greatest probability of success. But while these traits are essentially the cornerstone of social engineering, they are also its weakness. Security awareness training has been singled out as one of the most important initiatives when combating social engineering because it arms employees with the knowledge of what a typical social engineer will do (Allen, 2006). Given this raised awareness, employees can more effectively detect a social engineer, limiting or completely negating potential data leaks.

Increased security awareness goes hand-in-hand with a solid, well-defined, and easily interpreted security policy (Allen, 2006). From the security policy a set of ‘hard and fast’ rules should be derived that can be used by perimeter facing personnel (receptionists, security guards and the like), as they are the most likely to be faced with possible situations that could jeopardise the security of the organisation. Having these two controls in place should allow staff to detect a social engineer and, in the best-case scenario, block one from breaching the organisation. Looking at the increase in literature associated with the detection and prevention of social engineering at Defcon DC over the conference’s 19 years. This rise can be seen in Figure 1, where it is evident that social engineering awareness has enjoyed a drastic increase in recent years, particularly from 2008 to 2010 (Defcon, 2012). The industry has targeted social engineering as a high-risk area of security and has been trying to solve the problem, as shown by the increased number of research papers presented on the topic. As Allen points out, there is no effective way to fully protect against social engineering attacks (Allen, 2006), but this is true for all technical controls as well (defined as residual risk) (NIST, 2003). However, with the increase in general awareness of the subject, the human link is not as fragile as it was when social engineering made its debut.

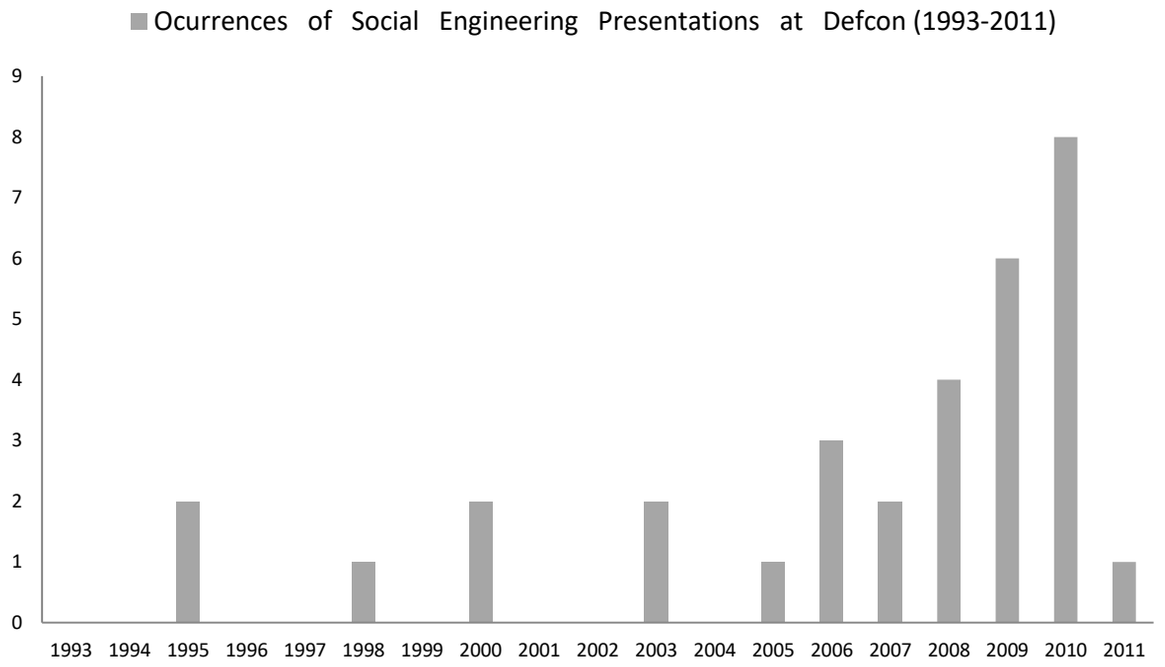

Figure 1: Number of social engineering references in Defcon presentations per year

The social recruiting attack: choosing the right target

Where social engineering relies on a distinct lack of widespread detection in order to succeed, social recruiting builds and improves upon the strengths of human hacking. It takes into consideration that detection will occur, and instead of letting its deception based attack collapse under those circumstances, it instead leverages it as part of the attack vector, hijacking the chain of command within a corporation and repurposing it for the attackers needs.

The process starts off as any other targeted social engineering attack, whereby an individual is chosen as a target based on his or her internal privileges and the potential for breaching network assets by taking control of their workstation. Research into the interests or hobbies of this person is paramount to the success of the attack, as it is this that will be used as the bait for a spear phishing campaign (Burstein, 2009).

This attack's social engineering roots are quite clearly established in the first phase, which could be described as a traditional social engineering attack (spear phishing), but changes slightly from the next step. In the first case, the social engineer builds a dummy website that looks like a web shop front end: a shop that the target would likely want to visit based on their interests and hobbies. However, in the second (social recruiting) case, the social recruiter would spend more time building the reputation of the website, with special attention being paid to a fictitious Help section. The website would have the illusion of a strong user base to help convince the target of its legitimacy, and would require a prospective new member to install an application in order to utilise the site's functionality. A professional-looking installation guide would then clearly state that certain antivirus programs have been known to conflict with the installation process and would 'helpfully' offer ways to remedy that, usually by asking the user to simply turn them off. As this is the crux of the attack, these steps would need to be clearly visible.

This is what differentiates the social recruiter attack: social engineering relies on tricking a human, whereas social recruiting relies on tricking and using one. Knowing that the front-facing low-level employees are increasingly aware of attack vectors, social recruiting instead targets those higher up: it assumes that an upper-tiered executive will have enough influence within the organisation that he or she will be able to have a change made to the technical protections that would leave the company vulnerable to attack. It is assumed that upper managers have this heightened internal privilege and do not understand the potential harm that could come to the organisation by side stepping the security policy (Gabriel, 2011). By creating a convincing installation process that tells the user that the antivirus blocking the program is normal, and shifting the nuance of fixing the problem onto the 'client', the target will hopefully instruct the security team to allow access and whitelist the application.

This form of attack overcomes the inadequacy of social engineering by exploiting two common flaws in organisational security policy: a weakening regard and understanding of the security policy amongst higher level employees in a hierarchical organisation (Gabriel, 2011) (InsightExpress, 2008), and the common managerial assumption that information security is a barrier that prohibits legitimate business transactions (Albrechtsen, 2007).

Detection nullified: the difficulties of combating social recruiting

If both vulnerabilities exist within a corporation's environment, the social recruiting attack allows the attacker to subvert technical controls to infect a station, and uses the station-owner's managerial privileges to open up the technical controls that would prevent the malware from running. Upon a successful installation, the malware could then disable controls that could block a remote shell or similar malicious application from phoning home.

This creates a sizable problem for information security engineers because they could be faced with a situation where they could know very well that an attack is in progress, but be helpless to utilise their arsenal of technical controls to prevent it. This happens due to the weakened security policy posture as it applies to the targeted higher-tiered employee. An information security engineer that attempts to block the attack could put their job in jeopardy, as it could seem to the managerial target that the employee is not performing and not complying with management's requests.

It also means that most of the normal defences used to detect social engineering attacks are severely diminished because the social recruiting attack does not need to keep itself cloaked from security experts to succeed. By disguising the malware as a legitimate piece of software that is being hampered by the numerous security controls, the social recruiter creates an environment where the attack does not need to be changed based on any technical controls that may be protecting the victim. Therefore the attack does not need to know how the internal security landscape of the victim looks in order to craft this attack.

Social recruiting is also immune to the defensive security mantra of protecting against all known forms of attack such as blocking predefined known bad ports, antivirus signatures, IPS signatures and the like (Harris, 2010) .Even though the security department is aware of the attack, it is often powerless to act against it in an environment where the two human vulnerabilities exist.

Out of the box tactics needed to mitigate a social recruiting attack

Since the social recruiting attack exploits two human vulnerabilities in an organisation's security posture, a method that directly mitigates the risk associated with those two

vulnerabilities would be best suited. This means that if procedures were in place that prohibited the altering of the security policy by individuals, regardless of their rank or power within the company, the social recruiting attack would be rendered useless.

However, the weakening of the security policy is not due to a lack of process and procedures, but instead is based on special case privileges that are granted through the hierarchical model and a lack of understanding regarding the reasoning behind the security policy. It is therefore impractical to defend against this attack by addressing the security policy head on.

Fortunately, while difficult to prevent, this form of attack's biggest weakness is that it is extremely easy to detect. This may sound paradoxical at first, given that the social recruiter makes the assumption that detection will occur, but for the defender, this ease of detection gives the information security department the opportunity to react to the attack, specifically by decompiling and disproving the authenticity of each piece associated with the overall deception.

For example, the domain name would probably only have been registered recently (Stakmans et al, 2011). An exception to this would be where the domain was bought by the attacker from a parked domain store, but the resources required for this would normally be too large to justify or require an unrealistic amount of pre-planning. Such action could result in contradicting statements made by the fake users on the website regarding how long they have been members. Any claims that relate to how long the website has been doing business are also worth investigating as timelines are relatively easy to dispute.

Depending on the amount of time that the attacker has put into the website and the overall back story, a general search for the website might render few or no links to it. This would typically be another sign that the site is not what it is reporting to be. If the attacker has gone to the trouble of building a reputable back story for the website though the use of techniques such as cross posting on other forums and so forth, it is unlikely that the attacker would have been able to correlate the posts with the website's date of establishment. A timeline of cross posts would reveal that a surge of activity appears around a certain date and continues forward, but very little before that, which shows that the posts have been fabricated.

While building a docket that disproves the attacker's platform is essential to countering the overall social recruiting attack, its ability to sway the victim is diminished unless the second vulnerability exploited by the attack has been addressed. Once sufficient evidence has been compiled a case needs to be made to a body within the organisation that, if persuaded that the website is malicious, could reliably convince the managerial target of the same, or simply possess sufficient power to override him or her.

The existence of a third party within an organisation that can be activated to aid the security department in breaking the traditional top-down hierarchical enforcement path is essential in the interim, while a mitigation process is put in place to address the difficult relationship between security and the general management of the organisation. Fixing this relationship defect is not achieved quickly or easily, and therefore it requires a stopgap in the form of the third party body to mitigate social recruiting attacks.

In the medium to longer term, the organisation should focus on instituting some form of social reform with the aim of improving the relationship between the security department and the

rest of the company. This is not a focal point for this paper due to the amount of work required, but some areas that can be looked at are:

1. Actively marketing defensive security in the company by highlighting the attacks that have been prevented, possibly aided by showing the theoretical maintenance costs or data loss had those attacks been allowed to pass the control points.
2. Drawing on the incident response team's knowledge in this type of scenario, as they might have internal case studies of breaches that have occurred in the past that match this new attack's fingerprint. There is also value in forwarding the digital forensic education of the security team to management, arming them with the tools to successfully combat the social recruiting attack before it takes place.

Conclusion

Security has evolved over the years from simply applying ACLs on perimeter routers, to layering multi technical controls over each other, to a point now where deep packet inspection is required on both the inbound and outbound network paths of the organisation (Ross et al, 2011). As the technical controls increased in strength, attackers have redirected their efforts towards the easier targets: human operators.

Social engineering has gained momentum because of its ability to bypass many of the technical controls found in a typical corporation's network, but due to tactics based in deception, the infamy of social engineering is often a double edged sword. By exploiting the human element, it is humans who become personally motivated to encourage a greater level of education and response, thereby diminishing the probability of an attack successfully breaching an asset in the future.

While an environment of stronger technical security controls and heightened awareness is not conducive to traditional social engineering attacks, the social recruiting attack thrives in it by combining the most powerful aspects of social engineering with two common human and organisational vulnerabilities often found in companies.

Because of this attack's ability to shatter the technical controls of an organisation via managerial edict, there is no suitable technical platform that can be used to remedy the attack vector. Instead the information security team must employ non-traditional forms of security such as research and information gathering with the purpose of disproving the legitimacy of a seemingly honest website or piece of software.

The remediation strategies for the social recruiting attack are limited, resource intensive and require that the attacker has not covered his or her back story correctly, placing the security team on the back foot. Also it requires a lot of time and precise work from the attacker, who needs to make sure that the timeline of the website makes sense and is plausible, since it is the easiest portion of the attack to investigate. Coupling this with the assumption that the company has a weakening security policy at the higher echelons (and that a negative attitude towards the security department exists), the possible attack surface and frequency of this attack can be viewed as relatively low compared to those that information security specialists face on a daily basis.

However, in the contemporary world it has become worthwhile for a group of hackers to attack a security company, steal secrets from them and then use those secrets to successfully attack a military contractor Finkle (2011) describes this attack that took patience, planning

and out-the-box thinking, and while it could be classified as an unlikely occurrence on a daily basis, the truth of the matter is that it did happen and could happen again.

As the attack is so dynamic and time sensitive, the security team needs to focus on being able to quickly and efficiently label a social recruiter attack. They can then identify which parts of the deception need to be dissected and disproved, and finally have a predefined process in place to escalate the docket to a pre-formed body with both the technical and managerial power to address these types of attacks.

The steps required to combat social recruiting attacks have their difficulties, but they are not expensive from a capital expenditure point of view nor are they unrealistic, but they do not fall under the traditional armoury of the security specialist. While this might cause the responsibility of the attack to be passed on to some other department, security personnel that defend a company's assets need to realise that a dynamic mind set needs to be used to combat dynamic attacks. Unless security professionals realise that the trench-warfare style of defending needs to be abandoned, their prospects of being able to successfully protect their corporation's assets are bleak at best.

References

Albrechtsen E. (2007) A qualitative study of users' view on information security, *Computers & Security*, 26 (4): 276 – 289.

Allen M. (2006) Social engineering: A means to violate a computer system, *SANS Institute InfoSec Reading Room*, pp. 1–13, SANS Institute

Black S. E., Lynch L M. (2001) How to compete: The impact of workplace practices and information technology on productivity, *The Review of Economics and Statistics* , **83**(3)434-445 Defcon Communications Inc. (2012) Defon archives. Electronic. URL: https://www.defcon.org/html/links/dc-archives.html [Accessed 3rd July, 2012]

Finkle J. (2011) Exclusive: Hackers breached U.S. Defense Contractors, *Reuters*. URL: http://www.reuters.com/article/2011/05/27/us-usa-defense-hackers-idUSTRE74Q6VY20110527 [Accessed:17th May 2012]

Gabriel Consulting Group (2011), *2011 GCG Data Center Security Survey*, Gabriel Consulting Group, Beaverton, Oregon, United States of America

Goss R., Botha R. (2011) Traffic flow management in next generation. Service provider networks - are we there yet? Proceedings ISSA 2011, *Information Security South Africa Conference 2011*, Balalaika Hotel, Sandton, South Africa, pp. 1–6..

Hadnagy C. (2010) *Social Engineering: The Art of Human Hacking*, Hoboken, New Jersey, United States of America, Wiley

Harris S. (2010) *CISSP All-in-One Exam Guide*, Fifth Ed, Columbus, Ohio, United States, McGraw-Hill Osborne Media

InsightExpress (2008) *Cisco research reveals common data loss mistakes*, CISCO.com the network.URL:

http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-499060.pdf [Accessed: 30 June 2012]

Mitnick K. (2003) *The Art of Deception: Controlling the Human Element of Security*, ed, Hoboken, New Jersey, United States, Wiley.

National Institute of Standards and Technology (2002) *Risk management guide for Information Technology Systems*, NIST Special Publication 800-30, Gaithersburg, Maryland, United States.

Ridpath M. (2011) *Covert calling*, BsidesPDX Portland Track 1, URL: http://www.upstream.tv/recorded/17736407 [Accessed 3rd July, 2012]

Stalmans E., Irwin B. (2011) A framework for DNS based detection and mitigation of malware infections on a network, Proceedings ISSA 2011, , *Information Security South Africa Conference 2011*, Balalaika Hotel, Sandton, South Africa, p.3.

Winkler I. S., Dealy B. (1995) Information security technology?... don't rely on it. A case study in social engineering, Proceedings of the 5th conference on USENIX UNIX Security Symposium - Volume 5, *USENIX Association.* URL: http://dl.acm.org/citation.cfm?id=1267591.1267592 [Accessed 30th June 2012]