

Social Engineering: Strategies and Defence

A whitepaper by encription limited

**Author: Campbell Murray
January 2011**

**encription limited
encription house
Foley Drive
Kidderminster
DY11 7PG**

+44 (0) 330 100 2345

ABSTRACT

Social engineering is the Art / Science of manipulating someone in order to bypass security measures and tools. The purpose is to obtain confidential information from users through phone, e-mail, snail mail or direct contact and to use these data to gain illegal access or obtain confidential information.

This whitepaper aims to outline the author's approach to, and thinking on, the subject of social engineering. It is not intended to be exhaustive with respect to the myriad of techniques and broad knowledge base which apply to the art of social engineering. Instead this is but a short introduction to the drivers, for and devastating effect a well played social engineering attack can have.

The author does not hold any qualifications on the subjects of psychology or influence, however the subject matter contained within has been derived from observation over several years of involvement in social engineering. From taking part in, and leading, building incursions to remote social engineering via email, telephone and fax. The author has gained a wealth of experience in extracting information from targets and has developed their own strategies, techniques and opinions on the motives and drivers behind why social engineering works.

INTRODUCTION

The security threat surface has changed dramatically over the last decade and, as a result, so have the activities of criminals and fraudsters who are always looking for ways in which the public can be exploited for criminal or illegal gain.

Since the boom of broadband criminals have found ways to exploit technical vulnerabilities in firewalls and operating systems to gain access to remote [and local] systems and manipulate them to their advantage. A notable shift occurred within the IT industry around 2003 when the latest operating systems came with fewer services enabled by default, dramatically lowering the threat surface and slowing the tide of remote exploitation.

Users slowly became more aware of the threat after large scale virus outbreaks and adopted the baseline requirements for enabling their local firewalls and installing anti-virus and anti-spyware software.

In short the threat surface was shrinking and as the digital landscape changed so did the criminals activity. Instead of worm viruses; which spread by automatically infecting unprotected hosts, the prevalence of 'Trojan horse' viruses; which required the computer user to perform an action to become infected, increased dramatically. The term 'Drive by Pharming' was spawned as users could become infected with malware simply by visiting a website which exploited vulnerabilities in computer user's web browsers. All of this indicating a drop in directly targeted remote exploitation of systems.

HOW DOES IT WORK?

The shift in the criminal's behaviour is both surprising and expected at the same time. A criminal utilising technological vulnerability to obtain what they want – either your data or control of your computer system – by whatever means necessary is to be expected. What is surprising is how long it took to start using **social engineering** techniques to spread malware.

Social Engineering is as old as human communication. We perform social engineering whenever we request another person to perform a task for us. This may sound flippant but if the request is made in the right way, by the right person then we are normally happy to oblige.

We can achieve what we want by adhering to 3 simple principles.

- ⤴ Compliance
- ⤴ Trust
- ⤴ Benefit

Expanding on these principles we gain a fuller view of the process of social engineering.

Compliance

We do as we are told. This is an inalienable fact which we cannot escape from. When we are children we are instructed in what to do by our parents. When we go to school we are instructed in what to do by our teachers. When we embark on our careers we are instructed in what to do by our managers, peers and employers. We are conditioned, from before we can walk, to follow instructions.

Trust

As we get older however we do not take instructions from just anyone. As children we listened to adults as we saw them as an authority. As we become adults we are less inclined to blindly follow instructions from other adults. We do still follow instructions from authority figures though. Imagine I came into your place of work dressed as a fireman and instructed everyone in the building to leave. Would you? Of course you would.

By combining a direct instruction to leave the building coupled with the belief that I really am a fireman would be enough to gain what I wanted in that situation.

Benefit

Using the above example the benefit is clear to the office staff. A fireman is telling me to evacuate the premises ... surely this is in my interests!

Although this may sound flippant benefit cannot be over looked as a powerful social engineering driver. Not only are we conditioned to follow instructions we are also, by and large, very helpful people. The majority of the populace feel good about themselves if

they assist another member of the public; a very useful piece of knowledge for the social engineer, and one which has been exploited endlessly. For example several years ago a 'hoax virus' circulated by email. The email did not contain any attachments or any technical exploit, but did inform the recipient that they should view the C:\Windows directory of their systems, and if they had a file named lsass.exe installed, they should delete it immediately and restart their machines.

At the time that this was circulating the Sasser worm, which some variants of did indeed infect the lsass.exe file, was also rising in media attention. Unfortunately if the victim did delete lsass.exe they would find that their computers would then restart endlessly every 60 seconds or so rendering them useless!

So how did this hoax spread? By using all of the principals described above.

Compliance was gained as the email specified a series of actions to undertake. Clear and simple orders are seldom disobeyed. **Trust** was gained as the email would be received by someone you knew. Remember that this hoax did not spread by previously infecting the sender's machine, but it was genuinely forwarded by concerned recipients, which brings us onto **benefit**.

The sender would hope to benefit by basking in the reflected glory earned by assisting all of their associates within their contact directory. The recipient would benefit by disinfecting their computers and then forwarding the email on and thus similarly enjoying the feeling that they had assisted their friends.

The spread of Trojan viruses, as mentioned earlier, work on the same principles. Let's take an example.

The 'Anna Kournikova' or 'I love you' virus spread in much the same way. Someone would receive an email from someone they knew with an attachment entitled 'I love you' and instructing the recipient to open the attachment. Compliance is gained by issuing a simple, direct and unambiguous instruction. Trust is gained as the recipient may recognise the sender. Benefit is gained by tantalising the recipient with a gift ... I love you ... or the potential to view images of Anna Kournikova. If the recipient opens this attachment, and their system is vulnerable to the exploit, then all of their contacts will be forwarded, the message and thus the virus spreads.

Much has been written about gift giving in the context of social engineering (Navarro, J 2008) and the influence on individuals this can bring, this technique is thousands of years old – The Trojan horse dates back to the Greek Hellenic period when following a fruitless 10 year siege of the city of Troy the invading Greek army appeared to depart and leave a gift for their foe, a wooden horse. Within the horse lay an elite army of Greek soldiers who facilitated the fall of the city. Today a 'Trojan Horse' is largely associated with computer malware however the processes are universally the same ... compliance, trust and benefit (CTB).

The CTB concept works as a triad. Depending on the situation, and your expected outcome, varying degrees of each element need to be applied. Each case is individual however the basic concepts remain the same.

Let's take a real world, live penetration test example.

EXAMPLE OF SE

During the run up to the summer holidays 2010 encription limited were asked to perform a remote social engineering exercise against a large Local Authority within the UK. The population of individuals randomly selected as targets for the test was in this case very small. Only 10 names were provided.

To start the exercise some Open Source Intelligence Gathering [OSIG] was required. Looking the authority up via a search engine then browsing their website revealed that the email format most commonly in use was [firstname.lastname@authority.gov.uk](#) thus we created a list of email addresses based on this format from the given names.

Now we had a list of targets we attempted to confirm that the email addresses were valid by connecting to the authorities' mail servers over port 25 and issuing a VRFY query. VRFY enables a sending mail server to verify if the email address is valid or not. Once we had cleaned our list in this way we now needed a sting to get the targets to perform an action for us.

We decided that nothing less than network logon usernames and passwords would do.

As this project was shortly before the summer holiday season in the UK we decided to use a voucher offer website to obtain logins. Some more time researching on the internet provided us with the tourist board website for the authority. As the tourist board is effectively a part of the authority it served to start to answer one of our criteria – **Trust**.

By spoofing / copying the tourist board website and registering a domain name very similar to the real website we were able to have an identical copy running on the internet in less than 30 minutes. This spoofed site was modified to contain a login page which would capture any data entered.

Now we needed to lure our targets to the site, however we still needed to maintain the trust element to our attack. An email was sent to an invalid email address, e.g. [asjklajsdf@authority.gov.uk](#) and the subsequent non-delivery reply email in this case contained the standard email disclaimer used by the target. An email was created using the same font and footer as in use by the authority and our targets were sent a phishing email. We will refrain from divulging the full content of the email however it would suffice to mention one or two aspect of its contents, The two other elements in our triad, **compliance** and **benefit**. Compliance was achieved by issuing an instruction to the

target. In this case the instruction was to log into the website before a particular date in order to gain the **benefit** of what was being offered.

The exercise took less than an hour and a half to set up and gather all of the information necessary to successfully gain valid usernames and passwords to log on to the clients network. A total of 6 people from our selection of 10 provided us with valid information, whilst the other four either did not respond or filled in the login screen with invalid data.

CONCLUSIONS

A well executed social engineering attack is nearly impossible to defend against. Only by ensuring that employees and management are trained and aware of the techniques used by social engineers will the business be able to provide an adequate defence against a determined attacker.

