Bachelor's thesis

Business Information Technology

Business Data Communications and Information Security

2016

Mika Kontio

SOCIAL ENGINEERING 101

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

2016 | 67

Jarkko Paavola (Turku University of Applied Sciences)

Mika Kontio

SOCIAL ENGINEERING 101

This thesis was carried out in collaboration with Phirelight Security Solutions Inc. which is a Canadian information security company. The practical part of this thesis was commissioned by them. The purpose of the thesis was to create an all-inclusive handbook that outlines different social engineering methods and give the reader a basis on how to protect themselves against social engineering attacks.

The main research method was finding previous experiences of social engineering attacks from the Internet as well as research the psychology behind manipulating people and their behavior based on literature on the subject. The references used in the analysis of the techniques were mostly collected from various scientific publications while the case study references were collected principally but not exclusively from various reputable online publications.

The result of the research is a simple but comprehensive study which is meant to educate the reader with the help of examples of real life scenarios and incidents. The practical experiment carried out as the commission of Phirelight Security Solutions Inc. further underlines the importance of understanding why guarding one’s own personal information is important as well as why everyone working in a modern corporate environment should always be aware of social engineering attacks and how they work.

This thesis as a whole is meant to be used as a beginner’s guide for understanding social engineering attacks. It does not include each and every single method used for these attacks. The intent has been to bring every reader's awareness to an acceptable level while maintaining a reasonable length for this publication. The Phirelight experiment has resulted in the company offering this kind of a service to its customers as well.

KEYWORDS:

Social Engineering, Hacking, Phishing, Information Security

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittelyn koulutusohjelma | Yrityksen tietoliikenne ja tietoturva

2016 | 67

Jarkko Paavola (Turun Ammattikorkeakoulu)

Mika Kontio

SOSIAALISEN MANIPULOINNIN PERUSTEET

Opinnäytetyön aihe oli sosiaalisen manipuloinnin perusteet ja hyökkäystavat. Päätavoitteena oli luoda kattava opas, jota voidaan käyttää koulutustarkoituksiin. Tästä syystä opinnäytetyö on kirjoitettu englanniksi. Opinnäytetyön tukena toteutettiin myös pienimuotoinen koe, jossa testattiin kanadalaisen tietoturvayhtiö Phirelight Security Solutions Inc:n sisäistä valmiutta sosiaaliseen manipulointiin perustuviin hyökkäyksiin.

Tutkimus- ja kirjoitustyö tapahtui kvalitatiivisena tutkimuksena ja toimintatutkimuksena. Pääkysymyksenä oli selvittää, mistä syystä sosiaalinen manipulointi on helpoin hyökkäysmetodi tietoturvamaailmassa ja tästä näkökulmasta kirjoittaa opas sen torjumiseen. Tutkimuksen tukena käytetty aineisto koostui internetistä haetuista julkaisuista samoin kuin kirjallisista teoksista. Opinnäytetyöhön kuuluu myös case-tutkimus, jossa analysoitiin kolmea tietomurtoa, joissa jokaisessa käytettiin hyväksi sosiaaliseen manipulointiin perustuvia hyökkäysmetodeja. Phirelightilla suoritettu koe toteutettiin konstruktiivisena tutkimuksena, jonka toisena tavoitteena oli selvittää voisiko vastaavaa palvelua tarjota myös asiakkaille tulevaisuudessa.

Tutkimustyön keskeisimmät tulokset olivat samoja opinnäytetyön jokaisessa osuudessa. Perimmäisimpiä syitä sosiaalisen manipuloinnin helppoudelle ovat ihmisten opitut käyttäytymissäännöt ja -ohjeet, jotka tekevät käytöksestä helposti ennakoitavaa. Tästä seuraa väistämättä se, että myös ihmisiä on mahdollista hakkeroida käyttämällä hyväksi heidän valmiiksi opittuja käyttäytymismalleja. Ihmisten luontaista käyttäytymistä ei myös voi päivittää samaan tapaan kuin tietoturva-aukon sisältävää ohjelmaa. Phirelightilla suoritettu koe osoitti saman todeksi, kun noin kolmannes työntekijöistä antoi oikeat käyttäjätunnuksensa sähköpostin kautta välitetylle phishing-sivulle.

Tutkimustulosten pohjalta keskeisin johtopäätös on että yritysmaailmassa viime kädessä tietoturvasta ovat vastuussa aina työntekijät itse, eikä yrityksen sisäiseen turvallisuuteen erikoistunut elin. Sosiaaliseen manipulointiin perustuvat hyökkäykset kohdistuvat usein niin laajaan yleisöön, että niiden estäminen on käytännössä mahdotonta. Tästä syystä tehokkain puolustus on kouluttaa ihmiset niitä vastaan. Phirelightilla toteutettu koe johtanee kyseisenlaisen testauspalvelun ja koulutuksen tarjoamiseen myös asiakkaille.

ASIASANAT:

Manipulointi, hakkerointi, verkkourkinta, tietoturva

CONTENT

APPENDICES

PICTURES

LIST OF ABBREVIATIONS

Baiting	Using a promise of an item or goods to entice the victim to act in a desired way (Bisson 2015).
CMS	Content Management System is a system used to manage the contents of a website without deeper knowledge of HTML (TechTarget 2011).
CTO	Chief Technology Officer is an individual overseeing the technology in the company and has knowledge of both business and technology (TechTarget 2013).
DoS	Denial of Service is an attack where the attacker uses a single connection to cause harm to the functionality of the Internet facing service (Imperva 2016).
DDoS	Distributed Denial of Service is an attack where the attacker uses multiple devices and connections to flood and drown the target in a big volume of traffic (Imperva 2016).
Excel	Excel is a part of Microsoft Office family used for manipulating tables (Microsoft 2016).
Hash	Hash is a string created from another string with a one-way algorithm with the goal of protecting the original string (Defuse Security 2014).
ICS	Industrial Control System is a command and control network designed to support industrial processes (ENISA 2016).
IRC	Internet Relay Chat is a program and protocol used for communicating in real time with people from all over the world (irchelp.org 2013).
JS	JavaScript is a programming language mainly used for making interactive webpages (About.com 2014).
MIME	Multipurpose Internet Mail Extensions is an Internet standard meant for expanding the functionality of the regular email (Techopedia Inc. 2016a).
Phishing	Phishing means the act of seeking to obtain personal or sensitive information by tricking the victim to reveal it (Bisson 2015).
Trojan	Trojan is a type of malware that is disguised as a legitimate software (Kaspersky Lab 2016).
SE	Social Engineering means influencing and manipulating people without their knowledge towards a goal (Social Engineer Inc. 2016a).

Steam	Steam is a video gaming marketplace and hub software made by Valve Corporation (Valve Corporation 2016a).
Steam Guard	Steam Guard is essentially Steam's 2-factor authentication component (Valve Corporation 2015).
Spear phishing	Spear phishing means phishing that targets a smaller group of people and tailoring the attacks with greater precision (Hoffman 2013).
Salting a hash	Salting means adding another string to the original string before hashing it so that the attacker cannot guess the original string just from the hash (Defuse Security 2014).
SMTP	Simple Mail Transfer Protocol is a TCP/IP protocol meant for storing and forwarding email (What is My IP Address 2016).
SSH	Secure Shell is a protocol used for accessing a remote server safely in an encrypted session (The Computer Language Company In. 2016).
SSL	Secure Sockets Layer is a standard technology used for creating encrypted connection between the client and the server (DigiCert Inc. 2016).
SSN	Social Security Number is varying length number and alphabet combination string used for identifying people (Investopedia LLC. 2016).
SWAT	Special Weapons And Tactics is a special team working under FBI assembled for extremely high-risk situations (FBI 2016).
Swatting	Swatting means calling the authorities in the US with the intent of getting SWAT to deploy at victim's address because of a fake distress call (Fagone 2015).
TLS	Transport Layer Security is essentially the newer version of SSL (PC Plus 2012).
URL	Uniform Resource Locator is a reference to a resource on the Internet though it can be used for local network resources as well (Oracle 2015).
VM	Virtual Machine is virtualized software computer running inside a real bare-metal computer (VMware Inc. 2016).
VPS	Virtual Private Server is a virtualized server that mimics a real dedicated server (Markle 2015).
Waterholing	Waterholing or water hole attack means for example that the attacker has infected a legit website and waits for their real target to visit it (Grimes 2013).
Zero-day/0-day	0-day vulnerability is a hole or bug in software unknown to the vendor and which is exploited (PC Tools 2016).

1 INTRODUCTION

The subject of this thesis rose from the realization how prevalent Social Engineering (SE) is in the business world and among ordinary people today. My studies have been primarily focused on writing code, configuring networks and of course information security. Social engineering however has been only glanced at even though in 2015 the annual costs of phishing attacks alone were $3.77 million for the average company. Social engineering attacks are frequently underestimated especially in corporations even though just by preparing the employees against these kinds of attacks with basic training would substantially reduce phishing-related costs (Ponemon Institute 2015, 1.)

Social engineering is perhaps the easiest approach when attacking any individual or organization. Its main strength is the fact that the attacker can get other people to do their work for them. My personal experience is that once you learn about phishing, baiting and other types of social engineering attacks you start spotting them in your day-to-day life as well. As for the question who will fall a victim to social engineering there really is not a single answer to, though there are clearly some groups of people that seem to be more susceptible to frauds (FINRA 2013, 6). No one is perfect though and everyone can make mistakes. Humans are curious beings by nature and our inquisitive nature is one of the reasons we originally came to realize there is a whole new world in the savannahs near our trees. From the information security professional’s point of view it is just too bad that our natural reaction when encountering new and exciting things is trust before doubt.

2 SOCIAL ENGINEERING – WHAT IS IT?

By one definition social engineering means “any act that influences a person to take an action that may or may not be in their best interest” (Social Engineer Inc. 2016a). This pretty much encompasses the whole term in one sentence, but to really understand the meaning of it we need to explore it a bit further.

2.1 History of Social Engineering

Social engineering is not by any means a new phenomenon. Throughout the years people have found ways to influence the way others act in certain situations and take advantage of it. Probably the most known historical example of SE is of course the Trojan Horse from Odyssey by Homer. The tale is so famous that we have even named a malware family after it. In the story the Greeks have fought a long war with the Trojans and finally feign giving up the battle. The Trojans see the last ship of the Greeks sailing off into the sunset and to further support their story the Greeks have left one warrior to stay behind and spin a tale of their retreat and symbol of surrender, the actual wooden hollow Trojan Horse. Naturally during their celebration the Trojans are killed by the Greeks who emerge from inside the horse. From a contemporary point of view the tale might not seem as genius as it actually was. Whether or not the story actually happened is not relevant, it is the elements of it that matter.

Today anyone hearing the story probably would not be surprised by the hollow horse but the point is that in that time period no one could not even imagine such a thing. In this day and age we have come to expect plot twists and unexpected outcomes from all the tales we see in TV or movies, but a few thousand years ago the stories people told each other lacked the same kind of a structure. These stories essentially shape how we perceive the world and at the time of Homer writing the Odyssey people had a different view of the world. The idea of a hollow wooden horse was completely new and different. The same principle holds true

with all SE. People act based on things they have learned previously in life and they expect the outcomes of actions and events to be predictable.

2.2 Psychology of Social Engineering

The human brain excels in creating habits. The brain in a way is a machine, and everything it does consumes resources, which means energy. From the brain's perspective the optimal situation is using as little energy as possible. This is why we create patterns in our everyday life, such as having a coffee when we arrive at work, smoking a cigarette after 10 o'clock or reading the news while having lunch. The patterns save energy, an individual does not have to think about what they are going to do next all the time (925 TV 2012.) In the computer world the hacker finds a way to trick a program that is supposed to accomplish task X into doing task Y while still staying inside the limitations of the program. The same kind of a mindset is present in SE as well. When you know how people react in certain situations it is easy to abuse these existing behavioral models to achieve your real goal.

Social engineering is not anything new, that much we have already established. That does, however, raise the question how come it has not really been acknowledged until modern times? Partly this is because the root of social engineering, psychology, did not really exist as its own branch of science before a German professor Wilhelm Wundt founded the first laboratory dedicated solely to psychology in 1879 in the University of Leipzig. Wundt's research was focused on the test participants' reactions to external stimuli, for example he would expose participants to the sound of metronome and ask them to report their sensations (McLeod 2008.) While this is still far from studying facial micro expressions it was a good start. Wundt is also known for many of his students that became famous psychologists as well, such as Edward Titchener who continued his work.

Wundt's view on the mind was called structuralism, or the study of the basic elements that constitute the mind. Whereas Wundt focused on the relationships be-

tween the elements of the consciousness, Titchener gave his attention to the individual elements. The structuralist approach had it faults though and it went out of fashion so to speak because the results of experiments were hard to reproduce. The results were not unambiguous, which is the basic requirement for scientific theory to hold any merit (Schacter etc. 2011, 8-9.)

There is, however, one important thing to take away from all of this: while people do react to stimuli in somewhat predictable ways, all people are still individuals. What might cause an outrage in one person might produce a laughter in another. A successful social engineer keeps this in mind and does not use the same tricks for different people.

3 SOCIAL TECHNIQUES

Social engineering is a very wide phenomenon, but I will try to cover most of its more common techniques. SE is more of an art form than a set of certain skills and this is why it is easier to try and understand it by looking at the steps most attacks follow. Even though SE has more in common with psychology than IT, the mindset needed for it is very similar to that of a regular hacker's. This is why defending against it is easiest by understanding how the attacks work. According to Interpol (2016) social engineering frauds typically follow the same four steps: gathering information, developing a relationship, exploiting any identified vulnerabilities and the execution. This is pretty much true in cases where social engineering means actual interaction between the attacker and the target. In this chapter I will go through most of the social techniques used in various parts of the attacks. Later on we will discuss the sort of SE that does not require the attacking party to maintain a personal connection to the victim.

3.1 Doxing

Gathering information, or doxing like I am going to refer to it from now on, is by far the most important part of any successful attack. Doxing is something that is hard at first to master but once you get the hang of it, it is surprising how much information you can find online from a previously completely unknown person. Doxing is the most important part of all attacks because it creates the base on which the rest is built on. Once you know the target's name, home address, social security number and perhaps even the spouse's name, it is relatively easy to impersonate the target and gain even more information about them. Many people underestimate the power they are giving to complete strangers just by posting their hometown in their pseudo-anonymous Instagram account. By having a name and the city the possible results are already narrowed down greatly. Personally I have the guilty pleasure of doxing online all the new people I meet and it does not usually take longer than 10 minutes to find the person's Facebook

page just with their forename and hometown. It just takes some patient page-scrolling, nothing more.

One of the most recent cases of big information leaks happened in December when Valve's popular gaming and digital store platform Steam allowed by mistake its users to view each other's store pages. People were able to see other users' billing addresses, the last four digits of their Steam Guard phone number, their purchase history, the last two digits of their credit card number and/or their email address. The incident only lasted for about an hour or two but the damage was already done. The fault was apparently in bad caching rules that were deployed because of the simultaneous Denial of Service (DoS) attack as well as a huge volume of users browsing the store during the holiday sales (Valve Corporation 2016b.) This level of detail from anyone is the holy grail of a social engineer. The details revealed make it possible to impersonate the targets very convincingly. Because of the random nature of the leak it is hard to estimate the real damages of the incident. Furthermore having a person's billing address allows the malicious person to cause even actual damage to the target. In his video podcast the video games critic John Bain, or Totalbiscuit as he is known online, expressed his worries over the matter as well. Bain is known as a very vocal critic in the video game world and his opinions are often very straightforward have a tendency to irritate many people. In his case it would be a completely legit fear that if someone obtained his home address this way, they might swat him for example (Totalbiscuit, The Cynical Brit 2015.) Swatting in this case means the phenomenon present mostly in the US where the malicious person calls the emergency authorities with the false pretense that some serious crime is taking place in the victim's address. The goal of the attacker is to get the law enforcement Special Weapons and Tactics (SWAT) team deployed there. Swatting is one of the more deviant ways an attacker can use just the target's home address to cause harm to them (Fagone 2015.)

Besides impersonating the target or causing actual harm to them, the contact details give the attacker other kind of power as well. I used to work one summer as a telemarketer and we were using this software that was doing the calling for

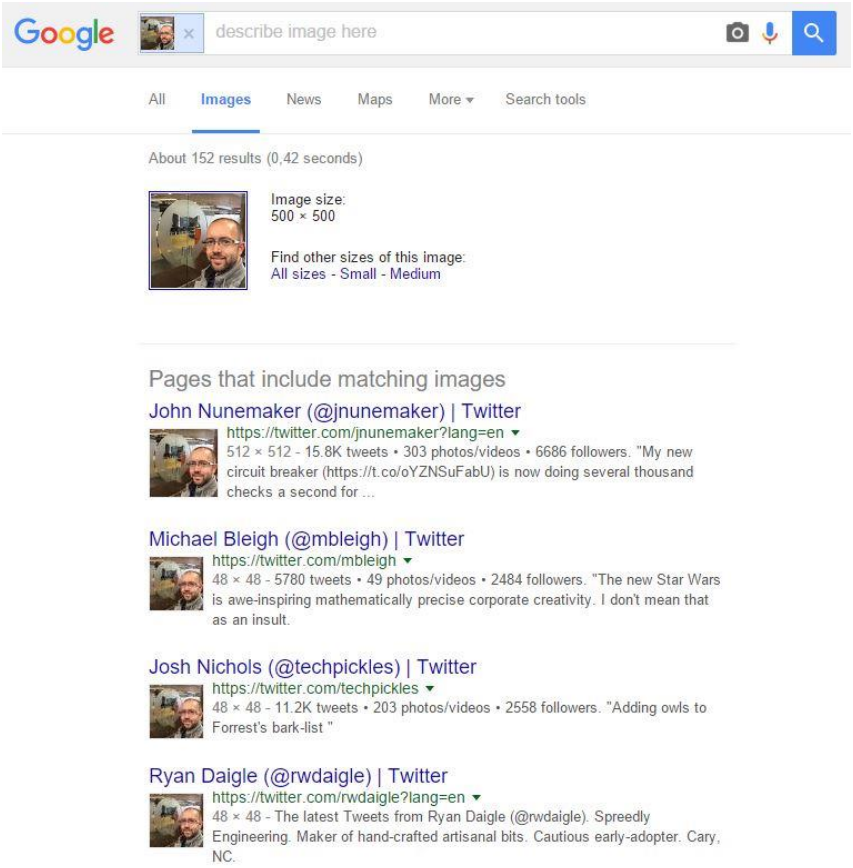
us. In the software we could see all the contact information of the person we were calling apart from their Social Security Number (SSN). Our goal was to sell them these new electricity contracts and we had a sales speech already written for us. The speech was formatted in a way that made the possible customer think that we were calling on behalf of their electricity company and we wanted just to update their contract when in reality we were selling them a completely new contract from another company. In the beginning of the call we would first check the name of the person answering the call, “This is John Doe, right?” After checking the name we would “verify” if the address we had was correct for the person in question. I will discuss this even more further on but the whole point of the beginning of the call is to make sure the callee answers yes on two occasions. This was a way to create a feeling for the potential customer that we know exactly who he or she was and we were in control and they could trust us. Today people have grown accustomed to telemarketers and they are already wary of anyone calling from an unknown number and most people rejected all offers once they realized I was actually selling something. The people most receptive to my offer were mostly the elderly and occasionally the young adults. The deceitful nature of the company I was working in was completely unknown to us regular employees. No one told us that we were in a way scamming the customers. All we knew the boss had given us a handout to read and a program to handle all the calling for us. We did not suspect anything until we started receiving somewhat sour feedback from the customers who had been previously contacted by some other telemarketing company selling the same electricity contracts. Needless to say I did not stay for long there after I learned about the true nature of my work.

But how did the company get the addresses and contact information of all the people on the list besides their phone numbers? The answer is in your everyday supermarket. Remember those competitions that sometimes pop up in their small stands next to some lonely aisle with the headline “Participate for a chance to win a brand new Ferrari”? To participate just fill the form with your contact information. This is why telemarketers sometimes call even those people who have set their phone numbers unlisted or like in some countries they have listed their numbers in a service that is supposed to prevent telemarketing calls. If anything people

should always remember there is no such thing as a free meal. Google's Gmail is only free because it keeps you using Google and therefore letting Google know what you are doing online. The same goes with Facebook as well. The currency you are paying with is information about yourself, what kind of ice-cream you like, what kind of social circles you have and even the more personal matters such as what kind of sexual preferences you have. Information is always power and in social engineering it is the most important ingredient before anything else.

3.1.1 Hacker's perspective

So what kind of techniques do the social engineers with a hacker background use? There are several ways to find information online and I will list some of the ones I have used the most here. First and foremost are not surprisingly Google and all the other search engines. If you know your target's full name you have already got a pretty good start. Oftentimes you can find the target's Facebook page or other online handles among the first search results. In case you have a picture you are doxing there is also a nice little-known function called reverse image search. With it you can use Google's search engine to look for pages that host the picture in question. They even list the Instagram profiles that have been set public. If you are using Google Chrome you can just right-click and you will find the option to search for the image online in the menu that opens up. Otherwise you can just drag the image to Google's search bar. Below is an example of John Nunemaker's profile photo from his Twitter account that has been run through Google Reverse Image search.



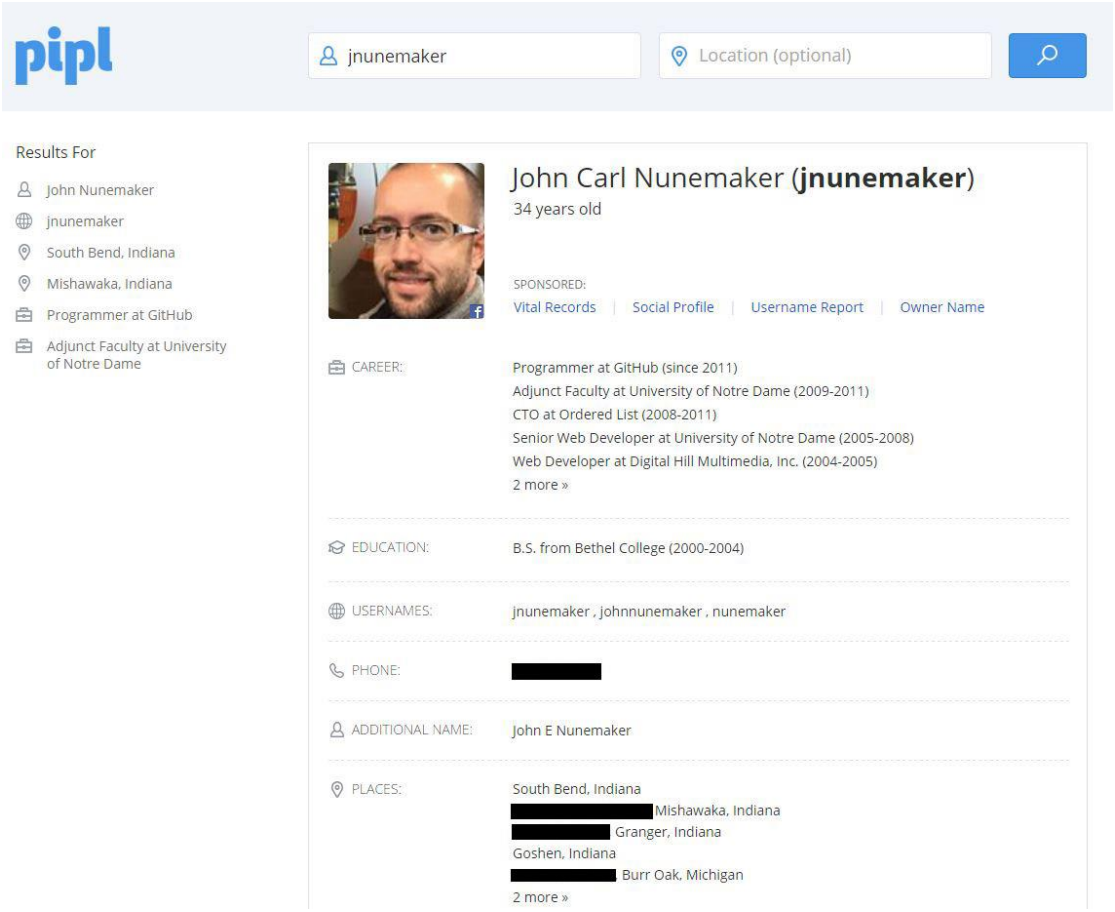
Picture 1. John Nunemaker's picture in Google Reverse image search.

Bing offers the same kind of functionality as well these days and several other options are available too. One of the oldest independent search engines focused mainly on reverse image searching is called Tineye. Additionally another good option is Image Raider that scrapes Google, Bing and Yandex and lists the results in one place.

Besides the regular search engines a good social engineer does not limit themselves at those. Some Facebook profiles are set to be not indexed in any search engine but you might find them in Facebook's own search function (Facebook 2016). This is true for other social media accounts the targets might be using like Twitter and Instagram. Usually the information accumulates little by little, you might find the person's real name in their Facebook and with some googling comes up their Twitter account that lists one of their other online handles. Most

of the time this is the way the process works but every once in a while you might get even luckier.

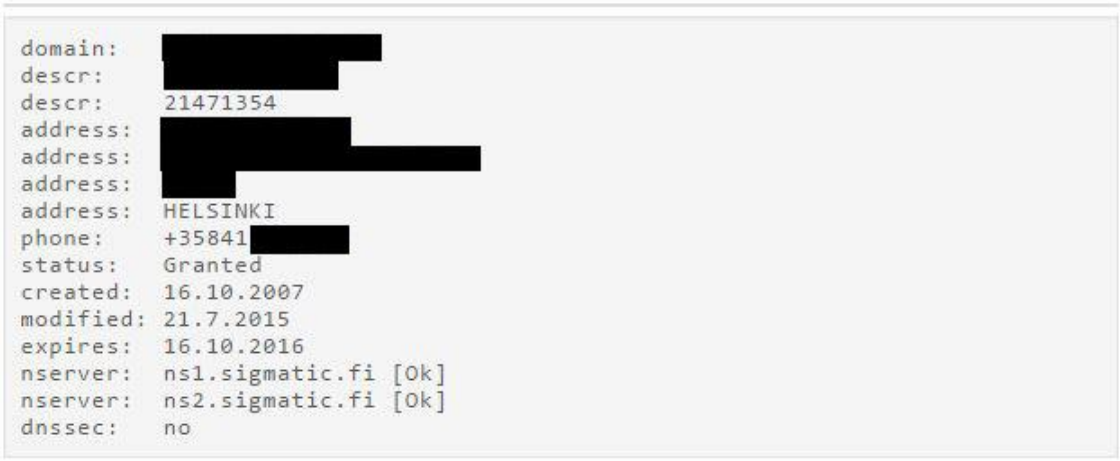
There are few search engines that are made especially for looking up people online and one the best ones right now is pipl. Say I am still looking up John Nunemaker, who is a known Core Application Engineer at Github and I have found his Github page linked on his Twitter account. On his page his username is listed as jnunemaker. A quick pipl search reveals all the following about him and more. Not visible in the picture are all of the accounts that pipl could find in the Internet that seem to belong to him. It should be taken into account that Nunemaker is a very well-known programmer so the amount of results correlate appropriately. Pipl usually works well with people who have a large digital footprint but I have to admit I did not anticipate his home address to be among the results. Of course the results are only as accurate as the information posted online. The address listed in the results might be an old one or just completely wrong so oftentimes it is smart to check the results from several sources if possible. Pipl indexes several different social media websites such as LinkedIn, Twitter, Flickr, Facebook, Pinterest and many more and is an excellent way to find more accounts and usernames for the target.



Picture 2. John Nunemaker's handle in pipl search.

Lastly one good resource of information is a whois search. If the target has a website or domain registered under their name, there is a chance you will find more about them in the domain's whois records kept by ICANN. The following considerably censored screenshot is the whois records of a well-known Finnish blogger's website. In the records there are clearly visible the name, home address and even the phone number. The bigger websites and domains usually have something else in their records in place of the registrant's name like simply admin and the address is the company's own address. Several smaller website owners though use their own information when registering the domain. Oftentimes even if you are submitting fake information when registering a domain your billing information might be used in place of the phony contact details. Most registrars however do offer a service in which their information is used instead of regis-

trant's, for a price of course (Ars Technica 2015.) Changing the information afterwards might be too late since the information is already indexed and can be found in several caching services of the Internet like the Internet Archive's Wayback Machine.



Picture 3. Whois records of a well-known Finnish blogger.

There are many other ways to find information about people and organizations online but were I to list them all here, this paper would be considerably longer. These are the most common ones that everyone can easily check themselves and see how much information they are leaking online.

3.2 Developing a Relationship

After the attacker has learned everything they can about the target, their next step is all about creating a relationship with the target. The relationship does not even have to be a positive one if it achieves the original goal of the attacker. The more the attacker knows about the target the easier it is to manipulate the target and gain their trust. Generally speaking there are 6-8 different commonly used principles that can be used to influence other people (Social Engineer Inc. 2016b.) In the following chapters I will go through the six rules of influence according to Robert Cialdini (2001, 10) and give examples on how they can be used in social engineering.

3.3 Social Proof

Social Proof is perhaps the simplest and most widely used ones of the six principles of influence. At its simplest it just means information, opinions and behavior received from other people (Richardson 2014, 214). One amusing example is an old and famous video experiment from Candid Camera Inc. in which at first one actor and later on several are placed inside an elevator. The victim of this prank demonstrates our innate need to belong in a group as he walks in the elevator and mimics the behavior of the other people in the elevator by facing the same direction as they are or taking off his hat off just like everyone else present in the same space (Prudential – Bring Your Challenges 2013.) Humans still possess a herd mentality to some extent and when everyone else in the elevator is facing the opposite way as you are, you will naturally start feeling awkward or uncomfortable. This is also known as peer pressure.

Social proof is a well-known phenomenon in the marketing world and it has been used for a long time. There are different ways to utilize it of course but in an article in Techcrunch there are listed five different ways social proof is used: expert social proof, celebrity social proof, user social proof, wisdom of the crowds social proof and wisdom of the your friends social proof (Lee 2011.) The last two use exactly the aforementioned group mentality: if your friends or the majority in your hometown are buying their cars from a certain place, you are more than likely to buy yours from the same store as well. The user social proof is a bit more obscure and it means the marketing leans on positive user experiences. This is also partly the principle network marketing is built on. When you are introduced to a new product by an ordinary person who does not have background in marketing you are more likely to trust their own experiences of the product than as opposed to seeing an ad in TV in which a well-groomed and good-looking person introduces you to the same product. Another good contemporary examples of this are the Youtube videos in which a regular content producer promotes a certain game or product for example. The first two – expert social proof and celebrity proof – are ones that use the human trait of being responsive to assertions of authority to their advantage.

3.4 Authority

Using authority in social engineering feels almost like cheating because of how easy it is. Regent's Professor Emeritus of Psychology and Marketing Robert Cialdini writes in his book Influence (2001, 185) about authority the following: "After all, as Milgram suggests, conforming to the dictates of authority figures has always had genuine practical advantages for us. Early on, these people (parents, teachers) knew more than we did, and we found that taking their advice proved beneficial—partly because of their greater wisdom and partly because they controlled our rewards and punishments." He also goes on to address the structure of our society as a whole that teaches us that following the proper authorities such as the police, political decision-makers and government is the right thing to do. Religions play their part as well in reinforcing the idea of following authorities. The idea of how authorities should always be followed is in fact so deeply rooted that we associate everything anti-authoritarian with negative feelings and ideas so one could argue authority is one highly refined aspect of social proof.

3.5 Reciprocity

Another important principle when influencing other people is reciprocity, which in this case means that people have a built-in need to return a favor. Oftentimes the favor is returned unconsciously. In his book, Social Engineering: The Art of Human Hacking, Christopher Hadnagy mentions that pharmaceutical companies spend over $10,000 on a single doctor with gifts that range from dinners and books to clothing and even computers. This way the companies wish to influence the doctors' decision making when subscribing drugs to their patients (Hadnagy 2010, 188.) I can personally confirm this as two of my friends are studying right now in Turku University Faculty of Medicine and they both received their first gifts, brand new stethoscopes that apparently cost over €100 a piece, already during their first week. Another friend of mine has a father who works as an MD and he showed me once a computer mouse he had received from Pfizer. It had blue liquid inside a transparent compartment as well as two Viagra pills floating

around. The monetary value of this gift is likely to be close to nothing, but its purpose of sitting on the doctor's desk every day reminding him of this pharmaceutical company is a brilliant way of subtly influencing his thoughts.

The gift the social engineer gives to his victim does not even have to be anything physical. Even a compliment or a pat on the back might be enough. In fact those are social engineering in their own right when received for a job well done. They encourage the employee to keep up the good work and produce more results of similar or even greater level and this way pay back the favor. The same goes for the attacker. It is oftentimes more profitable to give a few compliments to the secretary replying to your phone call or for example to bring two cups of coffee when entering a lobby. One for you and one for the co-worker who "had called sick and could not meet you this morning". Perhaps the kind receptionist would like the extra $4.95 Mocha Frappuccino you have? Combine this with a friendly smile and few sympathizing comments about the drafty lobby and you already have a great start. However, here is where a good doxing effort really pays off: the receptionist might not even like coffee and only drinks tea. This is why finding information about the targets beforehand is invaluable.

3.6 Liking

Liking is the fourth principle we are discussing. It goes without saying you are more likely to respond better to a request from a person that you already like. Liking is also the second principle of network marketing. If you know the person who is trying to sell you a new household device you are far more likely to actually buy it than in a situation where the seller is an unknown person. Liking someone can rarely be faked and this is why it is perhaps the hardest principle to master. A lot of this part of social engineering comes down to the attacker being actually interested in their targets besides just presenting themselves as easily likable (Hadnagy 2011, 207.) There are also ways to make people like you more such as positive reinforcement. This means for example starting a conversation by

complimenting the perfume the receptionist is wearing and asking its name because you want to buy it for your girlfriend (Hadnagy 2011, 209.) People love talking about themselves as I noticed in my brief visit to the telemarketing world. When dealing with people you need to have the patience for it. It is always beneficial to be interested in the target and ask questions about the things they care about.

Compliments and interest are good tools both, but an experienced social engineer does not overuse neither. The overuse of positive reinforcement is referred to as satiation. Essentially it means that after a time all incentives lose their effect if used too many times or in too big portions. Compliments do not work if you use them repeatedly or give too many inside a too short timeframe (University of Minnesota 2016.) Instead of making the target like you more, they make the situation awkward and the attacker loses the potential advantage they might have had.

Lastly there are of course the good looks. In a study published in the Journal of Personality and Social Psychology it was discovered that people are more inclined to believe a person that they perceive as attractive possesses even more good social traits not visible from the outside (Dion etc. 1972, 288). Again it should be noted that what people perceive as desirable varies greatly. Besides their personal taste other factors affect this as well like the environment they are currently in. It is more than likely that if you are not outright denied a loan you are applying for in a bank, you are at least likely to be considerably delayed if you are not dressed properly when first meeting with your loan officer. Preparation for the interaction with the target never goes to waste. What passes as a smart outfit in a bank might make you seem out of place in a metal concert. When interacting with a person it is also useful to know something about their personal taste, do they like people dressed in suits or leather jackets and so on. Regardless of how you are preparing yourself the effort will always to pay off to some extent if it is clear you have spent time honing your attire.

3.7 Commitment and Consistency

The fifth principle of influencing other people is commitment and consistency. When working as a telemarketer I would always start the phone call by making sure the callee answered two times “yes” to my questions. The way the human mind works is that it tries to be consistent with the previously taken actions. When you have already answered in the affirmative twice it is easy to keep on going. The next question in the call would be something like “Wow, you sure are paying a lot for electricity right now! It would be great if the prices were lower for you, right?” What happens is the callee starts making small commitments of agreeing with you about things that seem insignificant. Little by little the level of commitment is raised until the actual product is sold to the customer. In the end some of the most easily persuaded customers practically sold the contract to themselves.

People want to be consistent and they appreciate consistency in others as well. Consistency and commitment go well in hand-to-hand because people do not want to take back the commitments they have already made (Hadnagy 2014, 202.) A good example of this are Internet penny auctions and to an extent auctions in general. Oftentimes the product on sale starts with a meager price that is only a fraction of its original worth and people viewing it will think that this here is a real bargain and bid on it. After a while someone else, who has had the same idea outbids them and the cycle goes on because people still perceive the product as a low hanging fruit and continue bidding on it. The fact that someone else is bidding on it is barely a nuisance. In reality the price of the product is actually way higher because every time someone bids on it they pay a small fee for the right to bid in addition to their actual bid on the product.

The way a social engineer works with consistency and commitment is subtle. It is no use asking for the real goal right away in the beginning of the conversation, no one is going to give you their account password after you have barely introduced yourself. Instead when manipulating people into keeping their commitments a good social engineer starts small and gets the snowball rolling (Hadnagy

2014, 204.) When addressing the person responsible for managing accounts inside a company a good start could be for example “Hey, are you the password guy?” This gives already the impression that you might not be that well knowledgeable about computers and puts the target in their customer service mode when they reply. Or you could assert your authority by starting with “Hey, you’re John, right? You’re responsible for the HR department’s account management, right?” Depending on the target both or neither might work, it all depends on the person. One might not respond well to explaining anything IT related to anyone not familiar with the field whereas someone else might have trouble responding well to any kind of authority. Once again the more you know of the target the easier any kind of influencing or manipulating is.

3.8 Scarcity

The last principle of influencing people is scarcity. Scarcity in the context of social engineering means that people desire anything that is rare or scarce like a lower prices for clothes during the Christmas holidays. Humans have the peculiar way of valuing everything that is rare and divergent. A faulty stamp or coin is valued way higher than a good one. The same goes with opportunities, the rarer they are the more attractive they seem (Cialdini 2001, 204-205.) Scarcity is a tool to create urgency and desire in people’s minds and it works miracles along with the other principles of influencing people.

From the social engineer’s point of view scarcity is an excellent tool to create artificial time constraints for the target. If for example you are looking to get inside the server room it might help your cause even further to stress that you have come to solve a server problem that is causing downtime for all of the company’s customers. The person with the key to the room gets straight away a nasty time constraint, he could try verifying the story with someone else and risk the company losing money over downtime or just let you in straight away. If the person is not trained for these occasions they might be more than inclined to choose the latter.

4 INDIRECT ATTACKS

Social engineering is not limited to just physical interaction between the attacker and the victim. There are several ways it is utilized without the attacker ever being in the same room with the victim. In this chapter I will go through most of the common indirect approaches used in SE attacks. The way these attacks work is that they once again abuse some of the basic human traits such as curiosity.

4.1 Phishing and Spear Phishing

Phishing in general means an attempt to trick the target into sharing sensitive information with the attacker. Typically phishing attacks are carried out with email but they are not limited to using it alone. Most of the phishing attacks can classified as mass attacks, which means their target group is large and the content of the phishing attempt does not contain any specific details tailored for each recipient (Ramzan 2010.) Spear phishing means that the content of the message is at least to some extent tailored for the recipient (Hoffman 2013). As a part of this thesis I carried out a spear phishing experiment at Phirelight Inc. with the goal of finding out how well the employees were trained against such attacks. The results and how I executed the attack are outlined in chapters 6 and 7.

Phishing mass attacks are crafted in a way that they reach as much audience as possible while seeming as little out of place as possible. The end goal most of the time is acquiring the targets' accounts or for example their credit card numbers. The phishing email seems to originate from a source that the most of the recipients trust like eBay administrator. The nets cast by the phisher are often so wide that the attempt is easy to spot: if the target has no account in eBay yet receives an email from them they are less likely to even open it (Hoffman 2013.) Another good example of this are the phishing emails that have very bad grammar in them or have clearly been run through Google Translate.

Spear phishing is basically phishing on steroids. If the attacker knows their target and has collected a good amount of information about them, it is significantly

more probable that they will actually get the target to open the email. According to a study carried out by Cisco (2011, 5) the average chance of a person opening a phishing email that is part of a mass attack is a meager 3% whereas a targeted spear phishing email is opened in around 70% of the cases. It is common to combine spear phishing attacks with zero-day exploits that lie in wait behind the innocuous looking link in the email from the supposed CEO of the company. Attachments can also be used. In 2015 Symantec identified a new Trojan called Laziok, which was used for reconnaissance inside the corporate intranet so the attackers would gain a better understanding of the infected network. And how did the Trojan get into the corporate network? The exploit itself used a well-known vulnerability in Microsoft ActiveX and the Trojan was packed inside a regular looking Excel file that arrived as an attachment of a spam email. The exploit in question was not a zero-day but since the successfully exploited systems had not been properly patched it worked nonetheless (Symantec 2015.)

4.2 Baiting

Whereas phishing is focused on finding out sensitive information about the target, baiting could be called its physical counterpart. The goal is to gain information and assets from the target by infiltrating the target with for example an infected USB flash drive or a CD (Kovacs 2015). Baiting does not have to target just one person as pretty much anyone visiting the corporate parking lot could spot the lonely flash drive with company logo on it laying on the ground. Not many people would just ignore the flash drive and would at least return it to the lobby of the company. The USB stick and CD are just examples, however, and in reality the only limit is the imagination of the attacker. The attacker could for example deliver a new keyboard with embedded malicious commands to the newest intern of the company.

In a Trustwave SpiderLabs blogpost Wendel Guglielmetti Henrique (2013) describes the methods their company has used when auditing their customers' ca-

pability to respond to baiting attacks. They would start by sending packages containing either a CD-ROM or a USB pen-drive to all the employees. Later on they would email the employees impersonating employees from another department of the company and ask the target employees to install the new Anti-virus software in the packages. From 15 packages sent 1 resulted in a success. In a couple of other exercises they dropped USB pen-drives around the company, which resulted in a better success as one of them was opened by a person working as one of the physical security staff. Just by this person inserting the drive into a computer they were able to obtain the company Wi-Fi pre-shared key (Henrique 2013.) Baiting and phishing are both techniques that exploit people's curiosity in new situations.

4.3 Watering Hole

Watering hole is the next in the line of indirect ways of attacking a target. In a watering hole attack the attacker initiates the attack against the target by first compromising a legit website for example and patiently waits until the target or someone affiliated with the target visits the site (Abendan 2013). This is precisely the reason why it is always a risky decision to use third-party hosted code on your own website. Even though your own website might be secure the chain is again only as strong as its weakest link. Another good example of watering hole attacks is malvertising.

Malvertising or malicious advertising means an online ad that is infected with malware or a malicious link. Malvertising is a huge business and its benefits for the attacker are numerous. In the summer of 2015 Malwarebytes uncovered a large scale attack that was using Yahoo!'s own ad network to its advantage. Based on the numbers from SimilarWeb in December 2015 Yahoo!'s website got over 4.7 billion visits from the ads. At the time of the attack Yahoo! had over 6.9 billion hits a month so the volume of people reached this way was huge (Segura 2015; SimilarWeb 2016.)

4.4 Identity Thefts and Impersonation

Identity theft is not an attack technique per-se but it is what some social engineering attacks eventually lead to. Previously we have discussed using the target's personal information in gaining their trust and/or abusing it. However, if enough information is amassed nothing prevents the attacker from actually assuming the whole identity of the target. The more information the attacker has of the target the easier it just gets. The amount of information required for getting an instant loan for example is alarmingly small. Just the home address and SSN might be enough. According to Chicago Tribune (Coen, 2009) a contract worker hired by AT&T managed to steal personal data from 2,100 company employees and cash in over $70,000 in loans. In another article published by Reuters a thief managed to purchase $1,357 worth of electronics from Apple's web-store. This was achieved with stolen information as well but what makes the case stand out is the fact that the victim knew her identity had been stolen two years earlier (Lipka 2013.) You can move and change your address but once someone gets a hold of your SSN it is a whole another story. The amount of damage that can be done with your personal information is often overlooked by authorities and in Finland the identity theft itself was not even a crime until September 2015 (YLE 2015).

4.5 Tailgating

Tailgating simply means the act where an unauthorized person follows someone authorized inside somewhere they should not be able to get. Tailgating is not solely limited to the physical reality but it is more commonplace in person. The attacker might be having a cigarette outside the backdoor, dressed in office attire without any outer jacket and in a big company it is just natural that you do not know everyone working there. Again the worst enemy of security is the human nature. Some employees might not let the stranger pass but others might and there is nothing to stop the attacker from trying again with different people (Page 2004, 5-6.) Just like all the other attack techniques this one can be combined nicely with several of the other techniques. The attacker might be dressed for

example as a police officer and assert their authority over the employee outside the locked door. Best practice against tailgating is making sure that the employees are trained for it. All visitors should be escorted and secured areas should be locked at all times. One option is to use revolving doors and man-traps as well so that the employees cannot let even by accident anyone else through at the same time. Lastly you should have multiple checkpoints. The attacker might get lucky once but his chances drop already at the next checkpoint. Often it is said that people should carry their badges on them at all times while in reality it is a really bad idea. The badges should be worn only inside the office. Today it is not an impossible task at all to take a photo of the ID hanging of your neck when you are enjoying your morning coffee at the café and the image can be used with a very little effort to manufacture a counterfeit ID for the attacker (Page 2004, 6; Mr. Ford's Class 2014.)

5 CASE STUDIES

So far we have only discussed the attack methods themselves and now it is time to see where they can lead. I have picked the following cases of social engineering because of how well they are documented and how they illustrate the various dangers of for example leaving too much of your personal information online.

5.1 Ars Technica Reporter and GoDaddy

Naoki Hiroshima is a reporter working at Ars Technica. He is also the owner of the Twitter handle @N, which among all of the other short or easily remembered Twitter handles are very attractive targets for all hackers looking to gain some fame. Twitter handle hijacking has been going on for years and is a fairly lucrative business. The stolen handles are often sold and they fetch high prices. Hiroshima had earlier received offers for the handle and even ones as high as $50,000. Naoki's handle was accessed by indirect means which in turn exposed the lax security of GoDaddy's support phone (Hiroshima 2014; Smith 2012.) Another reason why this case is important is that it outlines very well how personal information alone can be used in SE attacks with little or no help from actual hacking.

5.1.1 The Attack

The first sign of the attack Hiroshima received was when he received a text message from PayPal for a one-time validation code. Shortly after ignoring the text message, as he had grown accustomed to people attacking his accounts, he received an email from GoDaddy that explained his account settings had been modified successfully. Hiroshima could not log back in GoDaddy and had to call them to resolve the issue. Unfortunately the attacker had already changed all the information associated with the account so he had no way of proving he was the original owner of the account. Hiroshima filed a case report for his account on GoDaddy's website but was told the response could take as much as 48 hours.

Soon after he received an anonymous tip from someone in Facebook that he should change his Twitter email address. Hiroshima's current email address, which was also the one linked to his Twitter account at the time, was under his own domain that now had been hijacked. The tip turned out to be a good one since shortly after the attacker opened a ticket at Twitter's Zendesk asking for a manual reset of the Twitter password (Hiroshima 2014.)

Twitter wanted to have more information though and the attacker discontinued this course of action. Instead they started to bargain with Hiroshima, they would give the domain back in exchange for the Twitter handle. GoDaddy's response for his claim earlier turned out to be of little help since they refused any help as Hiroshima was not anymore the registrant of the domain name. Hiroshima had no other choice but to give in to the attacker's extortion and after handing them over his Twitter handle he regained the control of his domain and email (Hiroshima 2014.)

5.1.2 How did it happen?

In this case the attacker was kind enough to gloat over his victory and actually offered to explain to Hiroshima how exactly they had managed to obtain his domain. At first the attacker had called PayPal and obtained the last four numbers of Hiroshima's credit card. According to an article published in Wired (Honan 2014) PayPal did not release this information though. This is hard to prove though and I would not take just the company's word for it especially since the attacker is not available for interview. Regardless those last numbers could have been obtained in other ways as well. One of the more physical ways of finding information about SE targets is called dumpster diving, which is precisely what it sounds like. Granted it can mean finding information about the target without actually diving into their garbage but that is one solid way of finding really sensitive personal information (Techopedia 2016b.) Oftentimes people overlook how smart it actually is to throw into the trash your bills or other documents that give away details about you. Even throwing away old CDs, DVDs or USB sticks is risky since

information can be recovered from them to an extent even if the files themselves have been deleted.

After obtaining the last four numbers of Hiroshima's credit card the attacker called GoDaddy and explained they had lost the card but could remember the last four numbers. The GoDaddy support staff actually let the attacker guess the first two digits of the credit card and even went as far as letting them guess from a range of numbers. This is even more dubious practice since several credit cards have easily guessed first numbers, for example Visa cards always start with a 4 (How Stuff Works? 2016). The attacker also explained that usually he has to keep guessing longer but this time he got it at first try (Hiroshima 2014.) It goes without saying that this should not have happened at all in the first place and the fault is entirely on PayPal and GoDaddy. The case shows very well that even a small bit of information in the wrong hand can lead to unexpected results. The attacker's path from PayPal to GoDaddy is also typical in all hacking and SE attacks. It is common to go after other parties first to find more information about the target or to gain sort of a foothold when attacking the real target.

5.1.3 Things Learned

Previously in this paper I briefly mentioned Steam's information leak in December. Among the information leaked were the last two numbers of the credit cards of some of the users. The case of Naoki Hiroshima and GoDaddy clearly shows that information alone can be used as a weapon in SE attacks. In Naoki's case he had previously used his Google Apps email address under his own domain which in turn gave the attacker the opportunity to take over his Facebook as well. The damage done was fairly limited but since Google Apps email can be used in various websites to log in, it might be an unnecessary risk to take. In case the domain gets hacked like in Naoki's case the email can be used to access way too many other places. Gmail in this regard would have been the safer option. Hiroshima made a mistake in using the same email in several other important places to him but he could not have influenced the way GoDaddy and PayPal

handled the situation. PayPal does offer the option to not disclose any information over the phone but I had not even heard of this before reading about it in Naoki's own article. GoDaddy's actions went just to show how badly they were prepared against social engineering and giving away freely any sensitive information from their customers is just inexcusable (Hiroshima 2014.) If anything should be learned from this, it is the same lesson my father taught me about driving a car: "Always assume the other people in their cars are complete idiots."

5.2 Aaron Barr vs Anonymous

Social engineering techniques are not always the methods that start the attack. Sometimes they are used in conjunction with regular hacking techniques like in the case of Aaron Bar. Aaron Barr was the CEO of a technology security company called HBGary Federal. In 2011 Barr had set his sights on the hacking collective Anonymous and wanted to expose their key figures and their real identities. The case is interesting because Barr himself used social engineering techniques to find out information about the Anonymous but in the end he became the victim of the real engineering. Barr infiltrated the Internet Relay Chat (IRC) channels the Anonymous were using and allegedly managed to identify three people who he claimed were the so called ring leaders. After releasing their identities, however, the company became a target of a DDoS attack and their internal systems were breached and their emails leaked. This analysis is based largely on the article published in Ars Technica about the incident and the information they had was extracted from the emails released in the aftermath of the attack (Anderson, 2011.)

5.2.1 The Attack

First sign of the malign intent was the DDoS on February the 5th. Barr responded by promising to take the gloves off. He went on to promise to release more details on the members of the Anonymou that were already arrested. However, on the very next day HBGary Federal's website was taken down and defaced with a

message from the Anonymous. They managed to access HBGary Federal's email server, which Barr administrated and released over 40,000 emails for everyone to see on the Pirate Bay. Some members of the Anonymous reportedly bragged how they had deleted over 1TB of HBGary backup data as well as wiped Barr's iPad remotely (Anderson, 2011.)

5.2.2 How did it happen?

The initial DDoS took only little part in actually bringing down the HBGary Federal's website. It acted more as a declaration of war than means to an end. The real attack began on right on the website itself (Bright 2011.)

HBGary Federal's website was using for reasons unknown a Content Management System (CMS) custom built just for it. This CMS was poorly designed and had numerous flaws in it. The biggest of them was an incorrectly filtered PHP parameter that made a regular SQL injection attack possible. The attackers gained access to the database running on the site and accessed the user part of it. Passwords are often stored as hashes that are computed from the actual password through various mathematical functions and the idea is that they are not reversible. The process does, however, always lead to the same hash when the same string is hashed. There are various databases freely available in the Internet that have a look up function for already calculated hashes, which makes finding a match almost an instant process for an unsalted hash. This is why before hashing the passwords are usually salted first. This means that another string is added to them so if anyone else would hash just the password, they would not get the same result. Another method of increasing the security is iterative hashing which means basically just hashing the hash all over again several times, sometimes even thousands of times. The HBGary Federal website database stored all of the accounts in MD5 hashes but as an oversight they were not in any way salted or iteratively hashed and thus were easy targets. The attackers managed to crack both the CEO's and COO's password that were both only six characters long and had only two numbers in them. (Bright 2011; Defuse Security 2014.)

After cracking the passwords the attackers quickly started to test what they could access with them. HBGary Federal's server had also a Secure Shell (SSH) access and as luck would have it the COO had the same password on his SSH account as he did on his email account. The first stop sign for the attackers arose when they found out the COO was only a regular user and lacked any root-privileges. Luck was however still on their side as the server they were accessing was running a vulnerable version of GNU C Library that allowed them to escalate their privileges to the root level. With the root access the attackers found and purged the HBGary Federal backup data from the server. Barr's password, however, gave the attackers even more. HBGary Federal were using Google Apps email so the password gave access to the whole company email service, which Barr administrated. It also allowed access to Greg Hoglund's mail. Greg was the original founder and CEO of the HBGary parent company. This is where the social engineering part of the attack started (Bright 2011.)

Greg was running another website called rootkit.com and in his email the attackers found out that the root password for the server running the website was either "88j4bb3rw0cky88" or "88Scr3am3r88". As a security practice a root access was not allowed through SSH so they needed a regular account on the system. They contacted the admin of the server from Greg's own email address and made up a story of being abroad and unable to login to Greg's account on the server. To support their story they casually mentioned the root password in the discussion, which was a clever way of using social proof to convince the admin. The email came from the customer's email address and it referenced the root password so it must be the customer speaking, right? I have included most of the discussion in a separate appendix and it illustrates better itself how easily the attacker actually managed to gain root access to the server than I can describe myself. The conversation was linked in the Ars Technica article but other than that I cannot verify if its origins so it should be taken with some grain of salt (Bright 2011; Pastebin 2011.)

5.2.3 Things Learned

In the defense of the rootkit.com administrator it has to be said that he fell a victim to a really good SE attack. In his position not many things could have been done differently with the practices they already had in place. Instead the practices should have been planned from the start differently in a way that no one could access their sensitive information just by emailing someone. The same kind of a practice would not stand at all in any bigger organization. As reported by Ars Technica (Brodkin 2012) Amazon only recently updated its security policy that allowed anyone calling them to find out the last four numbers of the credit card linked to the account. Security practices were in place, like only being able to view the last four numbers of the credit card but like in many other cases it was underestimated how much damage could be caused with the information provided. The problem when auditing any security system is that the auditor is often constrained by a time limit whereas the real attacker has all the time in the world. There have also been cases where the attacker has been actually an ex-employee from the IT department who has left himself a backdoor or credentials into the system. It is not likely that he is suspected at all especially if it has been years since he has worked in the company.

The original culprit of the whole ordeal was without doubt the faulty CMS. There is a lot of debate in the Internet over whether or not you should use your custom-built CMS or be satisfied with the already existing ones. Both have their pros and cons but one of the worst cons of having a custom CMS is that its security is only as competent as its developers. It is true the already existing CMSs are not void of vulnerabilities but their strength is that there is a solid developer base updating their code all the time. On the other hand open-source CMSs fall prey to vulnerabilities that affect all sites running them whereas custom CMSs have their unique vulnerabilities but their maintenance is also more expensive. Oftentimes the advocates of custom CMSs are themselves web development companies and the ones speaking on behalf of the open-source or proprietary CMSs are people that are already using them (Davis 2015; Edwards 2012; Finn 2014; JBSystems 2013; NewSprout 2016.)

Regardless of the choice the system should have been audited. In the end social engineering played only a small part in a chain of unfortunate events that could have been avoided if the CMS had been actually reviewed by professional penetration testers. Just like was the case with the hacking of Naoki Hiroshima's GoDaddy domain, the less trust you put in different components of your system the more secure you will be in the end.

5.3 Blackout in Ukraine

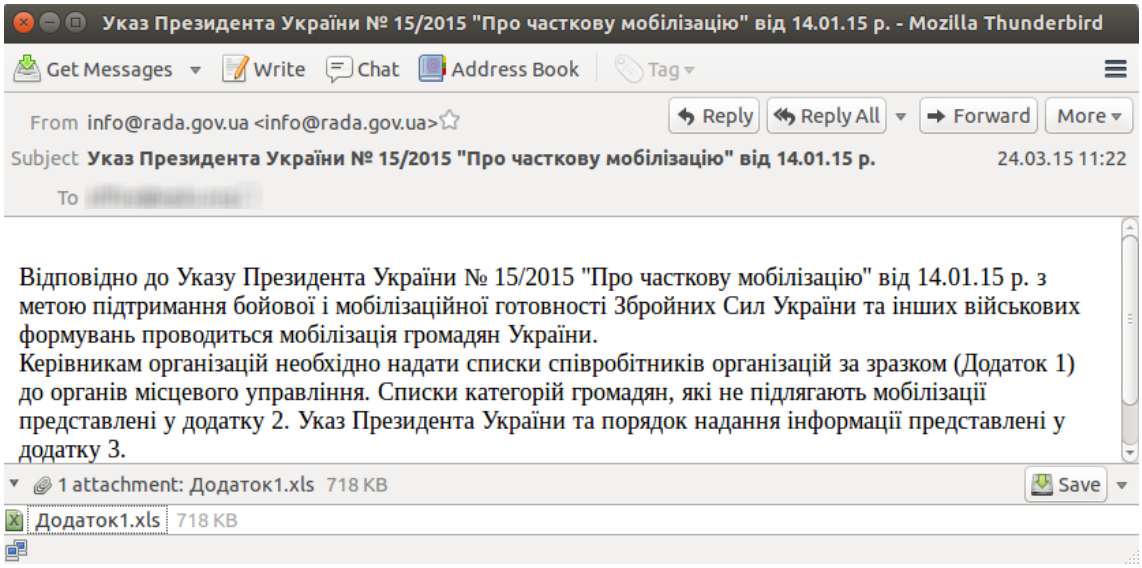
Social engineering techniques should never be underestimated. This became especially clear on December 23rd 2015 in a western Ukraine city called Ivano-Frankivsk when the lights started going out. A month earlier the power went out on the Crimean peninsula when someone armed with explosives destroyed the powerlines to Crimea. This time, however, no explosives were used. Instead several power stations were hacked and disabled leaving hundreds of thousands without electricity. At the time of writing this thesis the situation is still ongoing and on January 20th researchers from the antivirus company ESET uncovered a new wave of attacks that targeted Ukrainian electricity distribution companies (Goodin 2016; Lipovsky 2016a.)

5.3.1 The Attack

The attack comprised of at least three different parts. Ukrainian electricity company Kyivoenergo reported that there had been an intrusion to their systems that disconnected in total 30 of their substations which lead to a power outage to over 80,000 customers. The power outage lasted around three hours before the utility staff restored the system into a so called "manual mode". In total the outage lasted around six hours before all parts of the system could be brought back online.

5.3.2 How did it happen?

The whole attack started with spear phishing. The attackers sent several emails that appeared to be coming from the Ukrainian parliament, Rada. The content varied but the intent was to get the recipients to open the document included in the email. In the documents there were just a couple of pictures that looked like error messages that were intended to trick the user to enable document macros. The macro was the attacker's real way into the system as it downloaded Black-Energy Lite Trojan that eventually took control of the system. Below is a sample of one of the emails used in the attacks. In the email the sender pretends that the President of Ukraine has decreed a partial mobilization and all organizations receiving the email should submit a list of employees with the included attachment for mobilization purposes (Lipovsky 2016b; CyS Centrum 2016.)



Picture 4. A screenshot of one of the Ukrainian phishing emails (CyS Centrum 2016).

The content of the email and the sender address were a very clever way of gaining the trust of the recipients when you consider the current political climate in Ukraine and Crimea.

BlackEnergy is a very destructive modular Trojan, meaning it can download more components once it is already in the system depending on what it is used for. In

the power company attack it downloaded Win32/KillDisk malware that is used for making the system unbootable. The KillDisk was also responsible for terminating the process used in the Industrial Control Systems (ICS) and overwriting the executable file running it with random data thus making recovery even harder. It is still unclear whether or not BlackEnergy itself caused the actual power outage by opening the breakers in the substations or if this was caused directly by the attackers through an SSH backdoor that was discovered in the beginning of January (Lipovsky 2016b; Cherepanov 2016; Lee 2016.) The same Trojan was previously detected in various systems in US facilities in 2014 but at the time it did not succeed in damaging any systems (BBC 2016). On January 20th a new wave of attacks were observed with the same kind of attachments in the emails, but this time BlackEnergy was not the final payload but instead a modified version of the open-source gcat backdoor, which can be used for downloading more executables and running shell commands (Lipovsky 2016a).

5.3.3 Things Learned

This is yet another prime example that shows how much damage spear phishing can cause at its worst. The case is also the first documented case of a blackout caused by hacking. It emphasizes very well the recent worries of several researchers over having embedded systems accessible from the Internet (Goodin 2016). The systems should be at least inaccessible from the machines that are accessible from the outside. Air gaps do not prevent all of the attacks as evidenced by Stuxnet that got into the Iranian systems via a USB stick, but they do increase the security considerably (Zetter 2014.)

Regarding the spear phishing it is hard to say if it could have been prevented. I do not have access to the power companies' or Ukrainian government's usual protocols so it is possible that such an email could have been actually sent to the power companies from the parliament. It still should have been double-checked before any of the emails were opened. The best practice against these kinds of attacks are protocols that should always be followed. The spam filters and the

virus scans will not catch the malware embedded in the files all the time if they have been created especially for the target or just well encrypted. Furthermore even though the file contained a legit looking error report about macros, it would have revealed itself as a phony the minute someone actually looked at it any closer and noticed it was just an embedded picture.

6 PHIRELIGHT SPEARPHISHING EXPERIMENT

The idea of the experiment came from the Phirelight Chief Technical Officer (CTO) Chris Dodunski last summer. At the time I was busy with other projects and could not devote any time to it but when I started writing this thesis it occurred to me that it would be a perfect fit for it.

The idea was simple: I was to send an email to every Phirelight employee and pretend to be the CEO. In the emails there should an individual tracking pixel to see who has opened the email. The email also had to include a link that looked like it would lead to the real Phirelight webpage but instead lead to another domain where I had set up a simple login form to phish for user credentials.

Originally I was going to write all of the code needed for tracking etc. myself but during the weekend before starting the project I happened to upgrade my distro of Kali Linux that had just received its first distro upgrade in 2016. Among the new things added in the upgrade was a program called the King Phisher.

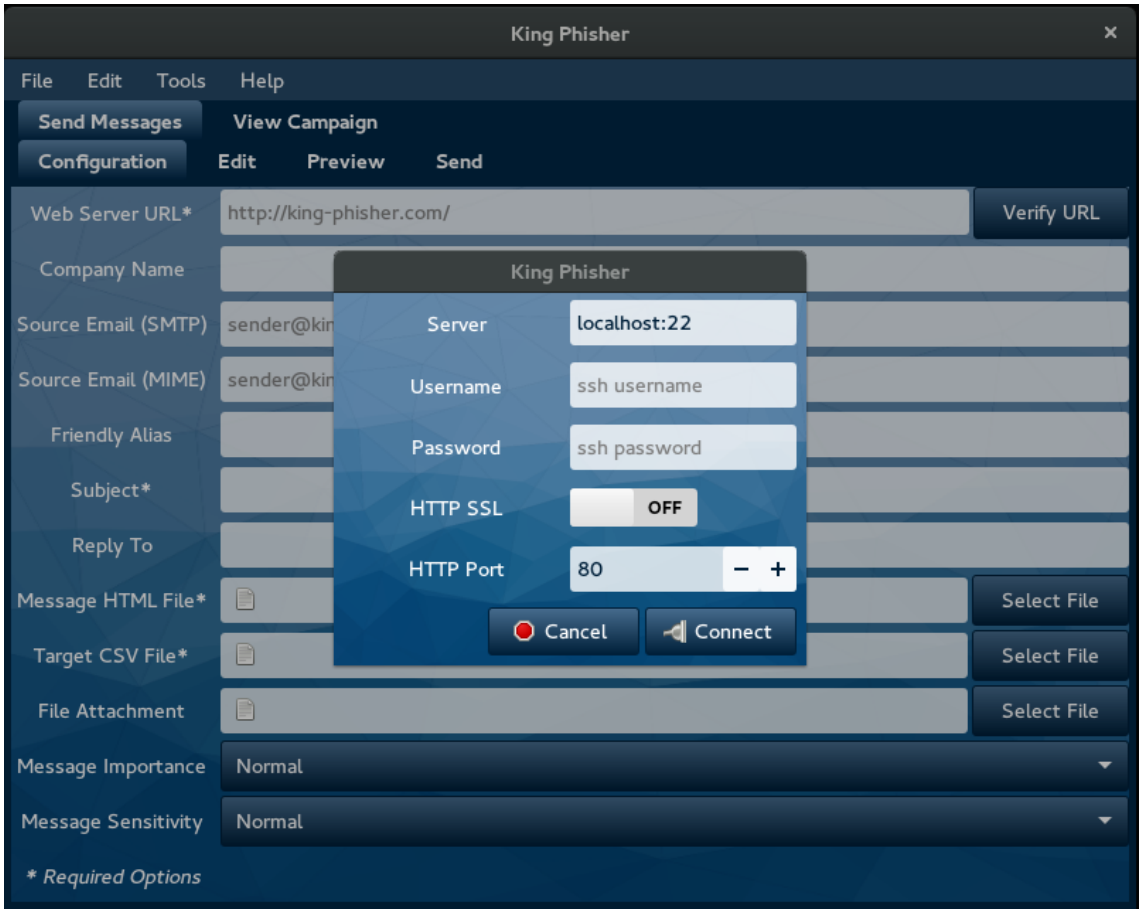
6.1 King Phisher

King Phisher is a tool meant for simulating real world phishing attacks. It runs on most Linux platforms and comes pre-installed in the new Kali Linux 2016.1. King Phisher is developed mainly by three people, Brendan Geise or @coldfusion39, Jeff McCutchan or @jamcut and Spencer McIntyre or @zeroSteiner. Spencer was an invaluable help during my testing and his input and support in the official #king-phisher IRC channel in Freenode.org pretty much made it possible that I got the experiment working like I wanted (SecureState 2016a.)

King Phisher is divided into two parts, the client and the server. The server is responsible for creating the phony webpage that the targets land on after following the link in the email and it even supports running the server with Secure Sockets Layer (SSL). The server component has its own integrated web server so no separate server is needed. The server can also serve as a Simple Mail Transfer

Protocol (SMTP) relay if need be and the emails can even be tunneled to it through SSH in case the ISP for example blocks the usual ports (SecureState 2016b.) My server was running in an external Virtual Private Server (VPS).

The client is responsible for crafting the actual phishing emails and it communicates with the server through SSH. My client was running inside an Ubuntu 14.04 Virtual Machine (VM). In the screenshot below is visible the login screen to the King Phisher server as well as the email crafting window under it.



Picture 5. King Phisher Client Login screen and email crafting.

The edit screen contains the actual message being sent in its HTML form. King Phisher comes with several pre-made emails for various test scenarios but in my phishing campaign I ended up creating my own which better suited my needs.

6.2 SMTP relay

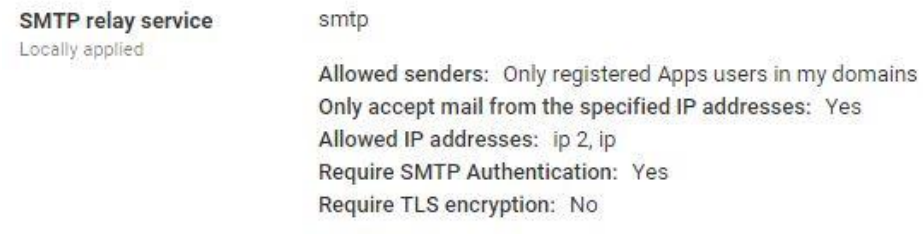
The key component needed for phishing campaign is obviously a mail server. At first I tried using the same server hosting King Phisher's server component as an SMTP relay but the emails could not get through Google's spam filter. When I tested with Microsoft's email servers the messages went straight into the spam folder so I came to the conclusion that I had to use a proper email server to get around this problem. The reason I needed to have a working SMTP relay was because King Phisher identifies each recipient with a unique tag as well as the unique tracking pixel and these are created and embedded into the messages by the program itself. Otherwise I could have just crafted all the emails by hand but since I wanted to see some in-depth data in the results I chose to use King Phisher.

There are many different options for an SMTP relay available and some are made especially for mailing a big number of people. One of the ones I looked into was called Mandrill but I could not find a straight answer whether or not the emails would or would not be tagged as spam by Google. I ended up purchasing a fake domain for the campaign and linked Google Apps for Work to it. The domain name I used looked like the real company domain, except it had switched places of the couple of letters in the name. This is one of the common techniques used in creating the fake domains. A few other tricks are adding letters that are located close to the real letters on the keyboard or replacing some letters with others that look like them when just glanced.

Google Apps for Work gives you the option to use Gmail as your mail-client while still using your own domain in the email address and since all of the emails that originate from Google's own servers are less likely to be flagged as spam it was a simple decision (Google 2016a.) Setting up the email was a relatively simple process. The address I created was obviously mimicking the real address of the Phirelight CEO but other than the address and profile picture I added, I really did not need anything else in it. The real trouble was setting up the SMTP.

The first step was to link my phony domain to the Google's mail server. This was accomplished by adding the MX records to my domain's DNS records. Additionally I added one TXT record that served as a way to identify the domain to Google. The last thing I did was to create a Sender Policy Framework (SPF) record for the domain in a TXT record as well. The SPF record is one of frequently used methods to prevent spoofing the sender address and it basically allows the domain owner to specify which mail servers they are going to use (Mehnle 2010).

Google Apps for Work does not have SMTP enabled by default and it is hidden behind countless other options that are accessible through the Google Admin panel. The first option under the SMTP relay service defines the allowed senders and it comes in when you are spoofing the SMTP headers in the crafted email. If it is set to "Only registered Apps users in my domains" it means you cannot spoof the SMTP email address as someone else's email address. I found out this the hard way when I spent one whole day trying to figure why the SMTP relay was not accepting my spoofed emails. However, the SMTP option in question does not stop you from spoofing the Multipurpose Internet Mail Extensions (MIME) email address which is the one you see in the "From:" field of any email you receive or send. Conflicting SMTP and MIME email addresses usually light up several warning lights and that is why in several of the real phishing attempts the MIME address is set to the same address as SMTP address even though it might mean that the sender's displayed address is something like steve@applle.com (Google 2016b.)



Picture 6. SMTP relay settings in Google Admin Panel.

Other things I had to configure were allowed IP addresses, though this can be left to any IP address but it is not a very secure practice so it is not recommended,

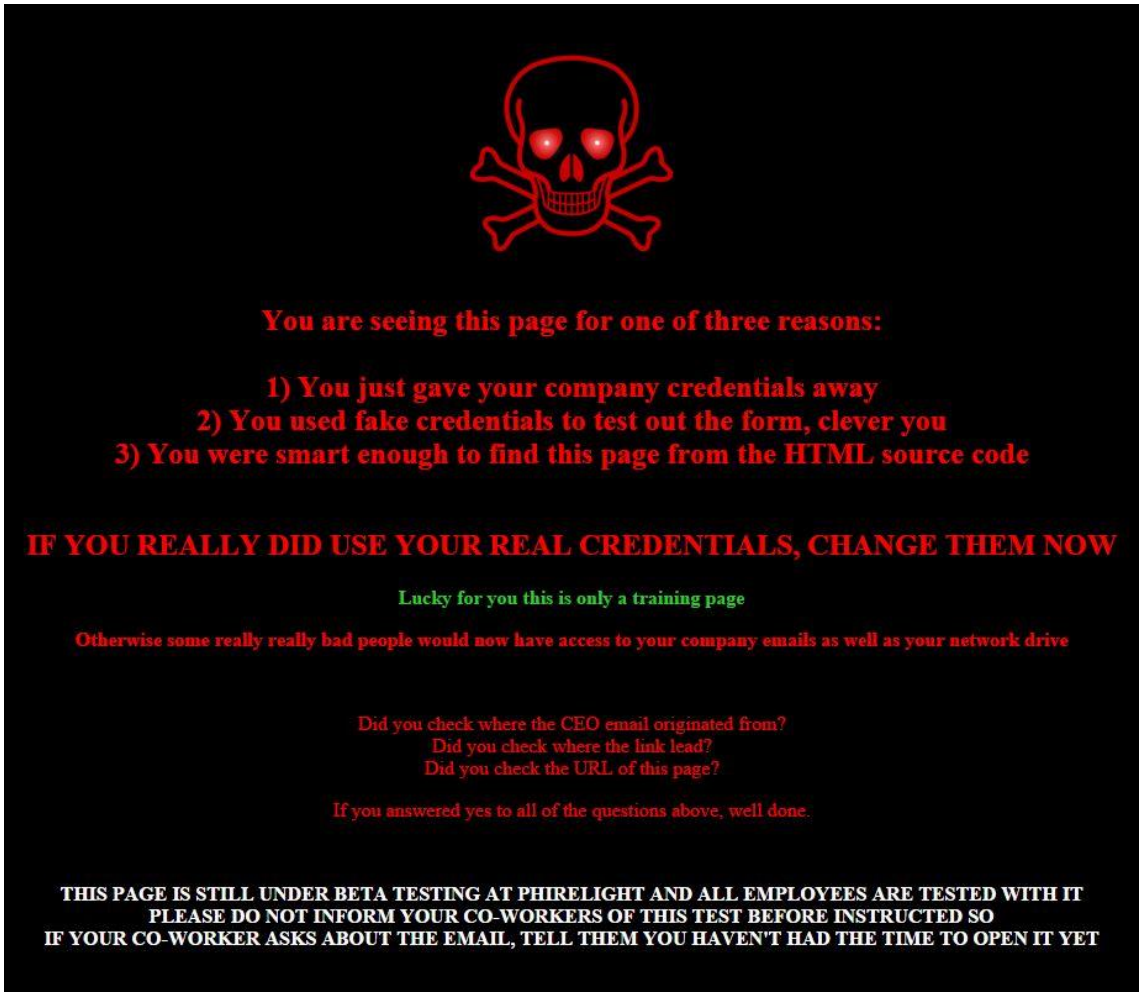
SMTP authentication and Transport Layer Security (TLS). I chose to use just the common SSL through port 465 to the Gmail's server and authenticate with the email credentials.

6.3 The Email

I was in a very lucky position when it came to creating the phishing email since I actually had some real emails that I could look at and mimic the style in them. In a real world scenario the attackers would seek to first acquire some kind of a template to use. For example an old business proposition email from the CEO or something like that would be a perfect start. I would not even rule out crafting a fake business proposition to the CEO just to see in the reply what his emails usually look like. Obviously I am not going to show in this thesis what the email exactly contained but the cherry on top of its icing was the spoofed link. Since the email was formatted in HTML I could insert a link that looked like just a regular Uniform Resource Locator (URL) like *http://www.example.com/login* but in reality it was hidden under the HTML <a> href attribute. The real link in its HTML form was similar to *http://www.example.com/login* meaning the receiver would only see supposed link in the email while the actual destination was elsewhere. In the actual link there was also a unique ID added by King Phisher to identify each person who had opened the link. Without the ID no one could not even see the pages behind the link as they would just display 404. Hiding the real URL behind the link is really often used in phishing emails and it is not easy to spot unless you are looking at your browser's or email client's bottom bar where the real URL shows up. Because I was spoofing the MIME address the email appeared as if it came from the CEO's address but anyone looking at the source code would have spotted that the real address was in the fake domain.

6.4 The Landing Page

The second reason for this test, other than just checking how well the Phirelight employees were trained against it, was to see if this kind of a test could be offered as a service to the customers as well. For this reason we needed a good landing page for the link, something that would do the job of really measuring whether or not the employees would fall for phishing attempt while not being too complicated. I ended up using a simple login portal that would redirect the user to the legit company website. As per the Phirelight CTO's request I crafted another landing page that warned the employees in case they had actually given their credentials away. All of the pages were created almost entirely in just plain HTML with the exception of one utility JavaScript (JS). The appearance of the landing page was mostly a placeholder for the internal test and will most likely be completely different if this kind of a spear phishing test is turned into a product at Phirelight. Below is a sample screenshot of the landing page used in the test.



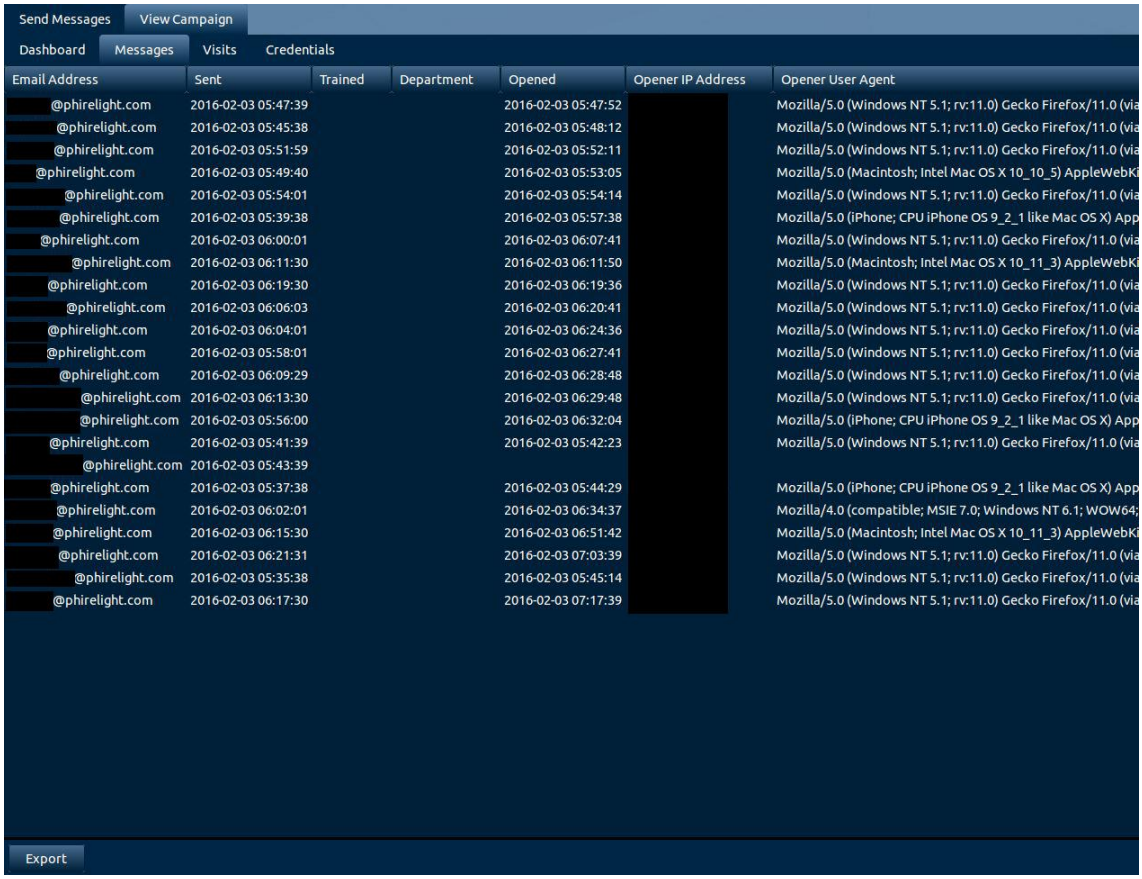
Picture 7. Screenshot of the landing page used in the test.

7 SUMMARY OF THE EXPERIMENT AND SUGGESTIONS FOR IMPROVEMENT

Before the actual test I did several tests with the Phirelight CTO to get the formatting of the email right and to test if it went into spam folder or not. During the preliminary testing we ran one quick test with one of the employees from sales department who will further on be referred as Fred. Fred went as far as to open the email and click the link in it. I heard from Chris that after that he had come in his office asking, and I quote, “What the hell is this?” This is the reaction everyone should have at least at this point. Though if the attacker had hidden a malicious JS on the page behind the link and not just a login form, Fred would have already lost. With the JS the attacker could have for example injected malicious iframes on top of legit ones on the other websites Fred visited even if he had seemingly closed the tab containing the JS. This is precisely why it is never a good idea to open a link in an email that you do not trust.

7.1 The Results

All in all the test surpassed my expectations. In total 23 employees and their emails were targeted and I had hoped to get one or two legit credentials. Instead I got 8. In the screenshot below you can see all the people who opened the email they received. Parts of the screenshot have been cropped because of the size limitations and identifying parts have been censored. All of the targeted employees except one opened the email they received.

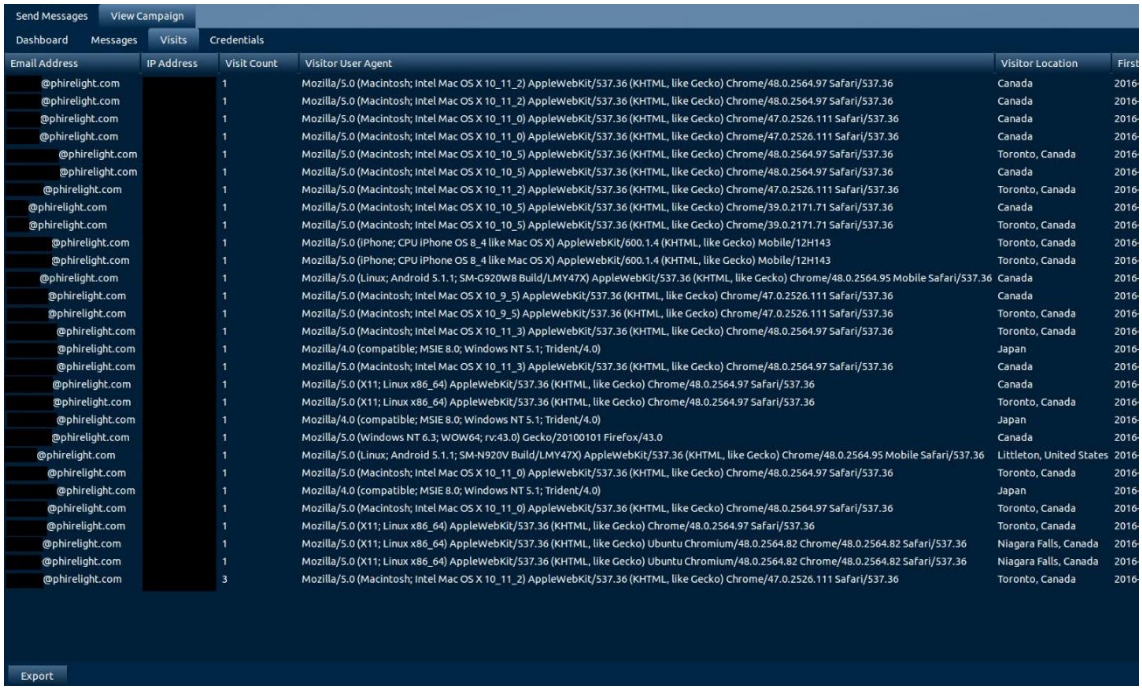


Picture 8. People who opened the email they received.

During the project my first test emails ended up in Gmail's spam folder but later on they went straight to the inbox. The emails had at least two easily flagged features: the MIME address and the SMTP sender address did not match and the link in the email lead somewhere else than it seemed. I suspect I might have trained the spam detectors not to flag the emails because I kept tagging the emails as not spam. Were this really the case it would be somewhat worrying if this is the only way Google checks whether or not the emails are spam. After some post-testing research I did find a mention about Google's spam filters that apply some kind of artificial neural network to figure out which of the emails are spam and which are not. To put it simply if a certain message or sender gets flagged by the users as spam, it is added to the filters as well (Whitney 2015.) This kind of a defense is only good against the regular phishing messages though as this experiment proved. The only program to actually classify the emails as spam in the end was Thunderbird, which I was using to check my own emails.

According to one co-worker his Airmail and Mail for Mac clients let the email straight through as did another co-worker's Microsoft Outlook.

The following screenshot depicts all of the recipients who actually opened the link in the email they received. In total 16 people visited the login portal I had set up. The people who also typed in their credentials or fake credentials show up twice on the list. The two visits from Japan were apparently caused by the antivirus software of one of the employees.

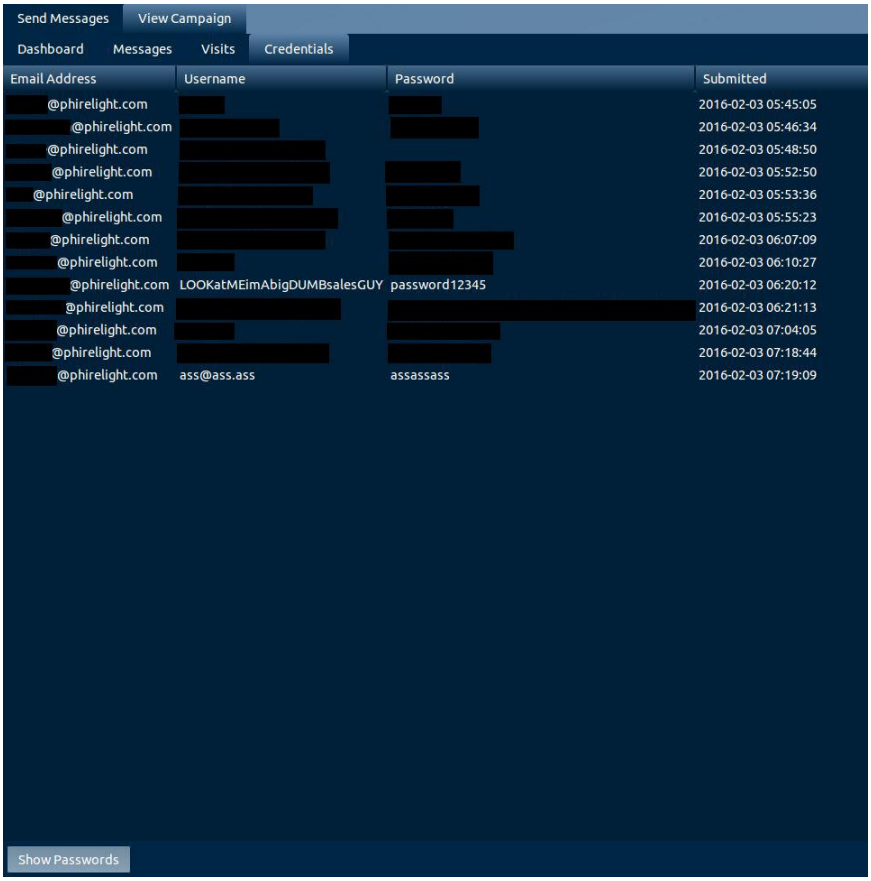


Picture 9. People who opened the link and visited the login portal.

Needless to say the number is worryingly big. This is way too big of a number considering the size of the target group. In this test I was using just a simple login portal, but like I mentioned earlier I could have set up a malicious JS on the page as well.

Finally there were in total 9 people who used their real credentials in the login form and at least one of them an admin user. The number might have some error marginal but based on the passwords received I am fairly certain it is accurate. At least one of the employees was clever enough to use fake credentials and another one tried the form later on with fake credentials as well. The same person

also tried a Structured Query Language injection on the form. The results are visible in the screenshot below.



Picture 10. People who submitted the login form.

Based on the comments I received from some of the employees apparently my initial prediction had been pretty accurate and one department had gone into a total panic mode whereas the other department had one well-informed person who immediately spotted the phishing attempt and warned everyone else physically present.

7.2 What to Improve

First of all way too many people trusted the email right on the first sight. I had a discussion with one of the employees who had submitted their real credentials and according to him the email and the way it was written was spot on. Now I did

have a good look what the CEO's emails looked like but that information could have easily been obtained just by sending him an email asking for a quote on some service for example.

What is worrying is the lack of skepticism. The email did appear at first to come from the real address but everyone's alarm bells should be ringing at least when the email contains a link. You should never ever open a link that you are not sure of where it leads. The real destination can always be seen just by hovering the mouse cursor over the link excluding the cases where the site behind the link redirects the user to some other site.

As for the obtained real credentials this is something that should never happen. In the email the employees were instructed to use their work email credentials. Google's credentials are never used in any other form than in Gmail login screen. In a real situation a 2-factor authentication would be an employee's best friend as the attacker could not login even with the obtained credentials. This is something that should be mandatory in all of the company email accounts.

I did not get much data on what the emergency response was inside the company as people realized they were tricked. What I have gathered is based on the discussions with several of the employees. Apparently there had been some panic at one department and people had been told to "change their credentials and run scans." In the other department things had gone much more smoothly as one of the employees had spotted the ruse and alarmed others in the vicinity, though still the admin who worked in the same room had already typed in his real credentials. Based on this the things seemed to have gone pretty well but more order is still needed. For example the last one to put in his credentials did so even while the panic was still going on in one department and the other department had already learned that it was me behind the test. This should not happen, everyone needs to be informed immediately something like this happens so that they are well-prepared for it. The only way this can be achieved is to have rules to follow when incidents happen and all employees have to be aware of them as well as follow them at all times.

All in all the number of people successfully fooled surprised me but to my knowledge none of the employees had received previously any official training against phishing attempts so that needs to be taken into account. The good thing though is that these weak points came up in an internal review and not in a real incident.

8 HOW TO PROTECT ONESELF?

As it became evident in the Phirelight phishing experiment, the best defenses against social engineering attacks are a healthy dose of skepticism and security awareness. I have already established in this thesis that the weakest link of any system is almost always its human component. In the experiment I analyzed the passwords that people had submitted and they were not in any way bad. All of them were over 8 characters long, they had upper and lower case letters as well as numbers and special characters and the longest one was almost 40 characters long. The passphrases can be over 100 characters long but they matter little if they are given away freely. To maintain a credible and good defense against social engineering people need to be aware of how it works and which things to watch out for. People need to have a good security awareness.

8.1 Security Awareness

Security awareness is not something you are born with. It is best obtained by learning how different SE attacks work and to maintain it, it has to be regularly tested. It is also as much about the individuals' attitudes as it is about their know-how (Cisco 2016). One of the Phirelight employees made a few fitting comments, and I quote, "I'm not sure if it really should count, because I mean it was clear CEO'd written it … If it was a phishing attempt it'd be like 'get ur s3x pill5 hERE' … or if the phisher was so good to have actually learned how CEO composes emails, and our recent hires, then I'd willingly give my info." All joking aside this really is the problem. It never happens to me. What do I have the attackers could possibly want? I would not fall for it, I could see the scam a mile away! Several risky character traits seem to pop up constantly in different studies besides the ways people can be influenced outlined in the previous chapter on social techniques. Some of the more common ones include over-confidence, pride, large ego and ignorance. The thing that should be realized is that there really is not a single human type that will fall a victim to social engineering. Anyone can be the

scammed one. All it takes for the attacker is to find the things that make you tick (Phys.org 2009; Fraud Aid Inc. 2014.)

People need to understand that SE attacks are personal. The attacker knows the target or the target group and their habits. They know how the targets will react in certain situations or at least have a pretty good idea of it. This is why the security is also a personal matter. It is a normal practice to have a department or some of the personnel responsible for the internal security since it is the cheaper option, but in a situation where all employees are targeted in an attack it barely hinders the attacker. No internal security department can possibly take into account every single interaction of the rest of the employees. The employees themselves have to be aware of the possible attacks and understand the risks involved. The responsibility of creating this kind of a mentality in the employees' minds is on the executive branch of any company. People need to take responsibility for their actions as well and not just rely on Google's automatic spam protection to keep their inbox clean and safe.

8.2 Information Is Power

The successful phishers are good. Granted the whole spear phishing experiment I carried out could be classified as a worst case scenario from Phirelight's point of view but it is still not unreasonable to assume that the attacker could have obtained the information they had just by long and arduous leg work. For example the email addresses themselves are really easy to obtain just by first creating a list of known employees, which is a simple task to accomplish with public information sources like LinkedIn. After creating the employee list it would be simple enough task to first grab a few known email addresses that are visible on the company website and make an educated guess based on them how the email addresses are formatted for the rest of the employees. This is why people should be well aware of what information exactly they put online for everyone to see.

One of the things that people often forget is that every little detail counts towards a greater goal. One office working employee might not have anything that interesting on their compromised email account and their personal network drive might also be somewhat empty, but that does not matter since the attacker has already gained a foothold inside the company. Now they can use the completely legit email to send emails to the other employees or upload malicious files into the corporate network drive.

Like I have already repeated many times people should value their own personal information. Facebook contrary to the popular belief is not free. Facebook monetizes its services by selling its users' information to the advertisers. The same goes with all of the social networks. LinkedIn is especially evil from the information security point of view since people are willingly sharing their personal work history and details to anyone interested. It is a really quick task to see yourself how much information you can find online about yourself. The attacker is sure to find all that and perhaps even more. In today's corporate environment the usage of LinkedIn seems to be almost mandatory and people need to maintain a Facebook account to keep in touch with their friends. It still does not mean that you should just openly trust the services that you are using. Read their EULAs and investigate their privacy options because there are ways you can affect how much data you are giving out. In the end the advertisement industry will make sure that you are always leaking information but you do not have to make it too easy for them or anyone else for that matter.

9 CONCLUSION

As I started writing this thesis I had the intention of creating a simple guide that could tell anyone how to protect themselves against social engineering. As I learned more about SE and the psychology behind it, it became apparent that the appearance of my thesis would be somewhat different from my original plan. The main problem is that there really is not just one thing to prepare for but instead as many ways to attack people and organizations with SE as the attacker comes up with. In software the holes and bugs can be fixed but there does not exist any service yet that would patch the human bugs and security holes.

The best practice for defending against hackers is learning their tricks yourself so you will have a better understanding where your weak spots are. The same principle is applicable in SE attacks but cannot be used in an entirely black and white environment where every compliment you receive is an attempt to manipulate you and every email contains a malicious attachment. People need to have a level of trust in their environment to function properly. The only way is to find the middle ground between paranoia and naïve trust.

People will perhaps always remain as the weakest link in any chain, but they can also be its strongest ones. The fact that one employee started warning others of the phishing attempt during the experiment almost right away was something I did not anticipate, but it was something that should be the norm. This thesis was built on the shoulders of giants so it is only fitting I end it with a quote from perhaps the most well-known social engineer of our time Kevin Mitnick: “The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education. Enacting policies and procedures simply will not suffice. Even with oversight the policies and procedures may not be effective: my access to Motorola, Nokia, ATT, Sun depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully.”

REFERENCES

925 TV. 2012. Tapojen muistijäljet mielessä - Kiti Müller | 12/15. Cited: 10.1.2016. https://www.youtube.com/watch?v=zcVLQQXZBzs

Abendan, O. 2013. Watering Hole 101. Cited: 15.1.2016. http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/137/watering-hole-101

About.com 2014. What Is JavaScript? Cited: 9.2.2016. http://javascript.about.com/od/reference/p/javascript.htm

Anderson, N. 2011. How one man tracked down Anonymous - and paid a heavy price. Cited: 21.1.2016. http://arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price/

Ars Technica 2015. Anti-doxing strategy - or, how to avoid 50 Qurans and $287 of Chick-Fil-A. Cited: 11.1.2016. http://arstechnica.com/security/2015/03/anti-doxing-strategy-or-how-to-avoid-50-qurans-and-287-of-chick-fil-a/

BBC 2016. Hackers caused power cut in Western Ukraine - US. Cited: 22.1.2016. http://www.bbc.com/news/technology-35297464

Bisson, D. 2015. 5 Social Engineering Attacks to Watch Out For. Cited: 9.2.2016. http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Bright, P. 2011. Anonymous speaks: the inside story of the HBGary hack. Cited: 21.1.2016 http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

Cherepanov, A. 2016. BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry. Cited: 22.1.2016. http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

Cialdini, R. 2001. Influence. Science and Practice. Fourth Edition. Needham:Allyn & Bacon

Cisco 2011. Email Attacks: This Time It's Personal. Cited: 15.1.2016. http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/targeted_attacks.pdf

Cisco 2016. Protect Against Social Engineering. Cited: 9.2.2016. http://www.cisco.com/c/en/us/about/security-center/protect-against-social-engineering.html

Coen, J. 2009. Identity thieves use payday loans to make a quick buck, authorities say. Cited: 15.1.2016. http://articles.chicagotribune.com/2009-07-21/news/0907200450_1_payday-loans-identity-thieves-identity-theft

CyS Centrum 2016. Конференция UISGCON11. Итоги по киберугрозам в Украине в 2015 году. Cited: 22.1.2016. https://cys-centrum.com/ru/news/uisgcon11_2015

Davis. M. 2015. WordPress vs. Drupal vs. Custom CMS, which is the best for your business? Cited 21.1.2016. http://inspiredm.com/wordpress-vs-drupal-vs-custom-cms-best-business/

Defuse Security 2014. Salted Password Hashing - Doing it Right. Cited: 21.1.2016. https://crackstation.net/hashing-security.htm

DigiCert Inc. 2016. What is SSL (Secure Sockets Layer) and What Are SSL Certificates? Cited: 9.2.2016. https://www.digicert.com/ssl.htm

Dion, K.; Berscheid, E. & Walster, E. 1972. What Is Beautiful Is Good. Journal of Personality and Social Psychology. Vol. 24, No. 3, 285-300.

ENISA 2016. Industrial Control Systems/SCADA. Cited: 9.2.2016. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems

Edwards, J. 2012. Why Would You Write Your Own CMS? Cited: 21.1.2016. http://www.sitepoint.com/why-would-you-write-your-own-cms/

FBI 2016. FBI SWAT. Cited: 9.2.2016. https://www.fbi.gov/about-us/capabilities/fbi-swat-graphic

FINRA 2013. Financial Fraud and Fraud Susceptibility in the United States. Cited: 8.1.2016. http://www.finrafoundation.org/web/groups/sai/@sai/documents/sai_original_content/p337731.pdf

Facebook 2016. Privacy Settings & Tools. Cited: 11.1.2016. https://www.facebook.com/settings?tab=privacy

Fagone, J. 2015. The Serial Swatter. Cited: 12.1.2016. http://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html?_r=0

Finn, G. 2014. Open Source CMS vs Proprietary CMS: An Unbiased Content Management System Comparison. Cited: 21.1.2016. http://cypressnorth.com/web-programming-and-development/open-source-cms-vs-proprietary-cms/

Fraud Aid Inc. 2014. What a con artist looks for in a scam victim. Cited: 9.2.2016. http://www.fraudaid.com/backstage/victims_con_artists_look_for.htm

Goodin, D. 2016. First known hacker-caused power outage signals troubling escalation. Cited: 22.1.2016. http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

Google 2016a. Google Apps for Work. Cited: 29.1.2016. https://apps.google.com/

Google 2016b. SMTP relay service setting. Cited: 29.1.2016. https://support.google.com/a/answer/2956491?hl=en

Grimes, R. 2013. Watch out for waterhole attacks -- hackers' latest stealth weapon. Cited: 9.2.2016. http://www.infoworld.com/article/2614643/security/watch-out-for-waterhole-attacks----hackers--latest-stealth-weapon.html

Hadnagy, C. 2010. Social Engineering: The Art of Human Hacking. First Edition. Indianapolis:Wiley Publishing Inc.

Hadnagy, C. 2014. Social Engineering and Nonverbal Behavior Set. First Edition. Indianapolis:Wiley Publishing Inc.

Henrique, W. 2013. Baiting Attack Exercise – The Old School Way Still Works. Cited 15.1.2016. https://www.trustwave.com/Resources/SpiderLabs-Blog/Baiting-Attack-Exercise-%E2%80%93-The-Old-School-Way-Still-Works/

Hiroshima, N. 2014. How I lost my $50,000 Twitter username. Cited: 20.1.2016. https://medium.com/@N/how-i-lost-my-50-000-twitter-username-24eb09e026dd#.u2sfc4xvx

Hoffman, C. 2013. HTG Explains: What Spear Phishing Attacks Are and Why They're Taking Down Big Corporations. Cited: 15.1.2016. http://www.howtogeek.com/142635/htg-explains-what-spear-phishing-attacks-are-and-why-theyre-taking-down-big-corporations/

Honan, M. 2014. Social Engineering Always Wins: An Epic Hack, Revisited. Cited: 20.1.2016. http://www.wired.com/2014/01/my-epic-hack-revisited/

How Stuff Works? 2016. How Credit Cards Work. Cited: 9.2.2016. http://money.howstuffworks.com/personal-finance/debt-management/credit-card1.htm

Imperva 2016. Denial of Service Attacks. Cited: 9.2.2016. https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html

Interpol 2016. Social engineering fraud. Cited: 11.1.2016. http://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud

Investopedia LLC. 2016. Social Security Number - SSN. Cited: 9.2.2016. http://www.investopedia.com/terms/s/ssn.asp

JBSystems 2013. Debunking the Open Source vs. Custom CMS Myth. Cited 21.1.2016. http://www.jbsystemsllc.com/blog/debunking-the-open-source-vs-custom-cms-myth/

Kaspersky Lab 2016. What is a Trojan Virus? - Definition. Cited: 9.2.2016. http://usa.kaspersky.com/internet-security-center/threats/trojans#.VrmtuFh969I

Kovacs, N. 2015. What is Social Engineering? Cited: 15.1.2016. http://community.norton.com/en/blogs/norton-protection-blog/what-social-engineering

Lee, A. 2011. Social Proof Is The New Marketing. Cited: 13.1.2016. http://techcrunch.com/2011/11/27/social-proof-why-people-like-to-follow-the-crowd/

Lee, R. 2016. Confirmation of a Coordinated Attack on the Ukrainian Power Grid. Cited: 22.1.2016. https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

Lipka, M. 2013. Identity thieves go shopping for Apple products. Cited: 15.1.2016. http://www.reuters.com/article/us-theft-identity-apple-idUSBRE9060EE20130107

Lipovsky, R. 2016a. New wave of cyberattacks against Ukrainian power industry. Cited: 22.1.2016. http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/

Lipovsky, R. 2016b. BlackEnergy Trojan strikes again: Attacks Ukrainian electric power indus-try. Cited: 22.1.2016. http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

Markle, B. 2015. What is VPS Hosting? Cited: 9.2.2016. http://www.inmotionhosting.com/support/website/what-is-vps-hosting

McLeod, S. A. 2008. Wilhelm Wundt. Cited: 10.1.2016. http://www.simplypsychology.org/wundt.html

Mehnle, J. 2010. Sender Policy Framework. Cited: 29.1.2016. http://www.openspf.org/Introduction

Microsoft 2016. Excel. Cited: 9.2.2016. https://products.office.com/en/excel

Mr. Ford's Class 2014. Information Security: Social Engineering (06:08). Cited 15.1.2016. https://www.youtube.com/watch?v=HIwqcYwNWh4

NewSprout 2015. Open Source or Custom CMS. Cited: 21.1.2016. https://www.newsprout.com.au/open-source-or-custom-cms/

Oracle 2015. What Is a URL? Cited: 9.2.2016. https://docs.oracle.com/javase/tutorial/networking/urls/definition.html

PC Plus 2012. How SSL and TLS works. Cited: 9.2.2016. http://www.techradar.com/news/software/how-ssl-and-tls-works-1047412

PC Tools 2016. What is a Zero-Day Vulnerability? Cited: 9.2.2016. http://www.pctools.com/security-news/zero-day-vulnerability

Page, M. 2004. Global Information Assurance Certification Paper. Social Engineering: Information Bandits. Cited 15.1.2016. https://www.giac.org/paper/gsec/4202/social-engineering-information-bandits/106723

Phys.org 2009. Why people fall victim to scams. Cited: 9.2.2016. http://phys.org/news/2009-05-people-fall-victim-scams.html

Ponemon Institute 2015. Cost of Phishing. Cited: 6.1.2016. http://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf

Prudential - Bring Your Challenges 2013. Prudential: Everybody's Doing It. Cited: 13.1.2016. https://www.youtube.com/watch?v=BgRoiTWkBHU

Ramzan, Z. 2001. Phishing Attacks and Countermeasures. Handbook of Information and Communication Security. Berling:Springer

Richardson, D. 2014. Social Psychology for Dummies. First Edition. Chichester:John Wiley & Sons Ltd

Schacter, D. Gilbert, D. & Wegner, D. 2011. Introducing Psychology. First Edition. New York:Worth Publishers

SecureState 2016a. King Phisher. Cited: 29.1.2016. https://github.com/securestate/king-phisher

SecureState 2016b. King Phisher. Cited: 29.1.2016. https://github.com/securestate/king-phisher/wiki

Segura, J. 2015. Large Malvertising Campaign Takes on Yahoo! Cited: 15.1.2016. https://blog.malwarebytes.org/malvertising-2/2015/08/large-malvertising-campaign-takes-on-yahoo/

SimilarWeb 2016. Yahoo.com. Cited: 15.1.2016. http://www.similarweb.com/website/yahoo.com#overview

Smith, G. 2012. Twitter Hacking Victims Find Stolen Accounts Sold On Black Market. Cited 20.1.2016. http://arstechnica.com/security/2014/01/how-i-lost-my-50000-twitter-username/

Social Engineer Inc. 2016a. Social Engineering Defined. Cited: 8.1.2016. http://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

Social Engineer Inc. 2016b. Influencing Others. Cited: 13.1.2016. http://www.social-engineer.org/framework/influencing-others/

Symantec 2015. New reconnaissance threat Trojan.Laziok targets the energy sector. Cited: 15.1.2016. http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector

TechTarget 2011. content management system (CMS). Cited: 9.2.2016. http://searchsoa.techtarget.com/definition/content-management-system

TechTarget 2013. Chief Technology Officer (CTO). Cited: 9.2.2016. http://searchcio.techtarget.com/definition/Chief-Technology-Officer-CTO

Techopedia Inc. 2016a. Multipurpose Internet Mail Extensions (MIME). Cited: 9.2.2016. https://www.techopedia.com/definition/1693/multipurpose-internet-mail-extensions-mime

Techopedia Inc. 2016b. Dumpster Diving. Cited: 20.1.2016. https://www.techopedia.com/definition/10267/dumpster-diving

The Computer Language Company Inc. 2016. Definition of: SSH. Cited: 9.2.2016. http://www.pcmag.com/encyclopedia/term/51940/ssh

Totalbiscuit, The Cynical Brit 2015. I will now talk about Valve's Christmas screw-up for just over 27 minutes. Cited: 11.1.2016. https://www.youtube.com/watch?v=esmKdMDvSGI

University of Minnesota 2016. Positive Reinforcement... a proactive intervention for the classroom. Cited 14.1.2016. http://www.cehd.umn.edu/ceed/publications/tipsheets/preschoolbehavior/posrein.pdf

VMware Inc. 2016. What Is a Virtual Machine? Cited: 9.2.2016. https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc_50%2FGUID-CEFF6D89-8C19-4143-8C26-4B6D6734D2CB.html

Valve Corporation 2015. Steam Guard. Cited: 9.2.2016. https://support.steampowered.com/kb_article.php?ref=4020-ALZM-5519

Valve Corporation 2016a. Welcome to Steam. Cited: 9.2.2016. http://store.steampowered.com/about/

Valve Corporation 2016b. Update on Christmas Issues. Cited: 11.1.2016. http://store.steampowered.com/news/19852/

What is My IP Address 2016. The Mailman Inside Our Computers. Or: What is Simple Mail Transfer Protocol? Cited: 9.2.2016. http://whatismyipaddress.com/smtp

Whitney, L. 2015. How Google tries to keep 'sneaky' spam from your inbox. Cited: 9.2.2016. http://www.cnet.com/news/how-google-tries-to-prevent-spam-from-reaching-your-inbox/

YLE 2015. Online identity theft to become a crime. Cited: 15.1.2016. http://yle.fi/uutiset/online_identity_theft_to_become_a_crime/8262093

Zetter, K. 2014. An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Cited: 22.1.2016. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

irchelp.org 2013. Welcome to #irchelp. Cited: 9.2.2016. http://www.irchelp.org/

Appendix: Email exchange between a hacker and rootkit.com admin

From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 1:59 PM

To: jussi <jussij@gmail.com>

im in europe and need to ssh into the server. can you drop open up

firewall and allow ssh through port 59022 or something vague?

and is our root password still 88j4bb3rw0cky88 or did we change to

88Scr3am3r88 ?

thanks

From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:06 PM

To: Greg Hoglund <greg@hbgary.com>

hi, do you have public ip? or should i just drop fw?

and it is w0cky - tho no remote root access allowed

From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 2:08 PM

To: jussi jaakonaho <jussij@gmail.com>

no i dont have the public ip with me at the moment because im ready

for a small meeting and im in a rush.

if anything just reset my password to changeme123 and give me public ip and ill ssh in and reset my pw.

From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:10 PM

To: Greg Hoglund <greg@hbgary.com>

ok,

takes couple mins, i will mail you when ready. ssh runs on 47152

...a little later:

```
bash-3.2# ssh hoglund@65.74.181.141 -p 47152
[unauthorized access prohibited]
hoglund@65.74.181.141's password:
[hoglund@www hoglund]$ unset
hoglund@www hoglund]$ w
11:23:50  up 30 days,  5:45,  4 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
jussi    pts/0    cs145060.pp.htv. Wed11pm 59.00s  0.38s  0.35s  screen -r
jussi    pts/1    -                Thu 5am  1:13   0.38s  4.90s  SCREEN
jussi    pts/2    -                Thu 5am 59.00s  0.68s  4.90s  SCREEN
hoglund  pts/3    132.181.74.65.st 11:23am  0.00s  0.03s  0.00s  w
[hoglund@www hoglund]$ unset HIST
```

[hoglund@www hoglund]$ unset HISTFLE

[hoglund@www hoglund]$ unset HISTFILE

[hoglund@www hoglund]$ uname -a;hostname

Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP Wed Mar 15 14:21:45 EST 2006 i686 i686 i386 GNU/Linux

www.rootkit.com

[hoglund@www hoglund]$ su -

Password:

[root@www root]# unset HIST

[root@www root]# unset HISTFILE

[root@www root]# uname -a;hostname;id

Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP Wed Mar 15 14:21:45 EST 2006 i686 i686 i386 GNU/Linux

www.rootkit.com

uid=0(root) gid=0(root) groups=0(root),1200(varmistus)