SOCIAL ENGINEERING AND EDUCATION IN FIGHT AGAINST CYBER CRIMINALITY

Incze Arpad

Abstract. In the latest years a spectacular growth of hacking cracking activity is going one. In many cases behind this activities young students are involved. What are the their motivation for taking the road of cyber criminality? Why they use their skills and knowledge to harm other people? What can we, teachers, do abut it? Not all cyber criminals start their activity with financial benefits in mind. The majority of them are simply thrilled by the provocation of braking into a system. For them this is just for fun, for showing up, for demonstrating their skills. But after the firs successes there is a very short road to thru criminal activity. In this paper a new method of diverting this student is proposed based, ironically, on a principles of social engineering so much beloved by this cyber criminals

1998 Subject Classification for Computer Science.: A.1

1. INTRODUCTION

"A criminal might be based in Romania, using servers hosted in Russia, stealing data from people in Germany, to buy goods from an American retailer for delivery in the UK, using an Australian credit card " according to a site called Lucid In-telligence[6]

When the president of the United States of America, in a speech addressed to the nation declares the followings : "It's now clear this cyber threat is one of the most serious economic and national security challenges we face. We're not as prepared as we should be, as a government or as a country." (May 29, 2009 CBS NEWS) it is more than obvious that cyber criminality is a serious issue...

Alarming facts Since the beginning of the internet criminals are trying to make a profit out of it using in their benefit this tool of com-munication. Unfortunately these activities are growing in an exponential way. According to security reports emitted by prestigious organizations and firms there is a significant in-crease especially in the last few years regarding cyber crime. For instance according to Symantec, malicious activity in 2008 amounted to 60 percent of all the activity they have recorded since they started keeping records. Last year, they recorded 1.6 million new malicious code signatures and blocked 245 million malware attacks from their users every month.

The numbers emitted by Symantec are alarming:

- a 31% increase of zombie computers in 2008, Symantec observed an average of more than 75,000 active boot-infected computers each day.

- 55389 phishing website hosts detected

- 349.6 billion spam messages in 2008 compared to 119.6 billion spam messages in 2007, which is a 192% increase.

- 20% increase in spoofed financial services companies web sites

Another player in security fields, Verizon released a report showing that 285 million information records were compro-mised in 2008, alone. This number is greater than the whole number for the entire 2004-2007 period.

These numbers presented here are only the known facts. The real numbers regarding the attacks and losses are unknown, making the criminals very happy since the most valuable in-formation stolen is the data no one knows has been stolen.

Figure 1. Dollar loss of referred complaints was at an all time high in 2008, $264.59 million, exceeding last year's record breaking dollar loss of $239.09 million

Why we use 2008 data ? Because it seems that year 2008 rep-resented a peak in cyber criminal activity if the number of compromised records are taken in consideration.

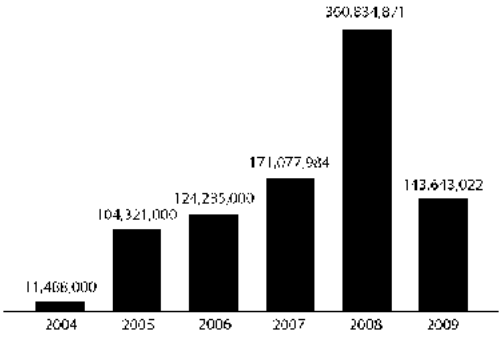

Figure 2. Number of compromised records reported by VERIZONE

There is also a new underground market emerging for stolen data. Criminals specialized in stealing personal, financial data are no longer the criminals who use the data directly. They prefer to sell to the highest bidder the sensitive information they posses. The economic principle of supply and demand has come into play with this underground economy too. Credit cards go anywhere from less than a dollar to about $30 and bank account credentials sell for anywhere from $10 to $100. Much of the cost depends on the perceived value of information and the amount of it, which is purchased[1].

2."I WANT TO BE A HACKER"

.. said Andrei, a 12 year old secondary school student who several minutes ago managed to find out his friends yahoo password.
The learning process of using the access tool to the computers network is a chaotic endeavor, by following the examples of colleagues or other close relatives, generally without taking into consideration the rules of the ISP or the advice's of parents or education staff. The current curricula of the Informatics courses in schools are focused mainly on programming and using the Microsoft Windows platform, being taught, in some cases, by not interested or inexpert teachers, which recommend their pupils to download and reproduce texts "from the Internet". The lack of minimum education and of the informatics ethical

norms are reflected in an irresponsible behavior and lack of discernment in a professional use of Internet. This is leading in some cases to a real "passion" for illegal activities in the computer networks and a glorification of the ones that are good in this endeavor. In order to try to identify possible solutions to improve the present situation, we would try to discuss the following subjects:

1. the motivation factors of youngsters to become a hacker
2. the public image of those who "infringe the law on the Internet";
3. the attitude towards other young people involved in such activities in correlation with involvement of a higher number of youth in cybercrimes activities;
4. the level of knowledge and awareness regarding the no-tions of cybercrime;
5. reactions of youth in relation with the educational activities mentioned above;
6. the role and "image" of cybercrime law enforcement au-thorities;
7. involvement of other actors from the public or private sector in combating or preventing cybercrime.

A. Why ?

Maybe the most complex part of being a hacker is finding the motivation. The main aspects should be resumed in the followings:

1. Psychological motivation. The need to prove something to themselves but especially to the circle of friends. Step up, show off, be somebody no matter how. Some times it is doubled by a desire to revenge after being rejected for some reasons from the circle of friends. What could have better taste than a revenge like stealing someone's credentials to his favorite socializing site and making fun of him or even hearting the person who make us feel bad ?! But this first successful steps has the potential to open the appetite of a young mind to such kind of activities.

Another psychological factor is the need for adrenalin rush. The hacking can provide that feeling in almost the safest way because there is no danger to the physical health, no such activities that can cause injuries. A successful hacking and the action of deleting the trace of it, in some cases may have the same neurophysiological effect as a chase and escape after a robbery.

The next step in the evolution of a hacker is when the psychological needs are replaced by socio-economical ones. Lets face it we talk about MONEY, SOCIAL STATUS. Successful hackers are discovered by criminal groupsorganizations

or they start by themselves to act as criminals. They use their knowledge, their expertise for *making money*. Such a hacker is motivated financially and will work for interest not for pleasure.

B. Reaction of the public

The society has its own guilt by not condemning firmly the cyber criminals. Even more in several cases the society rises their cyber criminals to the rank of hero, glorifying their achievement. Often it is related to some kind of national pride something like *my fellow citizen hacked the FBI network, how good we are..?*. This kind of reaction has an unwanted effect of encouraging cyber criminality. (a.n. especially in east-ern European countries) . Often multimedia organizations, news studios presents such persons as results of an excellent educational system diverting the attention from the criminal act itself to the intellectual potential of the citizens of the country.

C. The ignorance of the public

Due mainly to the lack of information of the society regard-ing the imminent risks of the internet. The painful truth is that the majority of home users, also a considerable amount of SOHO users have no idea about the risks they face each time thee connect to the internet , read a mail, download a *free* application.

There are peoples who hear about cyber criminality when it is too late for them, being already a victim of some form of internet fraud. While in the case of older generations the only solution for them to be informed about cyber threads would be mainly the television, in the case of students there is a huge opportunity to inform them while they are in school. We do not say they should learn the techniques of hacking but at least the should recognize an attack or a fraud attempt.

B. Means of attack

Attacks involving malware or malicious code are used/designed to steal mostly financial information or take command and control of a computer. Such a remotely con-trolled computer is called a zombie and the network of these computers forms a botnet which works as a super computer and is used to gather sensitive data and to spread further more malware, which infects more unprotected systems. The most relevant fraud techniques listed on the FBI crime schemes site are as follows[7]

Auction fraud involves fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Auction fraud is the most prevalent of Internet crimes associated with Romania. The subjects have saturated the Internet auctions and offer almost every in-demand product. The subjects have also become more flexible, allowing victims to send half the funds now, and the other half when the item arrives

- **Credit Card Fraud** means subjects are using fraudulent credit cards. The unauthorized use of a credit/debit card, or card number, to fraudulently obtain money or property is considered credit card fraud. Credit/debit card numbers can be stolen from unsecured websites, or can be obtained in an identity theft scheme.

Employment/business opportunity schemes have sur-faced wherein bogus foreign-based companies are recruiting citizens on several employment-search websites for work-at-home employment opportunities.

Identity theft occurs when someone appropriates another's personal information without their knowledge to com-mit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes

Internet extortion involves hacking into and controlling various industry databases, promising to release control back to the company if funds are received, or the subjects are given web administrator jobs

The lottery scheme deals with persons randomly contact-ing email addresses advising them they have been selected as the winner of an International lottery

Nigerian letter ore 419 Named for the violation of Section 419 of the Nigerian Criminal Code, the 419 scam combines the threat of impersonation fraud with a variation of an advance fee scheme in which a letter, email, or fax is received by the potential victim.

Phishing and spoofing are somewhat synonymous in that they refer to forged or faked electronic documents. Spoofing generally refers to the dissemination of email which is forged to appear as though it was sent by someone other than the actual source. Phishing, often utilized in conjunction with a spoofed email, is the act of sending an email falsely claiming to be an established legitimate business in an attempt to dupe the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank ac-count information after directing the user to visit a specified website. The website, however, is not genuine and was set up only as

an attempt to steal the user's information.

Spam or unsolicited bulk email, is now a widely used medium for committing traditional white collar crimes in-cluding financial institution fraud, credit card fraud, and iden-tity theft, among others Means of protection

C. Means of protection

Fighting against cyber criminality consist mainly in defensive/preventive action[2] .

- Antivirus software capabilities are extended for malware and Trojan detection.
- Internet browsers now comes with enhanced security options when browsing the net.
- Encryption algorithms are becoming more and more complex therefore harder to break the code with classic methods.
- Users and employers are becoming more and more aware of the risks and therefore implementing rigorous security policies. Non profit organizations maintain web pages with information related to fraud attempts.
- Financial institutions are taking more and more measures for securing the transactions and informing their clients about the risks.
- Governments are hardening the punishment for cybercrime corroborated with training of specialized law enforcement units.

Unfortunately all these actions are far from being a solution to the problem as demonstrated by the numbers presented in the first chapter.

Cyber criminals are very talented in finding and exploiting security breaches of all kinds also they are the masters of act-ing without leaving a trail. Even if the police can pinpoint a computer after IP address ore other means, the owner can be an innocent citizen who's computer acted as a zombie ore the owner can be the criminal but he has left deliberately some malware on its own computer so he can act as an innocent user.

Despite all the effort to reduce the number of these attacks criminal activity in this domain seems to be increasing day after day. Attackers become more and more aggressive. They even targeted a website belonging to an organization which was fighting against cyber fraud and they managed to block and

permanently close the access to that site.
How has this become possible? Why are these hackers so aggressive? Well the results of this war is pretty much on their favor. Also the reaction of the society is very pale. Even advanced users when they recognize an fraud attempt, in the majority of the situations all they do is to ignore, maybe with a smile, the attempting letter and soon after they forget the inci-dent. Very few people take real action for instance reporting a spoofed site .
By implementing more and more security measures hacking in the traditional way is becoming more and more difficult so the criminals are turning to their favorite weapon in their arsenal.

3.Social Engineering. The Achilles heel

"Why try the hard way when you can ask nicely?!" (the password)

Social engineering definition: A deceptive process in which crackers *engineer* or design a social situation to trick others into allowing them access to an otherwise closed network, or into believing a reality that does not exist. [4]. Social engineering is the act of manipulating people into per-forming actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim. In the majority of these attacks a certain level of Social En-gineering is used usually at the beginning of the attack. Social Engineering is used to deploy malicious software which will allow later the takeover of the computer. Social engineering is used to collect private/confidential information (login names passwords) or bank account related information (card number, PIN). Those who use social engineering in their criminal activity are exploiting the most powerful human feelings: fear and joy. Under the influence of this two sensations the criminals are driving their victims in a direction in which they will give up their private information ore they will do a set of actions that will allow to the criminal to deploy his means of attack.
Just two short examples:

- the use of joy, of happiness related with greed : *You win the jackpot !!! al you have to do is to give us .. your everything.*

- the use of fear (of loosing something, money for in-stance): *We inform You that Your Credit card has been used to purchase a rocket engine by Taliban extremist. If You wish to stop the transfer of Your founds please fill in the fields in the following confirmation web page:.. .*

A final, more advanced method of gaining illicit information is known as **reverse social engineering**. This is when the hacker creates a persona that appears to be in a position of authority so that employees will ask him for information, rather than the other way around. If researched, planned and executed well, reverse social engineering attacks may offer the hacker an even better chance of obtaining valuable data from the employ-ees; however, this requires a great deal of preparation, research, and pre-hacking to pull off[5]. The term Reverse Social Engineering is under a debate be-tween the members of the scientific community, many of them reclaiming the mean of the word Reverse. In the following a new meaning is given to this term in the method proposed to fight against cyber criminals.

4.Reverse social engineering

A new meaning for the term: Reverse social engineering is proposed in this paper as a method based on social engineering tools. The very same psychological considerations are used to deploy a set of actions with the intention of discourage cyber criminal activities.

A. The proposal. Let's Scam the scammer If the cyber criminals use social engineering to gain access to their victims computer systems/ bank accounts/ personal information, why not use the same tool to deploy a counter-measure?!

The focus is to mislead the perpetrator by making him to be-lieve that he is about to gain some success. Instead in the end he will realize that he is the one who got fooled and lost pre-cious time, some money and in some cases even his freedom.

The method under discussion is easier to understand by an example:

Let there be a spoofed financial site, from a prestigious bank. Through that site a victim is asked, under a certain pretext, to enter personal information about his/her credit card which will allow to the perpetrator to fabricate a clone card with the inten-tion to draw money out from the victims bank account.

An experienced user quickly realizes the fraud attempt. He knows that a bank never ask for that kind of information.

There are two options available for the user:

- ignore the event
- report the event. For this he can contact a law enforcement representative, ore hi can inform the bank about the fraud attempt. Also there is a web forgery reporting option embed-ded in several web browser applications.

Our experienced user instead of ignoring the attempt but before reporting the spoofed site to the authorities, decides to fill the forms of the spoofed site with fake data. He pays attention to the required format of the certain fields. He will enter a name, surname card number, PIN but everything being mock data. He does this operation several times, each time with apparently usable information.

On the other end the criminal is grubbing his hands, he is happy because he thinks he found some victims. He urgently manufactures from a bulk card a cloned credit card with the obscurely obtained data. He rushes to an ATM slides in the card, enters the PIN and surprise!!! ERORR. He tries again and again. Hmmm, something went wrong during the card printing process. He goes home verifies the data from the card complies with the data he received. Well, everything seems OK but just for sure he prints another bulk card. And he rushes again toward the ATM where he gets the same error . Well maybe the data he received is not accurate, he thinks the user maybe entered a wrong key during the input process.

Finally he concludes that the data he received for that credit card number is unusable. No problem because he received data from about a dozen potential clients. But he is having a real surprise after he gets the same error message for the fifth, sixth set of data because the experienced user filled not once but for several times the spoofed site with fake information. What goes one in the criminal's mind after many failures ?

-He is having a problem whit the spoofed site. He tries to find and solve the problem. Waste of time if he is the creator and maybe money if somebody else made the page for him for a fee.

-He is having a problem with the blank cards. He goes to by a new set and start to write it and use it at the ATM. Again he gets nothing but looses time and money.

-He can conclude also that he is having a problem with the card writer. He buys a new one. Also wasting money and time.

- The bank uses extra security to protect his clients.

In a very optimistic situation this method can lead even to the capture of the criminal. If he insist at an ATM with a cloned card there is a chance that an ATM will retain the card with some usable fingerprints on it for the police.

The new meaning of **Reverse** now becomes obvious. The same social engineering tool is used to fool the attacker by re-versing the roles between the criminal and the victim.

For almost each type of web forgery a certain scenario can be developed and deployed. All of them with the intention of mislead the perpetrator making him to loose time and/or money until he finally will give up and this is exactly the goal.

In the case of auction fraud, lottery scheme, Nigerian letter; there is the possibility to bombard the seller with questions regarding the product or the payment method just to make him spend more time to answer to your questions. Fake information can be served to the criminal regarding the money transfer making him to believe that his money is on the way. Also several useless walks to a nearby money transfer office can be frustrating for the criminal.

If the number of such fake, unusable, information is high enough, a certain level of insecurity installs between the criminals. They do not know anymore if a set of data is usable ore fake. Like in cryptography were if the resources spent to crack a key is higher than the value of the gained information, leads to the abandon of the cracking, likewise with reverse social engineering, finding a few usable information among many, many fake data can be too expensive ore time consuming, so most likely the criminals will give up.

Conclusions

Like in many other fields where huge masses are targeted with a certain action the response must came from the masses in as many numbers as possible. Actually the breakthrough will come not after few annoying vigilante citizens who by there actions maybe will stop a limited number of criminals or at least will remove them for a short period of time but for a more and more increasing number of baffled fraud attempts .

Unfortunately there is no way to automate this process of answering to the provocation. Therefore groups of users should be involved in this kind of countermeasures. These group should play two roles:

- answering the attacks like described above. Groups should work together not only for sending more useless data to criminals but also they can exchange

data regarding spoofed sites, phishing attempts. There are currently such attempts in this direction but they are limited in action to discover and report such criminal activity.

- spreading the concept among other users so more and more should step up against this illegal actions or at least become aware of the dangers. Universities are in big advantage here because IT teachers can inform and enroll huge groups of students to take action.

There is another psychological issue worth mentioning here. It is well known that cyber criminals are highly literate in the field of IT and security. If one day a paper like this would be published in a widely spread PC magazine, just this appearance could induce some confusion among the criminals because they wont know anymore if the data they receive is genuine usable data ore some overzealous users red the article and acting accordingly.

For the criminal, if the publication of the idea is followed by an increase in the number of responses (they receive more data/information from their spoofed sites), most certainly they will assign this fact to a response to such an article.

Therefore the author of the article, after publication on in scientific magazine, intends to publish the idea in as many PC magazines as possible both on paper ore in electronic format via WWW. Quantifying the results is possible only after publicizing the method .

It would be desirable to find some ways to measure the effects of this method, but right now it is in a concept phase.

This is not the miracle medicine to the cyber criminality problem of the world but it can add some advantage like the other means of protectionprevention used in this fight. As it was stated in the introduction of this paper, the phenomenon of cyber criminality is rapidly growing, there fore any method which can score some points against it should be used. This one should not be an exception.

References

[1] Jim Doherty, A Brief History of Data Theft, The ISSA Journal, June 2008

[2] Yuval Ben-Itzhak, The Cybercrime 2.0 Evolution, The ISSA Journal, June 2008

[3] Yuval Ben-Itzhak, Organized Cybercrime, The ISSA Journal, October 2008

[4] Schell, B.H. and Martin, C. Contemporary World Issues Series: Cybercrime: A Reference Handbook. Santa Barbara, CA: ABC-CLIO, 2004.

[5] Sarah Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, on http:www.securityfocus.cominfocus1527

[6] https:www.lucidintelligence.com/index.php (accessed in April 2009)

[7] http:www.ic3.gov/crimeschemes.aspx
item-2 (accessed in February 2009)

Incze Arpad
Department of Informatisc, mathematics and Electronics
University of "1 Decembrie 1918"
Address Alba Iulia, Nicolae Iorga str. nr.1
email:*aincze@uab.ro*