A greater involvement of education in fight against cybercrime

Incze Árpád

Abstract

In the latest years a spectacular growth of hacking cracking activity is going one. In many cases behind these activities young students are involved. What is their motivation for taking the road of cyber criminality? Why do they use their skills and knowledge to harm other people? What can we, teachers, do about it? Not all cyber criminals start their activity with financial benefits in mind. In order to try to identify possible solutions to improve the present situation, we would try to briefly discuss the following subjects; the motivation factors of youngsters to become a hacker, the public image of those who "infringe the law on the Internet"; The attitude towards other young people involved in such activities in correlation with involvement of a higher number of youth in cybercrime activities; the level of knowledge and awareness regarding the notions of cybercrime; reactions of youth in relation with the educational activities mentioned above; the role and "image" of cybercrime law enforcement authorities; involvement of other actors from the public or private sector in combating or preventing cybercrime. Considering the actual level of knowledge of the wide masses in the field of cyber criminality, we propose a higher involvement of education in preparing the people to face the threat of a cyber attack

Corresponding Author: Incze Arpad
Tel: +19 37682307
Email: dwdstudio2000@gmail.com

1. Introduction

"I want to be a hacker" .. said 12 year old Andrei, a secondary school student who several minutes ago managed to steal his friends yahoo password.

The learning process of using the access tool to the computer 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 educational 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 is reflected in an irresponsible behavior and lack of discernment in a professional use of the 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.

Keywords: education, cyber crime, curricula, prevention
1.1. Cybercrime facts

"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 Intelligence.¹

When the president of the United States of America, in a speech addressed to the nation declare 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." ² it is more than obvious that cyber crime is a serious issue...

Since the beginning of the internet criminals are trying to make a profit out of it using in their benefit this tool of communication. Unfortunately these activities are growing in an exponential way. According to security reports emitted by prestigious organizations and firms there is a significant increase 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. In 2009, 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, Verizone released a report showing that 360 million information records were compromised in 2008, alone(fig. 2). 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 information stolen is the data no one knows has been stolen.

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].

This criminal activity translates in billions of dollars stolen or lost from citizens or companies. (fig . 1) Dollar loss of referring complaints was at an all time high in 2008, $264.59 million, exceeding the previous year’s record breaking dollar loss of $239.09 million

¹ https://www.lucidintelligence.com/index.php (accessed in April 2009)
² President Obama adress the nation speech May 29, 2009 CBS NEWS at http://www.cbsnews.com/2100-18560_162-5555565.html
2. **Why become a hacker?**

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

### 2.1. 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. Sometimes 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 hurting the person who make us feel bad?! But this first successful step 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 physiological effect as a chase and escape after a robbery.

### 2.2. Financial, economical reasons

The next step in the evolution of a hacker is when the psychological needs are replaced by socio-economical ones. Let's face it, we talk about MONEY, SOCIAL STATUS. Successful hackers are discovered by criminal groups/organizations or they start by themselves to act in disrespect for the law. They use their knowledge, their expertise for “making money”. Such a hacker is motivated financially and will work for interest not for pleasure.

---

3 Internet Crime Report 2008 http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

4 http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf
2.3. 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 eastern European countries). Often multimedia organizations, news studios present such persons as the results of an excellent educational system diverting the attention from the criminal act itself to the intellectual potential of the citizens of the country.

2.3.1. The ignorance of the public

Due mainly to the lack of information of the society regarding the imminent risks of the internet. The painful truth is that the majority of home users, also a considerable amount of SOHO users has no idea about the risks they face each time they connect to the internet, read a mail, download a “free” application.

There are people 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 threats would be mainly the media (TV), in the case of students there is a huge opportunity to inform them while they are in school.

3. Are we prepared?

Several authors[6][7], including us, reached a strange conclusion: the current level of development of the hardware and software tools in the field of IT security if applied correctly would be more than enough to considerably reduce the number of successful attacks. Then why the huge number of victims? Kevin Mitnick in the introduction of his book [9] states that “the human factor is truly security's weakest link”.

3.1. Social engineering. The Achilles' heel.

Therefore hackers return to the oldest trick in the book: 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 performing 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 Engineering 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 these two sensations the criminals are driving their victims in a direction in which they will give up their private information or 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 !!! all you have to do is to give us ….. your everything.

∞ the use of fear (of loosing something, money for instance):” We inform You that Your Credit card has been used to purchase a rocket engine by an alien race. If You wish to stop the transfer of Your founds please fill in the fields in the following confirmation web page:….. “ and of course when the frightened victim opens the confirmation page to clarify the purchase, there is a spoofed website with a field for a PIN code for the card or a
username/password combination of the bank account.

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 employees; however, this requires a great deal of preparation, research, and pre-hacking to pull off[5].

In more than 80% of the cases hackers exploited not the system itself but the people behind the system or misconfigured system wrongly done by a prepared individual. The harsh conclusion is that the masses are not prepared, informed about the risks of the Internet or other IT related products. Also peoples develop a certain reflex like behavior, a routine, when working with computers as the results of the following test will demonstrate

3.2. Ignorance test

It may sound inappropriate but we also called this test the “stupidity test”

To evaluate the awareness of the masses the following test was set up: first we asked the test subjects to auto-evaluate their computer skills. Then we challenged the subjects to install a computer software thru a standard installation routine. But there was a catch. No real software installation occurred only a set of consecutive windows appeared on the screen similar to those used by installation packages with Yes No Next Finish buttons beside some text. We changed the usual installation messages with unusual information. For example the message “The software will be installed in the following folder” we wrote “The content of the following folder will be deleted”. Also other warning messages were added to few windows like “If You install this application You will lose your internet banking information. Do You wish to proceed ?”. On the last window we wrote “If You click Finish button You will lose any information from Your computer”

The test was conducted on three groups of 20 students each, from different fields: Public administration, Accounting, Computer science. The scope of this experiment was to determine the level of attention during a routine operation and if this level of blind routine is affected by the prior knowledge of the participants. Unfortunately the results a disaster from the security point of view.

| Table 1. Ignorance test results |
|-------------------------------|
| Groups                        | Average IT knowledge | Pass the test | Fail the test |
| Public Administration          | Average              | 5            | 15           |
| Accounting                     | Below average        | 8            | 12           |
| Computer science               | Above average        | 2            | 18           |
Pass the test stands for those who read carefully the information from the installation windows and interrupted the operation when realizing the danger, or those who asked assistance afterwards.

Fail the test represents the number of students who skipped over the reading of the information, considering it a routine installation where all they had to do was to click the Next or Finish buttons. And they did so !!!

The results speak for themselves. More than 80% of the test subjects “agreed” to install a harmful application on the computer. Even more interesting is the result concerning the correlation between the self accepted knowledge in the field.

The students from the computer science from who anybody would expect a better knowledge of the risk were instead those who failed in greater number. Such a high degree of “automation” among IT specialist is explicable if we consider that those students perform regularly this kind of action and they are the most familiarized with a standard installation process.

This test demonstrates only one of the many weaknesses represented by the human user. Other dangers are misconfigured settings, use of default configurations, inappropriate behavior (the use of weak passwords).

Regardless of the reason mentioned above the common element of all of them is the lack of information and education. People just don’t have the necessary knowledge to protect themselves, to recognize an attack or a potentially dangerous situation.

This is completely understandable considering the fact that there is almost no preoccupation for teaching computer security issues at any level of education at all. For instance in our country computer science students are learning about IT security in 3th or 4th year. Students from other specialisations aren’t so lucky. All they learn during some basic IT courses is to use an antivirus software and it is not recommended to share a password to others.

4. Conclusions. Teaching IT security should be a MUST

Therefore we militate for the introduction of IT security related knowledge in the educational curricula for all educational levels.

10-12 year old children should learn how not to fall in pedophile's trap, or that the latest version of some online game is not the healthiest thing for dad’s bank account.

Older student should learn how to recognize a phishing attempt or what personal data from social network sites are safe to share publicly and what information must stay confidential.

All the users should know about “default configuration” and their risk. If not to a certain level where users are able to change this configuration file accordingly but at least they should be aware of the risks and proceed accordingly, perhaps asking a specialist solving the problem.

And yes (!) although several voices are against teaching certain hacking techniques we consider that those teachings can help prevent further attacks. Knowing how a hacker will try to hack into a system can be useful for the victim in two ways: the user will be prepared with certain countermeasures (antivirus, firewall, more secure configurations) and will help the user to recognize an attack and act accordingly.

Never the less if IT security related issues would be widely spread, we consider that this can be helpful in fight against cybercrime not only because users would be more prepared, systems would be correctly configured but also hackers would have serious second thoughts before launching an attack based on the principle of “I know that You know”. If I am a hacker and I know that my victim, most likely, has the knowledge to recognize my attack, I face a dilemma: Should I deploy my attack knowing that the chances of success are minimal? Therefore we do not share the opinion that says that it is wrong to teach hacking techniques.

Bottom line: cyber crime is a serious issue and the society has his part of guilt. Education should be seriously involved in the fight against this plague. Manuals should be written or rewritten to prepare the present and the next generations to successfully take up the fight.
References

Jim Doherty, “A Brief History of Data Theft”, The ISSA Journal, June 2008
Yuval Ben-Itzhak, “The Cybercrime 2.0 Evolution”, The ISSA Journal, June 2008
Yuval Ben-Itzhak, “Organized Cybercrime”, The ISSA Journal, October 2008
Schell, B.H. and Martin, C. „Contemporary World Issues Series: Cybercrime: A Reference Handbook“. Santa Barbara, CA: ABC-CLIO, 2004.
Sarah Granger, „Social Engineering Fundamentals, Part I: Hacker Tactics”, on http://www.securityfocus.com/infocus/1527/
Bruce Schneier, Schneier on security, Wiley Publishing inc., 2008, ISBN 978-0470-39535-6, chapters 10, 11, 12
Bruce Schneier, Secrets & Lies Digital Security in a Networked World, John Wiley & Sons, 2000 ISBN 0-471-25311-1
Kevin Mitnick, William L. Simon, The Art of Deception, Wiley Publishing inc 2002, Hardback ISBN 0-471-23712-4, pg. 12