CYBERCRIMINALS AND THE VICTIMS OF CYBERCRIME

Lecturer Adriana Iuliana STANCU, PhD.
Faculty of Judicial, Social and Political Sciences, "Dunarea de Jos" University of Galati, Romania
adriana.tudorache@ugal.ro

Abstract:

Technological development and the large scale use of computer systems have led to unquestionable benefits, but to an equal extent exposed society to a series of risks related to the ill-intended use of these systems. In practical life the dependence degree of public institutions, legal and physical persons on the use of digital networks is translated into a similar degree of vulnerability, and exposure to the illegal use of these technical means. The computer has been a first rate crime-enabling factor providing wrongdoers with a new object (the information contained in digital systems) and a new tool.

Keywords: *cybercriminal, cybercrime victim, technology*

Introduction

”Cybercrime” is not just a change of name in regard to approaching former crimes in a new form, but a fundamental transformation in our manner of approaching digital crime.

This new type of crimes are committed by people as well, they are still deliberate and usually aim at obtaining financial benefits. In other words, they have a purpose, and in case it is reached, and break the law - they are criminally liable.

Computer experts are people with higher training and a structurally logical way of thinking. Still, what may make them use their knowledge for illegal purposes? Money? „Fame”? Frustration with a boss who is much better paid but less competent? Arrogance? These are but a few questions that cannot receive a definite answer. Probably the answer is somewhere in between all these possibilities.

Digital crimes are not committed only by people with superior training in informatics, but also by teenagers and persons with minimal digital knowledge, able to take advantage of the gullibility/ ignorance of their victims.

It is well known that hackers are usually apprehended only when they attack. Armed with patience and resourcefulness which are not in short supply in their case, they may stay „hidden” in our digital systems, planting their bugs, worms and bombs for a future disaster [1].

Some hackers become computer addicted, and turn their own programs into prisons for their own body. When they sleep, if at all, they cry in their sleep for the program stolen or unfulfilled, get out of bed with their hands clenched and jump directly to the computer, where they find the incorporable exaltation of the cyberspace, and take their drug red eyed and restless [2].

It should be mentioned that, in addition to the cyberspace addiction created, hackers position their power by anonymity. To them it is a dream that they recovered the power and got „inside”, where they can see everything without being seen. This strange dream to penetrate the computer logic by defeating the system victimises the system itself [3].

These people merely consider themselves addicted to hacking, and parting with their computer may be perceived as a tragedy [4].

To most law-enforcing individuals, hackers are just regular felons using unusual means to reach their goals [5].

But who are these perpetrators of cybercrime? What lies beneath the names mentioned in mass-media?

Digital criminals

3.1.1 Cybercriminals acting in cyberspace

The criminals called phearks are those individuals who use their phones to access cable communication networks, in order to illegally penetrate computer systems, to the purpose of exploring, getting information or merely out of curiosity.

Hackers are individuals who by means of computers illegally log in their system through password cracking, to the purpose of exploring or stealing information.

Hackers may be of various types. Many are just curious and want to learn how a certain program or system works. They generally do no harm, and may even be useful in finding weak areas of the programs (bugs). In any case, the activity of these individuals, if it gets out of hand, may cause a lot of harm to companies or even national security (as in the case of the attacks against the Pentagon site).

Professional hackers use their knowledge to cause harm. The actions of these individuals result in consequences ranging from mere inconveniences to considerable destruction. The latter category also includes attacks of the „denial-of- service” type (blocking the activity of famous sites like E-bay or Yahoo).

Crackers are the criminal category who manage to penetrate the informatic systems of an organism, institution or company, by breaching the digital security systems. The access is remote, through a mere PC equipped with a modem.

Information traffickers commit crimes that bring them huge financial benefits. They are involved in electronic espionage and sell the secrets of the firms who information networks they breach to competing firms.

Hucksiers are a category of spammers with a lower rate of message profit (e.g. at least a month) out of a high number of spam messages sent to an address. They may send spam for the delivery or download of a fraudulent product in itself.

Fraudsters are a category of spammers with a higher profit rate of a message (e.g. even in 12 hours since sending it) out of a low number of spam messages sent to an address. They are usually involved in frauds of the phishing or “Nigerian letter” type.

3.2 New and old modus operandi of digital criminals

a) Denial-of-Service attacks (DoS): flooding an IP address (identification number of a computer or another type of device) with data, resulting in blocking the computers or the internet connexion - most attacks of this type are launched against important websites, with the intention to prevent the access of their regular customers [6].

This type of attack is “an incident whereby a user or organization cannot use a resource that they normally have access to, … by blocking a certain network service or temporary loss of connectivity”, and may result in affecting the programs or files in the targeted system [7].

b) bofi type attacks (a bofi being a `type of worm that exploits the various vulnerabilities`) generally target specific points, like spamming or phishing [7].

c) Phishing type attacks affect the digital systems of physical and legal persons alike, consisting in `fishing` information on the user and other information stored in the computer.

d) Trojan: a malicious program masked as something harmless, usually an email attachment or an internet download - it opens up the computer, allowing access to a hacker. Unlike viruses, these programs cannot replicate themselves. The trojan is a program that "disguises itself as something else when being executed". The trojan "must be sent by someone or carried by another program an dit is usually received as a joke or a software" [7].

In point of effects, a trojan may destroy digital data or even block the access of the rightful user to the digital system.

a) The Dialler is a "program using the computer or a modem for the dial-up connection to a location, usually at high costs". The user may know or not when installing such a program, but more often then not it is executed without his permission [7].

b) Cookies consist short text information, transmitted by a web server together with a net page and stored on the hard-disk. Cookies contain information allowing the web supplier to count the access to his pages, and may at the same time adapt his offer to the users' desires [8].

These programs are not normally able to spy the data in the computer where they are installed nor start programs. However, there is the possibility that any „intruder" may read such a cookie, thus gathering personal data of the person using that particular computer.

a) Exploit is "a program or technology exploiting the vulnerability in a software, and may be used to breach the protection or attack in a manner or another a system in the network" [7].

b) Viruses are code sections able to replicate, sneaking through the programs inside a computer and triggering various effects, from erasing important files to destroying the whole system. These programs may multiply on their own, attacking other computers by means of the infected computer.

At the same time with the digital data transfer, the danger of infecting computers with viruses increases dramatically. The risk is higher if these computers make up a network. This is why certain viruses have managed to spread globally causing damage amounting to hundreds of millions dollars.

Any type of digital data stored in a computer may be affected by viruses, starting with simple programs, applications or documents, to boot or partition sectors.

There are encrypted viruses (that use “encryption to hide from virus scanners… modifying their own code”, to be as hard to detect as possible), polymorphic viruses (`that change the byte matrix when replicating and thus avoid detection by simple scanning techniques”), metamorphic viruses (“that change their own code but preserve the same functionalities from an infection to another”), retroviruses (“attacking one or more antivirus programs to avoid detection”) and even macro-viruses (“a program or code segment written in the internal language of an application; certain macros replicate, others infect documents”) [7].

a) Worms are self-distributing programs (even under different names) by copying from a computer to another, by e-mail or inside the network.

The Mailer is “a worm sending one or more emails with its code as an execution attachment” [7].

The Mass mailer is “an Internet worm that is transmitted to one or several emails with its code as execution attachment; it is usually done by accessing the local email list and sending mails to all the addresses found” [7].

b) Spyware consists of “programs able to scan systems or monitor activity and retransmit the information collected to other computers or locations” [7]. The collected information may consist of passwords, bank account numbers, any type of personal documents or information stored in the computer. Some of these programs may be used to find information about the programs installed on the computer and their activity.

c) Java: platform-independent programming language, created by Sun. Relatively harmless, certain programming errors allow hackers to get unauthorized access to a digital system.

d) A Bug is “a programming error in an application that may have undesired side effects, such as various security issues occurring in some browsers” [7].

e) Adware „facilitates the distribution of advertising content to the user either by means of their own windows, or by using the interface of a different program... they may collect information from the user’s computer, including information relative to browser use or other activities taking place on the computer, and relay this information to an internet location” [7].

f) IP-Spoofing: data exchange between two computers via the internet is always performed by means of an IP number, a series of figures consisting of 4 blocks of 8 bits each (this number corresponds to the digital address of the computer); there is a series of tricks hackers use to manipulate records, so that a fake web-server may be launched, which looks exactly like the original computer of a bank, for instance (but instead collects the passwords and then makes the connection with the real computer of the bank, thus making it possible to steal huge amounts of money).

g) Buffer overflow is a “a corruption of data resulting from copying a larger data block than the available buffer (without checking the size of the block)” [7].

h) Pharming consists in using a malware code to illegally access and steal personal information, the code being sent in an email or even through an unsecured webpage.

i) “Supervorms” do not require their activation by the user, and making and distributing them involves many resources and much time, their purpose being more to destroy than to obtain profits.

j) “Rootkits” work stealthily, unlike superworms, being in fact intelligent programs working in a part of the operating system that is inaccessible to antiviruses, and allow the remote control of the digital system and even data manipulation.

k) Bluesnarfing - attack against a mobile phone equipped with an operating system by exploiting the poorly configured profiles of the serial ports (Serial Port - ports used for serial communications, the transfer happening bit by bit) [9]. These ports are in fact concepts for headphones or other extensions connectable through Bluetooth.

These are just some of the methods used by the digital felons to reach their goals. Any internet-connected system is vulnerable to these attacks, even if they originate hundreds of thousands of miles away.

In regard to the felonies committed by these devices, the enumeration may only be exemplifying: from simple disturbances of the digital systems, to stealing and destroying data, from espionage to sabotage, from copyright infringements to very serious offences.

Victims of cybercrime

According to a study performed by the AVG security company, 43% of the British citizens feel more vulnerable to cybercriminals than thieves, muggers or robbers. It may be accounted for by the fact that one out of three people questioned has already been the victim of an online attack. Most often the victims complained about unauthorized bank transfers and credit card fraud.

In order to fight this type of crime, 90% of the respondents in that study specified that they installed antivirus software in their computers, although most of them are aware that it may not be enough.

The physical persons who become victims of cybercrime are generally people who, out of ignorance or superficiality, made available to the digital felons their personal data (among which bank account numbers or even PINs), which were subsequently used against them or for cyberfrauds.

Another category of victims that are particularly targeted by digital attacks are gullible persons who easily fall for offers that are “too good to be true” or pyramid schemes.

It is surprising how easily data are divulged over the internet, which in other circumstances would not be supplied. For instance, if a person is approach on the street and asked about his/her bank account number, the reaction would certainly be at least one of suspicion. But if such a request is made via the internet, integrated in an email that looks more or less official, the situation is completely different.

There are also studies showing that some individuals would unhesitatingly divulge personal passwords like the one for their email.

Internet fraud causes victims (physical persons, banks, online shops, etc.) losses of millions of millions of euros. For example, only on Christmas and New Year’s Eve 2002 online shops had losses of 100 millions euros [10].

In the internet world, there are not only victims of digital fraud. A new phenomenon causes concern in legal communities, i.e. harm caused to private life and online dignity. More specifically, online slander and online harassment, that more and more public or less public persons become victims of.

The most serious informatic attacks occur on legal persons. Out of these, the favourite target of these attacks is banks and great financial institutions.

They are targeted by attacks against the security systems resulting in the unauthorized access of felons into the digital systems and networks, as well as by attacks under the form of unauthorized transfers which steal the personal data of the customers of these institutions.

Multinational companies are also a target for cybercriminals who are well aware that a valuable confidential piece of information or blocking the site of a competitor may be `repaid` by another competitor.

Not only legal and physical persons are victims of cybercrime, but states themselves. It is about the practices that have been included within the phenomenon of digital terrorism.

Affecting the telecommunication networks or stock exchanges, paralysing public utility services as the effects of digital attacks are no longer science-fiction scenarios, but real problems that NATO has started to take measures against.

Out of the victims of cybercrime, a certain category deserves a separate analysis, i.e. the sites belonging to famous companies or institutions that are the preferred target of cybercriminals, namely hackers, who wish to `prove themselves`. These sites either are worth millions of dollars, or are centres of national security systems, or are important names on the international level. The damage sustained by them, when quantifiable, are impressive, and the echo of security vulnerabilities is resented worldwide.

An American hacker (Adrian Lamo) managed to compromise the internal security network of New York Times in the early 2002 and add his name to teh confidential database of collaborating experts (among whom there was also the former American president Jimmy Carter). In addition, Lamo illegally accessed information on officials of that company. Adrian Lamo also affected the networks of giants like Yahoo or Microsoft. Captured by the authorities, the notorious hacker pleaded guilty for the attacks against Microsoft, Lexis-Nexis and The New York Times. Lamo was sentenced to 6 months of house arrest at his parents' abode and two years of parole, as well as the payment of damages amounting to 65,000 dollars.

Upon investigation it was found that the hacker was also guilty of compromising the security measures of Yahoo, AOL Time Warner, Bank of America, Citigroup, McDonald's and Sun Microsystems. The parole period was accompanied by the compulsory requirement to use monitoring programs for all the activities taking place on the young man's PC.

When he was finally released, the former hacker declared that he wanted to set up his own company of security consulting.

The case of Victor Faur, 22, from Arad, is probably the most widely advertised in Romania in connection to the illegal access of digital systems, and at the same time of disturbing the operation of strategic networks in the US. He was indicted by a federal tribunal in Los Angeles for breaking the codes of over 150 computers at NASA and the Energy Department, as well as the American Marines, risking a sentence of up to 54 years in prison.

After an investigation of over a year, the prosecution found out that he had illegally accessed 114 NASA computers, causing damages of 1,366 million dollars, plus the costs incurred with the personnel who had to solve the intrusions and retrieve the affected data, as well as losses of 55,000 dollars caused to the Department of Energy, and 38,000 dollars caused to the American Marines.

The attacked computers contained data on spatial programs, new types of technologies, communications with space vehicles during missions and collecting data from the probes sent to the solar system. As a result of these attacks, the American scientists had to repair the damaged electronic systems, and to manually communicate with the space shuttles.

Conclusions

The previous data illustrate how young rebels manage, equipped only with their PC in their own home, to disturb the activity and cause damage of millions of dollars to institutions and international agencies.

Unfortunately, the ever increasing number of such attacks originating In Romania and the ever increasing number of victims of the Romanian hackers place Romania in the top of the countries with a high risk of cybercrime.

The victims of cybercrime rarely report such crimes. The motives are complex, from lack of noticing small unauthorized expenses to lack of confidence in the chances of identification and prosecution of the wrongdoers.

Some states created organizations that post information sources for the victims of cybercrime and addresses where they may report any suspicious activity.

Preventing and fighting the plague of digital crime can only happen starting from educational measures for the users of digital systems and internet services regarding the various online perils.

References :

[1] Ziauddin, S., Ravertz, J. (1996). “Cyberfutures: Culture and Politics on the Information Superhighway", London, Pluto Press.

[2] Courter, G., Marquis, A. (1998). “În lumea calculatoarelor”, ALL, Timișoara.

[3] Conley, V. (1993). “Rethinking technologies”, Minneapolis: University of Minnesota Press.

[4] Taylor, P. (1993). “Hackers: A Case Study of the Social Shaping of Computing”, PhD dissertation, Research Centre for Social Sciences, University of Edinburg.

[5] Hafner, K., Markoff, J. (1991). “Cyberpunk: Outlaws and Hackers on the Computer Frontier”, New York: Simon and Schuster.

[6] PCWorld Extra, (2000)

[7] PCWorld Extra, (2006) no. 1 January.

[8] Browning, J. (1999). “Info tehnologic”, Nemira, Bucharest.

[9] Dinu, C, “Dicționar IT”, Pocket Book Publishing House, Bucharest.

[10] Thompson, T. Cyber Theft Will Net Milions as Christmas Shoppers Go Online” htlp;//observer.guardian.co.uk.