DOI 10.20544/HORIZONS.B.03.1.16.P57
UDC 004.6:004.738.056.53

SECURITY OF THE COMPUTER DATA AND INFORMATION IN THE ELECTRONIC TRAFFIC[1]

Svetlana Nikoloska, Jovche Angjeleski
Faculty of Security - Skopje,
Skopje, R. Macedonia
svetlananikoloska@hotmail.com

Abstract

For the industry as well as for the entire humanity, the computer represent third industrial revolution, an invention that facilitates all aspects of life, an invention that allows fast communication and exchange of information and "the world on a palm" or the world became global communication village. Protection of data, information or other content used by computer systems and networks is realized through the incrimination of criminal behavior of individuals and legal entities who are using their knowledge and skills for misuse and achieving of property or other benefits or for damage causing. In order to breach the security of the data in the electronic traffic, the skilled computer guys create multipurpose computer viruses from non-risky or comic viruses to viruses that inflict massive damages with a financial and technical nature. A subject of this scientific work is studying of the security in the electronic traffic by analyzing the crimes foreseen within the Criminal Code of the Republic of Macedonia in terms of legal protection, but with a purpose to obtain indicators if the citizens are feeling safe in their electronic communication made through electronic survey with system questions. The normative method of analysis of legal documents is going to be applied and also electronic questionnaire as one of research instruments will be practiced.

Keywords - electronic traffic; computer systems; computer networks; computer data; computer viruses

INTRODUCTION

[1] Professional paper

A separate group of crime is deriving from the classical and the economic crime where the computer appears as a means or as an object of criminal attack [1]. The computer crime is a general formulation which includes a variety of shapes and forms of criminal behavior. Namely, it is crime that is directed against the security of information (computer) systems in general or in a single part in various ways and by various means with intention to obtain personal benefit or to damage someone else [2]. The cybercrime allows such an intellectual engagement of the culprit which gives the cybercrime an attribute “perfect crime” [3]. The perfect crimes relates to computer systems and networks, and of course with computer data circulating in the cyberspace. The cyberspace is a theoretical space in which data can be stored, transmitted and generated [4]. Cyberspace is a combination of virtual structures, physical components based on virtual structures, the information they contain, and the flow of information within those structures [5]. Computer crime is also known as cyber (computer) attack which include all actions aimed at disruption, blocking, degradation or destruction of the information stored in computers and computer networks.

The basic prerequisite for the prosecution of the computer crimes coulprits is their incrimination in the Criminal Code of the Republic of Macedonia with several amendments and changes, accepted recommendations of the international legal acts, in particular the Convention on Cybercrime of the Council of Europe since 2001. Within the changes and the amendments of 2004, the crime "Creating and importing computer viruses" in article 251-a is incriminated. This crime is executed in series with other computer crimes with elements of damaging the computer system and misuse of personal data and data from credit cards. Cybercrime is inherently international crime by the space of criminal activity enabled by the globalization and the use of information technology that has connected the entire world. The information connectivity enables to say that the world is already a global communications village, where information and computer data are moving at speeds in fractions of a second, that is a great achievement for the criminals. The Republic of Macedonia is harmonizing its criminal legislation with the EU in the interest of prosecuting the culprits and to the computer crime, providing assistance and cooperation with other police forces in the world, because in this criminal, the action can be from one place on the Globe, and the consequences to be felt on other places away thousands kilometers. For the prosecution of culprits of computer crime it is necessary to cooperate, exchange information, but also to take measures and actions in mutual operating actions of the police forces of the concerned countries in a criminal

operation. Namely, such an action of the Macedonian police and the USA FBI as case analysis is a subject of this scientific work.

COMPUTER VIRUSES

The computer virus is defined as a program that propagates its own replication, infection of another program by modifying its copy. Computer viruses are small programs from several kilobytes that aim to inflict damage on an infected computer. Mainly, the viruses are multiplying in a way that embed themselves in other files, and so do harm by deleting or modifying files on the disk. In a way the computer virus is a logical sabotage which includes deletion, damage or modification of data, programs or parts of the operating system. It is usually done by using standard service programs, own programs by using techniques such as logic bomb or virus [6]. Most important is to know that the virus or “worm” or “Trojan” can make the infection through: any media, e-mails and infected web sites. The computer virus is incorporating in the operating system and is able to “infect” quickly and completely, in all its programs, causing a complete slowdown of the entire system and destroy through its contents. If an infected program is transported directly (through media) or indirectly (through a computer network) from one computer to another, acts as a contagion. Although the mechanism of "infection" itself is not dangerous, the virus usually contains programming code that performs some additional functions. These functions cause changes in data files, giving command to the computer to delete any content on the disc, and is activated by programming through time mechanism or plugging of the computer [7]. The virus is placed in the programs that are widely and commonly used so that can be spread as quickly as possible. Whenever you run that particular program, the virus also runs, and it can activate another program. The virus can not affect the computer while the infected program is not activated. Ones the virus becomes active it goes into the computer's memory or system files or applications. Some viruses display only messages, create sound or comments at different time intervals after multiplying or when affected program is activated. Some viruses can disable or force the computer to behave erratically. Generally, people are not aware of the existance of a virus in the computer until it is detected [8].

The most famous “Trojan” virus presents a program which infiltrated in someone’s computer, sends all passwords to the e-mail of the one that infiltrated the virus, enabling the infiltrator of the “Trojan” virus to access the infected hard drive. The computer worms that can cause serious damage are also considered as computer virus. The first virus “Brain” [9] was developed in 1986 in Pakistan by

brothers Basit and Amiad Farooq Alvi, who owned the company “Brain Computer Service”. The virus has been developed in order to protect the company`s software. Subsequently, the virus was renamed in “Pakistan”. In the following paragraphs we are presenting most harmful computer viruses and warms [10]: . ILOVEYOU, perhaps the most virulent computer virus ever created, the ILOVEYOU virus managed to wreck PCs all across the world. Infecting almost 10% of the world’s PCs connected to the Internet, the virus caused a total damage of around $10 billion. The virus apparently got transmitted via email with a subject line “ILOVEYOU,” which is a radical human emotion that no one can ignore. To make it even more alluring, the email contained an attachment that read something like this: Love-Letter-For-You.TXT.vbs. The moment someone pened the file, the virus emailed itself to the first 50 contacts available in the PC’s Windows address book.

• Melissa, became the breaking news on March 26, 1999, after hitting the new age of emailing. Built by David L, Melissa was spread in the form of an email attachment by the name "list.doc." When a person clicked upon the attachment, the virus would find the Microsoft Outlook address book and email itself to the first 50 contacts on the list having a message "Here is that document you asked for…do not show anyone else." Later on, FBI arrested David L and slapped him with a fine of $5000 for creating the wildest virus of its time.
• Code Red, taking advantage of the Microsoft Internet Information Server's flaw, Code Red spread on the network servers in 2001. Here is an amusing fact about this dangerous virus—it didn't need you to open an email attachment or execute a file; it just required an active Internet connection with which it ruined the Web page that you opened by displaying a text "Hacked by Chinese!" It's no surprise that this virus devastated nearly $2.6 billion dollars by hitting almost one million PCs. And in less than a week's time, the virus brought down over 400,000 servers that included the White House Web server as well.
• Sasser, was a Windows worm that was discovered in 2004. Apparently, it would slow down and crash the PC, making it even hard to reset without cutting the power. And its effects were surprisingly troublesome as well, with millions of PCs being infected and crucial, significant infrastructure affected. The worm played on a buffer overflow susceptibility in Local Security Authority Subsystem Service (LSASS) that monitors the safety policy of local accounts causing crashes to the PC. The devastating effects of the virus were massive resulting in over a million infections. This included critical infrastructures, such as new agencies, hospitals, airlines, and public transportation.

CREATING AND IMPORTING A COMPUTER VIRUS

The crime with elements of creating and importing a computer virus is a criminal act that can be done by the culprit in two ways, one is creating the virus and the other is importing it. The Macedonian legislation stipulate fine or prison sentence up to one year for "the one that will create or use the virus with the sole intention of inserting in another computer or computer network; prison sentence from 6 months to 3 years for "the one that by using the computer virus will cause damage to another computer, system, data or program" and if the culprit causes bigger damage or the crime is done within a group created for doing a criminal act as described the punishment is from 1 to 5 years in prison; the act is punishable by law and a fine can be applied if the culprit is a legal entity"[11]. To be considered as a crime, the virus must be made with intention of inserting it in another computer or computer network. Furthermore, the consequence of the act

must follow i.e. any type of damage, meaning, damaging of other programs in the computer or computer network as well as preventing the usual, normal use of the inserted programs and data processing in the computer [12]. The criminal acts refer to:

. Creating a computer virus which is a special computer program that the culprit creates for certain aim by programming a way of transporting of any type of "attack" or to cause damages, but the act is criminal only if the created computer viruses are used and damage has been done. Because today thousands of computer viruses are created but most of them are harmless, some are funny, some irritating.

.Takeover, as in undertaking a computer virus as a program with the intent of using it, specifically to be inserted in certain computer network or computer system to cause damage or by destroying certain computer data that causes functioning problems, loss of significant data etc.

.Usage, meaning the culprit doesn't program the virus, he only uses it, the previous criminal acts are done by another culprit and have the same criminal aim. However, in certain cases the program can also be ordered with a specific intent as a final product to be created and installed with intent for further use.

.The production, takeover and the use of computer viruses more and more are becoming an organized criminal activity with the purpose of causing enormous material damages and even more the culprits with their programing and usage tend to gain high criminal profit, the purpose of those criminal acts is "criminal profiting".

. Because of the increasing business competition more and more companies acquire and use computer viruses, a juridical liability is stipulated for legal entity when the act is done by any employee employer or other responsible person in the company on behalf and at the expense of the legal entity [13].

The computer crime with elements of creating and importing a computer virus in the scientific and professional literature can be referred as computer or logic sabotage. This type of sabotage includes deleting; damaging or modifying the data, programs or parts of the operating system which is mostly done by using standard service programs, personal programs or techniques like logic bomb or virus. The saboteurs have various motives with political, economic, military, official or other private character [14]. The computer sabotage affects the competition in the economic – financial sphere, reduces market safety and the goal is unlawful gains via creation of uncompetitive market conditions especially in the uprising the e-market who becomes more popular in profit creation.

CASE ANALYSIS

In July 2015 in the Republic of Macedonia a successful action for preventing a computer criminal was conducted in which two Macedonian citizens were involved. The action was conducted in cooperation with FBI and culprits from 20 different states of different continents were arrested. The criminal action had been unwinding via the web page "Darcode" which actually was a forum used by 300 users that could have been accessed only by a recommendation from a previous forum member. The forum was used for sharing and selling stolen data, tools and information as well as details for security flaws and instructions how to use them. Software and other products were bought through this forum which was later used for stealing information from computers and cell phones. The Macedonian culprit during 2011 used malicious software to obtain bank information from foreign citizens via Internet to buy various luxury items but most of the bank information were sold to other internet pages created for selling illegally obtained bank information from credit cards. The money obtained by selling bank information from credit cards on Internet were withdrawn via the "Western Union" fast money transfer service and the money were deposited by people from Mexico, Russia, Lebanon, China, USA and other. According to the financial investigation he illegally obtained assets in the amount of 82.000$. This criminal activity included a culprit from Skopje who wasn't arrested because the person joined the jihadists in Iraq. The Macedonian police within the frames of the operating action have undertaken multiple legal actions in cooperation with the public prosecutor. During the search many computers, cell phones and other computer equipment were seized and given to processing to extract electronic evidence and to prepare them for a criminal procedure against the suspect perpetrator. The police action is supported by the European center for computer criminal of Europol as well as the police officials in 20 states. The preliminary investigation of collecting and exchanging data lasted 18 months and besides the Macedonian there were other hackers from Serbia, Bosnia and Herzegovina and Croatia. 28 people were arrested, 12 of them from USA. This police action helped to destroy a "cyber layer" of hackers who according to the prosecutor David Hickmon form USA have done some serious damage measured in billions of dollars and with too much casualties. EUROPOL actively participated in the investigation and its director Winehart stated for the media that "this global action caused serious damage to the grey economy and represents a reminder that these types of private forums are no sanctuary for the criminals because they as well can be caught by the long hand of the law; the police units will continue to work in order for the cyber space to be criminal free and be safer for all the people in the world". 12

culprits from USA were involved in this criminal action, one of them known on the forum as “Dendroid” where he was stealing data from phones who used the Android operating system. One of the arrested, via malicious software was spreading spams on the social network Facebook in order to contaminate user’s profiles, another infected millions of phones via spam messages, another was selling botnet access to the “Darcode” forum while the 27 year old D.P. from Wisconsin is one of the people who participated in the conspiracy for the creation of that criminal forum. The youngest associate in this criminal operation was an 18 year old Englishmen who was hacking the networks of “Sony Play Station” and “X-box.

ELECTRONIC QUESTIONNAIRE

An electronic survey on theme "Security of computer data from computer viruses” was made in a period of 24 hours. Ten questions were systematized, e-survey is designed so that the answers of the first hundred people who accept the questioner and answer the questions are going to be accepted. The questions and the possible choice of answer are enclosed below.

1. How much do you know about computer viruses?

□ Sufficient □ Little □ Do not know at all

2. Have you ever had a problem with a computer virus?

□ Yes □ No □ Do not know

3. Do you know what are the consequences of computer viruses?

□ It destroys and damages the data □ It damages the hardware □ Do not know

4. Do you know how a computer virus is transmitted?

□ Through memory USB, CD, DVD, Internet, computer network, via e-mail

□ When the computer is adjacent to another infected computer □ Do not know

5. Which files and parts of the computer system cannot be infected by computer viruses?

□ Viruses cannot infect compressed files, computer hardware (keyboard, mouse, etc.) □ E-mail □ Do not know

6. Is it creating and importing of computer viruses a crime?

□ Yes □ No □ Do not know

7. Are Macedonian law enforcement professional in dealing with cybercrime/computer viruses?

□ Yes □ No □ Do not know

8. Does the computer virus can intercept and destroy data in cyberspace?

□ Yes □ No □ Do not know

9. Does the creation and importing of a computer virus may facilitate the acquisition of material benefit?

□ Yes □ No □ Do not know

10. Is there an absolute protection against computer viruses?

□ Yes □ No □ Do not know

The results of the survey are shown in the chart below.

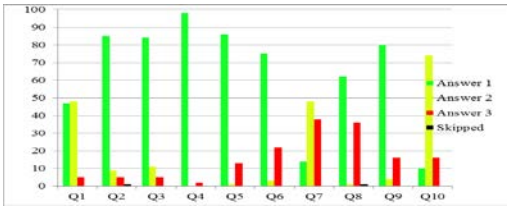

Fig. 1. The security of computer data from computer viruses

As you can see from the chart, the perception of respondents is that enough (47%) or somewhat (48%) know about computer viruses, 85% have ever had a problem with a computer virus, and most, i.e. 84% of respondents know that computer viruses destroy data. Also, 98% of respondents believe that computer viruses are transmitted via USB memory, CD, DVD, internet, computer network and via email. The perception about what can not be infected with a computer virus is satisfactory,so 86% of the respondents replied that viruses can not infect compressed files, computer hardware (keyboard, mouse, etc.). In 75% the respondents know that making and introducing computer viruses is a crime. But, according to their answer to the seventh question they express doubt in the expertise of the Macedonian law enforcement to deal with this type of criminal activity, by answering "No" (48%) and "do not know" (38%) confirm their suspicion. In terms of security of computer data in cyberspace, polled with 62% responded that it is possible with special viruses that have been specially programmed for that purpose, but 36% responded that it is a problem about what they do not know whether it is possible or not. With the positive respons (80%) to the ninth question, there is an impression that the respondents believe that the creation of special programs of computer viruses, enable acquisition of unlawful gains.The respondents perceive that there is no absolute protection against

computer viruses, that proof the answer to the last question to which 74% answered that there is no absolute protection against computer viruses.

CONCLUSION

The Republic of Macedonia has accepted the recommendations of the international legal acts and specific crime "Creating and introducing of computer viruses" have been incriminated in the Criminal Code. It's about a complex crime giving the method of execution, the necessary expertise for the creation of computer viruses in terms of the purpose of the virus itself. Macedonian criminal practice has seen criminal cases with elements of computer crime, the creation of computer viruses with an international character. In this context a case from the practice is analyzed. In terms of research on how the public is aware of this issue an online survey was made, in a short time the questionnaire was accepted and answers received according to which it can be concluded that: In Macedonia the public, i.e. the citizens are familiar with the problematic of computer viruses, they know that it is a dangerous criminal phenomenon, but also there is doubt in the professionalism of Macedonian law enforcement. According to the analysis of the criminal law, the incompetence of the Macedonian law enforcement cannot be concluded, au contrary the analyzed case shows that the Macedonian police has experience in international cooperation in the detection, clarification and providing evidence of committing computer crimes with involvement of culprits from our country. It should be emphasized that this is a newer form of crime with newer manifestations, which have their specificities, which still need to be recognized by law enforcement operatives who will independently in the future be able to disclose with initial findings of criminal cases, but international cooperation is something that should be improved primarily because this crime has in many cases international character.

REFERENCES

[1] Brvar, B. (1982). Pojavne oblike zlorabe računika. Ljubljana: Revija za kriminalističko in kriminologijo br. 2/1982, pp. 76

[2] Јовашевић, Д. Д. (2002). Лексикон кривичног права. Београд: ЈП Службени лист СРЈ, pp.121

[3] Џуклески, д-р. Г. (2000). Најчести облици на извршување на компјутерски криминал во САД (Vol. 1/2000). Скопје: Годишник на факултетот за безбедност, pp. 70

[4] Clarke, R. (1996). Information Technology & Cyberspace: Their Impact on Rights and Liberties. Melbourne: Mietta's, pp. 96

[5] Fischer, E. A. (2005). Creating a National Framework for Cybersecurity: An Analysis of Issues and Options. CRS Report for Congress, pp. 5
[6] Петровиħ., С. (2007). Полицијска информатика. Београд: Криминалистичко полициска академија, pp. 105
[7] Петровиħ., С. (2007). Полицијска информатика. Београд: Криминалистичко полициска академија, pp. 121.
[8] http://www.dalisteznaele.com.mk/index.php/internet/347. (n.d.). Retrieved 08.04.2012, from http://www.dalisteznaele.com.mk/index.php/internet/347
[9] http://science.discovery.com/top-ten/2009/computer-viruses/computer-viruses-08.htm (n.d.). Retrieved 08.03.2012
[10] https://in.news.yahoo.com/5-most-dangerous-computer-viruses-of-all-time-113637274.html Retrieved 08.03.2016
[11] Член 251-а. (n.d.). Закон за измена и дополнување на Кривичниот законик на РМ. Сл. весник на РМ бр. 19/04 и 114/09
[12] Тупанчевски, Н. & Кипријановска, Д. (2008). Основи на македонското информатичко казнено право. Скопје: МРКПК бр. 2-3, pp. 523
[13] Николоска, С. (2013). Методика на истражување на компјутерски криминалитет. Скопје: Ван Гог, pp. 205-206
[14] Петровиħ., С. (2007). Полицијска информатика. Београд: Криминалистичко полициска академија, pp. 105