Computer Viruses as a Threat to Home Users

Dr. Waqar Ahmad
Deaprtment of industrial Engineering
King Abdul Aziz University Jeddah 21589 Saudi Arabia
Wahmed@kaau.edu.sa , wahmed@ieee.org

Abstract

The Computer virus threat is growing and home users are threatened by them, especially with the increasing dependence on computers to accomplish the vast verity of tasks in our modern lives. The popularity of internet aggravates the threat and gives the virus writers the ideal environment to distribute their viruses, since computer viruses can spread through the universe in a few hours causing distractions to hundreds of thousands of computers around the globe. An abbreviated idea about computer viruses nature, history and development, the damage caused by some well known viruses and the different types of computer viruses is explained, also virus writers types, motivations, their point of view towards ethical and legal issues, and the effect of legal penalties on their practice is explained .The threat of computer viruses towards home users is proved, some solutions to eliminate the threat of computer viruses is highlighted. Home users can protect their systems based on their understanding of the foregoing.

1 Introduction

Due to the increasing dependence on computers to achieve most of our civilized life tasks, from simple word-processing to controlling and monitoring the most sensitive organizations like nuclear reactors and performing surgical operations. Therefore the need to be dependent on computers reliability and functionality is of high concern since any failure in the computer functionality could lead to loss of human lives or costly financially losses. There are many threats to computer functionality and reliability, and computer viruses is the most commune one. The threat of computer viruses are addressed to all computer operators in homes, business, and government, home users and how they can eliminate the threat of computer viruses and protect their systems is of concern. The relation between increasing the awareness and understanding of the nature of computer viruses, and home users ability to protect their systems will be tested. In order to accomplish the foregoing this paper is structured as follows: Firstly the definition of computer viruses, their nature, their history and development, and their different types is discussed. Secondly the threat of computer viruses to home users is proved. Thirdly computer virus writers nature, motivations and their perspective to legal and ethical issues is highlighted. Fourthly, ways to eliminate the threat of computer viruses is discussed. Finally the research occlusions is illustrated.

2 Computer Viruses

2.1 What Is Meant By Computer Viruses?

"A *virus* is potentially a destructive program code that attaches itself to a host (either a file or program) and then copies itself and spreads to other hosts. It may contain a damaged routine or payload, which activates when triggered "

(Cronkhite and McCullough, 2001, p.19)

So computer viruses are codes written by some people to cause serious damage to computers, this includes private, business and government computers. Computer viruses are similar to the biological ones in their ability to replicate themselves, infecting a large number of victims and having a lifecycle. "The term 'computer virus' was formally defined by Fred Cohen in 1983, while he performed academic experiments on a Digital Equipment Corporation VAX systems"

(Dwan, 2000, p.13)

2.1.1 Virus Structure

Computer viruses could have two parts at least (search and copy routines) or more depending on how sophisticated it might be, the additional parts will give it a unique characteristic(Ludwing,2002, p.23-24):

Search routine: this routine responsibility is to find a stabile target for infection.

Copy routine: to be able to infect the target which was found by search routine, the virus must copy itself to the target and this is the copy routine responsibility.

Anti-detection routine: this could be part of the search or copy routines or it could be a stand alone routine, the mission of this routine is to avoid detection either by the user or the anti-virus programs.

Payload routine this routine vary depending on it's porous, it could be a joke, destructive or perform a useful task.

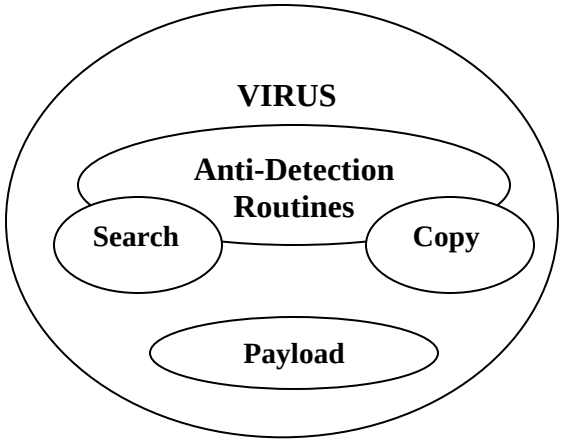


Figure 2.1: Virus Structure (Ludwing,2002, p.23)

2.1.2 Virus Lifecycle

Computer virus and biology one has a similar lifecycle, which consists of the following stages (Cronkhite and McCullough, 2001, p.19-20) :

Birth: bringing the computer virus to life, virus writer (the person who wrote the virus) designs the virus and then creates it using a programming language.

Release: in this stage the virus writer sends it out to the wild (the cyberspace, the virtual computer world).

Proliferation: the virus target in this stage is to replicate and infect as many victims as possible without drawing any attention.

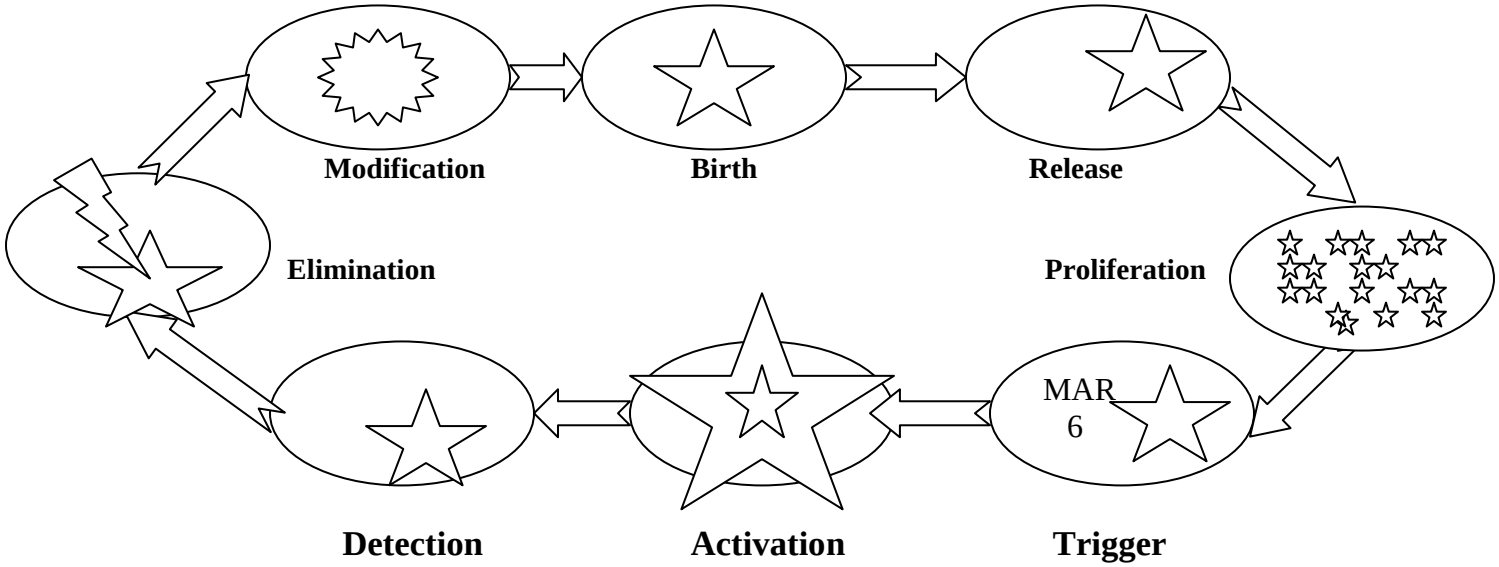
Trigger: in this stage the virus becomes alive when the trigger is reached. The virus writer usually determines the trigger, it could be a specific date, a certain task, or anything else depending on the writer's choice.

Activation: in this stage the virus has the ability to run its destructive routine. The effect of this could vary from erasing the hard disk content to making limited damage.

Detection: this could happen at any stage of the virus lifecycle, detecting the virus in the early stages makes it easer to remove it with out causing any damage. Unfortunately, real life viruses are usually discovered after they have caused havoc and damage..

Elimination: the ability to eliminate the effect of virus varies from one type to the another, and also depends on the available tools. The solution could be simple and inexpensive(e.g., deleting the virus) or complicated and expensive (e.g., reformatting and restoring the hard disk or buying a new one).

Modification: in this stage the virus lifecycle may be repeated with an improved version, this could be done by the original virus writer or some one else.



TriggerFigure 2.2: Virus Lifecycle (Cronkhite and McCullough, 2001, p.20)

2.2 Computer Viruses History and Development

Most of computer users whom have had hard times because of computer viruses want believe it's all started in 1982 as a joke by a teenager to tease his schoolmates.(Paquette,2000, p.1) Richerd Skrenta was in the 7th Grade when he got his first PC for Christmas an Apple II. He started to make use of this tool by doing something different and unexpected. "I had been playing jokes on schoolmates by altering copies of pirated games to self-destruct after a number of plays. I'd give out a new game, they'd get hooked, but then the game would stop working with a snickering comment from me on the screen " (9th grade humor at work here)"

(Paquette,2000, p.1-2)

When they noticed what was going on they prevented him from being near their disks. So, he has to think of away to bass his "booby trap" to their disks without putting his hands on them physically. "I hit on the idea to leave a residue in the operating system of the school's Apple II. The next user who cams by, if they didn't do a clean reboot with their own disk, could then be touched by the code I left behind. I realized that self-propagating programs could be written, but rather than blowing up quickly, to the extent that it laid low it could spread beyond the first person to others as well. I coded up Elk Cloner and gave it a good start in life by infecting everyone's disks I could get my hands on"

(Paquette,2000, p.2)

While Basit Farooq Alvi and Amjad Farooq Alvi seemed to have a totally different motive to write their virus. Software piracy was the software developer nightmare, so they started to think of a way to protect their effort from being lost.(Paquette,2000, p.2) Basit and Amjad used to run a computer store in Lahore, Pakistan. They decided to create a virus in order to inhabit the American software piracy to protect their business, and they called it (C) Brain virus. In October 1987 (C) Brain virus appeared in the University of Delaware, after one month the Lehigh or COMMAND.COM virus were found at Lehigh University in Pennsylvania, finally in December the Hebrew University at Jerusalem were attacked by the Friday the 13th virus (Highland ,1997, p.416).While in 1989 the 1260 was found on the wild as a result of variable encryption techniques, also in the same year stealth viruses (which have the ability to avoid detection by employing various techniques), such as Zero Bug, Dark Avenger, and Frodo were found in the wild for the first time (Dwan, 2000,13).

So it started to get more serious and virus writers accepted the undeclared challenge, and started to improve their malicious codes to avoid detection. In 1990 the virus writers released a virus called Whale,

which was a self-modifying virus and in 1991 GPI virus was found, the mission of this virus was to steal Novell NetWare passwords. In the same year Michelangelo was discovered in New Zealand (Dwan, 2000, p.13). It seems that this war would never end. In 1995 a new technique was found to cope with the communication revelation and internet popularity, " The first reported macro virus 'Concept', was seen in the wild by AV researcher Sarah Gordon in summertime of 1995. A set of five macros designed only to replicate, Concept's payload displays the virus author's ominous message: 'That's enough to prove my point' ".

(Paquette,2000, p.3)

Since then a new age was started and macro viruses were getting popular every year. 1996 brought Dubbed 'XM.Laroux' to life, while in March 1999 Melissa was able to infect approximately a million computers and caused $80m in damage(News.bbc.co.uk,2002, p.2). It's an e-mail message containing an infected word document in the form of an attachment addressed as an important message from a friend or college (News.bbc.co.uk,2002, p.2). A month later Chernobyl strain CIH hits around 540,000 computers in Turkey and South Korea, the purpose of it's payload was to reformat the hard drive and zap a key chip on the computer motherboard (Dwan, 2000, p.14). The increasing dependency on the companies networks or the internet to exchange documents using e-mails on a daily basis gave the macro virus a stabile spreading environment and made them the best example of convoying each age requirements.

In the year 2000 a new Millennium had just started and its seemed that the virus writers quiver is still full of surprises. It was an irresistible attractive message containing a love letter "Love Bug". All the user had to do in order to infect his system and automatically send copies of the virus to everyone on his e-mail address book was to open the attachment (Ruppe,2000, p.1). The "I LOVEYOU" virus caused havoc and damage to private, business, and government computers throughout the globe starting from Asia, Australia, Europe to North America (Ruppe,2000, p.1). The Asian Dow Jones's computers crashed and the Asian Wall Street Journal were struck, around 30% of British and 80% of Swedish companies e-mail systems were affected, finally in the U.S. at least 350,000 files were found hit (Ruppe,2000, p2-3). In 2001 Pentagon and the White House were forced to halt the public access to their Web sites for a limited period and 250,000 systems were infected in nine hours due to the "Code Red" worm, which was able to infiltrate hundreds of thousands of computers shortly after its first identification on July 19th (Stenger,2001, p.1). Virus writers were determined to prove their capability to threaten the world by releasing new viruses. In 2002 the top of the virus chart was Klez virus, which was able to have more then five million copies (advisor.com,2002, p.1).

Nevertheless we can say that the malware(short form of malicious ware) was started by releasing viruses in the wild, regardless of the virus writers motivations or intentions to write these viruses. When software developers started to notice the need for developing programs to protect computers from viruses, the malwar started between the virus writers and the antivirus companies.

2.3 Types Of Computer Viruses

Every year computers technology developers surprise the world with their new inventions, therefore virus writers need to create new generations of viruses to cope with the latest computing techniques. As a result of this competition each year hundreds of new viruses are found in the wild.

In this paragraph five different types will be discussed depending on (Cronkhite and McCullough, 2001, p.21-23) categorizations:

File-infecting virus: this virus technique is to attach itself to the executable files, which are the files ending with .exe, .com, .all, and .drv , and these are the main program files and drivers. If any of them is infected the virus code will be executed during the run first by loading itself to the memory and deceive the user by allowing the program to execute normally. When the user runs any other applications, the virus replicates itself in order to be attached to that application. The virus should remain undetected until trigger is reached and this depends on the virus writer choices.

Boot sector virus: this virus loads itself to the boot sector of the floppy disk or master record of hard disk in order to be loaded to the memory before the operating system is loaded. As soon as the virus becomes residence it will be able to infect each inserted disk to that computer.

Macro viruses: the macro language technology was invented by software companies in order to automat repetitive tasks. This virus depends on the macro language in order to infect the data files by attaching themselves to the global template and spreads when the data files is opened. So as we can see virus writers took advantage of a new invention and developed a stabile viruses for each age. These types of viruses are categorized as dangerous ones, because they are easy to write, spread easily, and its hard to eradicate them. The macro viruses effect could be an annoying massage, adding password protection to files, saving files as templates instead of saving them as documents, or moving and replacing the text randomly.

Script virus: this type of virus is written using script languages, they spread and infect files by taking advantage of vulnerabilities in the Microsoft Windows operating systems, opening e-mails or accessing Web pages which includes tainted scripts will activate the virus. This type of viruses has the ability to change its signature each time the virus is reproduced in order to remain undetected by antivirus software.

Polymorphic virus: this virus has the ability to change each time it replicates using different encryption

routines through its additional unique mutation engine. As a result of this invented combination the virus is very difficult to detect. One Half is an example of this virus, it has a distractive effect, its target is to encrypt the hard disk and make it unreadable, another example is Satan Bug.Natas which specialized in attacking the antivirus software.

Virus writers are so keen to cope with the technology development, each time antivirus software and software developers come up with a new technology to prevent computer viruses infection, virus writers find their way to surprise the world with a new threat by releasing the suitable virus for each age.

3 Are Computer Viruses A Threat To Home Users?

By the end of the 2nd Millennium computers have become an essential tool to every individual regardless of age or position. Computers have been used to perform a vast variety of operations, from simple word processing to sophisticated industrialization. As a result of these capabilities computers are a vital constituent of a modern home – nowadays computers have the same importance as TV and telephones in order to have an ideal modern home – since all of the family members need it to accomplish different tasks depending on their needs. In most cases the whole family shares the same computer. As a result of this strong interference of technology in peoples life, any failure in the computer functionality can result in serious effects. Computer viruses are one of the most common threats which threaten the computers functionality and reliability.

Home users represent a large portion of computer users today and since the families members are from different ages, positions, and computing back rounds, computer viruses have an ideal environment to rise. Whenever computer users vary in their computing knowledge the possibility of keeping this computer from being damaged for any reason is significant.

By comparing the increasing number of home users with the increasing number of computer viruses each year, we can easily realize the growing threat of computer viruses towards home users. “ By 1988, there were about 20 will known and widely spread computer viruses, in early 1990, the IBM high integrity research laboratory reported over 125 unique viruses detected in the environment (White,1990 cited Cohen, 1991), and by March of 1991, between 200 and 600 unique real-world viruses were known in the research community(Brunnstein,1991cited Cohen, 1991)”.

(Cohen,1991, p.1)

In 2002 more than 237 new viruses were found on the wild and this figure is nominated to rise throughout 2003 (advisor.com,2002, p.1).Considering the foregoing figures, the computer viruses threat is growing each year and needs more preparations from the operators and developers to face its harmful effects.

4 Computer Viruses Writers

4.1 Computer Viruses Writers Types

There are four different types of virus writers according to(Gordon,1994, p.9) categorizations :

The Adolescent: their age is between 13 and 17 , they should have written one computer virus at least, should have released at least one computer virus to the wild.

The College Student: their age is between 18 and 24 , they should have written one computer virus at least, should have released at least one computer virus to the wild. They should be students at university or studying classes at university level.

The Adult/Professionally Employed: they could be post-college or adults, professionally employed, they should have written one computer virus at least, should have release at least one computer virus to the wild.

The Ex-Virus Writer they should have written and released one or more computer viruses. Their viruses should have been found in the wild; they have to prove that they have not written or continued to write viruses for the last 6 months.

The previous categorizations depend on the age and education level. To classify virus writers in different groups in order to understand them and know more about their motivations to write and distribute computer viruses in to the wild.

4.2 The motivations of Computer Viruses writers

With the industry revelation people become materialistic and most of the human morality disappeared. The main target of most people is to achieve the dream of the luxurious life, bearing in mind the stars lives usually seen on movies or on TV programs which show the luxury of rich and famous people or simply seeing them on the streets driving expensive cars and wearing brand names clothes. Obviously the real world is so different. Most of our universes population suffer due to poverty and are unable to cover their basic needs. In some parts of the world millions of peoples live under the poverty line without getting any help from their governments or society. The logical result of this situation is to have some social resentment, which leads to secrete individuals whom looking forward to get their revenge from the unfair world in which they live. Their revenge could take many forms, writing and releasing computer

viruses is one of them. In addition computer viruses is a very effective tool for accomplishing their goals especially with the communication revelation. Viruses can spread around the universe in a few hours causing destructive damage to millions of computers among homes, businesses, and governments. “Virus writers’ motivations are generally located in the field of social resentment, fear of rejection, getting attention and revenge or identifying with a certain group”

(Opera,2002, p.2)

With a quick review of the tasks preformed by computers in our modern lives and how much we do rely on them to store our sensitive information like medical and social security, monitoring and running factories, guiding transportations facilities from trans to aircrafts on their domestic and internationals journeys, accomplishing almost all the financial transactions, and carrying our letters and messages (Skoudis,2002, p.2), we can imagine the effect of any failure in computers functionality. The effect of computer viruses could be very costly financially and some times incurable when it comes to human lives.

To conclude virus writers could be motivated by the need to express their dissatisfaction with their social level, drawing attention, being famous and well known. To achieve their revenge, or to prove their technical skills as klez.E writer aimed, it’s clearly stated in his message which was as follows “I’m sorry to do so, but it’s helpless to say sorry. I want a good job, I must support my parents. Now you have seen my technical capabilities. How much is my year-salary now? No more than $5,500. What do you think of this fact? Don’t call me names, I have no hostility. Can you help me?”

(Opera,2002, p.3)

4.3 To Which Extent Computer Viruses Writers Make Consideration To Ethics?

According to the study of (Gordon,1994) in which she has examined the ethics of virus writers using Kohlberg’s ethical model, the observation shows that the virus writers are not a homogenous group, since they vary in age, education level, economical level, background, manner of communication, perspective of their society, and have different preferences. All of the foregoing will lead to different modes of thinking and different motivations behind their behavior.

The adolescent and college virus writers are within the norms of their age group of the ethical development model, the reason for their behavior in writing and releasing viruses were unclear according to the collected information, and ‘The Enemy’ seems to be virtual one (Gordon,1994, p15). While adult virus writers seem to be under the norm for their age group of the ethical development model, and ‘The

Enemy' seem to be "Society" (Gordon,1994, p.15).It seems that virus writers desire to accomplish their goal conceals their vision from viewing the ethical issues, another reason could be their dissatisfaction with the society, since the ethics belong to it, and they want revenge against every thing in their society including the ethics.

4.4 What Is The Impact Of Legal Penalties On The Practice Of Computer Viruses Writers?

As with any new crime the society and authority take some time to perceive computer crimes or cyber crimes and start to create suitable legal codes for them. "The Council of Europe addressed the issue of computer crime in its recommendation R (89) 9.This recommendation provided a minimum list of computer crime laws, which all countries should enact"

(Hannaford,1995, p.10)

Most countries around the world have established legal codes for computer crimes and some of the will known viruses writers get caught and some of them are spending their sentences. David Smith the creator of Melissa virus pleaded guilty in Federal Court and must spend five year in prison and pay $250,000 fine (computer crime.gov,2001, p.2). He also pleaded guilty in Superior Court in Freehold and is facing the sentence of ten years in prison and $150,000 fine(computer crime.gov,2001, p.2). After Melissa virus hundreds of new viruses were found in the wild, so the legal penalties aren't deterring virus writes, but it seems to be the other way around. The difficulties encourage the writers to accept the challenge of writing and releasing a virus to cause the maximum destruction and get away or cause serious damage and be famous after being caught.

5 How Can Home Users Eliminate The Threat Of Computer Viruses?

Home users are not a homogeneous group, since they are from different ages, backgrounds, education levels, and computing experiences, this is the case in almost all homes. Unfortunately this non homogenous group usually shares the same computer. All family members should practice save computing in order to eliminate the threat of computer viruses. To accomplish this goal home users have to know their enemy by increasing their knowledge about computer viruses, antivirus software, firewalls, practice save computing, getting answers from security sites (e.g., Symantic.com, securityfocus.com), and finally take all the security cautions to protect their systems. "Computer users and systems managers must ensure that their computer systems are secured and that basic IT security principles are followed. Should a home owner who leaves his front door wide open receive much sympathy if his house is burgled? Most

would say no. Should a computer system operator receive any sympathy if his system is damaged when it is wide open to intruders with no computer security in place?"

(Hannaford,1995, p.14)

6 Conclusions

The number of computer viruses found in the world is increasing each year. Every time software and antivirus software developers invent new technology to prevent virus infection, computer virus writers thrilled the world with their ability to go around the new technology and develop the right virus for each age. Macro viruses were their ideal proof of their intention to accept the challenge and cope with the new technology developments. Script viruses were another prove, they have the ability to encrypt each time its reproduced to have a different signature in order to deceive the antivirus and remain undetected (Cronkhite and McCullough, 2001, p.22-23). The antivirus developer's reaction to this challenge is to develop their programs to detect the pattern in the decryption of the virus, virus writers reaction was creating polymorphic viruses (Cronkhite and McCullough, 2001, p.23). So the malwar will go on between software and antivirus software developers and virus writers.

Computer virus writers are not a homogenous group, their motivations could be the need to express their dissatisfaction with their social level, draw attention, become famous and well known, to achieve their revenge, or to prove their technical ability. It seems that the virus writers desire to accomplish their goal conceals their vision from viewing the ethical and legal issues. Another reason could be their dissatisfaction with their society, since the ethics and legal codes belongs to it, and they want revenge for everything in their society including the ethics and legal codes. The legal penalties are not deterring virus writers, but seems to encourage the writers to accept the challenge of writing and releasing a virus to cause the maximum destruction and get away with it or cause serious damage and become famous.

By comparing the increasing number of home users with the increasing number of computer viruses each year, we can easily realize the growing threat of computer viruses towards home users. The increasing awareness of computer viruses and basic IT security principles will help home users to eliminate the threat of computer viruses.

7 References

advisor.com.(2002)

http://www.e-businessadvisor.com/Articles.nsf/dp/29DD4BBF288F4FD488256C7C00610777

Accessed 28th Apr 2003.

Cohen, F.B. (1991). "Trends In Computer Virus Research"

http://www.all.net/books/integ/japan.html Accessed 26th Apr 2003

computer crime.gov(2001)

http://www.usdoj.gov/criminal/cypercrime/melissaSent.htm Accessed 5th May 2003.

Cronkhite, C. and McCullough, J. (2001) *Access Denied :The Complete Guide to Protecting Your Business Online.* Osborne: McGraw-Hill..

Dwan, B.(2000) "The Computer Virus — From There to Here.: An Historical Perspective" *Computer Fraud & Security*, 2000(12),pp. 13-16

Gordon, S. (1994). "The Generic Virus Writer"

http://www.research.ibm.com/antivirus/SciPapers/Gordon/Generic Virus Writer.html

Accessed 4th May 2003.

Gordon, S. (2000). "Virus Writer: The End of The Innocence"

http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.htm Accessed 27th Apr 2003.

Hannaford, C. S.(1995) "Can computer security really make a difference? ", *Managerial Auditing Journal*, 10, (5), pp. 10-15

Highland, H.J.(1997) "A History Of Computer Viruses — The Famous `Trio' ", *Computers & Security*, 16, (5), pp. 416-429

Ludwing, M.A. (2002) *The Little Black Book of Email Viruses* . Panama City: Lexington & Concord Partners, Ltd.

News.bbc.co.uk. (2002). "Melissa virus creator jailed"

http://news.bbc.co.uk/1/hi/word/americas/1966371.stm. Accessed 28th Apr 2003.

Opera, L. (2002). "The Klez Fever"

http://www.maclx-rz.uibk.ac.at/~maillists/focus-virus/msg01309.shtml Accessed 4th May 2003.

Paquette, J. (2000). "A History of Viruses"

http://www.securityfoucus.com/infocus/1286. Accessed 13th Apr 2003.

Ruppe,D. (2002). " 'Love Bug' Travels the Globe"

http://abcnews.go.com/1/sections/world/Daily News/Lovebug000503_world.html.

Accessed 28th Apr 2003.

Stenger, R. (2001). "Net braces for stronger 'Code Red' attack"

http://www.cnn.com/2001/TECH/internet/07/30/code.red/ Accessed 28th Apr 2003

Skoudis, E. (2002) *COUNTER HACK A step-by-Step Guide to Computer Attacks and Effective Defenses.* New Jersey: Prentice-Hall PTR.