*Journal of Zankoy Sulaimani (JZS), Part A, Dec. 2001, Vol. 4, No. (1), 45-50*
گۆڤاری زانکۆی سلێمانی/دیسمبر ۲۰۰۱، بەرگ ٤ ژمارە (١) بەشی A

# Parasitic Computer Viruses

**Amera. I. Melhum* (Assist.Lecturer)** **Susan A. Mahmood**(Assist.Lecturer)**
*Dept. of Physics , University of Duhok.
** Dept. of Computer , College of Science, University of Sulaimani

***Kurdistan Region - Iraq***

## ABSTRACT

*A computer virus is a piece of self-replicating code, that is code which can make copies of itself in such a way as to infect parts of operating system or environment.*

*In this study a new virus has been created "947" virus, which is a memory - resident parasitic. It is capable of infecting COM and EXE files and adds 947 bytes to the length of infected files .The Scanning & Cleaning programs has been created also.*

**Keywords:** *Computer viruses*

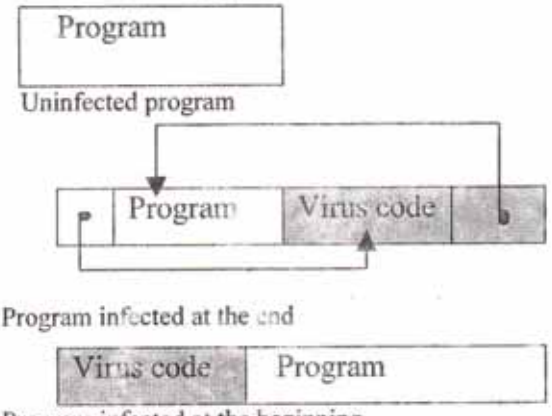
## INTRODUCTION

Computer viruses can be divided into five different types: bootstrap sector viruses (or sector viruses), parasitic viruses, multi-paratite viruses, companion viruses and link viruses. These classifications take into account the different ways in which the virus can infect different parts of the system. The manner in which each of these types operates has one thing in common: any virus has to be executed in order to operate. Each class, in effect, is simply a different way of ensuring that the virus code is executed.(1,2).

## Parasitic viruses

The large numbers of viruses are parasitic which infect executable files stored on the memory of computer. They generally leave the contents of the host program relatively unchanged. But append their code to the host, and change execution flow so that the virus code is executed first. Once the virus code has finished its task control is passed to the original program which, in most cases, executes normally. The extra execution time added by the virus is usually not perceptible, and the virus remains hidden to the user.

As parasitic viruses infect executable files they can spread through any media such as Network & floppy disk which can be used to store files, such as disks, infection usually spreads when an infected files is executed.




**(Fig.1) Program infection with a parasitic virus**

Parasitic viruses need to be able to distinguish between uninfected files and these, which are already infected. If the virus does not have this capability, it will repeatedly reinfect programs until they become either too large to fit on disk or in memory, Methods of marking infected include examing the first instruction of the program code or looking for a special infect marker which the virus uses to designate infected files (fig.1) . One common marker is the second field of the files date/time stamp set to 62. This is not noticeable by the user (as the DIR command only shows hours and minutes) but allows the virus to prevent multiple infections in the same file.(3,4)

## Instalation

When an infected program is run the virus will checks system memory to see whether the virus is already resident by using INT 21h functions 62h get program segments prefix (PSP), by calls INT 21h with value of 62h in AX register if the virus is resident the call routine returns a value of D500 in CX register and processing is passed to the host code, if not resident it alter the memory size by decreasing its value by the value of virus code (947 Bytes), the virus code is written there and becomes memory resident.

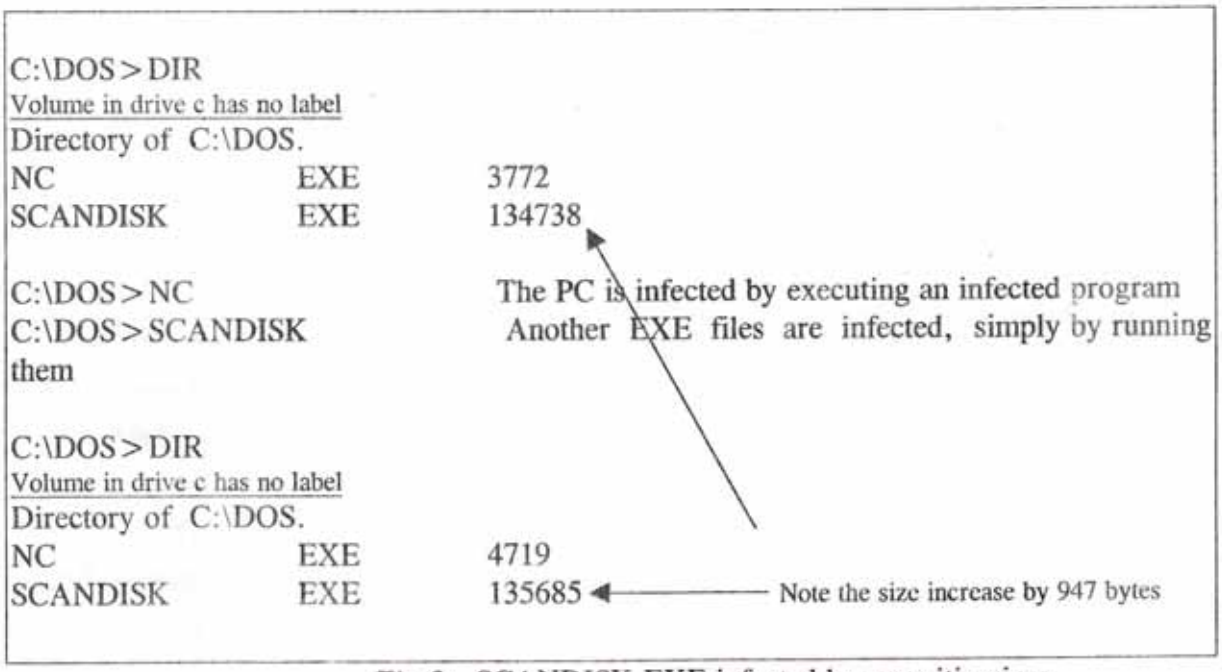



Fig.2: SCANDISK.EXE infected by parasitic virus

## Installation

When an infected program is run the virus will checks system memory to see whether the virus is already resident by using INT 21h functions 62h get program segments prefix (PSP), by calls INT 21h with value of 62h in AX register if the virus is resident the call routine returns a value of D500 in CX register and processing is passed to the host code, if not resident it alter the memory size by decreasing its value by the value of virus code (947 Bytes), the virus code is written there and becomes memory resident.

When the virus is memory-resident it intercept the main DOS interrupt INT 21h, function 4B00h (load and executes) and function 62h all other cases control is passed directly to the original INT 21h.

It also hooks INT 24h to prevent the standard DOS error message while writing to write-protected disks. The reason for intercepting INT 24h (critical error handler) is obvious – otherwise the familiar "Abort, Retry, Ignore " message would appear whenever the virus tried to infect a program on a write-protected diskette.

## Infection

Virus ' 947' infect program when it receives a load and execute request (INT 21h, function 4B00h) when such a call is made(fig.2). The virus code gains controls and starts by checking whether or not the target file has the extension EXE, it reads the first two bytes and checks to see whether they are 5A4Dh (which represent the ASCII characters MZ virtually all files in the executable format start with 5A4Dh.

The virus code is written to the end of a file. In the case of a COM file the first three bytes are overwritten with a JMP into the virus code. EXE files are modified in a different way by changing the information in the header including the initial CS and IP value to value of the address virus code.

As might be expected, The virus removes the read only attribute before infecting file and restores it after ward.

## Detection

The virus has an infect COM file for only once time but it infect EXE file to many time. And increasing the size file by 947 bytes.

Call INT 21h function 62h with CX = 00D5h returns D500h in CX.

## Virus"947"Scanning and Cleaning

The program checking files from the virus by searching the sequence code of virus and this code as follows:

E8 00 00 5E 81 EE 03 01 B4 62 B9 D5 00
CD 21 81 F9 00 D5
75 03 E9 9A 00 2E 8C 9C B3 04 2E 8C 94
B5 04 2E 89 A4 B7
04 0E 17 8D A4 B3 04

If program found this code it would display message declare that file infects with virus.

The second part of program includes cleaning file from virus. First checking whether the file has extension COM. if it has it will read the first three bytes of file by using (INT 21h, function 3D02h, open file for write/read) and these are starting address of virus code and then changed to the original address of program, then deletes part of virus code by moving the file pointer to the original end of program by using (INT 21h, function 4202h, move file pointer) and all these done after removing read only attribute if file has this attribute and returning it after doing all that by using (INT 21h, function 4301h ,set/get file attribute).

If file has extension EXE the situation is different because the structure of COM program is different from EXE. EXE file consist of header (which contains the value of some registers are stored there, also the beginning address of program, and the size of header), the program returns the original values of header to its positions and then follows the same steps of COM fille.

## Discusion

You can only get a virus by executing an infected program or booting from an infected diskette. If the backups of the infected files are available the safest solution to remove the virus can be done by booting your system from a clean diskette and restore these files from the backups even though it requires a lot of work if many files are involved. It is important to keep viruses in perspective .They are but one threat to your data and programs.

## Conclusions

**Through this study it is clear that :**

1-The user can detect directly the files which are infected by the 947 virus depending on our index for this purpose through noting the increasing in the size of the files with exe & com extensions after running the files by DIR command .

2- Sometimes the size of the files will become too large to fit in memory which led to stop loading operation , this point can be taken as a good indicator that the computer infected by this type of virus, so it's necessary to shut down it .

3- The standard DOS error message " Abort, Retry, Ignore" will appear whenever the virus tried to infect a program on a write-protected diskette For that the user must keep the disk write – protected to prevent spreading this virus to the disk or other computers.

4- Increasing the execution time ,also, can be taken as another indication of infection by this virus which must be taken carefully into consideration .

5- In future work , the guard program can be prepared to prevent your PC from infection.

## References


[1] Eugeue. Kaspersky., "*Virus Analyses*", Virus Bulletin, Dec. 1995, 9-14.

[2] Berna rd p.zajac, jr., "*computer virus: can they be prevented*", *computer & security*, 1990,9(1), 25-31.

[3] Ross M. Greenberg, " *know the viral enemy*", Byte, June 1989, 275-280.

٤- عامر ابو نزار ابو علي ، فيروسات الكمبيوتر ، عمان ، الأردن ، دار حنين، ١٩٩٤

# ڤایروس مشه خورێ کومبیوتەر

أمیرە اسماعیل ملهم/ زانکۆی دهوك
مامۆستا

سوزان عبدالله محمود/ زانکۆی سلیمانی
مامۆستای یاریدەدەر

هەرێمی کوردستان- عێراق

## پـــوختـــــه

ڤایروس برتی یە بەڕ بەرنامە یە کە کو ئارمانجین خرابکرنێ هە نە ، ئارمانج ژێ ئە و کوزیانێ دگە هینیتە سیستە مێ کومبیوتەرێ، بە رنامە بن یان ماددە ودشێت پێکئینانا یە رنامێت دی راست بکە ت چنکی پتیفە دبیت وکاردکە ت ژبوزیدە کرنا قەبارە وی.

ڤە کولین لسەر ئێك ژ جورێن ڤایروسا ژلای توش بوونی‌ێ وهە ست کرنێ ب ناخوشیێ کوئە وژی ڤایروسێ بلاڤە (parasitic virus). شیا ژ جورێن ڤایروسا مشه خورێ نوێ " ۹٤۷ چێ کرێ کە ئەف ژمارەیە لبایتات ژ بۆ دوسێت چی بە چێ کرێزیدە کر. هەر وی بەرنامەیا ( Scan & Clean ) پێکئینرا.

# فیروسات الکمبیوتر المتطفلة

أمیرة اسماعیل ملهم/ جامعة دهوك
مدرس

سوزان عبدالله محمود/ جامعة السلیمانیة
مدرس مساعد

اقلیم کردستان- العراق

## الخلاصــة

الفیروس عبارة عن برنامج له أهداف تدمیریة ، تهدف الی أحداث أضرار بنظام الحاسوب سواء البرامج أو الملفات ویستطیع أن یعدل ترکیب البرامج الأخری حیث یرتبط بها ویعمل علی زیادة حجمها .

یتناول البحث أحد أنواع الفیروسات من حیث الإصابة والانتشار وتحسس الإصابة وهي الفیروسات المتطفلة (parasitic virus)، حیث استطعنا خلق نوع جدید من الفایروسات المتطفلة " ۹٤۷ "کونها تضیف العدد المذکور من البایتات الی الملفات التنفیذیة ، وتم کذلك وضع برنامج ( Scan & Clean ) الیها .

وەرگیرا لە ۲۰۰۰/۵/۱
پەسەند کرا لە ۲۰۰۰/۹/۵ دا

Received 1/5/2000
Accepted 5/9/2000