ЛАБОРАТОРНАЯ РАБОТА № 6

"Исследование работы антивируса на простейший COM вирус"

Цель работы. Исследовать работу простейшего антивируса.

Краткие теоретические сведения

Одним из самых часто используемых типов антивирусных программ являются сканер, программы сканирующего типа. Они ищут по сигнатуре, Что такое сигнатура Рассмотрим алгоритм работы простейшего антивирусного сканера, выполняющего поиск вируса в текущем каталоге.

Алгоритм работы простейшего антивирусного сканера.

1. антивирус ищет файлы только в текущем каталоге
2. в начале файл проверяется на наличие команды jmp, если она присутствует, то проверяется есть ли 7 в конце, 10байт практически из начала
3. после лечения файла, длина его будет отличаться от исходного

COM программа - Антивирусный сканер на простейший перезаписывающий COM вирус (lab32.com)

Пример антивируса приведен ниже.

```
start:
find_first:
mov ah,4Eh
lea dx,fmask
find_first_next:
int 21h
jc exit
open:
mov ax,3D02h
mov dx,9Eh
int 21h
jc exit
xchg ax,bx
mov ah,3Fh
mov cx,ds:[9Ah]
lea dx,file_body
int 21h
```

```
jc exit
lea si,file_body
mov al,priznak
cmp al,byte ptr[si+3]
jne find_next
mov ax,[si+1]
add ax,3
add si,ax                                   ;Перешли на начало вируса
push si
mov di,offset sign
mov cx,10
ravn:
mov al,[si]
cmp al,[di]
jnz find_next
inc si
inc di
loop sravn
mov ax, 4200h ;Это вирус! Лечим его
xor cx, cx
xor dx, dx
int 21h
mov ah, 40h
mov dx,old_bytes_offset
pop si
add dx,si
mov cx, 4
int 21h
jc exit
mov dx, si
sub dx,offset file_body
xor cx, cx
mov ax, 4200h
int 21h
jc exit
mov ah, 40h
xor cx, cx
```

```
int 21h
jc exit
find_next:
mov ah, 3Eh
int 21h
mov ah, 4Fh
jmp find_first_next
exit:
Ret
fmask db '*.com', 0                    ;Область данных антивируса
priznak db '7'
old_bytes_offset dw 8Ch
sign db 0E8h, 00h, 00h, 05Dh, 81h, 0EDh,
07h, 01h, 8Bh, 86h
file_body equ $
end start
```

Порядок выполнения работы

1. Набрать, скомпилировать и исследовать работу простейшего антивируса из примера.
2. Изменить его под свой вирус, сделать сигнатуру - 16 байт.
3. Добавить интерфейс с выводом сообщения о том, что файл заражен и запросом на лечение.
4. Добавить, чтобы в диалоге выводились имена проверяемых файлов и имя зараженного файла,
5. Доработать, чтобы он лечил EXE вирус из предыдущих лабораторных.

Содержание отчета по выполненной работе

Отчет должен содержать номер и наименование лабораторной работы, данные о студентах, ее выполнивших, исходные тексты разработанных программ и исполняемые файлы с ними в электронном виде и выводы по результатам проделанной работы.

Контрольные вопросы

1. Какие виды антивирусов бывают.
2. Какие методы используют антивирусы.
3. Какие функции работают с файлами.
4. Какие команды можно применять в шифровании?
5. Объясните работу предложенного фрагмента из лабораторной.