Лабораторная работа №2 часть 2

Антивирус

**Задание**

2.1. Набрать исходный текст антивируса AntiDHog (4 балла, отсутствие – минус 4 балла).

2.2. Транслировать, линковать, получить исполнимый модуль в папке HOG (т.е. в папке, где файлы уже превратились в вирусы) (4 балла, отсутствие – минус 4 балла).

2.3. **Проверить, каким образом НА ПОЯВЛЕНИЕ ЭТОГО ФАЙЛА реагирует Ваша антивирусная защита. Объяснить, почему такая реакция – ведь в тексте сигнатура присутствует. Отчёт в виде совокупности скрин-шотов. 8 баллов, отсутствие – минус 8 баллов.**

2.4. Показать в шестнадцатеричном виде содержимое файла с бывшим исходным текстом вируса, используя какой-либо текстовый редактор и отладчик – 8 баллов, отсутствие – минус 8 баллов.

2.4. Отладить и протестировать АНТИВИРУСНУЮ ПРОГРАММУ.

2.5. **Проверить, действительно ли происходит УДАЛЕНИЕ или УБИЙСТВО всех файлов папки. То есть нужно дать ответ: убивает или удаляет. Для этого с помощью ОТЛАДЧИКА td.exe ПОШАГОВО ВЫПОЛНИТЬ программу, получаемую в результате загрузки в отладчик файла Mrak.asm. Отчёт в виде совокупности скрин-шотов. 8 баллов, отсутствие – минус 8 баллов.**

2.6. Получить ПРОГРАММУ-АНТИВИРУС, КОТОРАЯ ИЗНИЧТОЖАЕТ все зараженные файлы в папке HOG И ОСВОБОЖДАЕТ ВСЮ ОПЕРАТИВНУЮ ПАМЯТЬ, ЗАГРАБАСТАННУЮ БОРОВОМ! Помнить при этом, что согласно антивируснику, УДАЛИТЬ значит удалить имя файла из реестра файлов (реально же ТЕЛО исполнимого файла, который при загрузке в оперативную память и передаче ему управления превращается в вирус, ФИЗИЧЕСКИ ПРОДОЛЖАЕТ ЛЕЖАТЬ НА ВИНЧЕСТЕРЕ). УБИТЬ – означает сделать так, чтобы ТЕЛО ПЕРЕСТАЛО ИСПОЛНЯТЬ СВОЙ ФУНКЦИОНАЛ, что в антивируснике соответствует тому, что ПЕРВОЙ ИСПОЛНЯЕМОЙ КОМАНДОЙ ДЕЛАЕТСЯ КОМАНДА int 20h!! ИЗНИЧТОЖИТЬ ОЗНАЧАЕТ (В ДОПОЛНЕНИЕ К УБИТЬ и УДАЛИТЬ) НА МЕСТО ЗАРАЖЁННОГО ФАЙЛА НА ФИЗИЧЕСКОМ НОСИТЕЛЕ ЗАПИСЫВАЮТСЯ СЛУЧАЙНЫЕ ДАННЫЕ (например, ВСЁ чистится нулями или случайными значениями). ***Результат – три файла = 32 балла за полный результат, минус 16 баллов за его отсутствие.***

2.7. Определить, что произошло с самим исполнимым модулем-антивирусником после обработки им папки HOG, выведя на экран шестнадцатеричное представление этого файла после антивирусника. 8 баллов, отсутствие – минус 8 баллов.

**Ход решения**

На всякий случай продублирую код из лекции с антивирусом:

MoveFPos macro F\_Handle, FPos

mov ax, 4200h

mov bx, F\_Handle

xor cx, cx

mov dx, FPos

int 21h

endm

PutStr macro Text

mov ah,09h

mov dx,offset Text

int 21h

endm

seg000 segment byte public 'CODE'

assume cs:seg000

org 100h

assume es:nothing, ss:nothing, ds:seg000

public start

start proc near

PutStr TitleStr

mov ah, 1Ah

mov dx, offset DTA

mov cx, 27h

int 21h

mov ah, 4Eh

mov dx, offset a\_MaskForVir

int 21h

BegScan:

push ds

pop es

mov si, FN\_Ofs

mov di, offset FName

mov cx, 13

rep movsb

mov ah, 43h

mov al, 0

mov dx, offset FName

int 21h

mov ah, 43h

mov al, 1

mov dx, offset FName

mov cl, 0

int 21h

mov ax, 3D10h

mov dx, offset FName

int 21h

mov FHandle, ax

mov ah, 40h

mov cl, 44h

nop

nop

call InfoAboutFile

call ReadSignature

cmp SignatureFound, 0

je NextFile

call KillExecutable

call RemoveExecutable

NextFile:

call CureInfo

mov ah, 4Fh

int 21h

jnb BegScan

int 20h

start endp

a\_MaskForVir db '\*.\*', 0

DTA db 43 dup (0)

FN\_Ofs equ offset DTA + 1Eh

FName db 128 dup(0)

IName db 128 dup(0)

SignatureFound db 0

SignatureArray db 14 dup(0)

VirSignature db 0CDh, 21h, 0B4h, 43h, 0B0h, 01h, 0BAh

db 9Eh, 00h, 0B1h, 0h, 0CDh, 21h, 0B8h

Int20cmd db 0CDh, 20h

FHandle dw 0

TitleStr db '+---------------------------+', 13, 10

db 'AntiDHog - antivirus example!', 13, 10

db '+---------------------------+', 13, 10, '$'

NormStr db ' - Ok', 13, 10, '$'

CureStr db ' - has been deleted!', 13, 10, '$'

ReadSignature proc near

mov SignatureFound, 0

MoveFPos FHandle, 0Eh

mov ah, 3Fh

mov bx, FHandle

mov cx, 14

mov dx, offset SignatureArray

int 21h

cld

push ds

pop es

mov si, offset VirSignature

mov di, offset SignatureArray

mov cx, 14

repe cmpsb

jnz Finish

mov SignatureFound, 1

Finish:

ret

ReadSignature endp

KillExecutable proc near

MoveFPos FHandle, 0

mov ah, 40h

mov bx, FHandle

mov cx, 2

mov dx, offset Int20Cmd

int 21h

mov ah, 3Eh

mov bx, FHandle

int 21h

ret

KillExecutable endp

RemoveExecutable proc near

mov ah, 41h

mov dx, offset FName

int 21h

ret

RemoveExecutable endp

InfoAboutFile proc near

push ds

pop es

mov si, offset FName

mov di, offset IName

NextChar:

lodsb

stosb

cmp al, 0

jne NextChar

dec di

mov byte ptr [di], '$'

PutStr IName

ret

InfoAboutFile endp

CureInfo proc near

mov ah, 9

mov dx, offset NormStr

cmp SignatureFound, 0

je ContMsg

mov dx, offset CureStr

ContMsg:

int 21h

ret

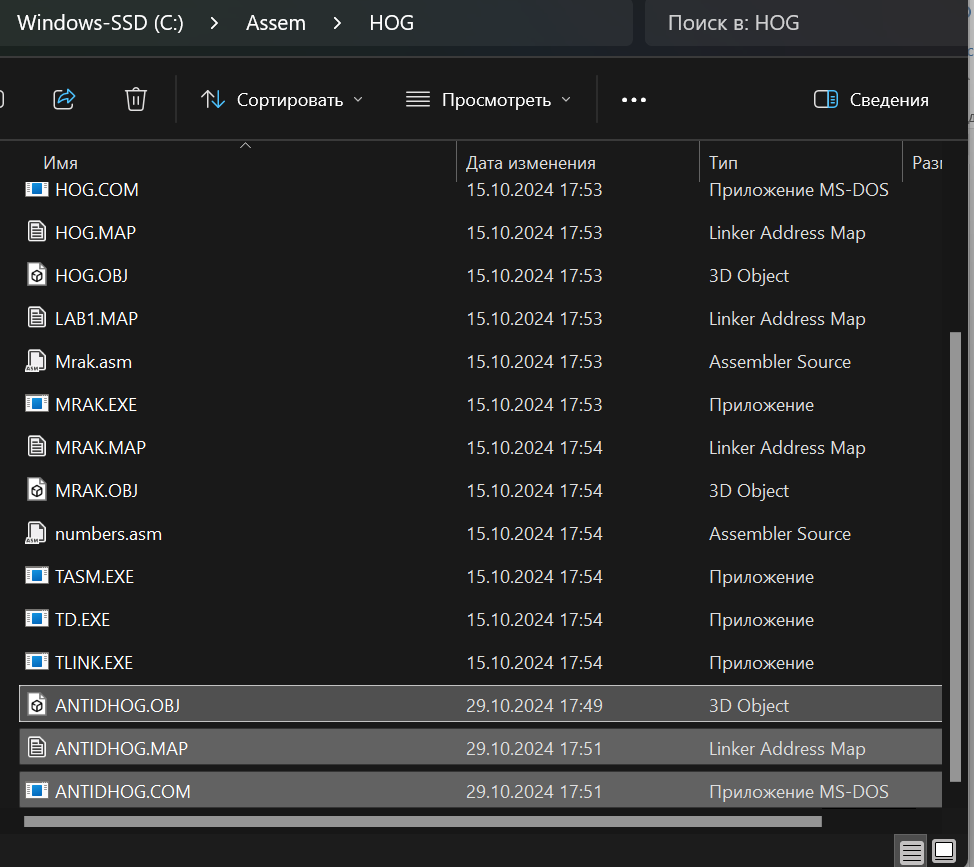
CureInfo endp

seg000 ends

end start

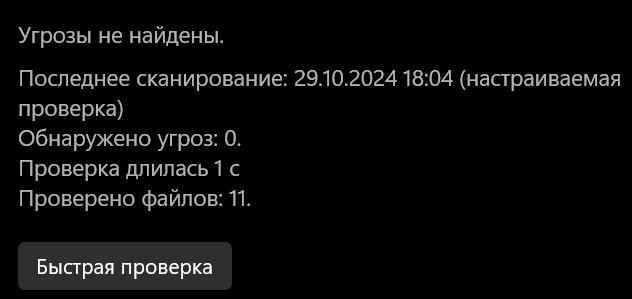
Теперь будем транслировать и линковать, используя уже известные нам TASM и TLINK.



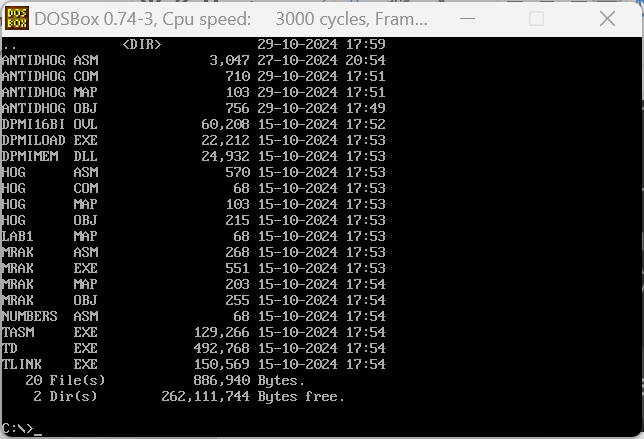


Я на картинке выделила то, что у нас создался нужные файлы.

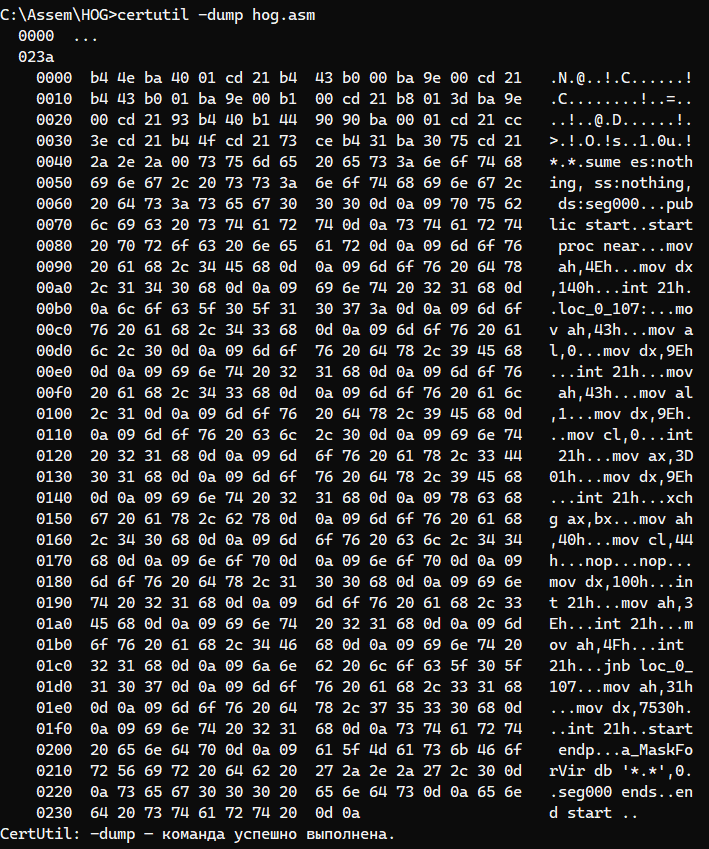
Реакция антивируса приблизительно такая:



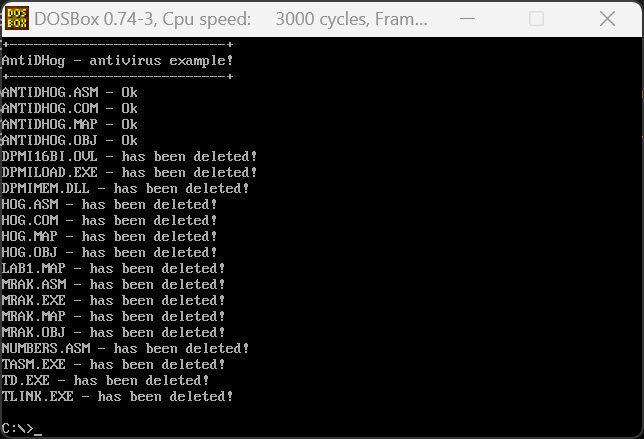
Зафиксируем, что лежит в папке до запуска антивируса:



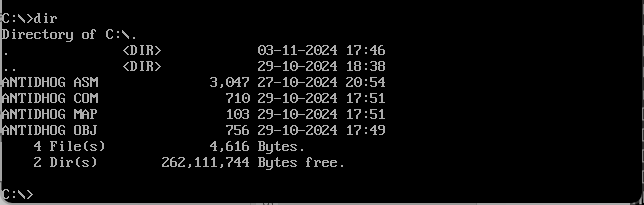
Посмотрим на наш файл с вирусом в шестнадцатеричном виде. Для этого я запустила команду **certutil -dump hog.asm** в командной строке:

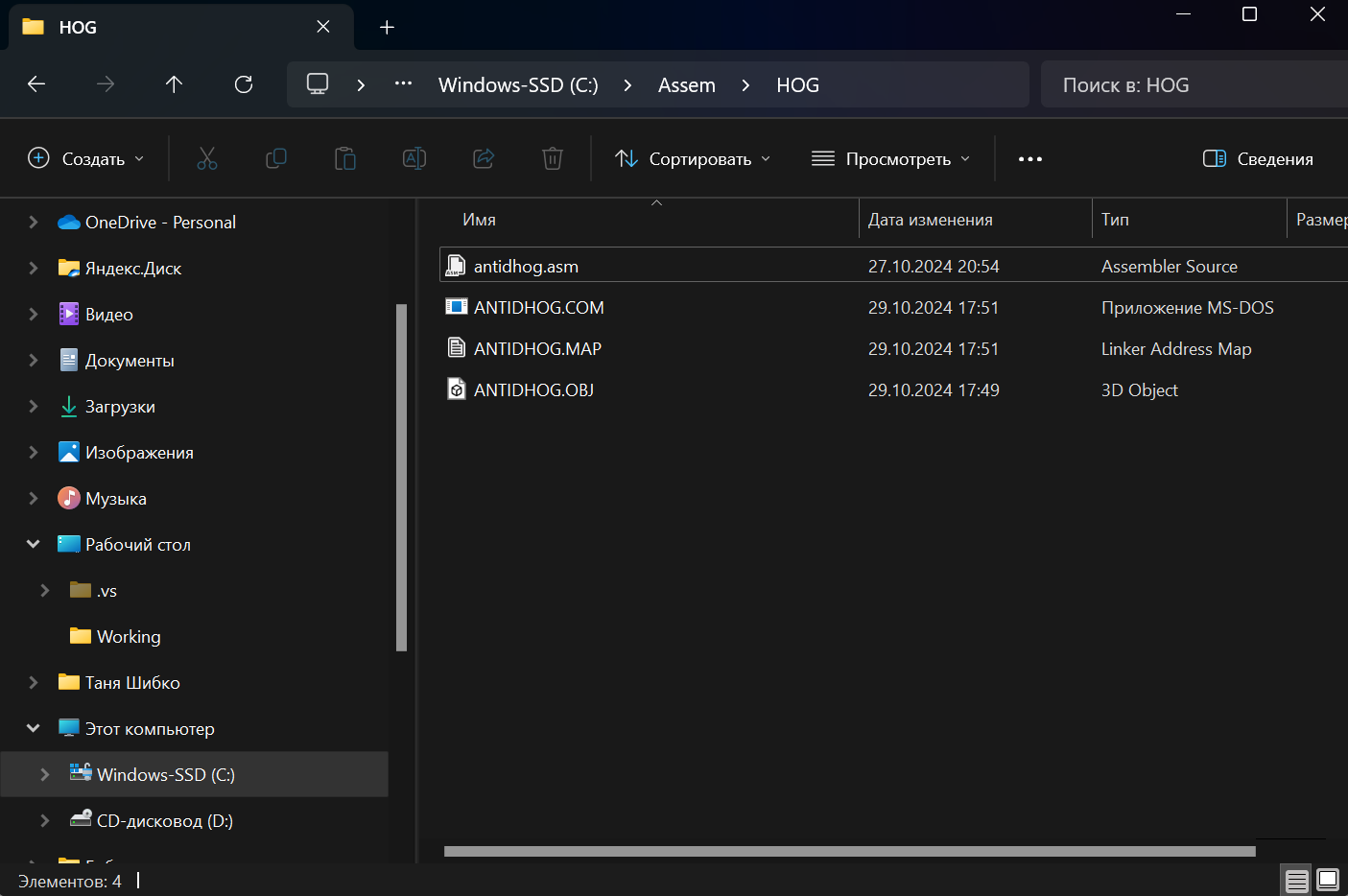


Теперь запустим антивирус.



Проверим, что лежит в папке HOG



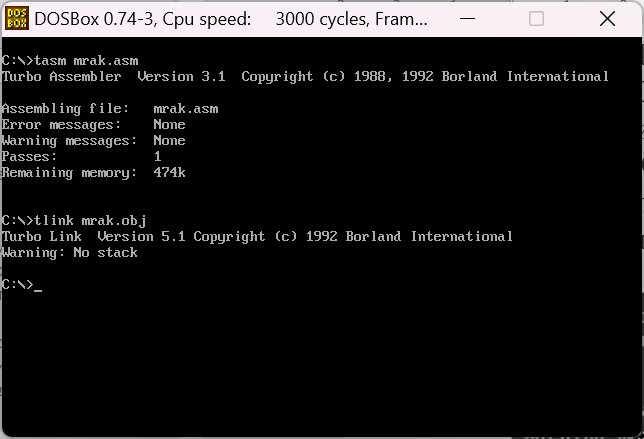


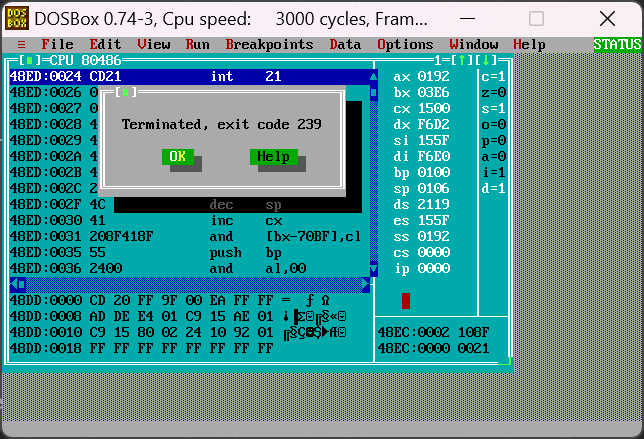
Для пункта 2.5 ещё раз внимательно почитаем определения:

*«Помнить при этом, что согласно антивируснику, УДАЛИТЬ значит удалить имя файла из реестра файлов (реально же ТЕЛО исполнимого файла, который при загрузке в оперативную память и передаче ему управления превращается в вирус, ФИЗИЧЕСКИ ПРОДОЛЖАЕТ ЛЕЖАТЬ НА ВИНЧЕСТЕРЕ). УБИТЬ – означает сделать так, чтобы ТЕЛО ПЕРЕСТАЛО ИСПОЛНЯТЬ СВОЙ ФУНКЦИОНАЛ, что в антивируснике соответствует тому, что ПЕРВОЙ ИСПОЛНЯЕМОЙ КОМАНДОЙ ДЕЛАЕТСЯ КОМАНДА int 20h!! ИЗНИЧТОЖИТЬ ОЗНАЧАЕТ (В ДОПОЛНЕНИЕ К УБИТЬ и УДАЛИТЬ) НА МЕСТО ЗАРАЖЁННОГО ФАЙЛА НА ФИЗИЧЕСКОМ НОСИТЕЛЕ ЗАПИСЫВАЮТСЯ СЛУЧАЙНЫЕ ДАННЫЕ (например, ВСЁ чистится нулями или случайными значениями).»*

В данном случае файлы у нас убивались.

Получим исполнимый файл mrak.exe и загрузим его в отладчик.

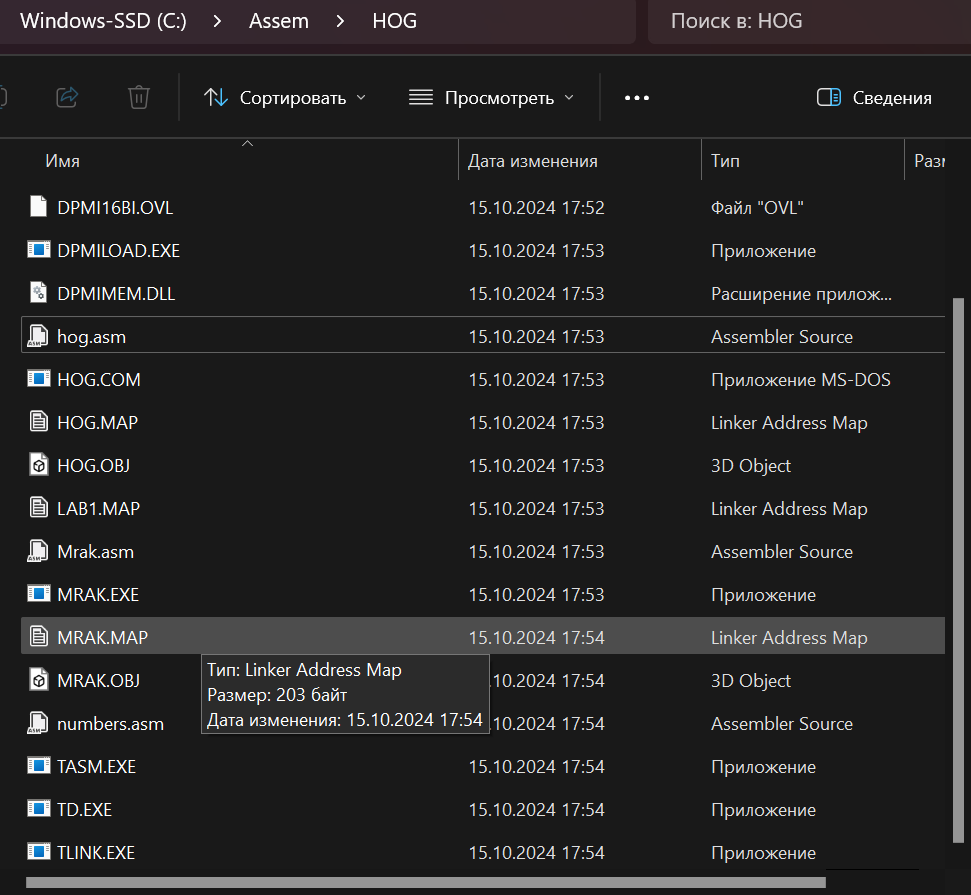




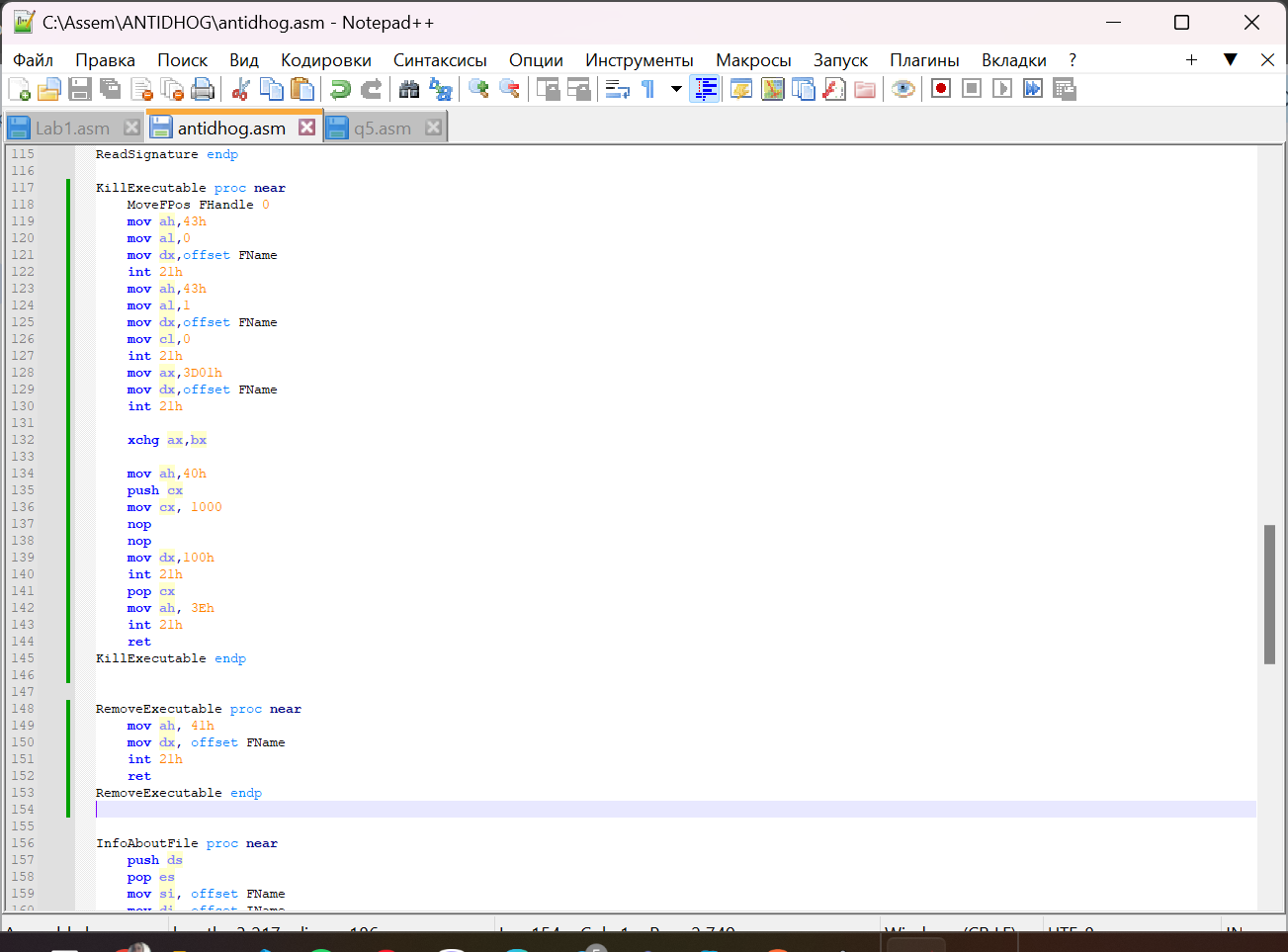
C:\Users\tshyb\YandexDisk\Скриншоты\2024-11-03_21-30-11.png

Система функционирует нормально при использовании Mrak и не зависает, что подтверждает удаление вируса и успешное выполнение функции, которая записывает 20h в начало файла.

Для пункта 2.6 я снова создала вирус в папке. Теперь нам надо немного видоизменить код антивируса.

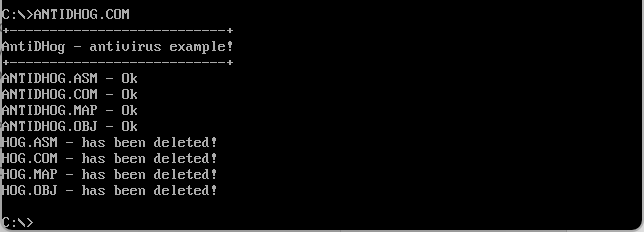


Я изменила KillExecutable и RemoveExecutable



Соберём заново исполнимый файл и запустим его.





Посмотрим, что стало с нашим исполнимым файлом антивирусом:

