Кражевский Алексей Игоревич, 4 курс 13 группа, кафедра ТП

**Лабораторная работа №2**

Постановка задачи:

Лабораторная работа №2. Часть 1.

1.1. Используя оболочку DosBox, книгу про ассемблер, текст Лекции 5 от

4.10.2023, набрать исходный текст ВИРУСА DHog68, транслировать,

линковать, получить com-файл в папке про ПАПУ.

1.2. Скопировать всё содержимое папки про ПАПУ в папку HOG.

1.3. Сделать папку HOG активной, используя исполнимый модуль td.exe

ПОШАГОВО ВЫПОЛНИТЬ программу DHog68.

1.4. Проверить, действительно ли происходит заражение всех файлов

папки. Для этого с помощью ОТЛАДЧИКА td.exe ПОШАГОВО

ВЫПОЛНИТЬ программу, получаемую в результате загрузки в отладчик

файла Mrak.asm (файл, в котором до выполнения шага 1.3. находился

исходный текст решения задачи про папу).

1.5. Проверить, каким образом НА ПОЯВЛЕНИЕ ЭТОГО ФАЙЛА.com

реагирует Ваша антивирусная защита (если пока её нет – установить любой

бесплатный антивирусник).

1.6. Используя защиту, протестировать файлы, находящиеся только в

папках DHOG и в папке про папу.

1.7. Весь процесс ЗАДОКУМЕНТИРОВАТЬ и прислать, как всегда, отчёт

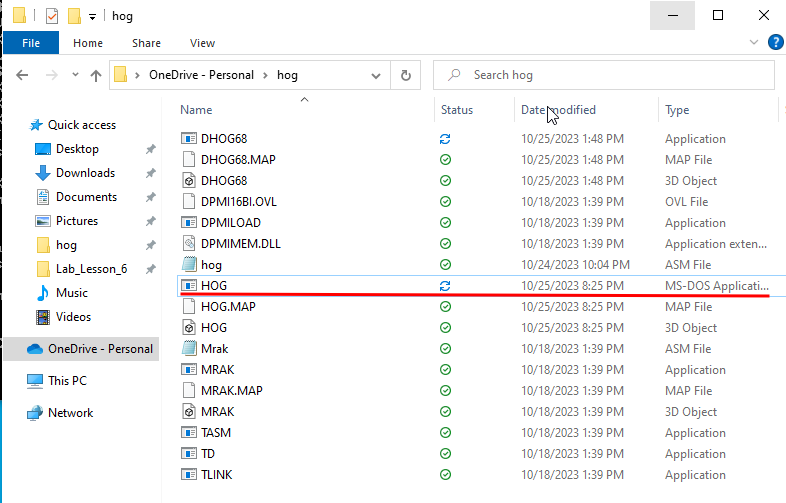
о проделанной работе в виде известных Вам трёх файлов

до 23-59 25.10.2023 года! Стоимость – 32

балла. Отсутствие – МИНУС 16 баллов.

Транслируем, линкуем и копируем:

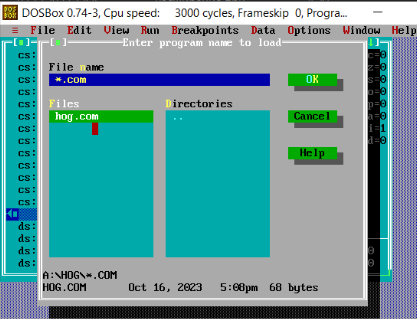




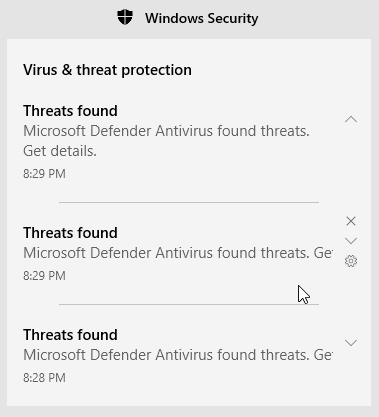
Исполняемый файл .com получен, можно продолжать.

С помощью турбо-отладчика выполняем пошагово вирус:

Загружаем исполняемый модуль

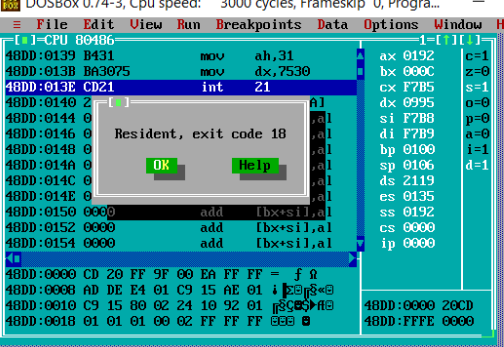


Уже на этом этапе получаем предупреждения и угрозы от антивируса

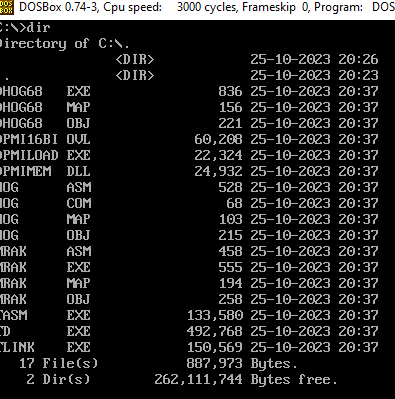


Стоит отключить антивирус, тк добавление файла в исключения не помогает.

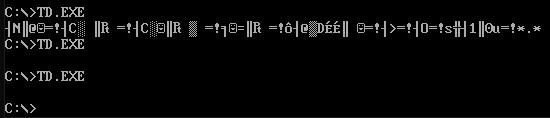
Выполняем (пошагово) в отладчике наш вирус.



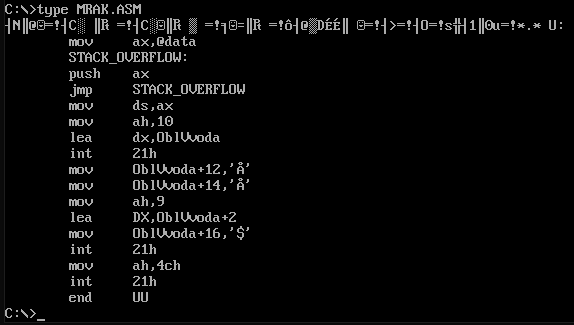
Проверяем что все файлы были изменены



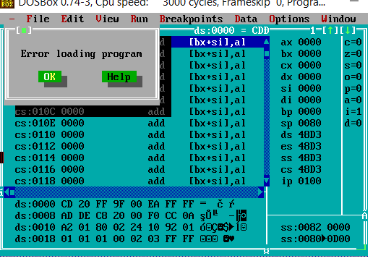
Прекрасно, теперь мы не можем запустить и отладчик



Посмотрим исходный текст mrak.ams ради интереса

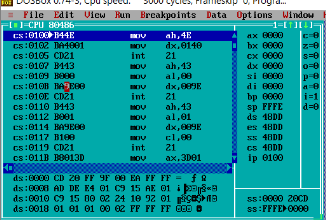


Заново копируем файл отладчика и запустим mrak.asm

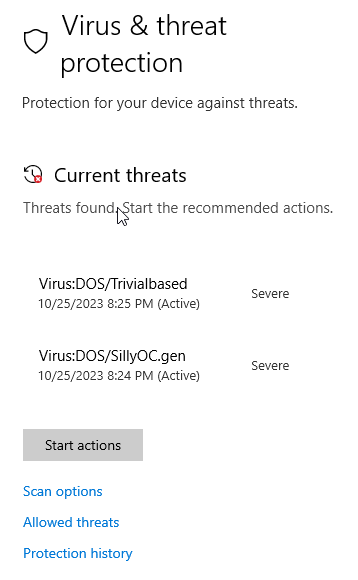


Нет, так мы сделать не можем

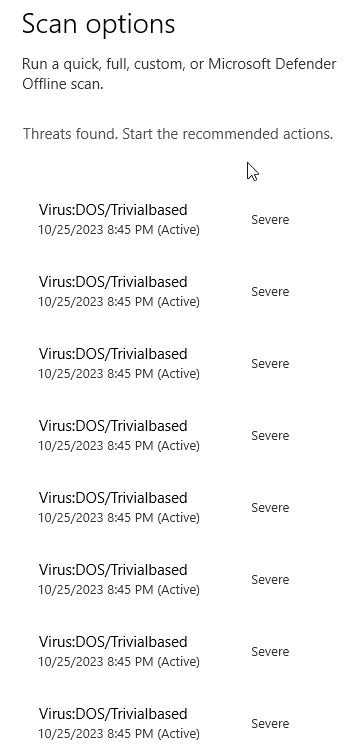
Попробуем выполнить mrak.exe, однако после определенного шага dosbox умирает



В качестве антивируса использовался Windows Defender, и он сразу говорил о наличии вируса.



Все файлы папки hog - вирусы



Во всем остальном все в порядке.