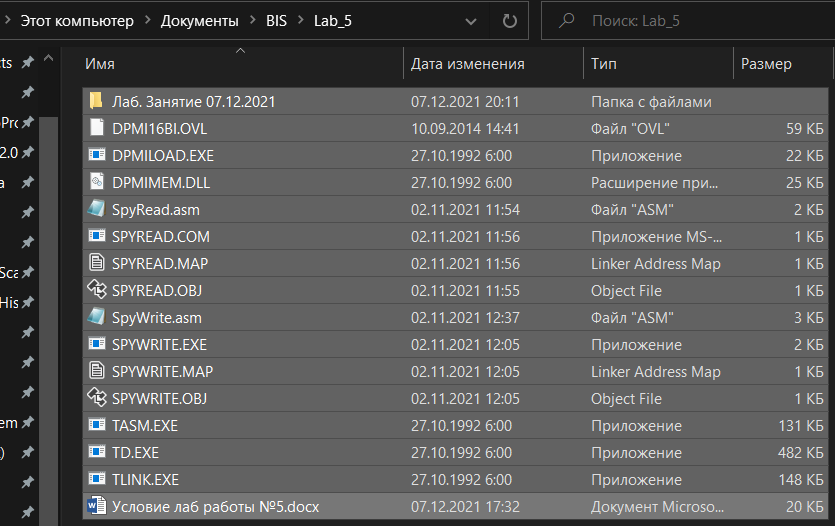
Жуковский Павел Сергеевич, 4 курс, 12 группа

Лабораторное занятие (**21.12.2021**)

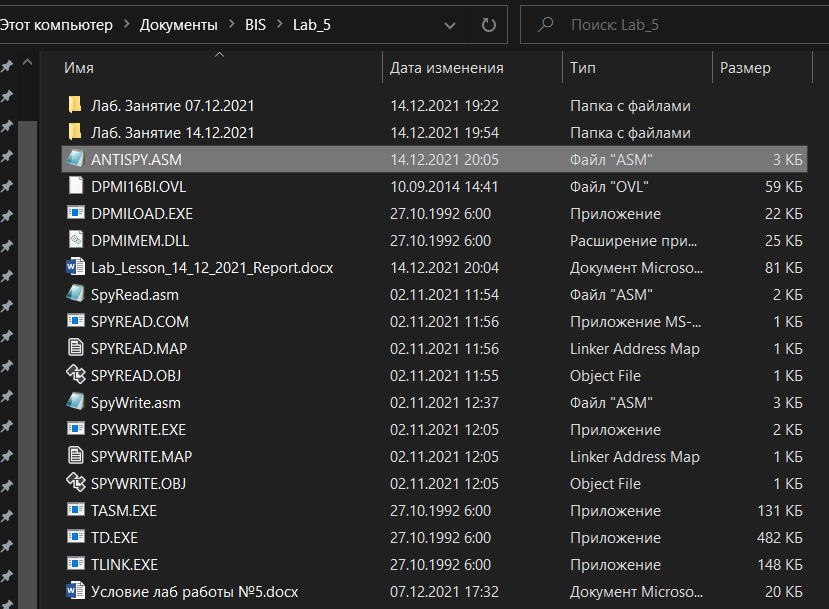
5-ая лабораторная работа (продолжение)

Две недели назад (**07.12.2021**) я создал папку **Lab\_5** и поместил туда такие исполнимые модули, как: TASM.EXE, TLINK.EXE, TD.EXE. А также DPMILOAD.EXE, DPMI16BI.OVL и DPMIMEM.DLL (на всякий случай). Также я поместил туда условие лабораторной, а также исходные текста, объектные и исполнимые модули клавиатурного шпиона (**SpyRead** отвечает за считывание нажатых клавиш, а **SpyWrite** – за их расшифровку).

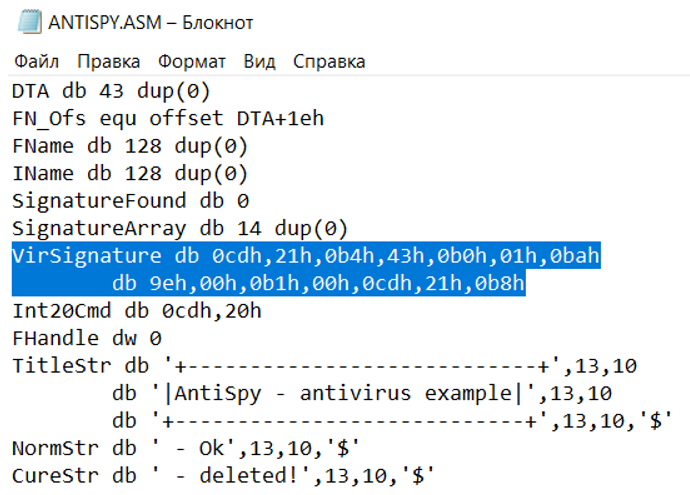


Неделю назад (**14.12.2021**) я взял антивирус ANTIDHOG.ASM и немного видоизменил его, а именно я изменил сигнатуру внутри ANTIDHOG.ASM на сигнатуру клавиатурного шпиона.

Для этого я брал исходный текст ANTIDHOG.ASM и сохранял его в файле **ANTISPY.ASM:**

****

В исходном тексте ANTISPY.ASM меня больше всего интересовало вот это место:



В этом месте записана сигнатура «свиньи». Мне пришлось заменить её на сигнатуру «шпиона». В одном из ответов на лекцию я уже как-то определял сигнатуру «шпиона».

Сигнатура осуществление доступа к файлам:

- создание подозрительного файла:

**b4 3c b9 01 00 ba 07 01 c7 06 16 01 01 00 cd 21**

mov ah, 3Ch

mov cx, 1

mov dx, offset FName

mov flag, 1

int 21h

- открытие подозрительного файла:

**ba 07 01 b0 01 b4 3d cd 21 eb b2 8b d8 b4 42 b0**

mov dx, offset FName

mov al, 1

mov ah, 3Dh

int 21h

jmp add\_position

mov bx, ax

mov ah, 42h

mov al, ...

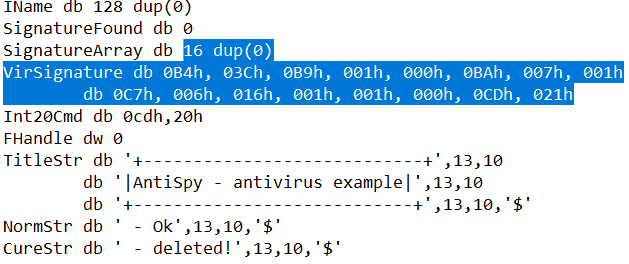
В качестве сигнатуры я брал первую (на создание файла):

**b4 3c b9 01 00 ba 07 01 c7 06 16 01 01 00 cd 21**

Именно эта сигнатура соответствует созданию шпионом файла с информацией о нажатых клавишах (вторая сигнатура подразумевает, что такой файл уже существует, однако в нашем случае этого никогда не произойдёт, если «антишпион» сразу устранит «шпиона»).

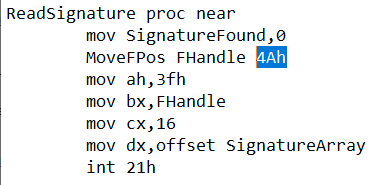
Стоит отметить, что данная сигнатура стоит из **16** байт.

По итогу, я внёс в исходный текст ANTISPY.ASM следующие изменения:



Перед всеми байтами также были добавлены нолики.

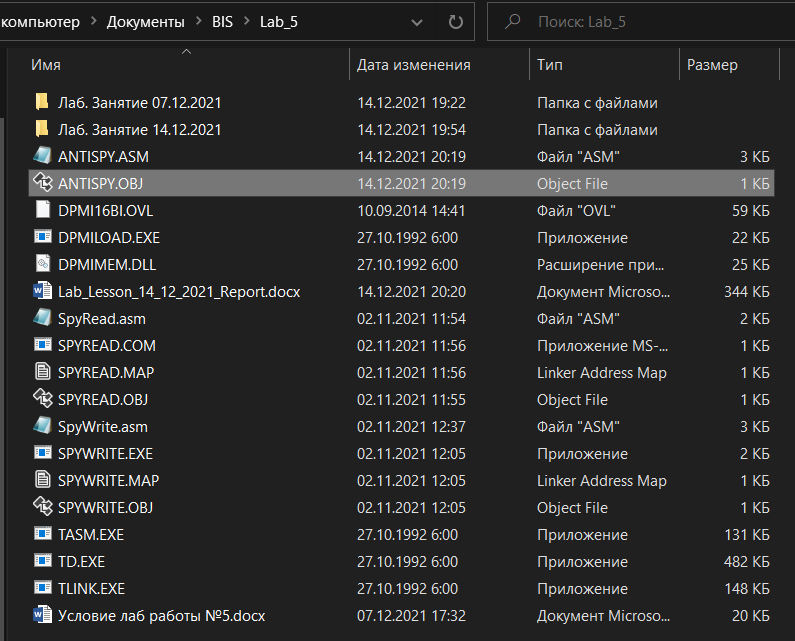
Также было сменено смещение для ReadSignature:



4Ah – это номер байта, начиная с которого в проверяемых исполнимых модулях будет искаться заданная сигнатура (это число было подобрано в процессе отладки, когда я искал ответ на один из вопросов с лекции №14)

Я получил сначала объектный модуль ANTISPY.OBJ:



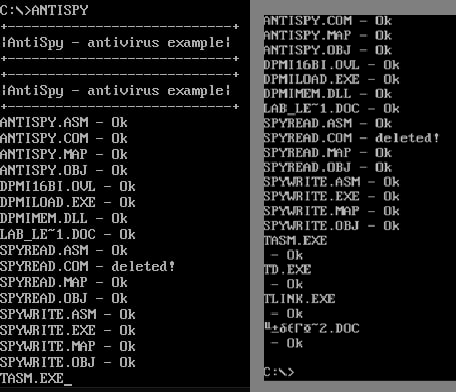


Затем я получил исполнимый модуль ANTISPY.COM:

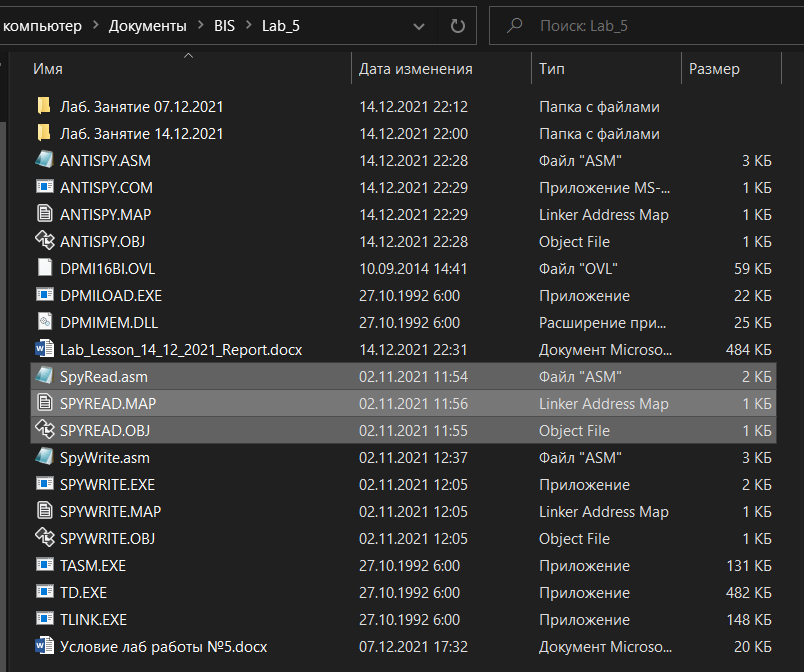


После этого я загурзил ANTISPY.COM в оперативную память компьютера и проверил, посчитает ли он SPYREAD.COM опасным или нем.

Запуск ANTISPY:



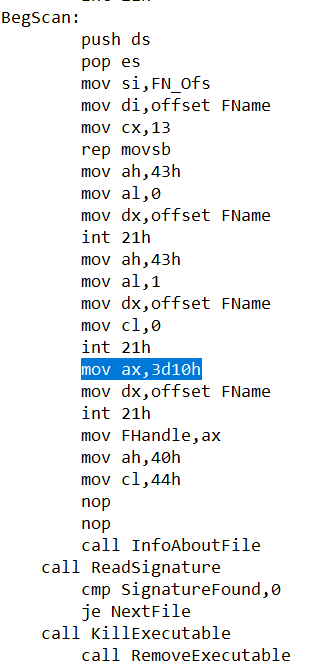
После этого исполнимый модуль SPYREAD.COM, внутри которого была обнаружена сигнатура команды создания подозрительного файла, был удалён из папки:



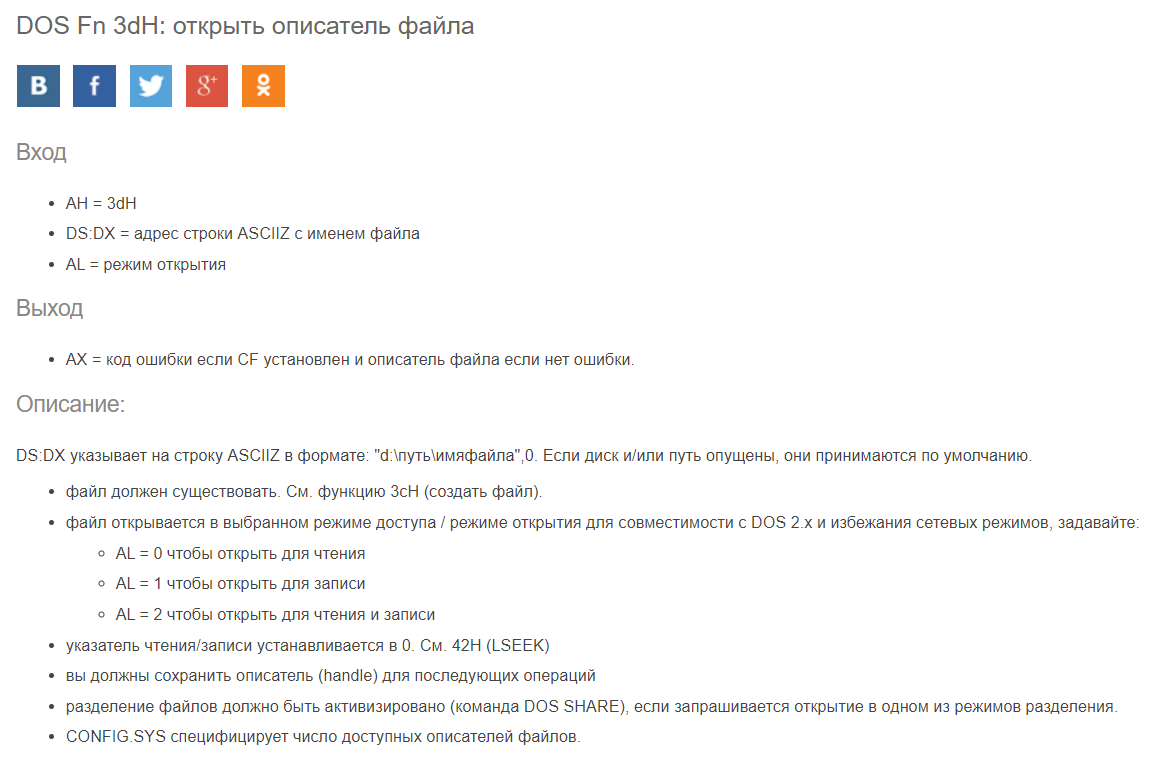
Таким образом, версия ANTISPY, сделанная 14.12.2021, была способна находить и удалять из папки исполнимые модуля, внутри которых находится сигнатура создания подозрительного файла.

Сегодня, **21.12.2021**, мы немного модифицируем наш антивирус ANTISPY.

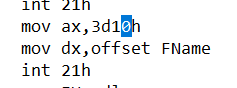
У версии ANTISPY 14.12.2021 есть серьёзный недостаток – при обнаружении файла с сигнатурой шпиона он на самом деле не «убивает» его. Если глянуть на наш исходный текст внимательно, то можно заметить, что во время проверки мы открываем файл **на чтение**:



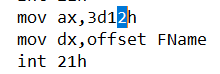
Я залез на помойку и нашёл там информацию о функции 3Dh прерывания 21h:



Регистр AX содержит в себе регистры AH и AL. Соответственно, когда мы записываем в него значение 3D10h, то в регистр AH попадает значение 3Dh, а в регистр AL попадает значение 10h. После этого мы вызываем функцию 3Dh прерывания INT 21h. Так как у нас на конце стоит **0**, то мы откроем файл лишь на чтение. Если же мы хотим полный доступ к файлу (и на запись, и на чтение), то нам следует записать туда **2**, тогда мы должны заменить



На

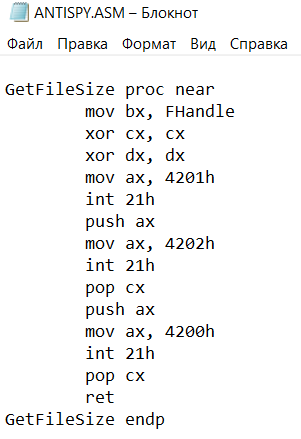


Если мы все сделали правильно, то теперь антивирус будет «убивать» шпиона.

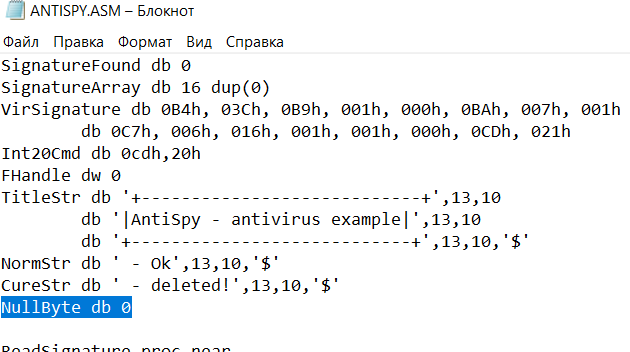
У нашей текущей версии антивируса есть ещё одна серьёзная проблема – мы на самом деле не уничтожаем исполнимый модуль шпиона так, чтобы его невозможно было бы восстановить, мы лишь удаляем запись об этом исполнимом модуле в указанной директории.

Чтобы добиться полного физического удаления исполнимого модуля шпиона – нам следует заполнить его нулями. Для этого я добавил в исходный текст ANTISPY.ASM следующее:

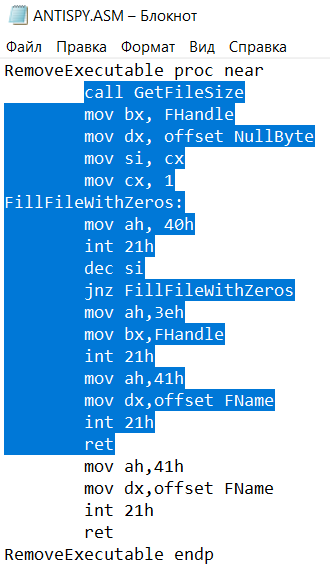
Метка, внутри которой определяется размер файла



Здесь мне понадобилось хранить нулевой байт:



Инструкции, позволяющие заполнить файл нулями:

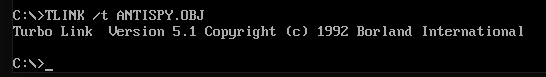


Благодаря этой модификации антивируса, шпион теперь будет удалён так, что его уже невозможно будет восстановить, так как он удалится физически.

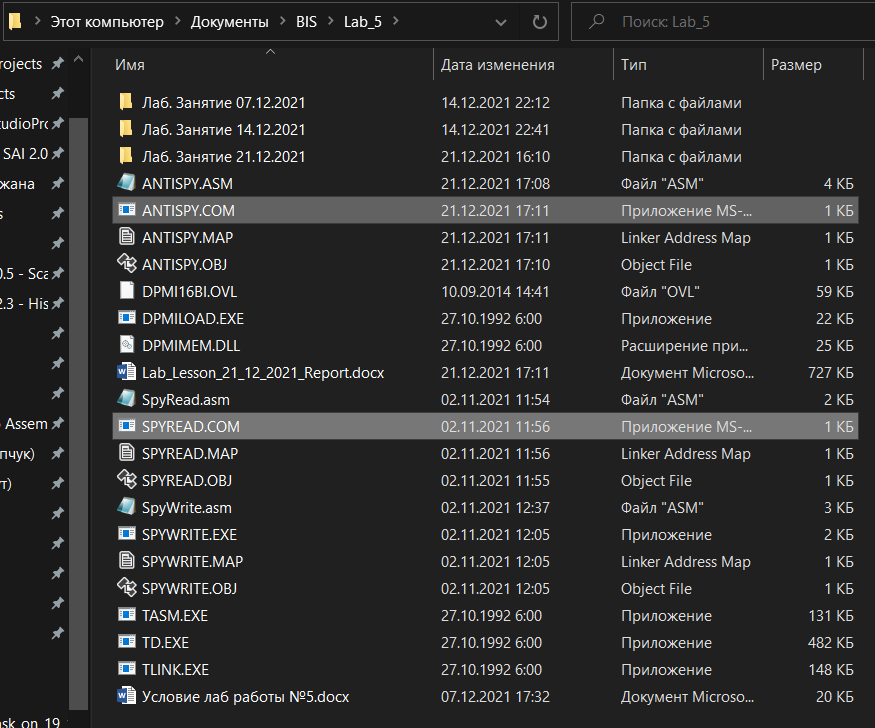
Получим новую версию объектного модуля ANTISPY.OBJ:



Теперь получим новую версию исполнимого модуля ANTISPY.COM:



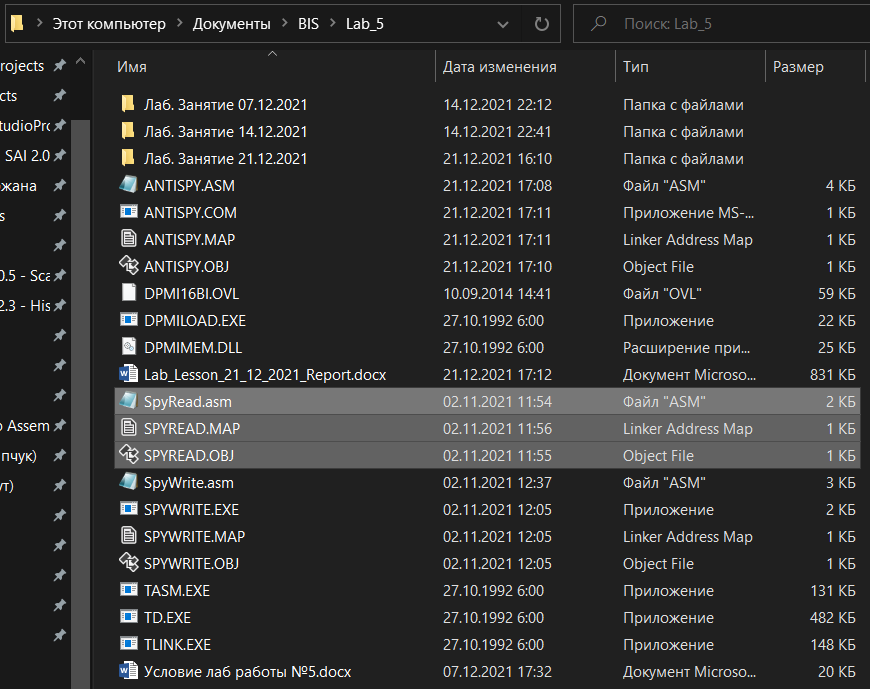
Итак, вот таким образом выглядит текущая директория:



Запустим ANTISPY:



Мы можем наблюдать, что SPYREAD.COM исчез из директории (и исчез не только из неё, а исчез в принципе):



В архив я помещу следующие файлы: SpyRead.ASM, SPYREAD.COM, ANTISPY.ASM, ANTISPY.COM, а также этот отчёт.

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