Жуковский Павел Сергеевич, 4 курс, 12 группа

Лабораторное занятие №12 (14.12.2021)

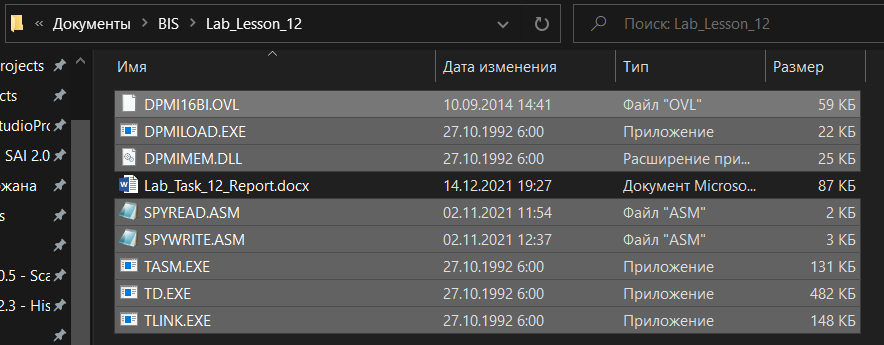
Пароль от архива: **041**

Постановка задачи:

«Сегодня на лаб занятии необходимо взять «клавиатурного шпиона» и определить, определяется ли исполнимый модуль .com  этого шпиона В КАЧЕСТВЕ ВИРУСА каким-либо антивирусником. И определяется ЛИ САМ АНТИВИРУСНИК в качестве вируса? Отчёт пра гэта даслаць да канца занятка»

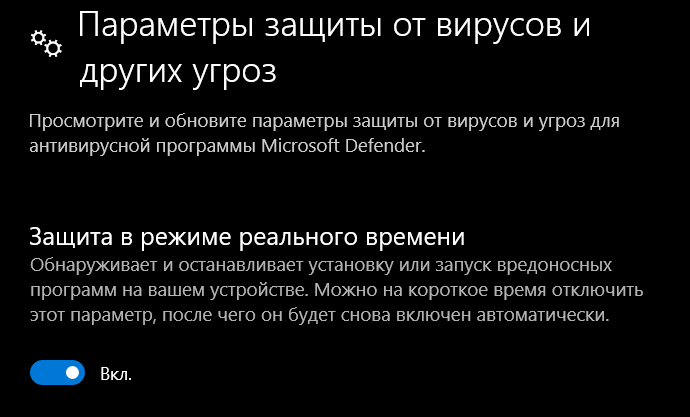
Алгоритм решения:

Для начала я создал папку **Lab\_Lesson\_12** 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 клавиатурного шпиона (**SpyRead** отвечает за считывание нажатых клавиш, а **SpyWrite** – за их расшифровку).



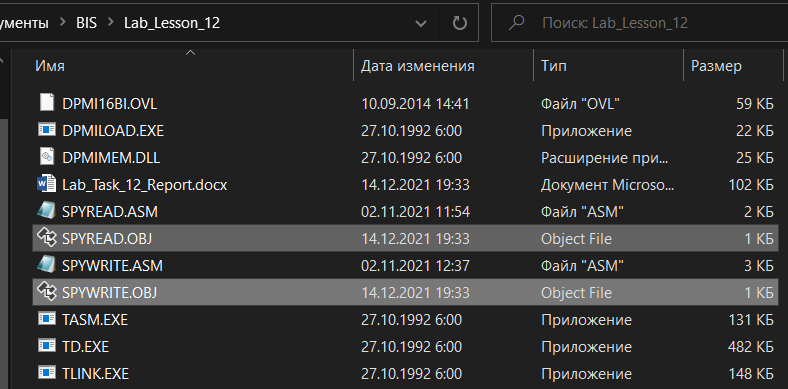
Теперь попробуем собрать .COM исполнимые модули для клавиатурного шпиона и посмотрим, отреагирует ли на них мой антивирусник (Windows Defender).

Для этого я специально включил свой антивирусник:



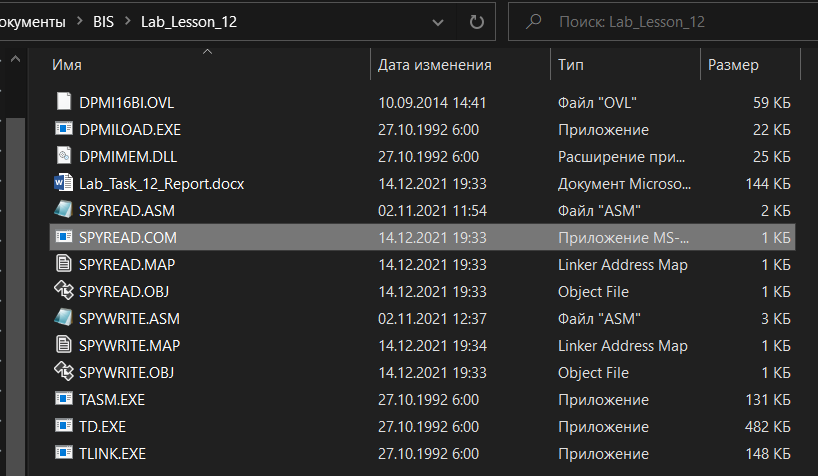
Теперь получим сначала объектные модули SPYREAD.OBJ и SPYWRITE.OBJ:





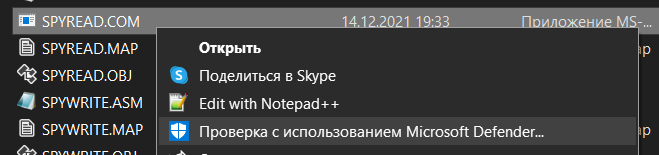
Теперь получим исполнимые модули SPYREAD.COM и SPYWRITE.COM (с помощью команды **TLINK /t**):





Почему-то SPYWRITE.COM не захотел создаваться, зато создался SPYREAD.COM. В общем-то, он то там и нужен, ибо расшифровка данных с нажатых клавиш нас сейчас не очень интересует.

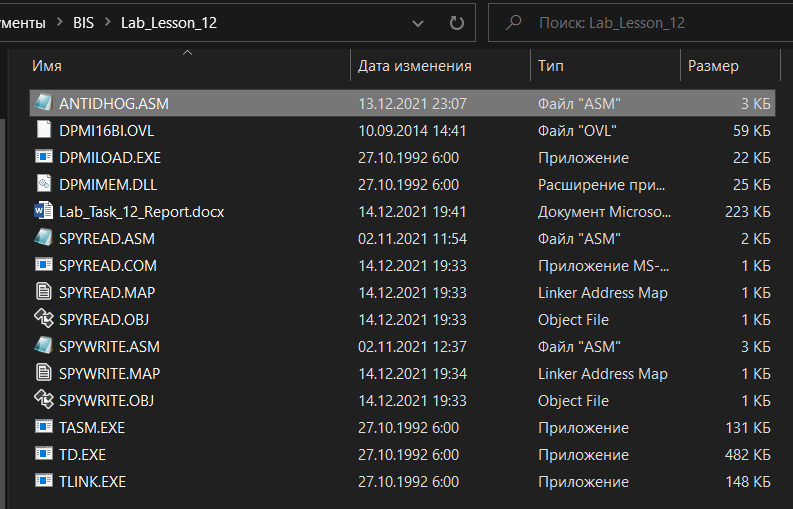
Мой антивирус не выдал никаких предупреждений в момент появления файла SPYREAD.COM. Например, когда я создавал DHOG68.COM, мой антивирус сразу выбрасывал об этом сообщение с предупреждением об опасном исполнимом модуле. Сейчас нету такого. Поэтому я на всякий случай вручную просканировал полученный исполнимый модуль:



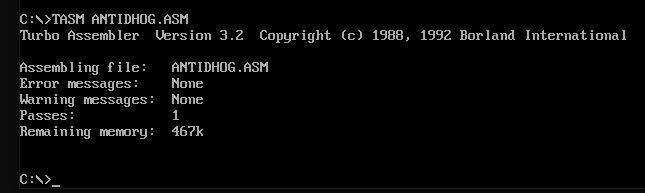
Проверка не дала никаких результатов. Мой антивирус не считает SPYREAD.COM опасным.

Так как у меня пока не готов «антиклавиатурник», я попробую посмотреть, что будет, если мы запустим «антисвинью» (которая есть у нас в наличии) в ту папку, в которой находится SPYREAD.COM. Я собираюсь проверить, удалит ли «антисвинья» SPYREAD.COM или нет.

За этим на пригодится исходный текст ANTIDGOH.ASM:

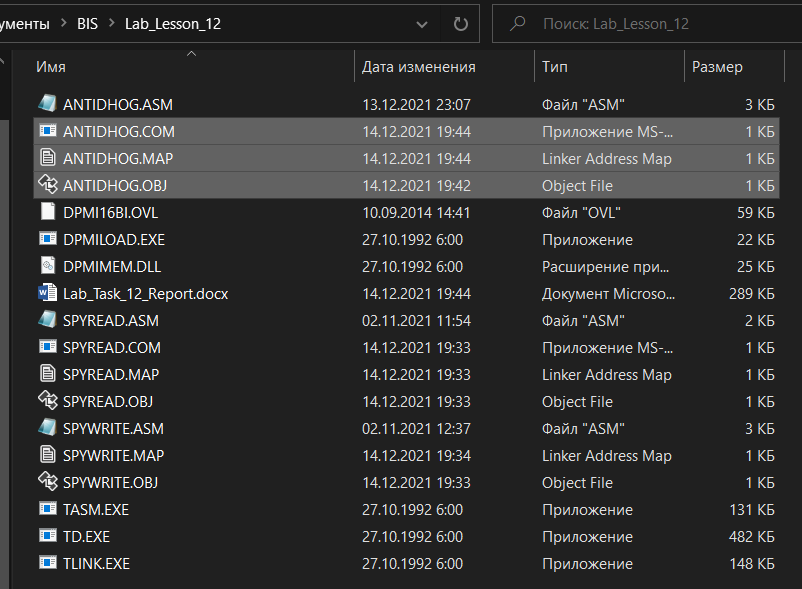


Быстренько получим сначала объектный модуль ANTIDHOG.OBJ:



А затем получим исполнимый модуль ANTIDHOG.COM:

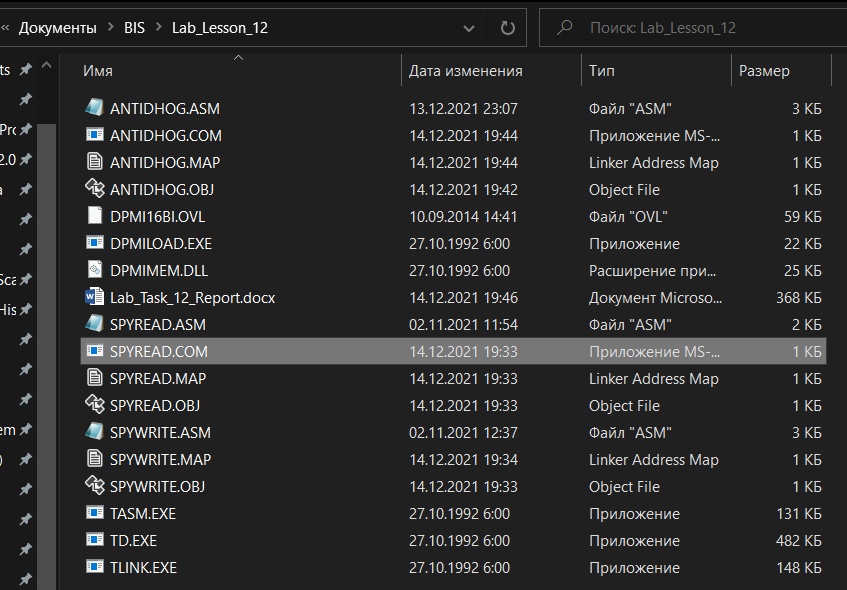




Стоит отметить, что мой антивирусник (Windows Defender) не посчитал и ANTIDHOG вирусом. Таким образом, мой антивирусник не считает ни SPYREAD.COM, ни ANTIDHOG.COM опасными…

Теперь проверим, удалит ли ANTIDHOG.COM исполнимый модуль SPYREAD.COM:





После запуска ANTIDHOG выяснилось, что он не удалил ни одного файла, в том числе и SPYREAD.COM. Из этого можно сделать вывод, что антивирусы всё-таки смотрят лишь на те «вирусы», внутри которых они видят соответствующую сигнатуру. Таким образом, если мы хотим избавиться от SPYREAD.COM, то нам необходимо исследовать его сигнатуру и создать соответствующий антивирус, ANTIDHOG нам для него не подходит.

В письме я постараюсь прикрепить архив, который будет включать в себя: SPYREAD.ASM, SPYREAD.COM, SPYWRITE.ASM, ANTIDHOG.ASM, ANTIDHOG.COM, а также этот отчёт.

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