**Лабораторное занятие №7.**

**Заканчиваем лабораторную работу №2 часть 1 и переходим к выполнению лабораторной работы №2 часть 2 (антивирус).**

**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 15.10.2024 года! Стоимость – 32 балла. Отсутствие – МИНУС 16 баллов.**

**Лабораторная работа №2. Часть 2.**

2.1. Набрать исходный текст антивируса AntiDHog (4 балла, отсутствие – минус 4 балла).

2.2. Транслировать, линковать, получить исполнимый модуль в папке HOG (т.е. в папке, где файлы уже превратились в вирусы) (4 балла, отсутствие – минус 4 балла).

2.3. **Проверить, каким образом НА ПОЯВЛЕНИЕ ЭТОГО ФАЙЛА реагирует Ваша антивирусная защита. Отчёт в виде совокупности скрин-шотов. 8 баллов, отсутствие – минус 8 баллов.**

2.4. Показать в шестнадцатеричном виде содержимое файла с бывшим исходным текстом вируса, используя какой-либо текстовый редактор и отладчик – 8 баллов, отсутствие – минус 8 баллов.

2.4. Отладить и протестировать АНТИВИРУСНУЮ ПРОГРАММУ.

2.5. **Проверить, действительно ли происходит УДАЛЕНИЕ или УБИЙСТВО всех файлов папки. То есть нужно дать ответ: убивает или удаляет. Для этого с помощью ОТЛАДЧИКА td.exe ПОШАГОВО ВЫПОЛНИТЬ программу, получаемую в результате загрузки в отладчик файла Mrak.asm. Отчёт в виде совокупности скрин-шотов. 8 баллов, отсутствие – минус 8 баллов.**

2.6. Получить ПРОГРАММУ-АНТИВИРУС, КОТОРАЯ ИЗНИЧТОЖАЕТ все зараженные файлы в папке HOG И ОСВОБОЖДАЕТ ВСЮ ОПЕРАТИВНУЮ ПАМЯТЬ, ЗАГРАБАСТАННУЮ БОРОВОМ! Помнить при этом, что согласно антивируснику, УДАЛИТЬ значит удалить имя файла из реестра файлов (реально же ТЕЛО исполнимого файла, который при загрузке в оперативную память и передаче ему управления превращается в вирус, ФИЗИЧЕСКИ ПРОДОЛЖАЕТ ЛЕЖАТЬ НА ВИНЧЕСТЕРЕ). УБИТЬ – означает сделать так, чтобы ТЕЛО ПЕРЕСТАЛО ИСПОЛНЯТЬ СВОЙ ФУНКЦИОНАЛ, что в антивируснике соответствует тому, что ПЕРВОЙ ИСПОЛНЯЕМОЙ КОМАНДОЙ ДЕЛАЕТСЯ КОМАНДА int 20h!! ИЗНИЧТОЖИТЬ ОЗНАЧАЕТ (В ДОПОЛНЕНИЕ К УБИТЬ и УДАЛИТЬ) НА МЕСТО ЗАРАЖЁННОГО ФАЙЛА НА ФИЗИЧЕСКОМ НОСИТЕЛЕ ЗАПИСЫВАЮТСЯ СЛУЧАЙНЫЕ ДАННЫЕ (например, ВСЁ чистится нулями или случайными значениями). ***Результат – три файла = 32 балла за полный результат, минус 16 баллов за его отсутствие.***

2.7. Определить, что произошло с самим исполнимым модулем-антивирусником после обработки им папки HOG, выведя на экран шестнадцатеричное представление этого файла после антивирусника. 8 баллов, отсутствие – минус 8 баллов.

2.8. Разработать программу, которая позволяет в уже полностью обезображенной папке HOG (среди уже убитых и удаленных файлов (до их изничтожения)) НАЙТИ файл, который когда-то был DHOG68.COM, И ВООСТАНОВИТЬ ЕГО (по аналогии с утилитой unerase, предварительно хорошенько изучив UNERASE). Результат – 64 балла, отсутствие попыток – минус 8 баллов.

Пункты 2.1 – 2.7 должны быть сданы в виде трёх файлов, присланных ко мне на почту ДО КОНЦА ДНЯ 04 ноября 2023 года.

Пункт 2.8 – ДО 23-59 18.11.2023 года.