Лекция 7 10.18.2022

***Вопрос 1: Какой файл функция 4eh определяет, как ПЕРВЫЙ СОВПАДАЮЩИЙ ФАЙЛ, всегда ли он (файл) будет одним и тем же, от чего это зависит?***

По договоренности врегистре AH будет выполняться функция при инициировании прерывания, 4EH эта функция будет осуществлять поиск по маске файла в текущем каталоге но в этом случае в качестве параметра для функции 4eh в регистр dx должен быть помещен адрес маски а точнее ее смещение по которой осуществляется поиск

Пример маски для вируса

\*.\*0 -> mask\_for\_vir

Очевидно что маска определяет имя и тип файл

***ВОПРОС 2: ПОЧЕМУ 140h? Нарисовать обязательно. Использовать прямоугольники для рисования оперативной памяти, областей памяти, стрелки ДЛЯ УКАЗАНИЯ АДРЕСОВ и 16-ичную систему счисления для числовых значений. Чтобы ответить на вопрос, ещё раз ПЕРЕЧИТЫВАЕМ про 4eh.***

Содержимое регистра DS CS указывает на PSP, размер этой области 100h далее располагается code segment и он содержит совокупность машинных команд которые получается в результате линковки и компиляции. Совокупность этих команд которая будет получена занимает 40h байт (64 в 10 десятичной системе счисления) а далее располагается область памяти в которой находится маска для нахождения первого попавшегося в текущем каталоге файла.

Тем самым мы и получаем 100h + 40h = 140h

|  |  |
| --- | --- |
| ***100h*** | ***DS CS -> PSP*** |
| ***40h*** | ***DATA*** |
| mask\_for\_vir | ***\*.\*0*** |
|  | ***…*** |

**ВОПРОС 3: После выполнения функции 43h в области DTA, начиная с адреса +15h получено значение, равное 6. Что это за файл? Точнее, какие атрибуты имеет этот файл. Ответ дать на русском языке.**

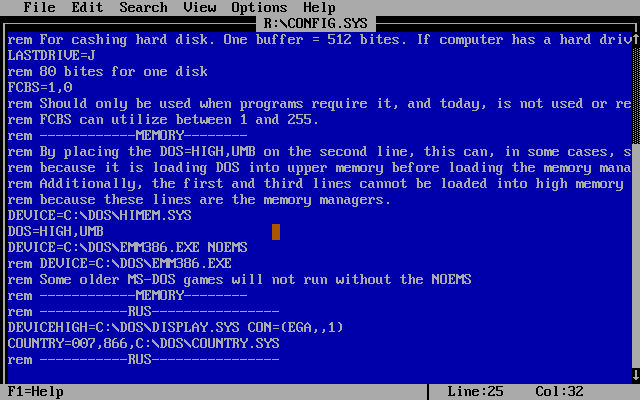
Атрибуты файла:

* время создания
* дата создания
* размер файла в байтах
* 13 байтовая область памяти в которой хранится сокращенное имя файла
* ***ВОПРОС 4: КАК ПОЛУЧАЕТСЯ 9Eh. Обязательно нарисовать.***

**Вопрос 5. Что значит «Открыть файл».**

**ОТКРЫТЬ ФАЙЛ - значит получить HANDLE (не шутка)**

**Вопрос 6. В рамках DosBox вывести на экран содержимое файла config.sys.**



***Вопрос 7. Что это за команда NOP? Для чего они здесь нужны? Что будет, если их убрать?***

NOP – No Operation. Это однобайтовая команда, которая ничего не выполняет. Данная команда нужна для небольшой задержки. Они используется, чтобы резко не перегружать процессор.

***Что будет, если их убрать? - НИЧЕГО***

***Вопрос 8. «…следующий совпадающий по маске файл» - «следующий» - это какой? Какие критерии «следующности»?***

***«следующий» это тот что соответсвует текущей сортировке*** Критерий сортировки. если в данный момент времени файлы отсортированны по имени то берем в лексиграфическом формате первый файл

***Вопрос 9. Какая разница между командами JNB и JNL?***

Обе эти программы используются как условные команды для передачи управления в другую точку программы.

Они совпадают по тому, что условием для перехода является >= и not <, но JNB выполняет также переход, если нет переноса.

**Вопрос 10: Как известно, описание функции 31h следующее:**

**31h выходит в родительский процесс, сохраняя код выхода в AL. OS устанавливает начальное распределение памяти, как специфицировано в DX, и возвращает управление родительскому процессу, оставляя указанную память резидентной (число байт = DX \* 16).**

**Вопрос 10.1. Что является «родительским процессом» когда вирус функционирует – исполняется.**

**Вопрос 10.2. Что такое параграф и чему он равен?**