Лекция 6. Чупа Чупс

Наш вирус при попадании в оперативную память

Будет состоять из 2 сегментов

1. PSP -> DS CS ES SS
2. Code Segment

Причем сказано что для определения начального адресса кодового сегмента будет испольщован регистр CS и при этом содержимое регистра DS тоже будет связано с адресом начала кодового сегмента (**ВСЕ это не правда**) на начало PSP указывает DS CS ES SS

При загрузке COM файла сожержимое регистров DS CS ES SS показывают не на точку входа а на то что называется программ сегмент префикс (ПСП)

Строчка старт проц неар говорит трансялтору что далее будет записана последжовательность команд котороая называется процедурой которая обызвается именем старт а передача упраления этой последовательности команд может быть осуществленна в том числе с помощью команды call

Изза артема я прослушал … То есть смещение не должно привышать 256 байт

Mov ah. 4eh

Mov dx, 140h

Int 21h

Записаны тут для того чтобы после из трансляцции линковки и загрузки в ОП модуля ком они бы были расшифрованы самостоятельно процессором и заставили бы комп выполнить строго опрелелнные действия эти 3 команды поерделеяют что необзодимо выполнить команду int 21h это команда нзывается инициализация прерывания с номером 21h(да да это номер)

Команды mov ah 4eh Mov dx, 140h это по сути дела входные параметры для прерывания 21h

Рас и навсегда договорились что на занятиях по БИС запрещзается справлять нужду справлять еще какие либо потребности (ссать срать … пить) ну если серъезно то договорили для всех команд инициирующих команд что в регистер ah будет выполняться функция которая будет выполняться при иницииировании прервыния 4EH эта функция будет осуществлять посик по маске файла в текущем каталоге но при этом в этом случае в качестве параметра для функуции для 4eh должен бытть помещен адрес в регистр dx должен быть помещен смещение маски по которой осуществялется поиск   
если ктото из вас добрался до этой программы то вы бы могли получить нарисовать след картинку   
содрежимое регистар DS CS указывает на ПСП размер этой области 100h далее распологается сегмент кодов и этот код сегмент содердит совокупность машинных команд которые получается в результате линковки и компиляции

И если бы вы еще раз залезли во внутенний мир этого вируса то вы бы могли бы понять что совакупность команд которая будет получена занимает 40h байт (64 в 10 дсс) а далее распологается облать памяти в которй находится маска для находления первого попавшегося в текущем каталоге файла

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

Очевидно что маска определяет имя и тип файл

В регистре ax будет содержаться так называемый код ошибки если при выполнение функции 4eh была обнаружена какя-то ошибка для того что бы определить произошла какаято ошибка необходимо обратиться к тому что называется регистр портов  
при обнаружение огибки в бите С будет установлено значение 1

Про то что такое регистр флажков как он используется можно почитать в лекциях зубович (6 7)

Этот регистр флажков существует для 16 32 64 машин

При этом если ошибки никакой не было то специальная область которая называется DTA (дитией) будет заполнена данными о файле который был найдена а именно в этой области храница следующая инфа атрибуты файла время создания дата создания и размер файла в байтах а так же 13 байтовая область памяти в которй хранится сокращенное имя файла

область памяти DTA (Data Transfer area) находится в области памяти а точнее в сегменте PSP

Например в первых 2 байтах находится int 20h 02ch распологается адресс области памяти Env Block в этом блоке распологается информация о текущем состоянии исполнимого модуля  
в том числе там находится послный путь,начиная с адреса 00ffh распологается область памяти DTA

В связи со сказаным область памяти DTA будет сохранена по тем 3 командам будет сохрпанена инфа о первом попавшевмся файле по маске (что означает по маске файл – это такой файл что имя его совпадает по маске)) первый в соответсвии с сортировки в файле на данный момент врмени (сортировка по ….)) если в данный момент времени файлы отсортированый по имени то он и будет первым !)

СИНОНИМ СЛОВА ПРЕРЫВАНИЕ это СОСТОЯНИЕ процессора которое возникает в тот момент когда просиходит некоторое событие.

Аппаратные и программыне прерывания бывают, договорились! С каждым прерыванием увязывать некоторе число и отталкиваясь от этого числа которое называется номером прерывания связывать некоторе событие ллибо код аппаратуры либо событие которе вызываетс программно програмные прерывания могут быть инициированы командой int (interapt)

Вектор прерывания который состоит из 2 компонент при чем эти 2 компоненты которые представлляют собой вектор размерности 2 определябт адрес так называемого обработчика прерывания (то есть адрес облатси памяти в которй назодится функция которой передается реализация того или иного прерывания)

Адрес и смещение ([адресс]:[ адресс]) есть еще таблица векторов прерыванияпр

При загрузке ОС формируется таблица векторов прерывания

При чем в 0 назолится адрес обработчика прерывания с номером 0 он называется ошибка деления при чем это прерывания возникает тогда когда с помощью команды div idiv осуществляется попытка деления на 0 прерывание с номером 1 которое распологается по адрессу

Это прерывание называется прерывание пошагового режима (это прерывание возникает после выполения каждой машинной командой если в регистре флажков если в регистре установлен ьит пошаговой трасировки жто еще используется для откладки программ) оно полезно в том случае

Прерывание 3- 4-преполнение нам в дальнейщем понадобится прерывание с номером 10 или с номером обслуживание видеоадаптреа и в дальнейшем понадобится прерывание при клавиатуре

И конечноже понадобится прерывание с номеров 21h это прерывание от опреационной системы которое была с составной частью машин 208 8 386 486 586 686

На сегодня это все что я хотел вам сказать мы разобрали 3 команды на след лекции продолжим разбирать команды котоыре остались