<<计算机安全>>

图书基本信息

书名：<<计算机安全>>

13位ISBN编号：9787505386006

10位ISBN编号：750538600X

出版时间：2003-7

出版时间：电子工业出版社

作者：朱海林

页数：208

字数：333

<<计算机安全>>

书籍目录

章节摘录

3.3.2病毒的检测和消除对磁盘杀手的检测比较方便，无论是软盘还是硬盘都可以借助于像Pctools和Debug等工具软件直接观察引导扇区内容，进行比较即可。
清除软盘中的病毒的方法是：从引导扇区中的病毒程序处找出存放原引导扇区内容在盘上的相对扇区号，进而读出正常引导扇区内容并写回引导扇区，然后把坏簇标志改为可用簇。
清除硬盘中病毒的方法是借助工具软件从隐含扇区的最后一个扇区中读出引导记录并写回到引导扇区，即可清除病毒。
3.4黑色星期五病毒黑色星期五病毒从字面上理解不难看出它一定与星期五有关。
那何为黑色呢？
黑色指的就是13日。
这种病毒在13日且又是星期五时发作，删除磁盘上的所有被执行文件。
由于在西方13是一个不吉利的数字，因此对于既是13日又是星期五，就称为黑色星期五。
最初这种病毒出现在以色列希伯莱大学，故也称为希伯莱病毒。
因为该大学位于耶路撒冷，又称为耶路撒冷病毒。
3.4.1黑色星期五病毒的特点黑色星期五病毒是一种流行广且危害很大的恶性病毒。
它是一种文件型病毒，传染对象是后缀为COM和EXE的可执行文件。
已感染病毒的.com文件，病毒程序位于最前端，而对于.exe文件则位于文件的后面。
但当运行含有病毒的文件时，最先运行的总是病毒程序，且首先获得系统的控制权。
感染黑色星期五病毒的文件属性和建立日期是不变的。
对于后缀是COM的文件，只感染一次，使其增加1813个字节，且病毒程序位于该文件的首部。
而对于后缀是EXE的文件，则可无限次的感染，其每次感染时都将病毒程序放在文件的尾部。
必须指出的是，病毒程序在对文件感染时，先是修改DOS的出错处理中断INT24H，从而使病毒的感染过程能悄悄地进行。
黑色星期五病毒的破坏分为两种。
一种是利用所截获的INT8H中断向量，在病毒程序内部设置计数器，当值为2时，在屏幕上显示“长方块”，若值为0时，则通过执行无用的字符循环程序来减慢系统速度。
另一种是日期和星期计数，当系统日历为13日且是星期五时，在系统中运行的EXE和COM文件就会被删除。
3.4.2病毒的工作原理黑色星期五病毒包含三个模块：引导模块、传染模块和表现／破坏模块。
运行受感染的文件时，病毒程序首先运行，对于尚未感染该病毒的系统，它将修改系统的INT2lH和INT8H中断向量，使其指向病毒的传染模块和表现臌坏模块，并把病毒程序（约1.8KB）移到内存某个地方驻留。
在完成把自身引导驻留在内存的工作后才去执行原来的可执行文件。

版权说明