通用电脑病毒免疫技术及疫苗的生成

杨德荣 (重庆市财政局信息中心)

摘要:利用电脑病毒传染的必要条件,根据微机*ROMBIOS*及*DOS*系统功能的特点,集中讨论了文件型病毒的免疫。文中的技术几乎能防御各种文件病毒。

"病苗"一词来源于生物学,它是与病毒相对应的。根据生物学中的原意:疫苗一般指用病毒或其它原生物所制作的生物制品,可见计算机病毒的疫苗也应该是一种程序,并且这种程序不具备传染性。因此,计算机病毒疫苗应具备以下几个特征:

(1)计算机病毒的疫苗是一种不具备传染性的计算机系统可执行程序。

(2)计算机病毒的疫苗在计算机系统的运行中,利用系统提供的硬件、软件资源,常驻内存,监视计算机系统的运行。

(3)计算机病毒的疫苗可以在发现病毒的入侵时防止或禁止病毒的入侵。

以往的病毒防护软件,或多或少的具有下列不足:需要用户频繁地确认;只能防御已经出现的特定病毒;感染病毒后才报警。用本文所述的技术,克服了以上不足,真正达到了"防患于未然"的目的。

1.文件型病毒传播的必要条件及可能伎俩

所谓文件型病毒是指以可执行文件作为宿主的病毒,可执行文件在DOS系统下主要是指COM和EXE文件,文件型病毒传播的过程为:运行带毒文件,病毒程序驻留内存;等待时机传播给其它的可执行文件。可见,一种病毒如果要传播给其它的可执行文件,它的必要条件是:顺利地完成写磁盘的操作,也就是说只要对磁盘写绝对把关,不让病毒的写请求获得成功,病毒就得不到传播,本文就是基于这种思想。

一种病毒如果要传播给其它的可执型文件,必须要在磁盘上写一个或改写一个与正在运行的程序同名的能被DOS承认的文件,然而病毒程序为了完成这一过程,采取的手段不外乎以下三种:一是直接调用DOS系统功能,二是间接调用DOS系统功能,三是绕开DOS系统功能,模仿DOS写文件的操作,直接调用BIOS的中断INT13H。

2.DOS进程加载及退出与被加载文件名称获取

在DOS环境下,可运行的文件主要有COM和EXE文件,可执行文件调入内存的方法通常有两种:一是在DOS提示符下,打入文件名,然后回车;二是使用中断21H的4B号功能调用来完成。分析DOS外部命令执行的过程可知,在DOS提示符下打入文件名运行可执行文件实质上是由COMMAND.COM利用中断21H的4B号功能来完成的。另外加载可执行文件还有一个未写入DOS文档的功能INT 2EH,但实际上,它也是通过COMMAND.COM的暂驻部分间接调用INT 21H的4B号功能。因此,INT 21H的4B号功能是装载一个可执行文件的唯一手段,INT 21H的4B号功能的入口处,DS:DX存放着含被加载文件的名称在内的字符串首址,故我们可以从此处得到被加载进程的文件名并给以保存。

在DOS环境下,结束一个进程返回父进程(或DOS)是通过调用下列中断之一完成的:INT 20H,INT 21H的OOH、31H、4CH子功能,INT 27H,故我们可以扩充这几个中断,使之告诉系统一个进程结束,该进程的名称可放弃,没必要保存了。

3.对付病毒伎俩的策略

首先,我们得承认,在运行一个可执行文件期间,把该文件又写回磁盘或从磁盘上删除该文件的这种需求几乎没有必要,然而病毒传染时,就是插入文件的执行过程,执行病毒传染程序,以达到把正在执行的文件作某种修改后写回磁盘的目的。对付病毒的策略就是阻断病毒程序向磁盘写文件的各种渠道,下面就讨论病毒程序向磁盘写文件的各种渠道以及阻断这些渠道的方法。

(1)直接调用DOS的文件管理功能。通过对DOS系统功能的分析筛选得到如下结论(有关DOS系统功能及DOS数据结构参见DOS手册):如果是用文件控制块方式FCB,首先必须至少调用INT 21H的13H、15H、22H、28H四子功能之一,入口处DS:DX为未打开的FCB始址;若采用句柄式,则它首先至少调用INT21H的3DH(AL=1或AL=2)和41H二子功能之一,在该二子功能的入口处,DS:DX中存有路径名字符串始址。因此,该种情形,可拦截INT 21H在入口处获得被写或被删的文件的名称,再把该名称与正在运行的文件名称相比较,若相同则认为是病毒正在传染。

(2)间接调用 DOS 的文件管理功能。所谓间接是指不通过 INT 方式调用,而是用 JMP 指令调用,只须扩充 INT 21H,在它的入口处设立 DOS 标志,再在 INT 21H 的出口处验证此标志:若是 DOS 标志,就清除 DOS 标志,再中断返回,否则就是非法 DOS 调用,很有可能是病毒在调用。当然 DOS 本身也间接调用它的某些子功能,然而它肯定是通过 INT 方式再间接调用,故 DOS 自己的调用可以顺利地通过 DOS 标志的检查。

(3)绕开 DOS 的文件管理功能,直接调用 INT 26H 或 INT 13H,但 INT 26H 是通过调用 INT 13H 来完成的,故实质是用 INT 13H。用 INT 13H 而非 DOS 功能在磁盘上写一个能被 DOS 承认的文件,必须对文件分配表 FAT 进行写操作,故我们可以扩充 INT 13H 的中断服务程序(ISR),使其完成下列功能:检查是否对 FAT 进行写,若是,再验证 DOS 标志以确定是否 DOS 在写,若不是 DOS 在对 FAT 写,则认为是病毒在传染;否则执行转到原 ISR。

4.疫苗的生成

源程序 VACCINE.ASM 是按本文中的技术编制的疫苗程序,经编译生成 VACCINE.COM 文件后,将其放在 AUTOEXE.BAT 文件中,系统启动后一次加载,驻留内存即可起到对 C 盘上的可执行文件免疫的效果,程序在 AST486,COMPAQ486 等机上运行通过,通过模拟病毒的试验,证明该程序的效果很好,误报警的可能性几乎没有,读者只须稍作改动,可以对 D、E 等盘同样起到免疫的效果。(编者注:因源程序较长,本刊略,有需要者请与作者联系)。

也谈软件加密技术

陈　导　(华东电管局 信息中心)

经过实践活动及经验积累,我探索出一套加密方法,在这里与大家探讨、交流。该方法在软件系统安装时必须采用安装盘,该盘为加密盘,不能拷贝;系统安装后,可脱离安装盘独立运行,但运行的软件系统不能移植到其它计算机中去,从而达到该软件的合法性、安全性。

一、安装盘的制作

安装盘需要达到的目标是:不能复制,安装应用软件时必须使用该盘。

先介绍一下 IBM-PC 软盘的标准格式。软盘的记录密度经常是用双面倍密度,也可用单面倍密度。一个软盘的每个面分为 0-39 磁道。而每个磁道又分成 8 或 9 个扇区,每个扇区为 512 字节/扇区长度。

IBM-PC 规定 0 磁道为操作系统 DOS 所占用,其中 0 面 0 磁盘道 1 扇区存放系统的引导程序。0 磁道两个面的其它扇区分别存放文件分配表,文件目录表。而 1-39 道,用户可以用来存放文件信息。

下面我们对研制的安装软盘实施加密保护措施。

1.编写一个格式化某一磁道为非标准格式的程序。例如把某一磁道格式化为 18 个扇区,每个扇区长 256 个字节,格式化时间隔宽为 20H,步进电机加速和去载时间为 AFH,这就需要修改 ROM 中的磁盘参数区第 1 字节,第 4 字节和第 8 字节。然后才调用 13H 中断功能去格式化。为此应该重写一个 11 字节磁盘参数区,并把 1EH 中断向量地址内容改为指向这个参数区的首地址。

2.编写一个写盘程序。也应按上述格式设定磁盘参数,修改 1EH 中断指针指向这个参数区。然后调用 13H 中断的写盘功能,把某些重要的数据写到由上一步骤已格式化的那条非标准磁盘上的某些扇区中。

3.编写应用安装程序时,也应按上述格式设定磁盘参数,修改 1EH 中断指针,调用 13H 中断读盘功能把由步骤 2 写入的重要数据从非标准磁道的指定扇区读出。这些数据是安装程序执行时一定要用到的,如果缺少这些数据则安装程序无法执行(称这些数据为安装许可标志),如果复制该盘时,复制不到这条特殊格式磁道,则安装许可标志将在副本中丢失,副本的安装程序因找不到这些数据将无法执行,从而达到不能复制之目的。

二、安装程序加工

我们可以控制用户使用安装盘安装应用软件的次数,只要在安装程序加一计数器,每一安装一次计数器加 1,直到预定的次数为止。方法是:把计数器内容放在非标准磁道的一扇区内,初值为 0,每次运行安装程序,该计数器内容加 1,当计数达到预定值时,修改安装许可标志,使该安装程序无效。

我们还要求该应用软件只能在安装后的计算机系统中运行,不能任意移植到其它计算机系统中去。因此,经