国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第13卷第2期 1991年6月 Vol. 13 No. 2

# 计算机病毒的防治

刘滨海

（电子计算机系）

**摘 要** 本文综合地探讨了计算机病毒的概念、原理及其防治。详细地分析了巴基斯坦病毒的结构和传播原理，并叙述了防治这种病毒的方法，包括消除方法和免疫方法。另外，作者认为病毒的防治尚没有完全统一的方法，必须具体情况具体分析，而最有效的措施是病毒预防。

**关键词** 微型计算机系统，计算机病毒，巴基斯坦病毒

**分类号** TP31

计算机病毒给计算机系统的安全构成了严重的威胁，可以说，计算机病毒的出现给计算机研制者、应用者乃至整个社会提出了一个严峻的课题。本文针对微型计算机中流行的病毒，对其概念、原理、防治等进行探讨，以使读者对病毒能有一个比较系统的了解。文章讨论了病毒的定义、特点及类别；详细地分析了病毒的一般结构及原理，揭示了病毒的传播实质；然后，分析了巴基斯坦病毒，并叙述了我们防治这种病毒的方法。最后，读者将会发现，病毒的多样性使得其防治尚没有完全统一的方法，必须具体情况具体分析，防治病毒的积极措施应是病毒预防。

## 1 计算机病毒的概念

### 1.1 定义

关于病毒的定义，众说纷纭。我们认为，病毒是依附于一定载体的指令序列或程序，在约定条件下，可直接或间接地运行，实现其对计算机系统的干扰和破坏作用。

### 1.2 特点

（1）可运行性

病毒是一个非正当的程序，可以与正当程序一样地运行，只不过其运行有可能是间接的。

（2）传染性

病毒具有再生能力。它利用自己的再生机制，可将自身复制到其它尚未被感染的对象。

（3）破坏性

病毒的目的在于破坏系统，其破坏作用取决于设计者。轻则干扰系统运行，消耗系

* 1990年5月20日收稿

统资源，降低处理速度等；重则破坏文件或数据，甚至摧毁系统。

(4) 隐蔽潜伏性

病毒依附一定载体而存在，侵入系统后，有一定的隐蔽潜伏期，只有满足约定条件后，才触发生效。

(5) 主动攻击性

病毒是通过主动攻击实现对计算机系统正常运行的干扰和破坏作用。

### 1.3 分类

目前，较为流行的分类是按病毒所依附的宿主来分。

(1) 操作系统型

这类病毒针对磁盘引导扇区，以含有病毒的引导扇区替代正常的引导扇区，系统启动时，病毒侵入内存潜伏起来；时机成熟，便秘密地进行感染、干扰或破坏。

(2) 源码病毒

这类病毒攻击高级语言编写的程序，可以在编译之前，插入到源程序中。

(3) 入侵病毒

这类病毒将其自身侵入到现有程序中，即将病毒的主体程序与其攻击对象以插入方式连接起来。

(4) 外壳病毒

这类病毒不修改原程序，而只是将其自身包围在所攻击对象的外围。

## 2 计算机病毒的原理

微机中的病毒一般可以分为三个组成部分：自举部分、传播部分和表现部分。

### 2.1 自举部分

DOS 初始启动时，是机械地将磁盘引导扇区内容读到内存 0：7C00H 处，并执行引导程序，使系统开始工作，而病毒正是强行将其自举部分放到引导扇区，置换了正常的引导扇区内容。这样，系统启动的过程就成为图 1 所示。其中，虚线框起部分是病毒增加的操作，而最后的启动结果仍是成功的。

### 2.2 传播部分

病毒自举部分将 INT13H 修改为病毒传播部分的入口，因而每一次磁盘操作都有可能导致传播部分的执行。

### 2.3 表现部分

这部分的目的是干扰系统，其表现形式随具体病毒而定，后果也不同。

### 2.4 小结

上述病毒概念的讨论只是从目前微机中流行的大多数病毒实例中总结出的一般情况。针对具体病毒，情况会有差异。

## 3 巴基斯坦病毒的防治

这类病毒是由巴基斯坦程序员拉哈尔编制的，其最初目的是跟踪他所开发软件的非法拷贝者和使用者。其症状是将被感染磁盘的卷标改为 (C) BRAIN 字样，故又称 BRAIN

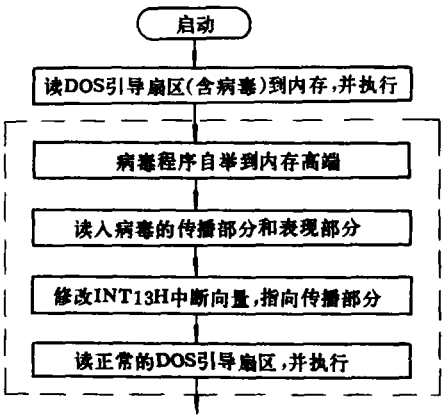


图 1　病毒自举部分工作流程

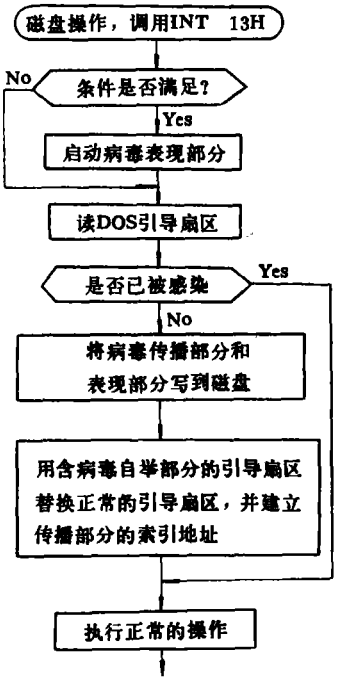


图 2　病毒传播部分工作流程

病毒，但这种病毒也有可能毁坏磁盘上的文件或数据。

### 3.1　BRAIN 病毒原理

该病毒属于操作系统型，传播环境为 IBM—PC 及其兼容机，只感染软盘。这种病毒更具有隐蔽性，因为它没有表现部分，只传染并不激发。传播途径有两条：一是对带有病毒的盘进行拷贝；二是在病毒活动系统中操作软盘。BRAIN 病毒自举部分和传播部分的流程框图可以参考图 2 和图 3.

关于 BRAIN 病毒，说明如下几点：

(1) 该病毒约为 3K 字节长，是连续存放的。除非磁盘满，否则只要仍有一个可用簇，它就要强行占用三个簇，并将其标记为坏簇，所以，它有可能破坏磁盘上的文件或数据。

(2) 在传播部分，有一个保护引导扇区的模块，用以判断是否是读引导扇区。若是，则修改读盘参数，读出正常的引导扇区，因而具有更大的迷惑性。

(3) 在自举部分，修改 DOS 保留未用的 INT06H 中断向量，使其指向正常的 INT13H 的中断向量，而传播部分中所谓执行正常的 INT13H 即是间接执行 INT06H.

### 3.2　BRAIN 病毒的防治

病毒的防治包括消除已感染病毒磁盘上的病毒和为未受感染磁盘提供免疫能力。

(1)　BRAIN 病毒的消除

首先是如何检测 BRAIN 病毒。一种方法是检查卷标。若卷标为 (C) BRAIN 字样，则表明该盘有可能感染了 BRAIN 病毒。另一种方法是检查磁盘空间，若有 3K 字节被标志

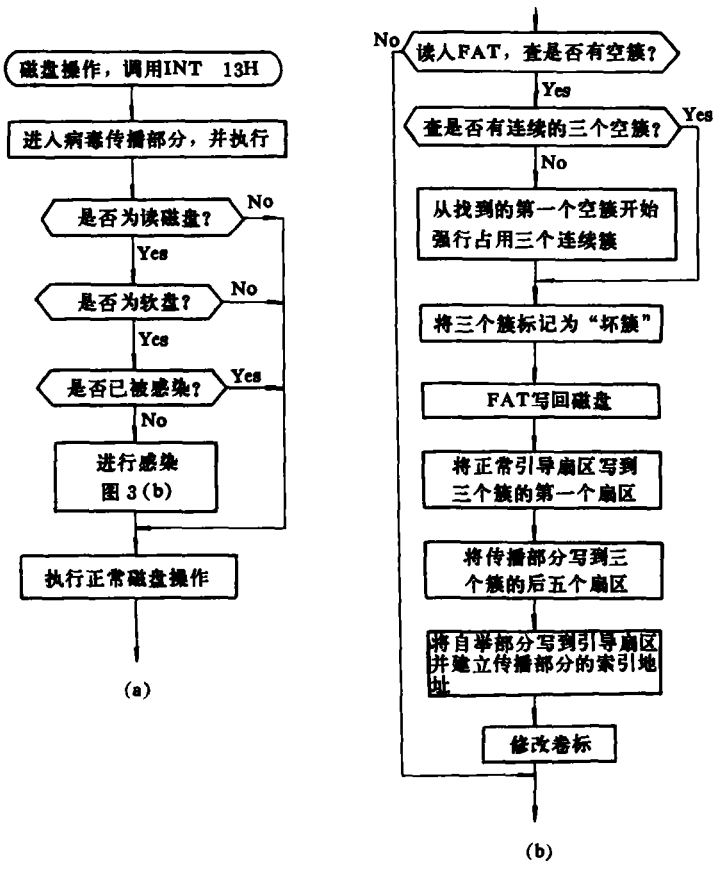


图 3 BRAIN 病毒传播部分工作流程

为坏簇，则表明有可能存在 BRAIN 病毒。所谓有可能，是因为如果清除了病毒自举部分，而未进一步修改 FAT 和 FDT，仍会出现上述情况。

彻底消除 BRAIN 病毒，应做如下工作：

(a) 重写引导扇区内容；

(b) 恢复 BRAIN 病毒所占“坏簇”；

(c) 破坏自举部分和传播部分的连接地址；

(d) 修复卷标。

可以利用 DEBUG 来完成上述工作，具体过程为：

(a) 在无病毒系统中，以 A 盘读出正常的 DOS 引导扇区，写入含有 BRAIN 病毒的 B 盘引导扇区。

```
-L  100  0  0  1 <CR>
-W  100  1  0  1 <CR>
```

(b) 重新标记病毒所占“坏簇”为可用簇，切断自举部分和传播部分的链接地址。

BRAIN 病毒在自举部分的第 6、7、8 字节分别存放了索引传播部分的面号、扇区号

和磁道号。读出后，将其转换为逻辑地址，并求得“坏簇”号。

设病毒传播部分占用 56H、57H 和 58H 簇，则如下操作：

```
-L 0 1 1 2 <CR>
-D 55 59 <CR>
    XXXX：0055 F7 7F FF-F7 9F
-E 55 00 00 00 00 90 <CR>
-W 0 1 1 2 <CR>
```

(c) 卷标的修复比较容易。在 DEBUG 状态下，通过查阅目录项的属性字段，将其卷标修改为所希望的名字，或者取消卷标。

(2) BRAIN 病毒的免疫

为了尽量避免病毒带来的困扰，有必要采取积极的防御措施，即病毒免疫。判断磁盘是否感染了某种病毒是根据磁盘中某一特定位置是否包含了这种病毒 的标志。例如，BRAIN 病毒是在逻辑 0 扇区的第 5、6 字节中存放 3412H 作为其标志。这样讲来，如果能在磁盘受病毒感染之前，就在其特定位置写进病毒标志，即可避免受其侵害。

例如：免疫 BRAIN 病毒

在系统无病毒情况下，运行 DEBUG。设要接受免疫的软盘放在 A 驱动器。

```
-L 100 0 0 1 <CR>
-E 104 34 12 <CR>
-W 100 0 0 1 <CR>
```

(3) 小结

上述病毒消除及免疫，我们是利用了调试工具 DEBUG 完成的。为了节省时间，避免对磁盘的误操作，成批地实现 BRAIN 病毒的防治，提高效率，可以将上述实现思想用一个汇编程序体现出来。在无病毒的系统中，运行这个程序，即可消除染有 BRAIN 病毒的磁盘，并且为尚未染有病毒的磁盘提供免疫能力。

## 4 结束语

至此，我们阐明了病毒的概念和原理，分析了 BRAIN 病毒，并且介绍了消除这种病毒及其免疫的方法。值得注意的是：这里叙述的方法并不能包医百病，因为病毒种类繁多，它们的类型、结构、传播原理和表现形式等均不完全相同，这就使得其检测和消除难以采取统一的措施。

在实际中，下述现象可以在一定程度上帮助用户尽早发现病毒：

(1) 屏幕出现无意义显示；

(2) 可执行文件长度发生变化；

(3) 写保护软盘出现未经授意的写操作错误；

(4) 磁盘出现坏簇；

(5) 文件或数据丢失；

(6) 可用内存空间变小；

(7) 出现来历不明的隐藏文件或系统文件；

(8) 机器速度变慢；

(9) 磁盘访问时间变长。

(10) 系统启动时间变长或程序装入时间变长；

(11) 系统出现异常重启动或经常死机；

(12) 机器喇叭出现蜂鸣声。

病毒的防治，最重要的一点是预防，以争取最大的主动性，避免病毒的困扰。病毒的预防既要从技术和使用上，也要从管理制度上着手。我们建议：

(1) 制定规章，甚至立法，制裁病毒制造者；

(2) 加强用户职业道德的培养；

(3) 加强管理，包括专机专用，集中管理系统软件和常用软件等；

(4) 谨慎使用公用软件、共享软件以及来历不明的软件；

(5) 禁止玩游戏；

(6) 对系统盘和文件进行写保护，不要将用户文件和数据写到系统盘；

(7) 对重要信息做备份；

(8) 在配置硬盘系统中，尽可能使用无病毒硬盘启动，并采取必要的硬盘保护措施；

(9) 定期检测病毒，发现之后及时消除；

(10) 在计算机网中，限制可执行代码的交换。

本文的目在于使读者系统地了解病毒的概念、原理和防治等知识。目前，国内外有不少人正从事于这方面的研究，并取得了一定的成果。作者希望本文能对读者有所帮助。

## 参 考 文 献


[1] Cohen F. Computer Viruses; Theory and Experiments Computer and Security, 1987, 6(1)

[2] John M. The Virus Cure. DATAMATION 1989, 15 (4)

[3] 熊璋. 计算机病毒与防治. 计算机世界报, 1989, (28)

[4] 季宗水, 裘杰. 计算机病毒的消除及预防. 计算机世界月刊, 1989, (1)


## The Prevention and Cure of Computer Virus


Liu Binhai

(Department of Computer Science)



### Abstract

This article approached comprehensively the conception, principle, prevention and cure of computer viruses, we analysed the mechanism and propagation principle of Pakistani Virus, and discribed ways to prevent and cure this virus, including thd elimination way and the immunity way. In addition, this article illustrated that no thorough common way can be obtained to prevent and cure all the viruses, and a concrete analysis of concrete virus must be made. The most effective measure is the virus prevention.



**Key words** microcomputer system, computer virus, pakistani virus