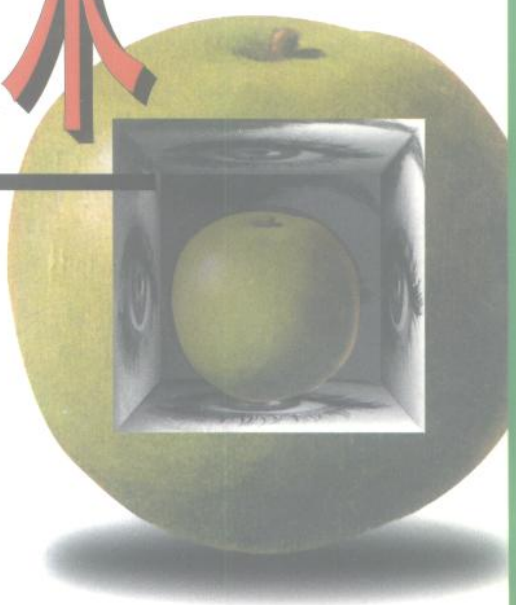
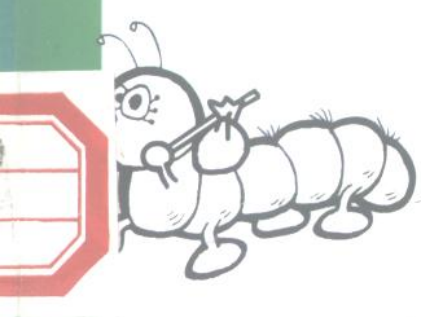
计算机病毒防治实用技术

袁忠良 主编





清华大学出版社
http://www.tup.tsinghua.edu.cn

计算机病毒防治实用技术

袁忠良　主编

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书叙述了计算机病毒防治的实用技术，包括计算机病毒的概念及特征、DOS 平台病毒的防治、Windows 平台病毒的防治、网络病毒的防治和病毒的分析与清除。

本书可作为广大计算机用户防治计算机病毒的工具书或参考书使用。

图书在版编目(CIP)数据

计算机病毒防治实用技术/袁忠良主编. —北京：清华大学出版社，1998.4

ISBN 7-302-02928-8

Ⅰ.计… Ⅱ.袁… Ⅲ.计算机病毒-防治 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（98）第 08674 号

出版者：清华大学出版社(北京清华大学校内，邮编 100084)
http://www.tup.tsinghua.edu.cn
印刷者：北京清华园胶印厂
发行者：新华书店总店北京科技发行所
开 本：787×1092 1/16 **印张**：25.75 **字数**：642 千字
版 次：1998 年 5 月第 1 版 1998 年 9 月第 2 次印刷
书 号：ISBN 7-302-02928-8/TP・1476
印 数：5001～11000
定 价：28.00 元

前　言

1977年，一些科幻小说的作者借用了生物学中的术语——病毒，将其引入计算机领域。当时认为这是荒诞的，但以后的事实却说明了计算机系统运行的一些程序在计算机实体间的活动过程同生物学中的病毒极为相似。当然，在计算领域中，计算机病毒的概念则有特定的内涵和外延。

从1987年美国的F. Cohe提出计算机病毒的概念到现在，计算机病毒的研究已经形成一门属于计算机领域中新兴的学科，即计算机病毒学。计算机病毒学是一门专门研究计算机病毒的产生、活动机制、传染机制以及计算机病毒免疫和防治的科学。研究计算机病毒学的目的，在于研究如何防止和抑制计算机病毒，作为一门新兴的学科，它是计算机程序设计技术发展与计算机技术发展极不平衡及当今操作系统开放性与折中性和倾斜性的产物。

正当计算机以日新月异的速度迅猛发展、广泛地深入到社会生活的各个方面的时候，计算机病毒的出现给全社会不仅仅是计算机工作者，而且包括政府、法律部门、各级领导乃至普通的工作人员敲响了警钟。一种新的利用计算机作为工具的高新技术犯罪正成为日益严重的社会问题。

微型计算机的出现将计算机引入家庭，大量的软硬件产品得到开发和运用。以计算机为核心的信息产业成为一个国家现代化水平的一个标志。在这种情况下，计算机病毒的出现和广泛传播正成为各国政府关注的一个问题。

虽然报刊杂志上均不同程度地报导了一些病毒的检测、清除方法和病毒的简单工作原理，为防止计算机病毒的泛滥，向计算机用户和微机使用人员介绍《计算机病毒防治实用技术》一书，使读者能较系统地了解计算机病毒的有关知识和清除方法，在遇到病毒侵袭时能尽快排除，减少损失。

全书共六章。第一章计算机病毒概念及特征，重点介绍计算机病毒的基础知识及主要特征。第二章DOS平台病毒防治，重点介绍计算机病毒的诊断方法及各种防病毒软件。第三章Windows平台病毒防治，重点介绍Word宏病毒的防治方法。第四章网络病毒防治，重点介绍网络病毒的防治方法。第五章病毒防治经验，汇总广大微机人员防治病毒的有效经验，供读者借鉴。第六章典型病毒分析与清除，按引导型病毒、文件型病毒、混合型病毒分类进行典型病毒的分析并介绍清除方法。

本书所列举的大量实例都是国内外广大用户在防病毒工作中亲身实践并经过总结提炼而成的，具有较强的针对性和实用性，可供读者直接借鉴。本书各章节自成体系，互相独立，可以根据实际需要有选择地阅读或查用有关章节，而无需按顺序阅读。

参加本书编写的有：袁庆华、尚法制、解可新、黄树基、王建勋、李向林、王秀平、袁胜华、朱静，由袁忠良负责全书的组织和定稿。

由于我们水平有限，书中定有疏漏和不妥之处，敬请读者和用户批评指正。

编 者

1997 年 6 月 2 日于天津大学

目　录

第一章　计算机病毒的概念及特征

1.1　什么是计算机病毒

计算机病毒是一种特殊的程序。由病毒程序引起的问题，属于软件故障，而不是硬件故障，诸如系统不能正常引导、程序不能正确执行、文件莫明其妙地丢失等等现象。

病毒程序区别于通常程序，它有以下特点：

病毒程序的存在是隐蔽的，它总是悄悄地附着在磁盘系统区或文件中。寄生于文件中的病毒是文件型病毒。其中病毒程序附在原来文件之前或之后的，称为文件外壳型病毒，如黑色星期五病毒、新世纪病毒、耶鲁撒冷病毒等等。另一种文件型病毒为嵌入型，其病毒程序嵌入到原来文件之中。病毒程序侵入磁盘系统区的称为系统型病毒，其中较常见的占据引导区的病毒，称为引导型病毒，如火矩病毒、大麻病毒、漂亮女孩病毒等等。带有病毒的磁盘上原来主引导区或引导区的内容被移到磁盘其它特定位置，或者被病毒程序归并。此外，还有一些既寄生于文件中又侵占系统区的病毒，称为混合型病毒，如 Flip 病毒、幽灵病毒、穷人病毒等等。

计算机病毒有两种存在方式：

1. 静态存在方式：计算机病毒寄生于磁盘、光盘等存储介质中，或存在于内存 RAM 虚拟盘，外部 RAM 盘或 ROM 盘，处于这种方式的病毒是“静态”的，不会去主动传染其它程序，更不会发作。当关机时，除了在内存 RAM 虚拟盘的病毒会消失以外，计算机外部存储介质上的病毒都会继续存在。静态病毒并不可怕，可怕的是它变成动态病毒。

2. 动态存在方式：计算机病毒已经被调入内存，已经或随时可以获得控制权，此时病毒可能马上传染或发作，即进入活跃态，也可能将自身驻留于计算机的内存之中进入潜伏态，一旦被激活就会进行传染和发作。病毒这种寄生在内存中的动态存在方式对用户来说是十分危险的，它像是一颗炸弹，随时会爆炸。不过，只要一关机动态病毒就消失。因此，消除计算机病毒的关键还是要清除静态病毒。没有静态病毒，自然就不会出现动态病毒。

病毒程序在一定条件下隐藏地进入系统。当使用带有系统病毒的磁盘引导系统时，病毒程序先进入内存并放在常驻区，然后才引导系统，这时系统即带有该系统病毒。当运行带有病毒的程序文件(COM 文件或 EXE 文件，有时包括覆盖文件)时，先执行病毒程序，然后才执行该文件的原来程序。执行病毒程序以后，有的病毒将自身程序常驻内存，使系统从此处于该文件病毒环境；有的病毒则不常驻内存，只在当时执行时起传染或破坏作用。执行完毕之后病毒不再留在系统中。

病毒程序执行的是非授权(非法)操作。当用户引导系统时，正常的操作只是引导系统，病毒乘机而入并不在人们预定目标之内。当运行带病毒文件时，执行该文件的原来程序是人们的预定目标，在此之前先执行的病毒程序并不是人们预定目标。但是，由于病毒程序的寄生性和进入的隐蔽性，人们开始时往往觉察不到它的存在和执行，直到产生比较严重后果时

才有所发现。

病毒程序所执行的非授权操作，通常包括以下几个方面：

1. 将病毒程序常驻内存。为此，修改一些系统参数，扩大内存常驻区，缩小用户可用空间大小，并将病毒程序存放到内存常驻区之内，使得当用户程序进入系统时，不占用病毒程序存储范围。

同时，为了使常驻内存的病毒程序监控系统运行情况，病毒程序还修改操作系统的中断向量表，即修改某些常用中断程序的入口地址，用病毒程序中某些段落的起始地址去代替它们。这样，当用户程序或DOS命令要求执行这些中断程序时，例如要求向磁盘写入或进行读操作时，以及文件操作、时钟操作等，对于感染了病毒的系统来说，实际上并不是立即执行所需求的中断程序，而是先执行了一段病毒程序，然后才能去执行正常的中断程序。这就使得调用这些中断时要付出额外的时间开销。

2. 在一定条件下，会“复制”病毒程序，即所谓“传染”、“感染”。病毒程序一旦进入正在运行的系统，它就如同盘踞在蜘蛛网中央的蜘蛛，虎视眈眈地监视磁盘和文件，一旦发现它们尚未感染病毒，就在适当时机，例如要执行某个系统中断程序时，先将病毒程序写入磁盘或文件中。这时，我们便称为这个磁盘或文件已经感染了病毒。

3. 在一定条件下进行破坏活动。例如，小球病毒在系统运行过程中会突然使屏幕上出现一个跳来跳去的小球，把屏幕显示弄乱，而以色列病毒在“黑色星期五”(既是13日又是星期五的日子)将使每一个要运行的程序消失不见，有些病毒“激活”(即发作)时会使整个磁盘内容受到破坏。在这些破坏中，像屏幕产生异常显示但不影响系统继续运行，特别是不破坏磁盘或文件的，属于“轻微”或有恶作剧的意思，又称为“表现”这种病毒也称为是“良性”的。而破坏磁盘或文件的病毒，则被称为是“恶性”的。

计算机病毒的定义是计算机病毒学的基本概念，它的科学定义是这样的：计算机病毒是隐藏在计算机系统的数据资源中的，利用系统数据资源进行繁殖并生存，能影响计算机系统正常运行并通过系统数据共享的途径进行感染的程序。

现在，对计算机病毒的定义有多种，但无论怎样定义都必须肯定这样一个事实，即计算机病毒实际上是一种特殊的程序。

1.2 计算机病毒的背景及起源

对计算机系统的攻击具有多种形式。最早期的一种是特洛伊木马程序(Trojan horse program)。借用古代特洛伊战争中，把士兵隐藏在木马中进入敌方城堡，出其不意而攻占城堡的故事，来表示某些有意骗人犯错误的程序。这由程序开发者开发一个表面上很有魅力而且显得可靠的程序，可是使用者使用一定时间或运行一定次数后，便会发生故障，出现各种问题。

1977年，Thomas . T. Ryan的科学幻想小说《The Aulescence of P－1》轰动了美国科普界。作者幻想出世界上第一个计算机病毒，可以从一台计算机传染到另一台计算机，最终将控制7000台计算机的操作系统，从而酿成一场灾难。有人认为，这实际上是计算机病毒的思想基础。

20世纪70年代后期，电子公告栏(BBS)在美国流行起来，计算机编程者所写的程序不

想在电子公告栏上被别人随意录下，而损坏自己的利益，便发展出一些间谍程序，要求使用者付账后，再将完整版本或密码交给使用者。

1982年，Shoke和Hupp提出了一种“蠕虫”(worm)程序的思想。这种蠕虫程序常驻于一台或多台机器中，并有自动重定位的能力。如果它检测到网络中的某个机器未被占用，便把自身的一个拷贝发送到那台机器，如此递归下去，便可检测到网络上一些机器的情况。1987年圣诞节那天，在IBM的全球网络上，一只圣诞树蠕虫活动起来，把整个网络弄成瘫痪。原来是那天有人受蠕虫诱惑，执行了蠕虫的程序“CHRISTMAS”，在屏幕上绘出一株圣诞树，并沿着使用者的资料，把它送到网络上的其它电脑上去。

1984年5月，Dewdney提出了一种叫做“磁心战”(Core war)的游戏，其大意为，“编写一个程序，用来分配计算机存储器内某个限定容量的空间，该空间由连续的单元构成。按模运算使得该存储器循环。然后再编写两个或更多个汇编程序，这些程序的唯一用途是试图破坏其它程序。它们被装填到任意的一些非覆盖区中并被执行，通过使用自动重定位，每个程序按存储器循环周期每次一条指令地逐渐接近其它程序。结果有二：若已执行N条指令仍未接触到对手，则为和局；否则，被对手修改而不能执行某条指令的一方为败者。

1984年，Fred Cohen获准首先在运行UNIX操作系统的VAX 11/750机上进行病毒试验。在5次试验中，使计算机系统工作瘫痪所需的平均时间为30分钟，最短为5分钟。他认为在对某特定系统有个基本了解的条件下，可以构成一种病毒代码，该病毒代码容许攻击者在平均30分钟内使大量程序受到感染，从而控制整个系统。此后，一些公司为了保护他们的软件不被非法复制，在发行软件中加入病毒，以期打击非法复制者。这就助长了各种病毒的传播。虽然在这类病毒中尚未发现恶性病毒，但他们的变种却可能造成严重的灾难。计算机病毒的另一个起源是一些恶作剧者、计算机狂以及在工作中心怀不满、蓄意报复的人，他们对计算机系统往往比较熟悉，也容易编写计算机病毒。

1980年，IBM公司的PC系列微型计算机逐渐成为世界微型计算机市场上的主机机型，由于其性能优良、价格便宜、发展潜力大，所以深受广大计算机用户的欢迎。但是，由于IBM-PC系列微型计算机系统自身的弱点，尤其是DOS操作系统的开放性，给计算机病毒的制造者们提供了可乘之机。因此，装有DOS操作系统的微型计算机成为其攻击的主要对象。

到1987年，即经过10年的时间，计算机病毒的幻想终于变成了现实。

1987年10月，在美国本土，世界上第一例电脑病毒(Brain)被发现，并以强劲的势头迅速蔓延。随后，其它病毒也相继出现。

1988年，各种病毒开始大肆流行。

1988年11月2日，世界上有史以来最严重的一次计算机病毒侵袭事件发生在美国康乃尔大学。该大学的一年级研究生罗特·莫里斯制作了一个蠕虫计算机病毒，并将其投入到美国Internet计算机网络中。该病毒从11月2日上午5时开始发作，到下午5时已使美国军事系统计算机网络中的6000多台计算机工作站受到感染，许多联网计算机被迫停机。直接经济损失达9600万美元，造成了不可收拾的局面。莫里斯也由此受到了法律的制裁。莫里斯的蠕虫事件引起了美国全社会和计算机界的震惊，专家们在法律、道德、反病毒技术等方面发表了大量的评论，许多公司、研究所纷纷发表道德宣言，表示要教育职工、学生不得制造也不得传播计算机病毒。

一般认为计算机病毒的发源地在美国。虽然尚无确切的统计资料，但据称1990年前在美国发现的计算机病毒已有140多种。如果加上这些病毒的变种，那就更是难以计数。在我国，计算机病毒虽然侵入时间不长，但也已发现多种病毒及其变种。如果能及时有效地普及计算机病毒的有关知识，那么有希望扼制住病毒泛滥的势头。

1.3 计算机病毒的来源渠道

计算机病毒的来源渠道主要从以下5个方面：

1. 盗版软件

盗版软件在互相拷贝流传的过程中，根本无法保证不会被病毒所寄生；而且因为盗版是一种非法的行为，故制造病毒的人，会专门利用盗版软件来传播他的作品，以避开法律的责任。

2. 公开软件

无论是完全开放的公开软件，或是半开放的共享软件，都是容许人们随便拷贝的。跟盗版软件一样，人们根本无法确认该公开软件是否有病毒寄生，但由于是合法的行为，故其带病毒的机率不如盗版软件高。

3. 电子公告栏

在使用电子公告栏(BBS)时要注意，由于任何人都可以随便地从公告栏载上或录下文件，所以根本无法保证录下来的程序是否有病毒寄生。

4. 通讯与网络

与电子公告栏的情况相似，我们无法保证传来的程序，或远程请求的程序有没有病毒寄生或感染。

5. 正版软件

有些软件公司，为了避免被盗版使用，会在其产品中放入口令暗号检查的程序，这种程序可促动早已准备好的类病毒病发，对盗用者示以惩戒。

了解计算机病毒来源渠道之后，在使用操作微机过程中，应注意软件的来源，尽量不与外界的软盘交换，提防病毒侵袭自己的微机。

1.4 计算机病毒的存储方式

计算机病毒的存储方式有两种：第一种是内存驻留方式，第二种是磁盘存储方式。驻留内存是计算机病毒能够发挥作用的必要条件，而磁盘存储是病毒存在的客观条件。我们只要破坏掉病毒存储方式中的任意一种，都可以使计算机病毒丧失其原有特性，从而也保证了我们的计算机系统免受计算机病毒的侵扰。

1. 内存驻留方式

病毒在内存中驻留的关键是选择存储空间，因而有以下几种内存驻留方式。

(1) 减少DOS系统可分配空间

PC DOS在0040:0013H处有一两字节的变量表示系统有多少可用的内存分配空间。如单元中有1FFH值，则表示内存可分配空间为512KB，计算机可用内存分配空间的公式是：

可用内存空间量＝单元内存值＋1(KB)

当用户执行 INT 12H 时，返回的就是用此公式计算的内容。在 0040:0015H 处 DOS 也有一个字变量，该变量用来表示除去系统基本配置以外的扩充可用内存分配空间。此单元以 KB 字节为度量单位。有关系统配置的参数值，都由 ROMBIOS 在系统自检时填充。病毒制造者可以在系统完成自检后，选用适当的方法将 40:13H 和 40:15H 两字节中的内容加以修改，从而减少 DOS 系统可分配空间，为其病毒开辟一个足够的空间。利用这种方法开辟的空间均在内存高端。用 DOS 系统的中断和功能调用检查不出减少的空间，因此也就不存在被 DOS 系统文件及用户文件覆盖的问题，病毒采用这样的方式驻留内存，使病毒的隐蔽性大为提高。

(2) 利用系统的间隙

如 DOS 系统中位于 50:00H～50:1FFH 的区域中只建立了一个软盘基数表，除此之外填入任何参数值，都不构成对 DOS 系统正常运行的威胁，在这段区域中足以存放一个病毒程序。另外，还有一些其它的内存空间都可以被病毒所利用。

(3) 利用功能调用驻留

DOS 系统为用户提供了程序驻留内存的中断和功能调用，这些功能也可用来加载计算机病毒。在一般情况下，这种方式经常被过程病毒使用。如使用 INT 21H 的 31H 功能，在进入时，AL 内是一个二进制的出口代码，DX 内是用段表示的内存容量的数值。这个功能调用终止当前的处理，并准备把开始分配的数据块记录置成 DX 内的段数，它将不释放属于这次处理过程的任何其它分配的数据块。实例如下：

```
MOV    AL,返回代码
MOV    DX,块大小
MOV    AH,31H
MOV    21H
RET
```

病毒程序在使用以上的驻留方式时，应与依附的主程序分离，使用较多的分离方式时应分段放置。

(4) 利用系统程序的使用空间

占用系统使用空间的方式又称为程序覆盖方式。这种方式可以在系统程序占用的有效空间内，选择一些不常使用的部分加以替换，使病毒不需要申请空间便可实现病毒在内存的驻留。

2. 磁盘存储方式

要防治计算机病毒，就必须了解病毒在磁盘上可能的存储方式。一般情况下，计算机病毒存储在磁盘中的前提条件是，病毒能够被系统重复载入内存，并且在条件成熟时，可获得对系统的控制权。目前较为流行的方式有文件驻入式和直接存取式两种。

(1) 文件驻入式

病毒的存储或传染多以可执行文件为主。.EXE 文件是由控制模块和代码模块两部分构成。在文件控制模块中，包含着指向第一条可执行指令的指针值和装入内存之后的段值修正量。这两个有效信息均存在文件控制模块中位移为 14 和 16 的两个字中。病毒程序可以通过修改这两个值，使得执行文件的第一条指令变为病毒程序的指令，从而能够保证病毒程

序对系统控制权的获取。病毒驻入.EXE 文件的一般步骤是：

① 打开选定的传染目标文件

② 修改文件头信息

③ 将文件指针移到文件尾

④ 将病毒体顺序写入磁盘文件

⑤ 关闭文件

⑥ 结束本次传染

病毒对.COM 文件的传染一般有两种方式。一种是将病毒程序从位移 100H 单元处插入；另一种是将病毒程序驻入文件的结尾部。病毒插入.COM 文件的一般步骤是：

① 打开欲传染的目标文件

② 判定文件大小是否适宜传染

③ 如可传染执行④，否则转⑧

④ 将病毒程序移入数据区

⑤ 计算正确程序的代码段值，并存入特定单元

⑥ 将打开文件读入数据区，并拼接在病毒程序之后

⑦ 将数据区中所有程序存入磁盘文件

⑧ 关闭文件

⑨ 退出本次传染操作

(2) 直接存取扇区

目前通过直接存取方式可驻入的磁盘区域有：

① 主引导记录区

② 引导记录区

③ 文件分配表

④ 文件目录区

⑤ 数据存储区

在这 5 个区域中，只有存入主引导记录区和引导记录区中的病毒程序有获得系统控制权的条件，而在其它区中存储的病毒程序，必须借助一定的加载手段，方可获得系统的控制权。

1.5 计算机病毒的感染媒介与途径

计算机病毒的感染媒介主要有两个：一个是磁介质，主要是软盘和硬盘；一个是计算机网络，对于微机而言，主要是局域网。由于我国目前计算机网络的开发利用还不普遍，因此二者比较，计算机病毒的感染媒介又以软盘、硬盘为主。

在微机系统中，由于硬盘容量大，读写速度快，所以用户读写文件主要是在硬盘上，因此硬盘就成了病毒的载体，也就成了再次感染病毒的媒介。

由于软盘具有携带方便及存储容量大等特点，因此成为感染病毒的主要媒介。目前很多单位互相交流应用软件、汇总数据资料等均使用软盘。如果将带有病毒的软盘在其它系统中使用，病毒就传染给使用该盘的系统。

计算机网络是在网络操作系统的支持下，采用某些计算机技术，以实现资源共享的环境。其中包括中心机服务器、工作站、用户终端等设备。在共享资源时，需要网中的通信系统传输数据和文件，如果被传输的文件染有病毒，那么这些病毒就会通过局域网传播到四面八方，因此，计算机网络也是病毒感染的一个媒介。

计算机病毒感染途径主要有以下两个方面：

1. 破坏操作系统式病毒的感染途径

若微机利用受到破坏操作系统式病毒所寄生的磁盘来建立 DOS 的话，在建立的同时，病毒便会感染到系统中去，例如对所有软磁盘、硬盘的读写动作，都极有可能让病毒感染、寄生。

2. 破坏应用程序病毒的感染途径

破坏应用程序病毒的感染途径较破坏操作系统程序病毒为多，它可以利用文件通过拷贝而传播，或以执行中的程序来找机会感染到下一个目标去，再加上通讯和网络系统，它就能把繁殖的范围扩展到别的电脑系统和文件服务器中。

1.6　计算机病毒是谁制造的

制造计算机病毒者，归纳起来有 7 类人：

1. 玩家

可能是个人，也可能是群体，因为他们迷恋于电脑的世界中，为了证明实力，或者找寻新的成就感，他们便会尝试着去编写一些新病毒。

2. 学生、研究生和学者

他们在一个自由又开放的环境中，拥有完善的设备，有人为了做研究或贪玩，试着发展和写作病毒。由于环境的不同，他们大多编写一些大型系统上运行的病毒或类病毒。

3. 职员

为了达到报复，或其他特别目的，有些职员会在公司的电脑系统中放入病毒或类病毒，达到不可告人的目的。

4. 电脑学会

在国外，有些电脑学会专门提供写作病毒的技术数据，传播电脑病毒。

5. 恐怖组织

有充分证据证明，有些组织或恐怖组织，专门研究和发展一些病毒来破坏敌对国家、政府或组织的电脑资源系统。

6. 软件商

有些软件公司，为了避免自己出售的软件被盗用，会在其产品中放入检查口令暗号的程序，从而会促动早已准备好的类病毒病发，对盗用者以示惩罚。

7. 电子公告栏的程序设计者

电子公告栏的程序设计者不想在电子公告栏上，被别人随意录下自己设计的程序，而损害自己的利益，便发展出一些间谍程序，要求使用者付账后，再将完整版本或密码交给使用者；否则间谍病毒病发，破坏使用者程序，从而保护自己的利益。