最流行软件丛书

谭浩强 主编

计算机反病毒软件

STOP-VIRUS

马 严 编著

国防工业出版社

计算机反病毒软件
STOP-VIRUS

马 严 编著

国防工业出版社

（京）新登字106号

图书在版编目(CIP)数据

计算机反病毒软件STOP-VIRUS/马严编著．—北京：国防工业出版社，1995.3
（最流行软件丛书/谭浩强主编）
ISBN 7-118-01288-2

Ⅰ．计… Ⅱ．马… Ⅲ．计算机病毒-防治-程序系统 Ⅳ．TP309

国防工业出版社出版发行
（北京市海淀区紫竹院南路23号）
（邮政编码 100044）
北京市怀柔新华印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 13¾ 310千字
1995年3月第1版 1995年3月北京第1次印刷
印数：1—4000册 定价：14.00元

丛书总序

电子计算机正以空前的速度发展，微型计算机更是其中的佼佼者，它几乎已深入到社会生活的一切领域。随着微型机的普及应用，众多的软件应运而生，其中有些软件因其功能丰富、实用性强、普及性好而流行于世。要使微型机发挥更大的作用，就必须掌握和熟悉这些软件的使用方法和技巧。为了适应广大初、中级计算机使用者的迫切需要，我们经过反复研究，特组织编写这套《最流行软件》丛书。我们企望尽此绵薄之力推动计算机在我国进一步普及应用。

本丛书采取“一种软件一本书”的模式，分别介绍国内广泛流行和经常使用的软件，力图突出其实用性强、普及面广、内容新颖、品种配套、概念清晰、通俗易懂等特点。

本丛书不同于计算机厂商销售的“使用手册”，也不同于一般教材。现在市面上有些译自国外资料的使用手册，虽然内容详实，但往往由于各种原因而难以阅读和理解，不适合于初、中级计算机使用者学习。考虑到多数读者的实际情况，我们采用循序渐进，深入浅出的编写方式，力求使那些从未接触过该软件的读者也可以做到“学了就能用，用了就见效”。限于篇幅不宜过大，每本书仅介绍该软件最基本、最常用功能的使用方法和技巧，不拟囊括其全部细节，也不列举较大规模的例题。一般也不详细介绍基本原理和名词概念，而以教会如何使用为目的。读者在掌握基本使用方法以后，可以通过实践更深入更巧妙地去使用有关软件。

考虑到国内微型机配置的现实情况，本丛书以 IBM PC 机及与其兼容的长城系列微型机上广泛使用的软件为主，兼顾其他。鉴于软件版本翻新很快，拟以当前广泛流行的版本为基础，并根据发展，不断更新。

本丛书的选题是根据我国软件应用发展状况和广大读者急需来确定的，特约高等院校和科研、设计单位有丰富实践经验的专家参加编撰，拟陆续分期分批奉献于世。“问渠哪得清如许，唯有源头活水来”。我们热切希望专家和读者能及时向我们提供有关信息，以使本丛书在选题、编撰、出版、发行等环节更具针对性和实时性。

本丛书无论在选题策划还是在编写细节上都可能会有不足甚至错误之处，恳切希望大家批评指正。谢谢！

丛书主编

谭浩强

前　言

“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。”① 由于计算机特别是IBM-PC及其兼容机近年来得到了非常广泛的应用，计算机病毒的传染及它对计算机正常工作和对存储在磁盘中的数据造成的破坏，将给用户带来严重的后果。

从1989年起，计算机病毒就已在我国出现并开始广泛传播。为清除计算机病毒、修复被病毒破坏的计算机系统，作者开始涉足这一反病毒研究领域。通过开发抗病毒系统和从事大量的系统维护、修复以及病毒防御工作，深感反病毒工作是一项实践性很强的工作。为有效地抵御计算机病毒的攻击，不仅需要使用商品化的反病毒软件，还需要增强抗病毒的思想准备和掌握一些手工检测及清除病毒的方法，以对付新出现的，尚不能被反病毒软件处理的病毒。本书介绍了这方面的知识，总结了一些实践经验，介绍了一些方法，希望能对读者有所帮助。

全书共分五章。第一章讨论了什么是计算机病毒，计算机病毒的特点，计算机病毒能通过哪些渠道传染到计算机中，以及反病毒技术的发展情况。第二章从抗病毒的立场出发来讨论IBM-PC机和DOS系统，这是反病毒技术的基础。第三章在介绍几种常见病毒之前讨论了病毒采用的特殊技术。第四章和第五章是本书的重点。第四章介绍检测和清除病毒的原理、常见清毒软件的使用方法及如何利用DOS的DEBUG程序在没有专用清毒软件时发现和清除病毒，特别是对付新出现的病毒。第五章介绍根据实践经验总结出来的预防计算机病毒的方法。防病毒卡是一种重要的抗病毒技术手段，利用这种手段再加上有效的管理措施，计算机病毒是完全可以被控制的。

我要感谢国防工业出版社陈子玉老师对我的鼓励和帮助，没有她和丛书编委会的支持，我没有机会完成这本书的写作。还要感谢沈树雍教授抽出他宝贵的时间仔细审阅全书。感谢魏伯丛高级工程师对作者的研究工作给予的大力支持。

本书写作十分仓促，错误和不足之处在所难免，希望读者不吝指正。

编　者

① 引自《中华人民共和国计算机系统安全保护条例》1994年2月28日国务院令174号。

内 容 简 介

最流行软件丛书系由著名计算机教育专家谭浩强教授主编。本从书采取“一种软件一本书”的模式，以教会如何使用为目的，分别介绍国内广泛流行和经常使用的软件，具有实用性强、普及面广、内容新颖、品种配套、概念清晰、通俗易懂等特点。

本书是该丛书之一，介绍目前最流行的几种计算机病毒检测、清除与预防软件。书中除介绍了什么是计算机病毒、计算机病毒的分类、计算机病毒与计算机系统的关系及计算机病毒对计算机系统的破坏作用外，还介绍了目前国内流行的 CPAV 等几种抗计算机病毒软件的使用方法，以及在没有抗计算机病毒软件而只有基本的 DOS 系统软件时，如何发现和清除计算机病毒。书中还讨论了预防计算机病毒的几种方法。

本书的主要读者对象是具有高中以上文化程度的初、中级计算机使用者，也可作为需要开拓计算机应用面的大中专师生和科技工作者的自学读物。

目　录

第一章　反计算机病毒技术概论

在20世纪人类的所有重大技术发明中，电子计算机的发明占有绝对重要的地位。今天，我们已经很难想象，现代社会离开了计算机将会变成什么样。从人们的日常生活到工业生产，从政府部门到军事机关，到处都可以发现计算机正在发挥着不可替代的作用。

1945年世界上第一台电子计算机ENIAC诞生之后，人们在计算机的理论和应用等诸多领域里作了大量的工作。从当初的庞然大物发展到今日具有强大功能、而体积却小巧玲珑的微型计算机系统，计算机的硬件和软件技术得到了巨大的发展，高速的计算机每秒钟可以完成200亿次以上的运算，带有图形用户界面的个人计算机可以让儿童在短时间内学会使用它。

任何事物总有其两面性。在人们大力研究如何进一步增强计算机的处理能力，让计算机在现代社会中发挥更大作用的同时，对于计算机的安全技术的研究却没有给予更多的重视，没有意识到当计算机系统受到破坏时，它将给现代社会带来什么样的危害。

今天的计算机的处理能力是强大的，但它自身又是十分脆弱的。计算机系统内无论是硬件系统还是软件系统，关键部位稍受损伤就足以使整台计算机瘫痪。我们对计算机技术的应用和计算机安全的研究应当予以同等的重视，就如同发展现代工业必须重视环境保护和防止污染一样。

在计算机安全技术的研究中，计算机病毒防范的研究占有特别重要的地位。计算机病毒对计算机系统安全性的威胁现在已大大超过了以往各种计算机犯罪手段。计算机系统，特别是软件系统的核心——操作系统的脆弱性是计算机病毒产生的重要原因之一。

由于计算机病毒的破坏，造成成千上万台计算机瘫痪，给社会造成巨大损失的实例已遍及全世界。最著名的是1988年美国的Internet网络蠕虫（Worm）事件和1989年的黑色星期五病毒对IBM-PC及其兼容机的攻击。

1988年11月2日，美国最大的计算机网络Internet受到了称为蠕虫（Worm）的计算机病毒程序的攻击。该蠕虫程序在网络内无限制地复制自身，抢占了大量的时间和空间资源，在短短的半天时间内，使6000多台联网工作的计算机受到了感染而无法工作，被迫关机，造成了巨大损失。这是一起在计算机发展史上影响深远的事件，它使人们认识到计算机病毒的存在，计算机病毒对计算机系统安全的威胁，及其对现代信息化社会产生的危害。

另一个例子是被称为黑色星期五的计算机病毒，它专门攻击IBM-PC及其兼容机。在1989年11月13日，星期五，黑色星期五病毒经过长期潜伏、广泛传播之后，在全世界数十万台运行DOS系统的PC机发作。在这天里，用户每运行一个程序，该程序就被删除掉。它迫使许多PC机用户关机，因此造成的损失难以估计。

随着计算机病毒的大量出现和广泛传播，人们也加强了对抗计算机病毒的反计算机

病毒技术的研究，开发了各种抗病毒产品，有纯软件的，有硬件与软件技术相结合的。在不同程度上，这些已经商品化的抗计算机病毒产品阻止了病毒对计算机系统的渗透和攻击。某些商品化的计算机病毒检测软件已经可以识别出 2700 种以上的攻击 PC 机的病毒。某些计算机病毒防御系统还可以抗御一些未知病毒对计算机的攻击。但我们应该认识到，抵抗计算机病毒的斗争是件长期的事情。计算机病毒技术随着计算机技术的发展而发展，反病毒技术也需要不断发展，就像矛与盾的关系一样。敌人有了锋利的矛，我们要制造出坚固的盾，敌人发明了更新式的矛，我们就要造出更坚韧的盾来抵抗它。任何事物都有其发生、发展和演化的过程，反计算机病毒技术也是随着计算机病毒的发展而发展的。

1.1 计算机病毒的特征

“计算机病毒”一词最早是由美国计算机病毒研究专家 F. Cohen 博士提出的。“病毒”一词是借用生物学中的病毒。通过分析、研究计算机病毒，人们发现它在很多方面与生物病毒有着相似之处。要做反计算机病毒技术的研究，首先应搞清楚计算机病毒的特点和行为机理，为防范和清除计算机病毒提供充实可靠的依据。

1.1.1 计算机病毒的再生机制

再生机制是生物病毒的一个重要特征。通过传染，病毒从一个生物体扩散到另一个生物体。在适宜的条件下，它得到大量繁殖，并进而使被感染的生物体表现出病症甚至死亡。同样地，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。这就是计算机病毒最重要的特征——**传染和破坏**。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，就与系统中的程序连接在一起，并不断地去传染（或连接、或覆盖）其它未被感染的程序。具有这种特殊功能的程序代码被称为计算机病毒。携带有这种程序代码的计算机程序被称为计算机病毒载体或被感染程序。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。正常的计算机程序是不会将自身的代码强行连接到其它程序之上的。比如 DOS 的 FORMAT. COM 程序决不会将其程序代码连接到别的程序中去。在系统生成过程中有些系统的安装程序会修改相关程序的参数配置，如 MS-Windows 系统。有些程序通过自身的设置功能，按用户要求会修改自己的参数设置，如 Borland 公司的 SideKick。还有些程序出于加密防拷贝或某些其它目的，在运行时动态改变自身的程序代码，如 Xcom 通信程序。在这几种情况下，那些被修改的程序内部的确发生了变化，但这些变化只局限于各自应用系统的内部，不会发生将自身代码连接到毫不相干的程序之上的情形。计算机病毒的再生机制，即它的传染机制却是使病毒代码强行传染到一切未受到传染的程序之上，迅速地在一台计算机内，甚至在一群计算机之间进行传染、扩散。每一台被感染了计算机病毒的计算机，本身既是一个受害者，又是一个新的计算机病毒的传染源。被感染的计算机往往在一定程度上丧失了正常工作的能力，运行速度降低，功能失常，文件和数据丢失，同时计算机

病毒通过各种可能的渠道，如软盘、计算机网络去传染其它的计算机。当你在一台机器上发现了病毒时，往往曾在这台计算机上用过的软盘已感染上了病毒；而与这台机器相邻的其它几台计算机也许早已被该病毒侵染上了。通过数据共享的途径，计算机病毒会非常迅速地蔓延开，若不加控制，就会在短时间内传播到世界各个角落里去。可见反计算机病毒的问题是一个全球范围的问题。在我国发现的首例计算机病毒就是国外称为意大利病毒的小球病毒。在我国首先发现的 Traveller 病毒随着国际间的交往，也扩散到国外，其大名出现在国外杀病毒软件的病毒黑名单中。

与生物病毒不同，所有的计算机病毒都是**人为编写**的计算机程序代码，是人为制造出来的而不是天生的。这些着意编写的计算机程序代码，其原始形式可以是 C 语言，可以是 BASIC 程序，可以是汇编语言程序，也可以是批命令程序，还可以是机器指令程序。其共同特点就是具有传染性和破坏性。

1.1.2 计算机病毒与 CPU 的控制权

计算机病毒的另一个特点是只有当它在计算机内得以运行时，才具有传染性和破坏性等活性。也就是说**计算机 CPU 的控制权是关键问题**。若计算机在正常程序控制下运行，而不运行带病毒的程序，则这台计算机总是可靠的。在这台计算机上可以查看病毒文件的名字，查看计算机病毒的代码，打印病毒的代码，甚至拷贝病毒程序，却都不会感染上病毒。反病毒技术人员整天就是在这样的环境下工作。他们的计算机虽也存有各种计算机病毒的代码，但已置这些病毒于控制之下，计算机不会运行病毒程序，整个系统是安全的。相反，计算机病毒一经在计算机上运行，绝大多数病毒首先要做初始化工作，在内存中找一片安身之处，随后将自身与系统软件挂起钩来，然后再执行原来被感染程序。这一系列的操作中，最重要的是病毒与系统软件挂起钩来，只要系统不瘫痪，系统每执行一次操作，病毒就有机会得以运行，去危害那些未曾被感染的程序。病毒程序与正常系统程序，或某种病毒与其它病毒程序，在同一台计算机内争夺系统控制权时往往会造成系统崩溃，导致计算机瘫痪。反病毒技术也就是要提前取得计算机系统的控制权，识别出计算机病毒的代码和行为，阻止其取得系统控制权。反病毒技术的优劣就是体现在这一点上。一个好的抗病毒系统应该不仅能可靠地识别出已知计算机病毒的代码，阻止其运行或旁路掉其对系统的控制权（实现安全带毒运行被感染程序），还应该识别出未知计算机病毒在系统内的行为，阻止其传染和破坏系统的行动。而低性能的抗病毒系统只能完成对抗已知病毒的任务，对未知病毒则束手无策，任其在系统内扩散与破坏。所谓未知病毒是指新出现的，以前未曾分析过的计算机病毒。在 1992 年初，DIR- Ⅱ 病毒对我国广大 PC 机用户来说就是一种未知病毒。与未曾相识的敌手对阵不是件容易的事。DIR-Ⅱ 病毒采用嵌入 DOS 系统的设备驱动程序链的方法攻击 IBM-PC 及其兼容机，是一种与以往病毒工作机制不同的新型计算机病毒。由于其夺取 PC 机系统控制权的方法很特别，在它的攻势下，大批抗病毒系统败下阵来。从这个例子可以看到，对付计算机病毒，目前尚无完满通用的解决方案，反病毒技术需要不断发展，以对抗各种新病毒。

1.1.3 计算机病毒的隐蔽性

不经过程序代码分析或计算机病毒代码扫描，病毒程序与正常程序是不容易区别开来的。在没有防护措施的情况下，计算机病毒程序经运行取得系统控制权后，可以在不到1秒钟的时间里传染几百个程序，而且在屏幕上没有任何异常显示。传染操作完成后，计算机系统仍能运行，被感染的程序仍能执行，好像不曾在计算机内发生过什么。这种现象就是计算机病毒传染的**隐蔽性**。正是由于这隐蔽性，计算机病毒得以在用户没有察觉的情况下游荡于世界上百万台计算机中。让我们设想，如果计算机病毒每当感染一个新的程序时都在屏幕上显示一条信息"我是病毒程序，我要干坏事了"，那么计算机病毒早就被控制住了。确实有些病毒非常"勇于暴露自己"，时不时在屏幕上显示一些图案或信息，或演奏一段乐曲。往往此时那台计算机内已有许多病毒的拷贝了。许多计算机用户对计算机病毒没有任何概念，更不用说心理上的警惕了。他们见到这些新奇的屏幕显示和音响效果，还以为是来自计算机系统，而没有意识到这些病毒正在损害计算机系统，正在制造灾难。如磁盘杀手(Disk Killer)病毒，当它破坏磁盘数据时，屏幕上显示如下信息：

"Disk Killer Version 1.00 by Ogre Software, April 1, 1989.

Don't turn off the power or remove the diskette while processing."

这两句话中，第一句的含义是："磁盘杀手1.00版 Ogre Software 公司1989年4月1日出版。"

第二句的含义是："在处理过程中请不要关机或取出磁盘。"

接着屏幕上显示出

"PROCESSING"

意思是"正在处理"这时 Disk Killer 病毒锁定键盘，对磁盘上的数据做加密变换处理。计算机的处理速度是很快的，当你在屏幕上见到上述显示信息时，已经有很多数据被病毒破坏掉了。

计算机病毒的第二个隐蔽性在于，被病毒感染的计算机在多数情况下仍能维持其部分功能，不会由于一感染上病毒，整台计算机就不能启动了，或者某个程序一旦被病毒所感染，就被损坏得不能运行了。如果出现这种情况，病毒也就不能流传于世了。计算机病毒设计的精巧之处也在这里。正常程序被计算机病毒感染后，其原有功能基本上不受影响，病毒代码附于其上而得以存活，得以不断地得到运行的机会，去传染出更多的复制体，与正常程序争夺系统的控制权和磁盘空间，不断地破坏系统，导致整个系统的瘫痪。病毒的代码设计得非常精巧而又短小。典型的是 Tiny 家族。这个家族的病毒都很短小，最小的病毒代码长度只有133字节。一般 PC 机对 DOS 文件的存取速度可达每秒100KB以上，所以病毒将这短短的几百字节感染到正常程序之中所花的时间只是转瞬之间，非常不易被察觉。

1.1.4 计算机病毒的潜伏性与破坏性

与隐蔽性相关联的是计算机病毒的潜伏性。潜伏性的第一种表现是指，病毒程序不

用专用检测程序是检查不出来的，因此病毒可以静静地躲在磁盘或磁带里呆上几天，甚至几年，一旦时机成熟，得到运行机会，就又要四处繁殖、扩散，继续为害。潜伏性的第二种表现是指，计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做什么破坏。触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘以及使系统死锁等。

计算机病毒使用的**触发条件**主要有以下三种。

（1）利用计算机内的实时时钟提供的时间作为触发器　这种触发条件被许多病毒所采用，触发的时间有的精确到百分之几秒，有的则只区分年份。表 1-1 列出了一些病毒触发的时间，可以供防范计算机病毒时参考。

（2）利用病毒体内自带的计数器作为触发器　计算机病毒利用计数器记录某种事件发生的次数，一旦计数器达到某一设定的值，就执行破坏操作。这些事件可以是计算机开机的次数，可以是病毒程序被运行的次数，还可以是从开机起被运行过的总的程序个数等。

（3）利用计算机内执行的某些特定操作作为触发器　特定操作可以是用户按下某种特定的键组合，可以是执行格式化命令，也可以是读写磁盘的某些扇区等。

表 1-1　计算机病毒触发时间一览表

发作时间	病毒名称	备　注	发作时间	病毒名称	备　注
每月 1 日、星期二	Tuseday 1st			Demon-B	
每月 12 日、星期四	CD			Kamasya	
每月 13 日、星期二	Anarkia		每月星期三	Victor	
每月 13 日、星期五	1720		每月星期六	Italian Pest	
	Black Friday			Phenome	
	13th Friday		每月 2 日	Flip	
	RAM Virus			Tormentor-1072	
	Suriv 3.00		每月 5 日	Frog's Alley	
	Westwood		每月 8 日	Taiwan	
	Jerusalem-E	1992 年起	每月 10 日	Day10	
非每月 15 日、星期五	Payday		每月 13 日	Monxia	
每月 14 日、星期六	Saturday 14th		每月 18 日	FORM Virus	
每月 15 日、星期五	Skism	15 日以后	每月 20 日	Day10	
	Skism-1		每月 24 日	FORM Virus	
每月星期日	Sunday		每月 30 日	Day10	
每月星期一	Carfield		1 月 1 日	Plastique COBOL	
	Badguy			Christmas	
	Badguy-2			ORGON	2000 年后发作
	Exterminator		1 月 2 日	Syslock	
每月星期二	AH		1 月 5 日	Joshi	
	Demon		1 月 15 日	Casino	

（续）

发作时间	病毒名称	备　注	发作时间	病毒名称	备　注
1月25日	January 25th		11月17日	November 17th	
2月2日	Amilia		11月18日	Kennedy	
3月6日	Michelangelo		11月22日	Kennedy	
3月15日	Maltese Amoeba		11月30日	Jerusalem 11-30	
4月1日	Casper		12月1日	1253	
	Christmas		12月4日	Violator B	
	Suriv 1.00		12月19日	Father Christmas	
	Suriv 2.01		12月21日	Poem	
	Suriv 4.02		12月24日	December 24th	
	5120	4月1日以后	12月25日	Christmas Japan	
4月15日	Casino			Violator B3	
	Murphy		12月28日	Spanish April Fools	
5月4日	Changsha		12月31日	Violator B2	
6月4日	Bloody 6.4			Father Christmas	
	6.4-2			1253	
6月6日	Kennedy			Plastique	
6月16日	June 16th			Plastique B	
6月30日	Exciting Day		12月	1704-C	
7月13日	July 13th			Got you	
8月15日	Casino			1704 Format	
8月16日	August 16th		3月	903	
9月1日	AirCop		5月1日到4日	1210	
9月4日	Violator B1		7月	Got you	
9月20日	Plastique		9月至12月	1701/1704	
	Plastique B			1704-A	
9月22日	4096			1704-B	
10月1日	1554		1989年8月1日后	Fu Manchu	
10月4日	Violator B1		1990年6月后	Flash	
10月12日	Anarkia-B		1990年8月后	Datalock	
	DatacrimeII		1990年8月14日后	Violator	
	Datacrime II-B		1990年11月11日后	Fingers	
10月23日	Karin		1991年12月31日后	Sicilian Mob	
10月31日	Hallween		1992年	Europe-92	
	Violator B2			Were Here	
11月1日	Maltese Amoeba			Year 1992	
11月4日	Violator B1				

被计算机病毒使用的触发条件是多种多样的，而且往往不只是使用上面所述的某一条件，而是使用由多个条件组合起来的触发条件。大多数病毒的组合触发条件是基于时间的，再辅以读、写盘操作，按键操作以及其它条件。

如在我国广为流传的小球病毒，每当系统时钟为整点或半点时，系统又正在进行读盘操作，而该盘是未被感染的，等等，一旦这些条件得到满足时，小球病毒的屏幕显示部分便被激活，一个小球弹跳在屏幕上。若显示器是CGA类型的，又正在使用汉字系统，则整个屏幕显示会不停地上下翻滚，使操作根本无法进行。小球病毒的触发条件在各种触发条件中是很典型的，既有时间的条件，又有功能操作的条件，而且条件之间还存在

着逻辑“与”和逻辑“或”的关系。利用这种触发条件，计算机病毒不是随时随地表现自己，而是在适当的时机——条件满足时才向你示威，轻则只是在屏幕上显示些信息，重则要销毁数据，弄垮整个系统。

计算机病毒的破坏作用是多种多样的。有一种分类方法是将病毒分为恶性病毒和良性病毒。恶性病毒就是指在其代码中包含有损伤和破坏计算机系统的操作，在其传染或发作时会对系统产生直接的破坏作用。这类病毒是很多的，如米开朗琪罗病毒。当米氏病毒发作时，硬盘的前17个扇区将被彻底破坏，使整个硬盘上的数据无法被恢复，造成的损失是无法挽回的。有的病毒还会对硬盘做格式化等破坏。这些操作代码都是刻意编写进病毒的，这是其本性之一。因此这类恶性病毒是很危险的，应当注意防范。所幸防病毒系统可以通过监控系统内的这类异常动作识别出计算机病毒的存在与否，或至少发出警报提醒用户注意。

良性病毒是指其不包含有立即对计算机系统产生直接破坏作用的代码。这类病毒为了表现其存在，只是不停地进行扩散，从一台计算机传染到另一台，并不破坏计算机内的数据。有些人对这类计算机病毒的传染不以为然，认为这只是恶作剧，没什么关系。其实良性、恶性都是相对而言的。良性病毒取得系统控制权后，会导致整个系统运行效率降低，系统可用内存总数减少，使某些应用程序不能运行。它还与操作系统和应用程序争抢CPU的控制权，时时导致整个系统死锁，给正常操作带来麻烦。有时系统内还会出现几种病毒交叉感染的现象，一个文件不停地反复被几种病毒所感染。例如原来只有10KB的文件变成约90KB，就是被几种病毒反复感染了数十次。这不仅消耗掉大量宝贵的磁盘存储空间，而且整个计算机系统也由于多种病毒寄生于其中而无法正常工作。因此也不能轻视所谓良性病毒对计算机系统造成的损害。

计算机病毒的实现方法是千差万别的，加上许多病毒采用加密处理技术，使得被感染的程序恢复原形的工作，即杀毒工作很困难。目前还没有通用的、能可靠自动清病毒的方法。很多研究人员在这方面作了很多努力，一些国外商品软件也具有免疫功能（Immunize），但都存在缺陷，不尽如人意。某些病毒对系统的感染所造成的损失是不可挽回的，要修复被感染的文件是不可能的。当被新病毒感染后，要清除这些病毒，不仅需要耗费大量时间和精力去仔细地分析病毒代码，而且还需要对病毒和计算机系统有全面的了解。因此抗计算机病毒工作最重要的就是防御病毒，不让病毒侵入系统。一旦遭到破坏，做修复工作就很麻烦了，甚至是不可能的。

1.1.5 计算机病毒的分类与命名

在对抗计算机病毒的斗争中，很重要的一项工作就是**计算机病毒的分类与命名**。

计算机病毒的分类可以有多种方法：

按病毒对计算机系统的破坏性划分，有良性病毒和恶性病毒，已如上述。按病毒攻击的机型划分，有苹果机病毒，IBM-PC机病毒，小型机病毒等。按危害对象划分，有损害计算机的病毒和损害网络通信的病毒。对于侵害IBM-PC机的PC机病毒，也就是本书要着重讨论、要重点对抗的病毒，可以有更科学的分类。进行这种分类的目的，就是要了解病毒的工作机理，针对其特点，采取更加有效的方法，防御和清除计算机病毒。

对 PC 机病毒，比较公认的、科学的划分是将 PC 机病毒分为引导区型病毒、文件型病毒和混合型病毒（即又侵染引导区又感染文件的病毒）。这种划分方法对于检测、清除和预防病毒工作是有指导意义的，它不仅指明了不同种类病毒各自在 PC 机内的寄生部位，而且也指明了病毒的攻击对象。因此，可以通过采取相应的措施保护易受病毒攻击的部位，如分区表所在的主引导扇区、DOS 引导扇区以及可执行文件等，并进而找到综合、有效的反计算机病毒措施。

与国际上的情况一样，国内常见的 PC 机病毒中，引导区型比文件型病毒种类少，而混合型的最少。这三种类型的病毒都是既有良性的又有恶性的。常见的文件型病毒有 Jerusalem、1575、扬基病毒、648、V2000、1701 落叶病毒等。常见的引导区型病毒有大麻、小球、米氏病毒、6.4 病毒和香港病毒等。混合型病毒常见的有新世纪病毒、Flip 等。

一种计算机病毒往往有多个名字。人们在讨论病毒防范时经常要弄清他们正在讨论的是不是同一种病毒。如 1701 病毒的别名有落叶病毒、落泪病毒、1704 病毒、雨点病毒、感冒病毒等。国外又称雨点病毒为 Flu 病毒和 JOJO 病毒。香港病毒又称为封锁病毒、不打印病毒、Blockade 病毒和端口病毒等。所以由此产生的统计数字有时也带有偏差。目前国际上也尚无统一的规范用以协调和指导这方面的命名工作。美国的抗病毒产品开发商集团 AVPD 正在各个成员单位间进行计算机病毒的收集、识别、命名以及抗病毒产品开发等协调工作。在没有见到对某种病毒的确切描述以及对它公认的命名时，人们会根据该病毒的工作机理、表现形式、内含的 ASCII 字符串、病毒程序的代码长度、发作日期或时间、该病毒的发现地、被病毒攻击的机型、病毒中表现模块发出的音响或显示的图形以及该病毒发现者当时能体会到的各种特征来为它命名。前面所列举的 1701、香港病毒就都属于这种情况。

为某种新出现的计算机病毒命名，目的就是要使人们能快速、准确地辨识出该病毒，以便防范和诊治。因此该命名应能最好地体现出该病毒的特征，使之不容易与其它现存的计算机病毒混淆。

计算机病毒如今已是 PC 机用户的一大公害，它造成的损失和破坏难以估计。而一些恶作剧者、一些怀有报复心理的程序员、一些蓄意破坏者和一些为了政治目的、经济利益以及军事目的的病毒编制者，仍在制造着各种各样的计算机病毒。有些病毒仅仅是以前某种病毒的变种。某些人通过反汇编等各种手段，对原病毒的内部模块，如表现模块、破坏模块、传染模块等加以修改，使之成为一种基于原病毒又不同于原病毒的新的计算机病毒，这就是计算机病毒的变种。某些病毒变种只是简单地对原种病毒的显示信息加以改动，而对传染模块等重要代码未动分毫。而另外一些变种在修改了一些重要的代码后，病毒以新的机制工作，此时，这种变种已演化为一种新的病毒，已不能被叫做其原型病毒的变种了。生物界里的病毒也几乎以相同的方式在演化着，一种病毒可能会衍生出若干种具有共同基本特征的病毒种系，成为一个病毒家族。而当发生突变时，则会产生出一种新的病毒。对付老病毒及其变种，人们已有成功的经验和药物作为对策，而对于新的尚未接触过的病毒，在未做仔细研究与试验之前，是很难采取合适的对策的。对付计算机病毒，人们也遇到类似的问题。如何准确地捕获用常用软件无法识别出的新病毒，以及分析和研究它的工作机理和特性，是需要专门知识的，不分析它的传染机制，就无法研制出防范和清除病毒的工具软件。

1.2 计算机病毒传染途径及其防治对策

据有关资料报道，计算机病毒的出现是在70年代，那时由于计算机还未普及，所以病毒造成的破坏和对社会公众造成的影响还不是十分大。1986年巴基斯坦智囊病毒的广泛传播，则把病毒对PC机的威胁实实在在地摆在了人们的面前。1987年黑色星期五大规模肆虐于全世界各国的IBM-PC及其兼容机之中，造成了相当大的病毒恐慌。这些计算机病毒如同其它计算机病毒一样，最基本的特性就是它的传染性。通过认真研究各种计算机病毒的传染途径，有的放矢地采取有效措施，必定能在对抗计算机病毒的斗争中占据有利地位，更好地防止病毒对计算机系统的侵袭。

由于计算机病毒是一种特殊形式的计算机软件，与其它正常的软件一样，在未被激活，即未被运行时，均存放在磁记录设备中或其它存储设备中。软盘、硬盘、磁带、光盘和ROM芯片等这些存储设备都可能因载有计算机病毒而成为病毒的载体。像生物病毒需要载体才能存活一样，计算机病毒只有寄生在这些存储设备中才得以被长期保留，一旦被激活就又四处传染。像PC机的硬盘这种使用频度很高的存储设备，被病毒感染成为带毒硬盘的概率是很高的。虽然在大多数情况下绝没必要为杀病毒而去做低级格式化（往往只需改写主引导扇区一个扇区就能将硬盘从找不到C盘的情况下解救出来），但做低级格式化，却因清理了被病毒占据的所有扇区，而彻底清除了硬盘上隐藏着的所有计算机病毒。

计算机病毒的传播首先要有病毒的载体。病毒通过载体进行传播。病毒是软件程序，是具有自我复制功能的计算机指令代码。编制计算机病毒的计算机成为该病毒的第一个传染载体。由这台计算机作为传染源，该病毒就通过各种渠道传播开去，由此开始它罪恶的一生。病毒的编制者从来不敢在公开场合宣称自己在编制病毒。它们的工作是隐蔽进行的，因此往往很难对病毒的编制环境（即第一传染源）定位。这样也就很难从根本上铲除计算机病毒的滋生地。但我们可以通过病毒的传染途径进行定位。对传染途径严加控制，就可以控制住计算机病毒的传播。反计算机病毒研究人员之所以能控制住病毒，就是因为他们掌握了病毒的传染机理并了解病毒的传染途径。他们接触各种计算机病毒，在研究用的计算机里往往存放有多种病毒，而计算机本身仍在DOS控制之下，并不带毒，并不向外扩散病毒，就是因为他们控制了计算机病毒的传染途径，不使病毒外传。这些控制并不需要复杂的装备，重要的是要遵守一定的规则，再加上磁盘读写控制措施。

从图1-1可以看到计算机病毒的各种传染途径及其防治对策。

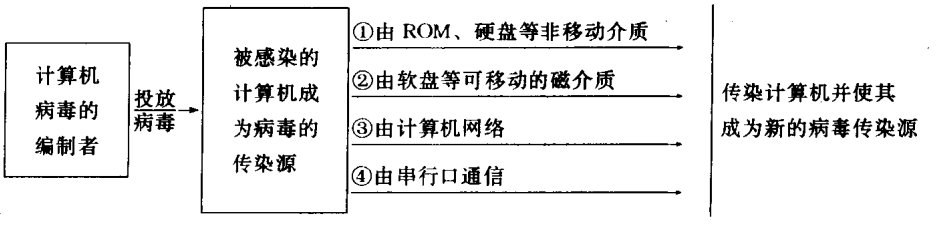

图1-1 计算机病毒的传染途径