完全手册系列丛书

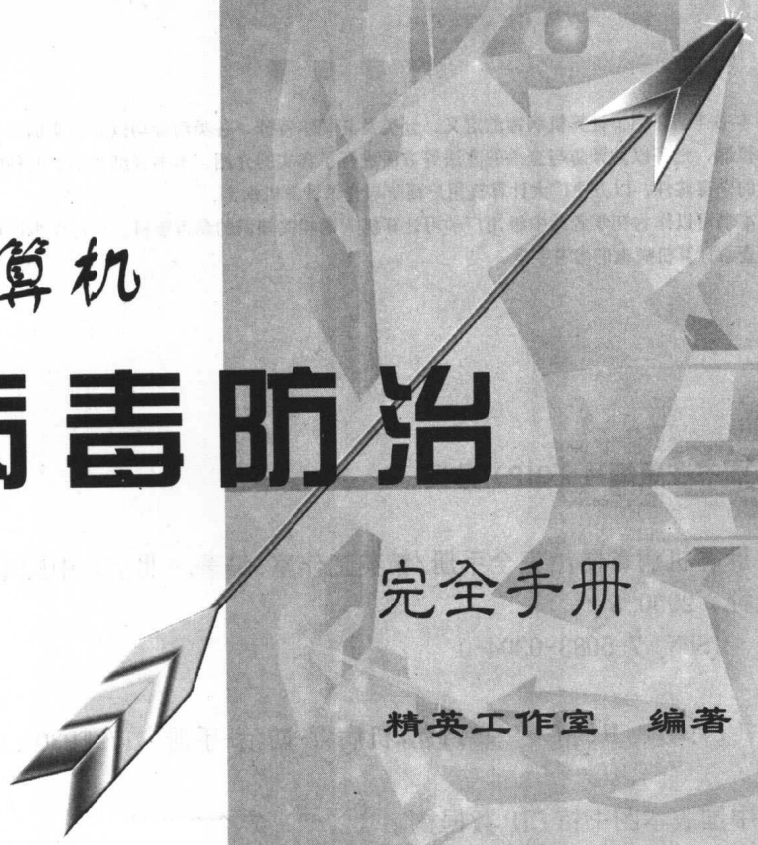
计算机病毒防治

完全手册

精英工作室　编著

中国电力出版社
www.cepp.com.cn

完全手册系列丛书



计算机病毒防治完全手册

精英工作室　编著

中国电力出版社

内 容 提 要

本书详细介绍了计算机病毒的定义、分类及其基本特征．各类病毒均以典型实例对其在特征、传染机制、危害以及预防与查杀的方法等方面进行了详实的介绍．本书详细介绍了七种国际、国内流行的杀毒软件，以方便广大计算机用户预防与查杀计算机病毒．

本书可以作为初学者或中级用户学习计算机病毒相关知识的参考资料，也可作为计算机用户预防、查杀计算机病毒的参考手册．

图书在版编目（CIP）数据

计算机病毒防治完全手册/精英工作室 编著.-北京：中国电力出版社，2000.5

ISBN 7-5083-0304-0

Ⅰ.计… Ⅱ.精… Ⅲ.计算机病毒-防治-手册 Ⅳ.TP309.5-62

中国版本图书馆 CIP 数据核字（2000）第 06939 号

中国电力出版社出版、发行

（北京三里河路 6 号 100044 http://www.cepp.com.cn）

实验小学印刷厂印刷

各地新华书店经售

*

2000 年 5 月第一版 2000 年 5 月北京第一次印刷

787 毫米×1092 毫米 16 开本 15 印张 338 千字

定价 **22.00** 元

目　录

第一章 计算机病毒概述

听说过“计算机病毒”吗？对于生物病毒，如流感病毒等，您也许并不陌生，您甚至还曾经用显微镜观察过一些生物病毒。那么什么是计算机病毒呢？难道它也是一条在计算机机箱里不断蠕动的“虫虫”吗？用显微镜可以观察到计算机病毒吗？

1.1 计算机病毒的定义

自 1946 年第一台电子计算机诞生以来，计算机的运行速度由最初的每秒几千次发展到每秒数亿次，其功能和容量都得到了很大提高。同时，随着个人电脑的推出，计算机得到了越来越广泛的应用，计算机已不仅是科学计算的工具，而且被广泛地用于各个领域的信息储存和处理。由于计算机的普及，越来越多的人掌握了计算机的使用技术，其中一部分人已成为使用计算机的行家里手。但是，由于计算机软硬件的脆弱性和计算机体系结构本身的局限，使得具有较高水平的计算机用户对计算机系统进行攻击成为可能。因此，在计算机技术发展到一定程度时，就出现了计算机病毒。

1.1.1 计算机病毒的起源

早在 60 年代，IBM 的程序员们在工作之余为了娱乐，就编制了一些“游戏程序”，这种程序可以在内存中将对方的程序“吃掉”。这就是计算机病毒最早的雏形。

1983 年，美国加利福尼亚州的计算机研究人员 Fred Cohen 博士开始研究计算机病毒对系统攻击的可能性，并于 1984 年在美国计算机安全会议上演示计算机病毒，用实验证实了计算机病毒的存在。

然而，仅仅只过了两年，真正的计算机病毒就问世了。这就是 1986 年发现的由巴基斯坦的 Basit 和 Amjad 编写的“巴基斯坦智囊”病毒，它是第一种被发现的计算机病毒。从此，新的病毒不断被制作出来，渐渐地开始在全世界蔓延开来。

1.1.2 计算机病毒的危害

迄今为止，世界上已有不下 15000 种计算机病毒，我国国内也已经发现了 600 多种。由于计算机网络的逐步普及，病毒的传播十分迅速。现在，很少有计算机用户从未遭到过计算机病毒的袭击，计算机病毒造成的破坏也越来越大。每一次病毒大爆发，都伴随着计算机用户的巨大损失。

计算机病毒对数据的危害

计算机病毒对数据的危害是多种多样的，常见的有：破坏文件分配表，改变磁盘的分配，从而导致数据写入错误；删除磁盘（包括硬盘和软盘）上的特定或全部文件，修改或删除文件中的数据，减少磁盘可用空间，影响文件存储；对整个磁盘或磁盘的特定磁道、

扇区进行格式化，对系统中用户存储的特定文件进行加密，中断用户正常操作，导致数据丢失，造成数据泄密等。

赫赫有名的宏病毒“台湾一号”（Tai Wan No.1）被触发后，会在用户编辑 Word 文档的时候出现一个对话框，要求用户进行复杂的四位数连乘运算（如图 1-1 所示）。

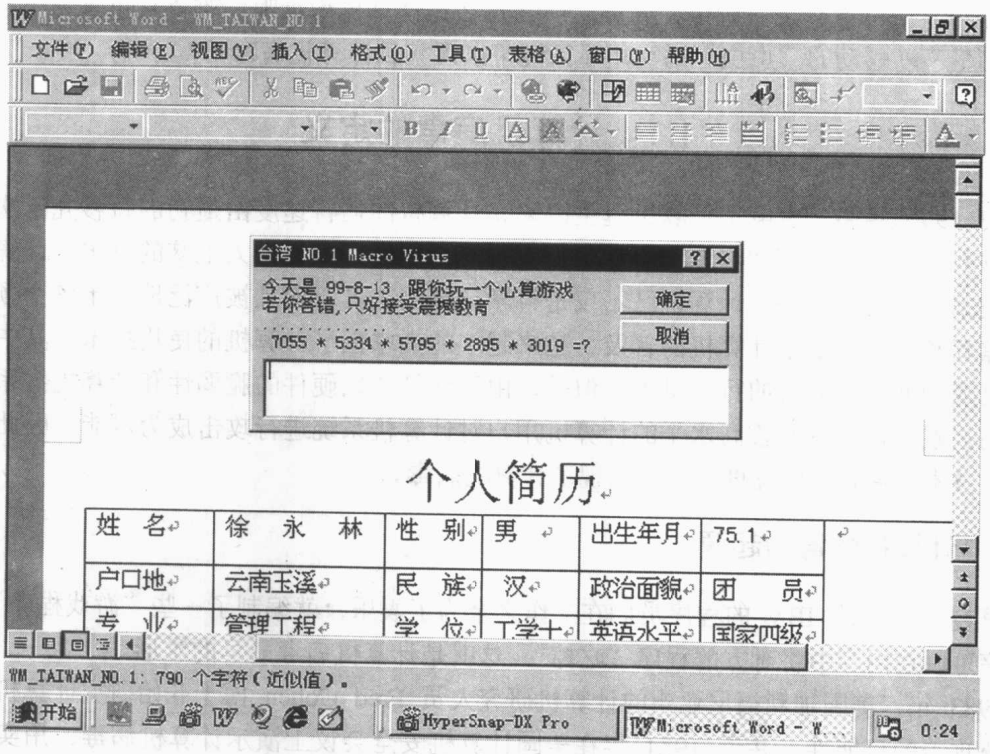


图 1-1　“台湾一号”宏病毒发作症状

如果用户回答正确，它就会打开一个文档，显示一些信息（详见第 3 章）；如果用户回答不正确，它会自动打开 20 个空文档，然后再次出现一个对话框，要求用户进行另一道复杂的计算，而且每次计算时出现的题目是随机的。“台湾一号”宏病毒就这样反反复复地要求用户进行计算，同时，它会封闭系统内的其他进程，关闭 Word 软件中定时自动存盘的功能，使正在编辑的文档无法保存。在用户进行了一遍又一遍的计算后，系统最终会因为不堪重负而死机。这类计算机病毒并不直接破坏用户数据，而是使用户正在编辑的内容丢失，辛辛苦苦的工作成果就这样付之东流，用户也无可奈何，只能从头再来，这严重影响了办公的效率。

总之，计算机病毒给用户造成的危害是多方面的。只要计算机病毒存在于系统中，它就必然会对系统的安全构成一定的威胁，所以，我们不应忽视计算机病毒可能造成的严重破坏，而应该采取积极措施，制止计算机病毒对系统的破坏。

计算机病毒对硬件的危害

计算机病毒只是一种程序，它要破坏硬件，不可能从硬盘或内存中跳出来大摔大砸，

只能根据计算机硬件的特点进行有针对性的破坏。计算机硬件比较多，并不是每一种硬件都会成为病毒攻击的目标，计算机病毒的攻击目标大致有：主板、CPU、显示卡、显示器、光盘驱动器、硬盘等等。

1.1.2　计算机病毒的定义

生活中人们难免会生病，所以我们对病毒并不陌生。但什么是计算机病毒呢？对这个问题的回答经历了一个不断发展的过程。我们可以从不同的角度给计算机病毒下不同的定义。

目前被人们广泛接受的一个定义是：计算机病毒是一种在计算机系统运行过程中能够把自身精确复制或有修改地复制到其他程序体内，从而造成一定程度影响和破坏的特殊的计算机程序。或者可以说，计算机病毒是一种传染其他程序的特殊程序，它通过修改其他程序使之含有病毒自身的精确副本或可能的衍化版本。

关于计算机病毒，有以下三个基本观点：计算机病毒是一种人为制造的特殊计算机程序；计算机病毒通过修改其他程序而隐藏在计算机系统的可存取信息资源中；计算机病毒利用系统资源进行传染，从而影响和破坏计算机系统的正常运行。

1.2　计算机病毒的基本特征

病毒（virus）一词是从生物学中借用的。生物学中的病毒具有传染性、流行性、繁殖性、表现性以及针对性等特征，而计算机病毒正是因为具备了与生物病毒几乎完全相同的特征，所以人们才将其称为“计算机病毒（computer virus）”。

具体说来，计算机病毒主要具有以下特征：

- 依附性（寄生性）　计算机病毒是一种特殊的计算机程序，它必须依附于其他程序，否则无处藏身。
- 传染性　“病毒”一词来源于生物学，传染性是生物病毒的一个重要特征。与之相对应，计算机病毒的一个重要特征就是计算机病毒具有传染性。

计算机病毒的传染性与生物病毒的传染性十分相似，但应该指出的是，计算机病毒传染系统一般都是通过夺取系统控制权的方法来实现的。一旦病毒夺取了系统控制权，对病毒的执行也就成为系统的“合法”调用，病毒的传染过程就成为系统的“合法”操作过程，使病毒传染的隐蔽性大大增强，不易被系统和用户察觉，直到病毒发作时，用户才会惊讶地发现，系统中已经存在着大量的这些病毒。因此，传染的隐蔽性也是病毒传染的一个重要特点。

- 潜伏性（隐蔽性）　计算机病毒程序为了达到不断传播并破坏系统的目的，一般不会在传染某一程序后立即发作，否则就暴露了自身。因此，它必须潜伏下来，通过各种方式隐藏自身，不被用户发现。

- 可触发性　　计算机病毒一般都有自身设置的触发条件，这种触发条件包括传染触发条件和破坏及表现触发条件。当病毒的触发条件得到满足时，计算机病毒就开始按照计算机病毒设计者预先设计的步骤活动起来，或进行传染，或出现表现症状，或破坏系统等等。

病毒的触发条件得到满足并使病毒开始活动被称之为“计算机病毒的激活”。

计算机病毒的传染触发条件用于触发病毒传染；计算机病毒的表现及破坏部分的触发条件则用于触发病毒的表现或破坏过程，使系统出现该病毒的表现症状或按病毒设计者的意图破坏系统或合法程序。

- 表现性（破坏性）　　不同的计算机病毒对系统有不同程度的破坏作用，轻者只是影响系统的工作效率，占用系统资源，造成系统运行不稳定；重者则可以删除系统的重要数据，甚至攻击计算机硬件，导致整个系统瘫痪，
- 针对性　　计算机病毒的运行需要特定的软、硬件环境，只能在特定的操作系统和硬件平台上运行，如 CIH 病毒只能在 Windows 95/98 环境下运行，在 DOS、Windows 3.x 和 Windows NT 环境下则不能运行，所以 DOS、Windows 3.x、Windows NT 用户大可不必害怕 CIH 病毒。
- 人为性　　计算机只是一台通电后能够运行的机器，在这一点上它与我们日常用的电视机、洗衣机没有多大区别。它既不会伤风感冒，也不会得高血压，也就是说，计算机自身不可能产生病毒。

1.3　计算机病毒的基本模式

通过对目前已经出现的计算机病毒的分析可以发现，所有的计算机病毒都是由三部分组成的，即病毒引导模块、病毒传染模块和病毒表现模块，如图 1-2 所示。

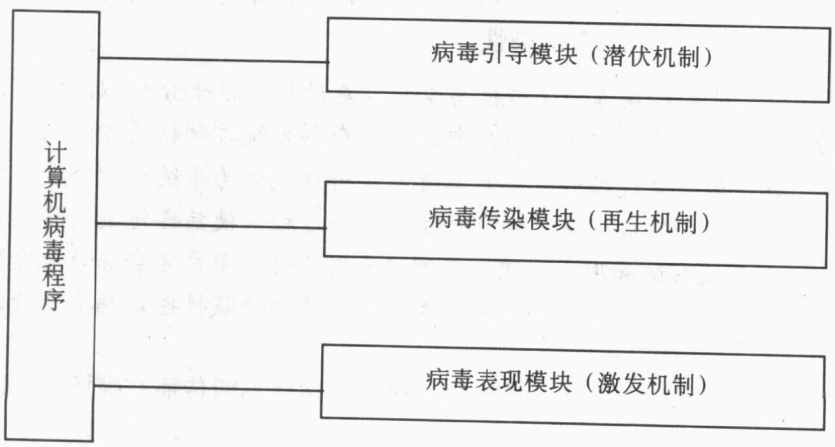


图 1-2　计算机病毒的基本模式

1.3.1 引导模块

计算机病毒的引导模块负责将病毒引导到内存中，并且向系统申请一定的存储空间，对相应的存储空间实施保护，以防止系统对其重新分配而使病毒程序被其他程序覆盖。同时，病毒的引导模块还修改系统的一些功能入口，在这些入口处引入病毒传染模块和病毒表现模块，使传染模块和表现模块处于活动状态，以监视系统运行。当系统运行中出现满足病毒传染触发条件或表现触发条件的情况时，病毒就进行传染或依照设计者的意图对系统发起攻击。

1.3.2 传染模块

计算机病毒的传染模块负责将病毒传染给其他计算机程序，它是整个计算机病毒程序的核心，也是病毒程序与一般计算机程序相区别的一个重要特征。

计算机病毒的传染模块由传染条件判断部分和传染部分组成。传染条件判断部分的作用是判断是否对某个程序进行传染，即病毒的传染条件是否得到满足。不同病毒的传染条件和传染对象都是不同的，但所有的病毒都有一定的传染条件，当病毒引导模块将传染模块引入系统之后，传染模块就监视系统中的程序并进行传染条件判断，一旦条件满足，病毒就开始传染。传染部分的作用就是负责实施病毒的传染过程，在传染条件满足时将病毒程序复制到传染目标中去。

1.3.3 表现模块

计算机病毒的表现模块也分为病毒触发条件判断部分和具体表现部分。为了达到隐蔽自身的目的，病毒只有在其触发条件满足时才运行其具体表现部分，而不是传染之后立即发作。在系统调用病毒触发条件判断部分，时刻根据病毒设计者的意图判断系统运行过程中是否出现了满足病毒触发条件的情况，如某一特定日期、某一特定的用户击键组合等等。只有在触发条件满足后，病毒才调用其具体表现部分。病毒的具体表现部分则负责实施病毒的表现或破坏工作，如删除文件、格式化磁盘、显示图形文字、发出异常声响等，这完全取决于病毒的设计者。因此，可以说计算机病毒的具体表现部分最直接地体现了病毒设计者的目的。

1.3.4 计算机病毒的工作流程

计算机病毒的一般工作流程如图 1-3 所示。

当通过第一次非授权地加载被病毒感染的程序，病毒的引导模块被执行后，病毒由静态转入动态，进入系统内存中，病毒的引导模块就会修改系统的参数，在系统的一些功能入口处引入病毒传染模块和病毒表现模块，然后动态的病毒就立即通过某种触发手段不停地检查系统中是否存在满足其传染或触发条件的情况，一旦满足，病毒就执行相应的传染或破坏功能。

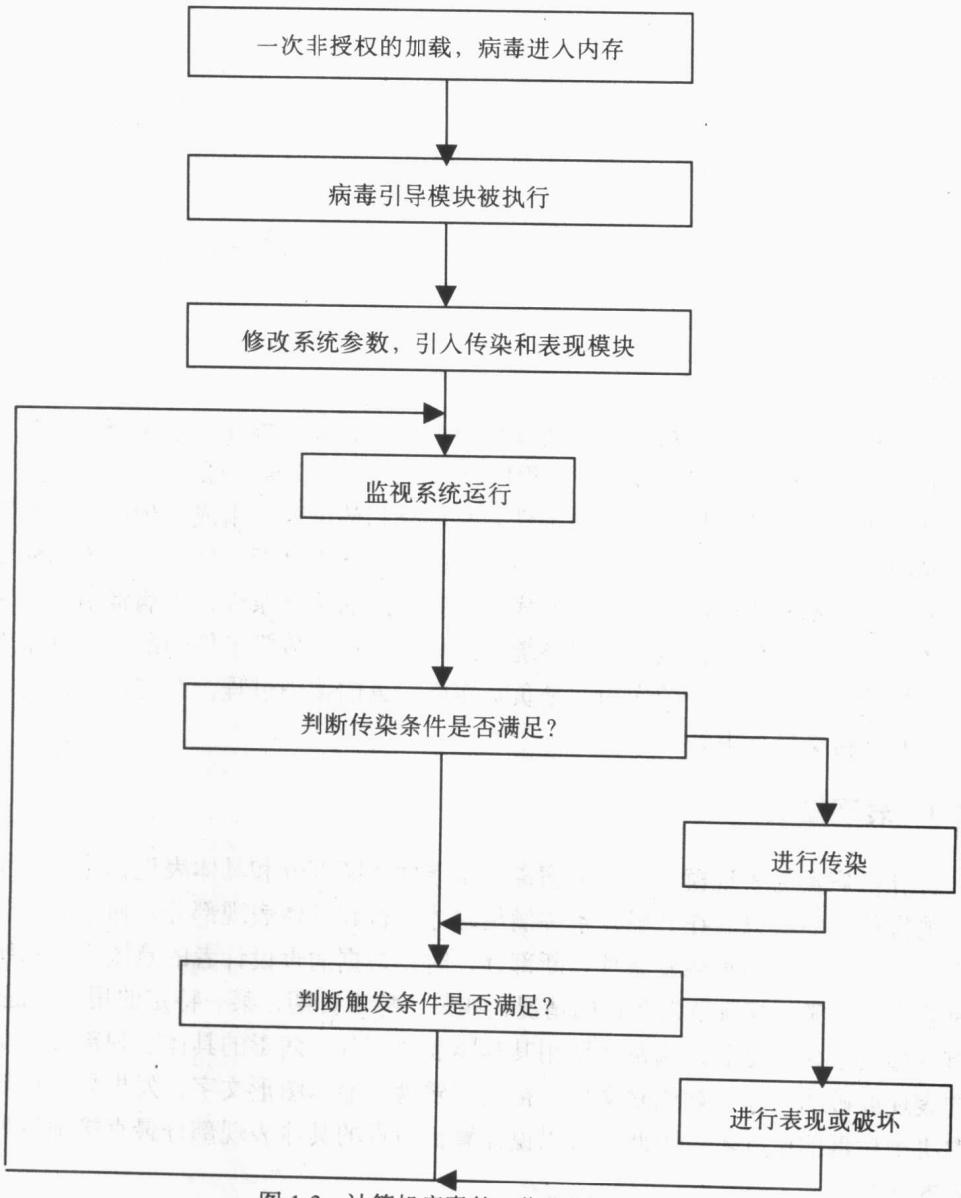


图 1-3　计算机病毒的工作流程

动态的病毒就是指已经进入系统内存、正处于运行状态或立即获得运行权的计算机病毒；静态的病毒则是指存储于磁盘上，还没有进入系统内存，无法获得系统控制权的计算机病毒。

1.4　计算机病毒的分类

自从计算机病毒出现以来，其发展速度非常快，病毒的种类急剧增加。根据计算机病毒的特点，从不同的角度出发，可以对计算机病毒进行不同的分类。以下着重介绍几种常见的分类方法。

1.4.1 按攻击对象划分

按照计算机病毒攻击对象的不同，可分为如下三类：

1．攻击 IBM-PC 及其兼容机的病毒

目前，这类病毒的种类最多，这是因为 IBM-PC 及其兼容机的使用非常广泛，而且这类计算机在过去相当长的一段时间里一直使用 DOS 操作系统（直到 Windows 95 发布之后，Windows 操作系统才成为主流），由于硬件资料以及 DOS 系统的开放性，人们对 DOS 的内部结构和计算机系统的硬件结构非常清楚，这就为病毒的设计者们编写针对 DOS 系统的病毒提供了便利。目前，IBM-PC 及其兼容机被广泛应用于政治、经济、军事、科技文教及日常生活等各个方面，所以这类病毒的流行范围很广。目前在我国发现的病毒绝大部分是这类病毒。

2．攻击 Macintosh 系列机的病毒

IBM-PC 及其兼容机虽然应用非常广泛，但还没有形成一统天下的局面。Apple 公司生产的 Macintosh 系列计算机在市场中也占有一席之地，该系列计算机的应用也比较广泛，因而它不可避免地成为病毒攻击的对象。但是，由于 Macintosh 系列计算机的使用范围有限，熟悉这类计算机的人相对较少，所以这类病毒相对于前一类病毒而言种类较少。

3．攻击 UNIX 操作系统的病毒

计算机病毒可以说是无孔不入的，具有较高安全性的 UNIX 操作系统也难以幸免。目前，大、中、小型机以及工作站多数仍采用 UNIX 操作系统。许多计算机系统，特别是在计算机网络中，更是以 UNIX 为其主操作系统，所以攻击 UNIX 操作系统的病毒尽管种类不多，但也对计算机信息系统构成了严重的威胁。

1.4.2 按攻击的机型划分

按照计算机病毒攻击的计算机种类，可以分为如下三类：

1．攻击微型计算机的病毒

这类病毒是针对目前广泛使用的微型计算机的软硬件特点设计的，是传染最广泛的一类病毒。

2．攻击小型计算机的病毒

随着计算机网络以及分布式计算机系统的不断发展，小型计算机的应用范围也越来越广。它不仅可以作为网络的节点，也可以作为小型网络的主机。一般来说，小型机的操作系统比较复杂，一般的计算机用户较难掌握，并且小型机绝大部分都采取了一定的安全保护措施，所以过去人们曾认为计算机病毒只能在微型计算机上出现，小型机不会受到病毒的攻击。但事实很快让人们改变了这种看法。1988 年 11 月，Internet 网络上的小型机就受到了蠕虫病毒的攻击，证明了无论操作系统是多么复杂，总会存在一定的漏洞。只要存在漏洞，就不免被病毒设计者加以利用，从而设计出专门攻击小型机的计算机病毒。

3．攻击工作站的病毒

随着计算机技术的进一步发展，计算机工作站得到不断普及应用，相应地就出现了攻击计算机工作站的计算机病毒。这类计算机病毒虽然种类不多，但由于其攻击造成的损失相当巨大，所以它也对计算机工作站的正常运作构成了巨大的威胁。

1.4.3　按链接方式划分

计算机病毒也是一种计算机程序，如果它只是被存储于计算机系统的存储介质中但却没有在系统中运行，那么它就无法进入系统，从而无法进行传染条件和触发条件的判断，也就不可能进行传染和破坏。因此，计算机病毒必须在隐蔽自身的同时被系统“合法”地调用执行。这一点是通过计算机病毒与系统内可被执行的文件建立链接来实现的。

计算机病毒程序链接的对象是系统中可被执行的文件，这些文件既包括操作系统文件，又包括以各种程序设计语言编写的应用程序，还包括应用程序所用到的数据文件，如Word 文档等。根据计算机病毒对这些文件的链接形式不同来划分病毒，可以分为如下四类：

1．操作系统病毒（Operating System Virus）

操作系统病毒在运行时，用自己的逻辑模块取代操作系统的部分合法程序模块。根据病毒自身的特点、被取代的操作系统合法模块在整个操作系统中的地位和作用以及病毒对操作系统模块的取代方式等诸因素的不同，这类病毒的结构、破坏性以及传染速度等都可能有很大的差异。它们可能有很强的破坏力，可导致整个系统瘫痪。目前出现的这种类型的病毒主要是针对操作系统自举区引导程序的，如大麻病毒、小球病毒以及巴基斯坦智囊病毒等。

2．源码病毒（Source Code Virus）

这类病毒攻击高级程序语言编写的源程序。它是在高级语言源程序被编译之前将病毒程序插入到源程序中，随后同源程序一起被编译，编译之后，病毒程序即可成为用户合法程序的一部分。这种病毒与用户合法程序紧密结合起来，使得清除工作十分困难。目前，应用的高级语言比较多，所以这种病毒也具有一定的威胁性。但是，这种病毒也具有其自身的局限性：首先，它要求设计者对所要侵入的高级语言源程序的掌握程度非常高，从而保证在病毒程序插入源程序后进行编译时不会出现编译错误而被用户发现，只有这样才能保证病毒传播得以进行；其次，它必须在用户合法的高级语言源程序进行编译之前插入其中，一旦错过这个机会，它就无法再传染被编译后的程序；再次，它修改了用户编写的源程序，一旦用户检查自己编写的源程序时，就很容易发现这种改动，从而使病毒暴露。这种病毒自身的局限性制约着它的发展，因此，目前这种病毒并不多见。

3．入侵型病毒（Intrusive Virus）

入侵型病毒将病毒程序嵌入到攻击目标中，而不是链接在它的首部或尾部。这种病毒的编写比较困难，危害也比较大。一旦这种病毒入侵到一个程序中，它就成为这个程序的一部分，但它不会使宿主程序文件的大小发生变化，因而很难被发现。即使发现这种病毒也较难清除。一般而言，清除这种病毒要破坏合法的宿主程序。但是，并不是所有的程序都可以被嵌入，因此，这种病毒能够传染的对象也受到了一定的限制。

4．外壳型病毒（Shell Virus）

外壳型病毒是将病毒程序本身包围在宿主程序的周围，对宿主程序基本不作任何修改，就像给宿主程序穿上了一件外衣一样。这种病毒是最常见的病毒，易于编写，传染的对象所受限制不大，传染性很强，如黑色星期五病毒就属于此类病毒。

1.4.4　按寄生方式划分

计算机病毒的一大特点是它的依附性，即它必须依附于某一合法程序。计算机病毒不能以独立的文件形式存在于系统中，否则，很容易被发现，而且它被激活的机会也极少。从目前已发现的病毒来看，病毒的寄生方式主要有以下两种：

1．寄生在磁盘引导区中的病毒（Boot Virus）

这类病毒将自身部分或全部代码寄生在磁盘引导区中，而且只传染磁盘引导区。由于磁盘引导区只有 512 字节，所以，对于较小的计算机病毒（长度小于 512 字节），可以全部寄生在引导区内；当病毒长度大于 512 字节时，就只能将部分病毒程序存放在引导区内，而剩余的部分则必须存储于磁盘的其他位置。此时，病毒一般都是将其引导部分放在磁盘引导区内，而将原正常引导区的内容和病毒的剩余部分一起存放于磁盘中的其他位置。这类病毒按其具体寄生方式又可分为置换式病毒、覆盖式病毒、填充式病毒、转储式病毒等。这类病毒的典型例子有小球病毒、大麻病毒，以及巴基斯坦智囊病毒等。

磁盘的第一个扇区为磁盘的引导扇区。

2．寄生在可执行文件中的病毒（File Virus）

这类病毒靠可执行文件的掩护而潜伏下来，并且随着合法的可执行文件的运行而不断扩散。需要特别指出的是：这里提到的可执行文件不仅仅包括 .exe 和 .com 文件，还包括这些文件运行过程中所使用的数据文件，如 Word 和 Excel 等软件所使用的文档文件，因为这些数据文件中可能包含有一些指令集，使得病毒可以利用这些指令集藏身并进行传播。宏病毒（Macro Virus）是这样一种病毒，它利用 Word 和 Excel 文档中所包含的宏隐匿自身，并利用宏的开放性不断传播。

这类病毒（除宏病毒外）的引导部分通常处于正常的程序代码之前，当执行被感染的文件时，病毒先于正常程序获得控制权。病毒获得控制权后，首先进行病毒的引导，完成病毒的加载，并为其他部分设置相应的激活条件，然后，病毒再将控制权转交给正常程序。从此，病毒就开始时刻监视着系统的运行，等待时机；一旦条件满足，病毒就会运作起来，完成一定的操作（传染、表现或破坏）。这类病毒按其具体的寄生方式又可分为链接式病毒、填充式病毒等。典型的例子有黑色星期五病毒、维也纳病毒以及宏病毒等。

1.4.5　按攻击目标划分

从目前的情况来看，计算机病毒的种类很多，特征各异。有攻击引导扇区的病毒，也有攻击命令处理程序的病毒，还有攻击.com 和.exe 以及其他类型文件的病毒等。因此，按病毒攻击目标的不同，计算机病毒可以分为以下几类：

1．引导扇区型病毒（BSI：Boot Sector Infectors）

引导扇区型病毒是一种常见的计算机病毒，它将自身复制到软盘或硬盘的引导扇区而进行传染，从而对系统造成严重危害。由于这类病毒程序存储在磁盘的引导扇区中，所以，它很容易获得系统的控制权，破坏力很强。

引导就是启动计算机运行的过程。计算机系统启动时，需要一张系统盘（硬盘或软盘），通过它的引导可以帮助计算机启动。引导过程是将系统盘上预先定义的一个区域的内容读入存储器预先定义的一个区域内，接着，将控制权交给该区域的程序，这个程序就是引导程序。引导程序执行后，将系统盘上其余的操作系统程序文件加载到内存中，这时操作系统才得到控制权。

系统盘上存储引导程序的区域称为“磁盘引导扇区”和“主引导记录”。专门对主引导记录中的程序进行修改、覆盖或用其他方法进行传染的病毒就是引导扇区型病毒。这类计算机病毒利用磁盘引导扇区传染具有一些其他传染方式所不具备的特点，最主要的是，当操作系统文件正常加载时，一旦系统启动，引导扇区病毒也就立即被加载，所以，该类病毒最先获得系统的控制权。这意味着引导扇区病毒是所有计算机对话期间真正最先被执行的程序。它在操作系统（内核）之前加载，也在命令处理程序（外壳）之前加载，亦在批处理文件和菜单系统之前，当然也在任何反病毒软件之前加载。

因此，一旦磁盘中有引导扇区病毒，用该磁盘引导后，病毒就会控制整个系统。引导扇区病毒可以常驻内存并活动，就像那些逐渐被用户熟悉和喜爱的“热键”程序一样。无论在什么时候，即使用户进行了热启动之后，它仍能驻留内存，并能传染尚未感染的启动磁盘。病毒可以监视用户的每一项操作，跟踪反病毒软件的扫描及杀毒工作。例如，在病毒代码添加到宿主程序后，实际的文件长度已经改变，而引导扇区病毒可以修改目录表，从而显示正确的原始文件长度。另外，引导扇区病毒和其他病毒一样，当满足设置的条件时，可以中断正常系统处理并进行破坏。

2．命令处理程序病毒（CPI：Command.com Processor Infectors）

目前，几乎所有的微机都使用 MS-DOS、Windows 9x 或 Windows NT 等操作系统。操作系统文件基本上分两类：低级系统支持文件和高级用户界面文件。低级系统支持文件主要包括 io.sys 和 msdos.sys，它们是隐含的系统文件，如果不借助其他工具，用户一般无法轻易地对其进行修改或转换。如果这些低级系统支持文件损坏，那么，它们所支持的系统就不能顺利运行；基本的用户界面程序文件包含在 command.com 文件中，command.com 文件在计算机完成启动后加载。这意味着已有两个系统支持文件 io.sys 和 msdos.sys 被加载并执行，计算机已作好准备响应用户的命令了。当用户输入命令时，command.com 文件对命令进行语法分析，然后，确定用户要求的操作。如果 command.com 文件不能识别用户的命令，就会返回出错信息，否则，command.com 文件将执行用户要求的操作。可见，command.com 相当于系统和用户之间的一个“翻译”，许多命令都要由 command.com 来处理后才能执行。因此，命令处理程序病毒一旦感染了 command.com 文件，它就能利用 command.com 文件的这个特点来检查人机对话，同时使自己的运行“合法化”。在执行用户命令时，命令处理程序病毒可以抢先搜索并感染其他程序，然后再执行正常的用户命令。尽管病毒捕获命令的执行时间要比执行正常命令的时间长，但由于增加执行的时间不会很长，加上现在计算机处理速度非常快，使大多数用户基本无法察觉到这个细微的差别。

3．一般目标病毒（GPI：General Purpose Infectors）

一般目标病毒恰如其名，是计算机病毒领域的多面手。它的传染范围最广，但通常不传染低级操作系统文件。不过 command.com 在很大程度上是正规的可执行文件，因此大多数一般目标病毒也传染 command.com。但一般目标病毒不能利用命令处理程序的有利条件

达到专门的命令处理程序病毒所传染的程度。这是它与命令处理程序病毒的重要区别。一般目标病毒不是以低级系统文件或命令处理程序为破坏目标，而是满足于传染所有的可执行文件。

当然，目前有些一般目标病毒仅限于传染某类或某几类可执行文件，其中，传染 .com 和 .exe 文件的最多。一般目标病毒擅长于整个系统的渗透感染，是计算机病毒中传播最快的一类。设计优良的一般目标病毒能很好地适应大多数可执行文件格式，能很快地在可执行文件中传播开，迅速达到传染所有可执行文件的目的。这种群发式的突袭方法就是一般目标病毒传染系统的主要机制。通过传染一般目标可执行文件，它经常传染多个系统和系统备份。引导扇区病毒和命令处理程序病毒一旦被发现，比较容易被清除"（通常只需重新安装系统和命令处理文件），而如果一般目标病毒感染了系统，特别是感染了系统备份时，用户几乎不可能彻底无损地根除它。

4．多目标病毒（MPI：Multipurpose Infectors）

多目标病毒结合了引导扇区病毒、命令处理程序病毒和一般目标病毒的传染特征，可以针对多个不同属性的传染目标。多目标病毒可能首先传染引导扇区，然后传染命令处理程序，从而引起病毒的泛滥。事实上，这也是一般目标病毒所具有的传染特征。

多目标病毒通过采用两种或更多的传染方法，增强了它的生命力，而且复制自身时比只有单一传染方法的病毒要顺利得多。在运行期间，多目标病毒获得系统控制权时，它们一般先在引导扇区和命令处理程序中寻找病毒标识（可识别被感染文件的病毒代码信息字节），如果没有发现，则传染未标识的文件并作标记；若找到病毒标识，则转而搜索并传染其他可执行文件。多目标病毒是一种适应性很强的计算机病毒，它全面综合了其他计算机病毒的各种传染技术。它的破坏性很强，可以毁坏引导扇区、内核、外壳以及用户文件系统的一般程序。

5．特定文件病毒（FSI：File-specific Infectors）

与引导扇区病毒、命令处理程序病毒只限于对已建立的文件类型进行传染一样，特定文件病毒以一定数量和特定不变的文件类型为传染目标。

与大多数病毒不同，作为特定文件病毒传染目标的那些文件通常是病毒设计者的敌手所作。特定文件病毒就像巡航导弹一样，按设计者拟定的程序搜索和摧毁预定目标文件。这种病毒采用正常的传染渠道进入无毒系统，它们寄生在看上去并未感染的磁盘文件中，等待机会进行繁衍。寻找目标文件的过程必然包括寄生到那些并不直接相关的程序中去的过程。这是因为搜索范围很广而且无搜索约束条件，所以传染各个文件可使特定文件病毒进入磁盘上各个子目录，执行快速搜索，当搜索不成功时则退出。从另一方面来看，传染非相关文件不会引起用户的怀疑。这样，传染非相关文件这个欺诈手段就掩盖了破坏目标文件的真实意图。这种病毒随着每一个被感染程序的加载以及每一个带毒磁盘的存取不断地搜索目标文件。当最后发现未标识的目标文件时，特定文件病毒就立即摧毁它们。

但是，保留在其他被感染文件中的特定文件病毒并不因其成功破坏目标文件而停止传染，除非已破坏目标文件的“先行者”留下了“使命已完成”的标识，对寄生在其他被感染程序中的同伙们发出“行动已结束”的信息，否则，这些寄生在系统中其他被感染文件中的病毒将继续不间断地搜索目标文件并进行传染。

6．驻留存储器病毒（MRI：Memory-Resident Infectors）

引导扇区病毒和命令处理程序病毒也可以归为驻留存储器病毒这个类型，因为这两类病毒运行时，仍然驻留和活跃在计算机存储器里。与许多用户所依赖的热键实用程序一样，这些计算机病毒能执行驻留存储器的操作。然而，与合法的驻留内存实用程序（TSR）不同，驻留存储器病毒通常没有为用户准备任何热键来呼叫它们运行，而是在宿主程序执行时立即驻留存储器并活跃于整个计算机运行过程中。由于驻留存储器病毒总是驻留并处于活动状态，所以，它能干扰大多数计算机操作，如阻截键盘命令、篡改屏幕输出、甚至修改磁盘数据。同时，它还在正常计算机操作间歇时间内不断地检查宿主系统，寻找未感染文件并传染它。

1.4.6 按侵害计算机系统的部位和发作模式划分

不同的计算机病毒侵害计算机系统的部位不尽相同，有的侵害文件系统，有的则侵害引导扇区。不仅如此，不同的计算机病毒发作模式各异，有的病毒通过用户按键组合触发而发作，有的病毒则判断系统时钟后发作。因此，还可以将计算机病毒分为以下三类：

1．磁盘启动型

磁盘启动型病毒隐藏在磁盘的引导扇区里，每次开机引导时触发。它又分为硬盘启动型和软盘启动型。此类病毒可以将整个磁盘格式化，使存储的大量数据荡然无存，难以恢复。

2．程序型

程序型病毒是感染各种可执行文件的病毒。它入侵计算机后，搜寻任何可执行文件，若可执行文件中不包含被该病毒感染的标记，就立即感染该文件，并添加感染标记。有的病毒程序还会修改正常程序的内容。带毒程序每次执行时，会启动隐藏其内的病毒，而病毒则立即开始搜寻其他可执行文件，并进行传染。这样，最终导致计算机系统内所有可执行文件均被感染。而且，一旦触发条件满足，病毒就会发作。

3．特洛伊木马型

特洛伊木马型病毒是指那些利用表面现象欺骗用户，背地里进行传染和破坏的计算机病毒。特洛伊木马型病毒的破坏力极大，它不但攻击可执行文件，还格式化磁盘或者覆盖部分或整个磁盘内容。特洛伊木马型病毒一般是通过设置时间或系统启动次数来触发的，它的传播极为隐密，因此，等到用户发现时，它已经散布很广了。

1.4.7 按计算机病毒的危害程度划分

严格地讲，任何计算机病毒都会对系统造成一定的危害，只是不同的计算机病毒造成的危害程度不同。根据计算机病毒所造成危害的严重程度，可以将计算机病毒分为以下三类：

1．良性病毒（表现型病毒）

尽管有人不同意“良性病毒”这个说法（他们认为计算机病毒不可能是良性的），但在本书中，我们还是将这个说法提出来，作为对计算机病毒的一种分类方法。这类计算机病毒是指那些不对计算机系统进行直接破坏，只是具有一定表现症状的计算机病毒。我们知道，计算机病毒的运行完全按照其设计者的设计意图来进行。如果其设计者并不想对计

算机系统造成严重破坏，而只是想通过编写计算机病毒展示一下他的才华，那么，他就会编写一些这样的良性病毒。这些良性病毒在发作时不会删除硬盘上的文件，也不会格式化磁盘，更不会攻击计算机硬件，它只会以一种特殊的方式让用户感觉到它的存在。例如，它会在计算机屏幕上显示一些带有特定意义的字符或图形，或者让计算机的蜂鸣器发出一些特殊的声响等等。这些病毒并不会对计算机系统造成直接的破坏，只是给用户添添乱而已。

2．恶性病毒（破坏型病毒）

恶性计算机病毒是指那些能对计算机系统造成严重破坏的计算机病毒。这类计算机病毒的设计者可就不像前一类设计者那么善良了。他们可能是疯子、恐怖分子或仇视社会的人。他们编写计算机病毒的目的就是要利用计算机病毒彻底地破坏计算机系统，因此，他们所设计出的恶性病毒将会对计算机系统造成严重的危害。这些恶性计算机病毒往往没有什么表现症状，在发作时才露出其狰狞的面目。它们可能会干净彻底地删除硬盘上的文件，使用户用任何软件都无法恢复被删除的文件；它们也可能会干脆将硬盘进行格式化，使硬盘上的数据荡然无存；它们甚至可能攻击计算机的硬件，造成硬件损坏而无法工作。大名鼎鼎的 CIH 病毒就是这样一种恶性计算机病毒。恶性计算机病毒给计算机系统造成的危害是十分严重的。每一次恶性计算机病毒的大爆发，都会给广大计算机用户留下痛苦的回忆。

3．中性病毒（蠕虫型病毒）

中性计算机病毒是指那些既不对计算机系统造成直接破坏，又没有表现症状，只是疯狂地复制自身的计算机病毒，也就是我们常说的蠕虫型病毒。蠕虫型计算机病毒比较特殊。之所以将它称之为“中性病毒”，是因为蠕虫型病毒对计算机系统造成的危害可大可小，视各个具体的病毒而定。从总体上来说，它的危害程度介于良性计算机病毒与恶性计算机病毒之间。说其危害程度轻，是指有的蠕虫型计算机病毒什么事也不干，只是在硬盘上疯狂地复制自身，挤占硬盘的大量存储空间，只影响一些文件的存储，但不对文件造成直接破坏；说其危害程度重，是指有的蠕虫型计算机病毒大量复制自身，耗尽了系统资源，使系统不堪重负而崩溃，造成严重的危害。如 1999 年 3 月横扫全世界的“美丽杀”病毒（Melissa）就是通过在宿主计算机中疯狂地向其他的计算机用户发送带有自身副本的电子邮件，从而导致 Internet 上的众多邮件服务器不堪重负而瘫痪，造成了严重的破坏。所以，对于蠕虫型计算机病毒的危害程度，不能一概而论。因此，我们既不能将其简单地归入良性计算机病毒中，也不能将其归入恶性计算机病毒中，只能用“中性病毒”这个概念来对其加以界定。

可见，计算机病毒的分类方法不是唯一的，不同的分类方法只是分类的角度不同。一种计算机病毒在不同的分类方法中可能会被归入多种类别中，这也是很正常的。认识计算机病毒，关键在于认清它的本质，即计算机病毒是一种能够复制自身并对计算机系统造成一定危害的特殊计算机程序。