# 第5章 计算机病毒及其防治

## 5.1 计算机病毒概述

从广义上定义，凡能够引起计算机故障，破坏计算机数据的程序统称为计算机病毒。依据此定义，诸如逻辑炸弹、蠕虫等均可称为计算机病毒。国内专家和研究者对计算机病毒也做过不尽相同的定义，但一直没有公认的明确定义。

直至1994年2月18日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》，在《条例》第二十八条中明确指出：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毁坏数据，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。

计算机病毒是一种人为制造的、在计算机运行中对计算机信息或系统起破坏作用的程序。这种程序不是独立存在的，它隐蔽在其他可执行的程序之中，既有破坏性，又有传染性和潜伏性。轻则影响机器运行速度，使机器不能正常运行；重则使机器处于瘫痪，会给用户带来不可估量的损失。通常就把这种具有破坏作用的程序称为计算机病毒。

自从Internet盛行以来，含有Java和ActiveX技术的网页逐渐被广泛使用，一些别有用心的人于是利用Java和ActiveX的特性来撰写病毒。以Java病毒为例，Java病毒并不能破坏储存媒介上的资料，但若使用浏览器来浏览含有Java病毒的网页，Java病毒就可以强迫Windows不断地开启新窗口，直到系统资源被耗尽，而我们也只有重新启动。所以在Internet出现后，计算机病毒就应加入只要是对使用者造成不便的程序代码，就可以被归类为计算机病毒。

除复制能力外，某些计算机病毒还有其他一些共同特性：一个被污染的程序能够传送病毒载体。当看到病毒载体似乎仅仅表现在文字和图像上时，它们可能也已毁坏了文件、再格式化了硬盘驱动或引发了其他类型的灾害。若是病毒并不寄生于一个污染程序，它仍然能通过占据存贮空间给我们带来麻烦，并降低计算机的全部性能。

可以从不同角度给出计算机病毒的定义。一种定义是通过磁盘、磁带和网络等作为媒介传播扩散，能“传染”其他程序的程序。另一种是能够实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。还有的定义是一种人为制造的程序，它通过不同的途径潜伏或寄生在存储媒体（如磁盘、内存等）或程序里。当某种条件或时机成熟时，它会自生复制并传播，使计算机的资源受到不同程序的破坏等。这些说法在某种意义上借用了生物学病毒的概念，计算机病毒同生物病毒的相似之处是能够侵入计算机系统和网络，危害正常工作的“病原体”。它能够对计算机系统进行各种破坏，同时能够自我复制，具有传染性。

所以，计算机病毒就是能够通过某种途径潜伏在计算机存储介质(或程序)里，当达到某种条件时即被激活的具有对计算机资源进行破坏作用的一组程序或指令集合。

## 5.2 计算机病毒的特点

计算机病毒是一个程序、一段可执行码。就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件中。当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。计算机病毒有如下特点：

(1) 寄生性。病毒程序的存在不是独立的，它总是悄悄地随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。其中病毒程序在原来文件之前或之后的，称为文件外壳型病毒，如以色列病毒(黑色星期五)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，在微机病毒中尚未见到。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，称为引导区病毒，如大麻病毒、2708 病毒等。此外，还有一些既寄生于文件中又侵占系统区的病毒，如“幽灵”病毒、Flip 病毒等，属于混合型。

(2) 隐蔽性。病毒程序在一定条件下隐蔽地进入系统。当使用带有系统病毒的磁盘来引导系统时，病毒程序先进入内存并放在常驻区，然后才开始引导系统，这时系统即带有该病毒。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。有的病毒是将自身程序常驻内存，使系统成为病毒环境，有的病毒则不常驻内存，只在执行当时进行传染或破坏，执行完毕之后病毒不再留在系统中。

(3) 非法性。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，病毒的乘虚而入并不在人们预定目标之内。

(4) 传染性。传染性是计算机病毒最重要的特征，是判断一段程序代码是否为计算机病毒的依据。病毒程序一旦侵入计算机系统就开始搜索可以传染的程序或者磁介质，然后通过自我复制迅速传播。由于目前计算机网络日益发达，计算机病毒可以在极短的时间内，通过像 Internet 这样的网络传遍世界。

(5) 破坏性。无论何种病毒程序一旦侵入系统都会对操作系统的运行造成不同程度的影响。即使不直接产生破坏作用的病毒程序也要占用系统资源(如占用内存空间，占用磁盘存储空间以及系统运行时间等)。而绝大多数病毒程序要显示一些文字或图像，影响系统的正常运行，还有一些病毒程序删除文件，加密磁盘中的数据，甚至摧毁整个系统和数据，使之无法恢复，造成无可挽回的损失。因此，病毒程序的副作用轻者降低系统工作效率，重者导致系统崩溃、数据丢失，造成重大损失。

(6) 潜伏性。计算机病毒具有依附于其他媒体而寄生的能力，这种媒体我们称之为计算机病毒的宿主。依靠病毒的寄生能力，病毒传染合法的程序和系统后，不立即发作，而是悄悄隐藏起来，然后在用户不察觉的情况下进行传染。这样，病毒的潜伏性越好，它在系统中存在的时间也就越长，病毒传染的范围也越广，其危害性也越大。

(7) 可触发性。计算机病毒一般都有一个或者几个触发条件。满足其触发条件或者激活病毒的传染机制，使之进行传染；或者激活病毒的表现部分或破坏部分。触发的实质是

一种条件的控制，病毒程序可以依据设计者的要求，在一定条件下实施攻击。这个条件可以是敲入特定字符，使用特定文件，某个特定日期或特定时刻，或者是病毒内置的计数器达到一定次数等。



## 5.3 计算机病毒的来源及其传播途径

计算机病毒的来源多种多样，有的是计算机工作人员或业余爱好者为了纯粹寻开心而制造出来的，有的则是软件公司为保护自己的产品被非法复制而制造的报复性惩罚，因为他们发现病毒比加密对付非法复制更有效且更有威胁，这种情况助长了病毒的传播等。具体可以分为以下几种：

(1) 从事计算机行业的人员和业余爱好者的恶作剧，寻开心制造出的病毒，例如像圆点一类的病毒。

(2) 软件公司及用户为保护自己的软件被非法复制而采取的报复性惩罚措施。因为它们发现对软件上锁，不如在其中藏有病毒对非法复制的打击大，这更加助长了各种病毒的传播。

(3) 旨在攻击和摧毁计算机信息系统和计算机系统而制造的病毒——就是蓄意进行破坏。例如 1987 年底出现在以色列耶路撒冷西伯莱大学的犹太人病毒，就是雇员在工作中受挫或被辞退时故意制造的。它针对性强，破坏大，产生于内部，防不胜防。

(4) 用于研究或有益目的而设计的程序，有益某种原因失去控制或产生意想不到的效果。例如，首例计算机病毒是一个简单的试验程序，科学家最初只是想测试该理论是否有效，结果是他们证实了该理论，但是同时也发现了部分负面影响，病毒可干扰某些正常的计算机处理，并导致误操作。

目前计算机病毒主要通过以下三种途径进行传播：

(1) 通过软盘和光盘传播。这是计算机病毒常见的传播途径。计算机由于使用带有病毒的软盘或光盘，使软盘或光盘所携带的计算机病毒传至本机。

(2) 通过硬盘传播。感染计算机病毒的硬盘，在计算机运行时，将病毒传至其他文件或通过对软盘的操作将计算机病毒传至软盘，从而被带走并感染其他的计算机。

(3) 通过计算机网络进行传播。现代信息技术的巨大进步已使空间距离不再遥远，但也为计算机病毒的传播提供了新的“高速公路”。计算机病毒可以附着在正常文件中通过网络进入一个又一个系统，国内计算机感染一种“进口”病毒已不再是什么大惊小怪的事了。在我们信息国际化的同时，我们的病毒也在国际化。估计以后这种方式将成为第一传播途径。

## 5.4 计算机病毒的防治

随着社会的发展，计算机变得越来越普及，而针对计算机的病毒也越来越多，几乎所有的计算机用户都遇到过病毒的侵袭。它使计算机的硬件系统遭到破坏、数据丢失，严重影响了人们的学习、生活和工作。因此，了解计算机病毒防治方法，对于计算机用户来说是十分必要的。

首先，在思想上重视，加强管理，防止病毒的入侵。凡是从外来的软盘往机器中复制信息，都应该先对软盘进行查毒，若有病毒必须清除，这样可以保证计算机不被新的病毒传染。此外，由于病毒具有潜伏性，可能机器中还隐蔽着某些旧病毒，一旦时机成熟还将发作，所以，要经常对磁盘进行检查，若发现病毒就及时杀除。思想重视是基础，采取有效的查毒与消毒方法是技术保证。检查病毒与消除病毒目前通常有两种手段，一种是在计算机中加一块防病毒卡，另一种是使用防病毒软件，两者工作原理基本一样，一般用防病毒软件的用户更多一些。切记要注意一点，预防与消除病毒是一项长期的工作任务，不是一劳永逸的，应坚持不懈。

病毒的侵入必将对系统资源构成威胁，即使是良性病毒，至少也要占用少量的系统空间，影响系统的正常运行。特别是通过网络传播的计算机病毒，能在很短的时间内使整个计算机网络处于瘫痪状态，从而造成巨大的损失。因此，防止病毒的侵入要比病毒入侵后再去发现和消除它更重要。因为没有病毒的入侵，也就没有病毒的传播，更不能需要消除病毒。另一方面，现有病毒已有万种，并且还在不断增多。而消毒是被动的，只有在发现病毒后，对其剖析、选取特征串，才能设计出该“已知”病毒的杀毒软件。它不能检测和消除研制者未曾见过的“未知”病毒，甚至对已知病毒的特征串稍作改动，就可能无法检测出这种变种病毒或者在杀毒时出错。这样，发现病毒时，可能该病毒已经流行起来或者已经造成破坏。

计算机病毒的防治方法：

(1) 没有一种杀毒软件是万能的。杀毒软件的编制，有赖于采集到的病毒样本。因此，对新病毒均有滞后性。而定期使用另一种杀毒软件进行查毒和杀毒，可提高防治效果。

(2) 查杀病毒的常用软件(如瑞星和金山毒霸等)一定要及时、定期升级。

(3) 由于网络传播速度快，新病毒出现后，杀毒软件往往不能及时升级，因此，防治网络传播病毒的最佳方法是不预览邮件，遇到可疑邮件立即删除。

(4) 在使用外来软盘或光盘中的数据(软件)前，应该先检查，确认无病毒后再使用。

(5) 由于数据交换频繁，感染病毒的可能性始终存在，因此，重要数据一定要备份，如存入软盘或刻入光盘。

## 5.5 计算机使用安全常识

保护计算机安全的几种方法：

(1) 注意防止盗窃计算机案件，在高校经常会发生此类案件。小偷趁学生疏忽、节假日外出、夜晚睡觉不关房门或外出不锁门等机会，偷盗台式电脑、笔记本电脑或掌上电脑，或者偷拆走计算机的 CPU、硬盘、内存条等部件，给学生造成学习困难和经济损失。

(2) 注意防止火灾、水害、雷电、静电、灰尘、强磁场、摔砸撞击等自然或人为因素对计算机的危害，要注意保证计算机运行环境和辅助保障系统的可靠性和安全性。

(3) 防止计算机病毒侵害电脑，要使用正版软件，不要使用盗版软件或来路不明的软件。从网络上下载免费软件要慎重，注意电子邮件的安全可靠性。不要自己制作或试验病毒。重创世界计算机界的 CIH 病毒，据说是一个台湾大学生制作的，它给全世界带来了非常严重的电子灾难。

(4) 如果把计算机接入互联网,经常进行网上冲浪,就必须小心“黑客”的袭击。

(5) 有了计算机,就要同时选用正版杀毒软件,应选用可靠的、具有实时(在线)杀毒能力的软件。

(6) 养成文件备份的好习惯。首先是系统软件的备份,重要的软件要多备份并进行写保护,有了系统软件备份就能迅速恢复被病毒破坏或因误操作被破坏的系统。其次是重要数据备份,不要以为硬盘是永不消失的保险数据库。

(7) 给计算机买个保险。据《中国经济时报》报道,中国人民保险公司开始在全国范围内推广计算机保险。包括计算机硬件损失保险、数据复制费用保险和增加费用险(设备租赁费用险)等,主要承保火灾、爆炸、水管爆裂、雷击、台风、盗抢等导致的硬件损失、数据复制费用和临时租赁费用。对于风险较难以控制的病毒、“黑客”侵害问题,则列入责任免除条款。

(8) 要树立计算机安全观念,心理上要设防。网络虽好,可是安全问题丛生,网络陷阱密布,“黑客”伺机作案,病毒层出不穷。

同时还要防止“黑客”的袭击,具体有以下几种方法:

(1) 要使用正版防病毒软件并且定期将其升级更新,这样可以防“黑客”程序侵入我们的计算机系统。

(2) 如果我们使用数字用户专线或是电缆调制解调器连接因特网,就要安装防火墙软件,监视数据流动。要尽量选用最先进的防火墙软件。

(3) 别按常规思维设置网络密码,要使用由数字、字母和汉字混排而成,令“黑客”难以破译的口令密码。另外,要经常性地变换自己的口令密码。

(4) 对不同的网站和程序,要使用不同的口令密码,而不要使用统一密码,以防止被“黑客”破译后产生“多米诺骨牌”效应。

(5) 对来路不明的电子邮件或亲友电子邮件的附件或邮件列表要保持警惕,不要一收到就马上打开。要首先用杀病毒软件查杀,确定无病毒和“黑客”程序后再打开。

(6) 要尽量使用最新版本的互联网浏览器软件、电子邮件软件和其他相关软件。

(7) 下载软件要去声誉好的专业网站,既安全又能保证较快速度,不要去资质不清楚的网站。

(8) 不要轻易给别人的网站留下我们的电子身份资料,不要允许电子商务企业随意储存你的信用卡资料。

(9) 只向有安全保证的网站发送个人信用卡资料,注意寻找浏览器底部显示的挂锁图标或钥匙形图标。

(10) 要注意确认我们要去的网站地址,注意输入的字母和标点符号的绝对正确,防止误入网上歧途,落入网络陷阱。

## 习　　题

### 一、填空题

1. 计算机病毒就是能够通过某种途径潜伏在计算机存储介质或程序里,当达到某种条件时即被激活的具有对计算机资源进行破坏作用的一组_____。

2. 计算机病毒特点有 _____、_____、_____、_____、_____、_____、_____。

3. 目前计算机病毒主要通过以下三种途径进行传播：_____、_____、_____。

**二、简答题**

1. 什么是计算机病毒？

2. 如何防治计算机病毒？

3. 如何安全使用计算机？