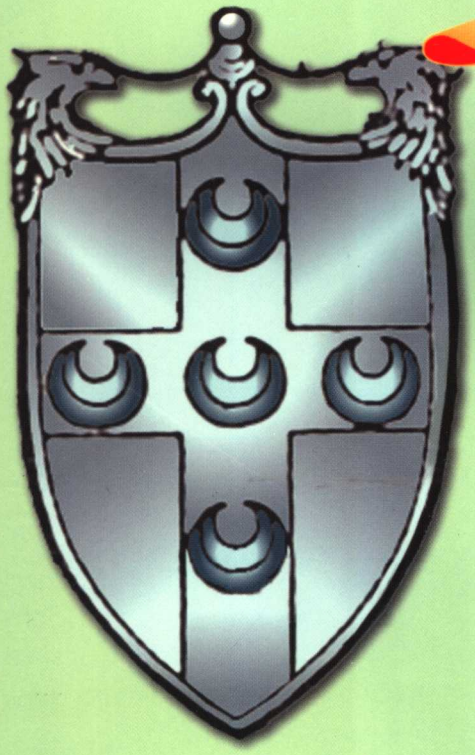
计算机病毒防治与信息安全知识300问



张 洁 张学志 王 鹏 编

冶金工业出版社
http://www.cnmip.com.cn

计算机病毒防治与信息安全知识300问

张 洁 张学志 王 鹏 编

北 京
冶 金 工 业 出 版 社
2006

内 容 提 要

本书从实用的角度出发，分析整理了计算机各种常见病毒和信息安全方面的300个问题，从病毒基础知识、病毒档案、病毒防治、杀毒软件、信息安全和防御黑客技术等六个方面介绍了相关的知识，深入分析了计算机病毒的生成机理、感染途径和防治方法，以帮助读者了解计算机病毒，并在日常生活中更好地加以防范，最低限度地降低计算机病毒对用户的伤害。

本书精选的300个问题具有很强的代表性，并深入浅出、简单明了地进行了解答，适合广大计算机爱好者以及软件开发人员学习和参考。

图书在版编目(CIP)数据

计算机病毒防治与信息安全知识300问/张洁等编.
北京：冶金工业出版社，2006.10
ISBN 7-5024-4085-2

Ⅰ.计… Ⅱ.张… Ⅲ.计算机病毒—防治—问答
Ⅳ. TP309.5-44

中国版本图书馆CIP数据核字（2006）第096547号

出 版 人 曹胜利（北京沙滩嵩祝院北巷39号，邮编100009）
责任编辑 张 卫（联系电话：010-64027930；电子信箱：bull2820@sina.com）
王雪涛（联系电话：010-64062877；电子信箱：2bs@cnmip.com.cn）
张爱平（联系电话：010-64027928；电子信息：zaptju99@163.com）
美术编辑 李 心 责任校对 符燕蓉 李文彦 责任印制 丁小晶
北京兴顺印刷厂印刷；冶金工业出版社发行；各地新华书店经销
2006年10月第1版，2006年10月第1次印刷
787mm×1092mm 1/16；15.75印张；377千字；235页；1—3000册
25.00元
冶金工业出版社发行部 电话：(010)64044283 传真：(010)64027893
冶金书店 地址：北京东四西大街46号(100711) 电话：(010)65289081
（本社图书如有印装质量问题，本社发行部负责退换）

前　言

计算机已经进入社会生活的各个方面，成为人们工作、学习、生活的工具。随着计算机在各行各业的广泛应用，计算机病毒也随之泛滥，已经危害到科学研究、工程实践、经济、军事，甚至危害到国家安全，其危害程度也越来越受到人们的关注。

虽然已出版的关于计算机病毒的书比较多，但其内容只是就杀毒软件的使用谈防治，而计算机病毒的时效性又非常强，更新速度也非常快，因此一些书的内容很快就会随着计算机病毒的更新而变得陈旧过时。本书根据计算机病毒的机理从实用的角度出发，分析整理了计算机病毒基础知识、病毒档案、病毒防治、杀毒软件、信息安全和防御黑客技术等方面的问题，深入浅出地介绍了计算机病毒的生成机理、感染途径和防治方法，通过举一反三，帮助读者了解计算机病毒的相关知识和掌握防治病毒的方法。同时书中也简要地介绍了最新的病毒和杀毒软件，读者也可以了解计算机最新病毒的信息。

本书适用于广大计算机爱好者，也可供广大编程爱好者、软件开发人员参考。

由于时间仓促，书中难免有些不妥之处，恳请读者谅解，并请指正。

编　者

2006 年 6 月

目　录

第1章 病毒基本知识

1. 什么是计算机病毒?

计算机病毒是具有自我复制能力的计算机程序，它能影响计算机软硬件的正常运行、破坏数据的正确与完整，它是一个程序、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，它可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上，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。

除复制能力外，某些计算机病毒还有其他一些特性：一个被污染的程序能够传送病毒载体。当病毒载体似乎仅仅表现在文字和图像上时，它们可能已经毁坏了文件、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储空间带来麻烦，并降低计算机的全部性能。

由此，我们可以从不同角度给出计算机病毒的定义：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；另一种是人为制造的程序，它通过不同的途径潜伏或寄生在存储介质（如磁盘、内存）或程序里，当某种条件或时机成熟时，它会自我复制并传播，使计算机的资源受到不同程度的破坏。

简单地说，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。

2. 计算机病毒是怎么产生的?

计算机病毒都是人为制造出来的，计算机病毒的主要来源有以下一些：

(1) 引进的计算机系统和软件中带有病毒；
(2) 各类出国人员带回的机器和软件染有病毒；
(3) 购买、使用一些染有病毒的游戏软件；
(4) 非法拷贝中毒；
(5) 计算机生产、经营单位销售的机器和软件染有病毒；
(6) 维修部门交叉感染；
(7) 有人研制、改造病毒；
(8) 敌对分子恶意以病毒进行宣传和破坏；
(9) 通过国际计算机网络传入。

3. 计算机病毒有哪些特性?

目前，在世界范围内发现的计算机病毒已超过 1000 种，国内已发现的计算机病毒也

有几十种，例如："小球"病毒、"大麻"病毒、"黑色星期五"病毒、"雨点"病毒、"磁盘杀手"病毒、"音乐"病毒等。尽管这些病毒各自的传染方式、传染目标不一样，发作条件各异，干扰和破坏程序不同，但是，它们都有如下共同的特性：

（1）计算机病毒的程序性（可执行性）。计算机病毒与其他合法程序一样，是一段可执行程序，但它不是一个完整的程序，而是寄生在其他可执行程序上，在病毒运行时，与合法程序争夺系统的控制权。计算机病毒只有当它在计算机内得以运行时，才具有传染性和破坏性，甚至会造成系统崩溃，导致计算机瘫痪。

（2）计算机病毒的传染性。传染性是病毒的基本特征。在生物界，病毒通过传染从一个生物体扩散到另一个生物体，在适当的条件下，它可得到大量繁殖，并使被感染的生物体表现出病症甚至死亡。同样，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。

（3）计算机病毒的潜伏性。

一个编制精巧的计算机病毒程序，进入系统后可以不马上发作，在几周或者几个月内甚至几年内隐藏在合法文件中，对其他系统进行传染，而不被发现。

潜伏性的第一种表现是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，一旦得到运行机会，就四处繁殖、扩散，继续为害。潜伏性的第二种表现是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、使系统锁死等。

（4）病毒的非授权性。

病毒未经授权而执行。一般正常的程序是由用户调用，再由系统分配资源，完成用户交给的任务。其目的对用户是可见的、透明的。而病毒具有正常程序的一切特性，它隐藏在正常程序中，当用户调用正常程序时窃取到系统的控制权，先于正常程序执行，病毒的动作、目的对用户是未知的，是未经用户允许的。

（5）计算机病毒的破坏性。

所有的计算机病毒都是一种可执行程序，而这一可执行程序又必然要运行，所以对系统来讲，所有的计算机病毒都存在一个共同的危害，即占用系统资源，降低计算机系统的工作效率，其具体情况取决于入侵系统的病毒程序。

同时，计算机病毒的破坏性主要取决于计算机病毒设计者的目的。如果病毒设计者的目的在于彻底破坏系统的正常运行的话，那么这种病毒对于计算机系统进行攻击造成的后果是难以设想的，它可以毁掉系统的部分数据，也可以破坏全部数据并使之无法恢复。但并非所有的病毒都对系统产生极其恶劣的破坏作用。

（6）病毒的寄生性（依附性）。

病毒程序嵌入到宿主程序中，依赖于宿主程序的执行而生存，这就是计算机病毒的寄生性。病毒程序在侵入到宿主程序中后，一般对宿主程序进行一定的修改，宿主程序一旦执行，病毒程序就被激活，从而可以进行自我复制和繁衍。

（7）病毒的针对性。

计算机病毒是针对特定的计算机和特定的操作系统的。例如，有针对IBM PC机及其

兼容机的，有针对 Apple 公司的 Macintosh 的，还有针对 Unix 操作系统的。例如“小球”病毒是针对 IBM PC 机及其兼容机上的 DOS 操作系统的。

（8）计算机病毒的可触发性。

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须潜伏。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

（9）病毒的衍生性。

病毒的衍生性为一些有意者提供了一种制造新病毒的捷径。分析计算机病毒的结构可知，传染的破坏部分反映了设计者的设计思想和设计目的。但是，这可以被其他掌握原理的人以其个人的企图进行任意改动，从而又衍生出一种不同于原版本的新的计算机病毒（又称为变种），这就是计算机病毒的衍生性。这种变种病毒造成的后果可能比原版病毒严重得多。

（10）计算机病毒的持久性。

即使在病毒程序被发现以后，数据和程序以至操作系统的恢复都非常困难。特别是在网络操作情况下，由于病毒程序由一个受感染的拷贝通过网络系统反复传播，使得病毒程序的清除非常复杂。

4. 计算机病毒主要有哪些传播途径?

随着计算机技术的发展，病毒的传播途径也随之多样化起来，但是归纳来讲，主要有以下几种：

第一种途径：通过不可移动的计算机硬件设备进行传播，这些设备通常有计算机的专用 ASIC 芯片和硬盘等；

第二种途径：通过移动存储设备来传播，这些设备包括软盘、磁带等；

第三种途径：通过计算机网络进行传播；

第四种途径：通过点对点通信系统和无线通道传播。

5. 计算机病毒是如何感染文件的?

在系统运行时，病毒通过病毒载体从系统的外存储器进入系统的内存储器，常驻内存。该病毒在系统内存中监视系统的运行，当它发现有攻击的目标存在并满足条件时，便从内存中将自身存入被攻击的目标，从而将病毒进行传播。而病毒利用系统 INT13H 读写磁盘的中断又将其写入系统的外存储器（软盘或硬盘）中，再感染其他系统。

6. 如何确定 Boot 区是否被病毒感染?

正常的 PC DOS 启动过程是：

（1）开机后进入系统的检测程序并执行该程序对系统基本设备进行检测；

（2）检测正常后从系统盘 0 面 0 道 1 扇区即逻辑 0 扇区读入 Boot 引导程序到内存的 0000：7C00 处；

（3）转入 Boot 执行；

(4) Boot 判断是否为系统盘，如果不是系统盘则提示；

Non-system disk or disk error

Replace and strike any key when ready

否则，读入 IBM BIO. COM 和 IBM DOS. COM 两个隐含文件；

(5) 执行 IBM BIO. COM 和 IBM DOS. COM 两个隐含文件，将 Command. com 装入内存；

(6) 系统正常运行，DOS 启动成功。

如果 Boot 区被病毒感染则会出现以下一些现象：

(1) 先用与硬盘上相同版本的干净 DOS 系统软盘启动计算机，启动过程中，按 F5 键，然后用 MEM 或 MI 查看并记下计算机自由内存空间大小；接着用硬盘引导计算机，引导过程中，按 F5 键，以便跳过 Config. sys 和 Autoexec. bat 中的驱动程序和执行文件，这时再用 MEM 或 MI 查看计算机的自由内存空间；如果上述两次自由内存空间大小不一致，则该计算机的硬盘 Boot 区肯定已被病毒感染。

(2) 用硬盘引导计算机，运行 DOS 中的 MEM，可以查看内存分配情况，尤其要注意基本内存，一般为 640K，有的微机为 639K。如果基本内存为 638K、637K 或 636K 等情况，那么 Boot 区肯定被感染上病毒。

(3) 机器在运行过程中刚设定好的时间、日期，运行一会儿被修改为缺省的时间、日期，这种情况下，系统很可能带有引导型病毒。

(4) 在开机过程中，CMOS 中刚设定好的软盘配置（即 1.44M 或 1.2M），用软盘启动时一切正常，但用硬盘引导后，再去读软盘则无法读取，此时 CMOS 中软盘设定情况为 None，这种情况肯定带有引导型病毒。

(5) 硬盘自引导正常，但用干净的 DOS 系统软盘引导时，看不到硬盘如 C \ 盘（除特殊的需外加驻留内存的大硬盘和 FAT32 位），这肯定感染上引导型病毒。

(6) Windows 95 经常无法启动，这很可能带有引导型病毒。

7. 计算机病毒主要存在哪些媒体上?

计算机病毒是一种可直接或间接执行的文件，是依附于系统特点的文件，是没有文件名的秘密程序，但它的存在却不能以独立文件的形式存在，它必须是以附着在现有的硬、软件资源上的形式而存在的。

微型计算机系统在目前来说永久性存储设备即外存储器主要是磁盘。磁盘包括硬盘和软盘。从存储容量角度来讲，硬盘容量是一般软盘容量的几百至几千倍，并且硬盘容量越来越大，软盘一般为 1.44MB。微型计算机系统所使用的文件存放于磁盘之中，所以微型计算机的病毒是以磁盘为主要载体的。

8. 计算机病毒的生命周期有多长?

计算机病毒的产生过程可分为：程序设计-传播-潜伏-触发-运行-实行攻击。计算机病毒拥有一个生命周期，从生成开始到完全根除结束。

开发期：在几年前，制造一个病毒需要计算机编程语言的知识。但是今天有一点计算机编程知识的人都可以制造一个病毒。通常计算机病毒是一些误入歧途的、试图传播计算