计算机病毒防治200问

徐建民 刘清波 编写

工商联合出版社

计算机病毒防治200问

主编：徐建民　刘振鹏　鸿　玺
编委：蔡淑珍　田俊峰　韩　勇
马　力　刘清波　张锁良
李宏中

中华工商联合出版社

(京)新登字 301 号

责任编辑：王凌云

封面设计：安　宏

图书在版编目(CIP)数据

计算机病毒防治 200 问/徐建民等编．—北京：中华工商联合出版社，1996.1
ISBN 7-80100-120-6

Ⅰ.计…　Ⅱ.徐…　Ⅲ.计算机病毒-防治-问答　Ⅳ.TP309—44

中国版本图书馆 CIP 数据核字(96)第 01221 号

中华工商联合出版社出版　发行

北京市朝阳区西大望路甲 27 号　邮编 100022

河北衡水冀峰印刷股份有限公司印刷

新华书店总经销

1996 年 1 月第 1 版　1996 年 1 月第 1 次印刷

787×1092 毫米　1/32　印张：7.125　150 千字

印数：1—5000 册

定价：10.00 元

前　言

自1987年美国发现第一例计算机病毒，几年时间，计算机病毒迅速在世界范围内蔓延，到目前已发现的计算机病毒有几千种，给广大计算机用户造成了极大的损失。面对如此之多的病毒，许多计算机用户常常感到束手无策，尤其初级计算机用户，对计算机病毒的概念、机理、防治方法知道的不多，即使在发现计算机病毒后也找不到防治方法，为此造成许多损失。我们编写这本书的目的，就是为广大计算机用户提供一本浅显易懂，便于学习的计算机病毒防治书籍。

本书共分四部分：第一部分介绍计算机病毒的概念和机理；第二部分讲述了计算机病毒的防治方法；第三部分剖析了几十种计算机病毒，并给出了防治方法；第四部分重点介绍了防病毒卡和消毒软件的使用。

本书采用一问一答的形式，通俗易懂，便于查阅学习。

由于计算机病毒种类增加很快，加之作者水平所限，书中难免有遗漏、失误之处，希望广大读者不吝赐教。

作　者

1994年12月　保定

目　录

第一部分　计算机病毒的概念和机理

1.什么是计算机犯罪?

所谓计算机犯罪就是以计算机为工具或以计算机资产为对象实施的犯罪行为,其具体表现在以下几个方面:

(1)计算机滥用:任何与计算机相关的事件,在该事件中受害者遭受或者可能已经遭受了损失,而犯罪者都有意获得或可能已经获得利益。

(2)计算机犯罪:任何利用计算机技术知识作为基本手段的非法行为。

(3)数据泄露:未经允许,私自从计算机系统中转移或取得数据拷贝。这里的数据泄露是有计划的盗窃活动,而数据泄露是偶然情况下的数据转移。

2.计算机在犯罪方面起哪些作用?

计算机在犯罪方面起以下四个作用:

(1)犯罪客体—— 计算资产是犯罪分子攻击的对象或目标。

(2)犯罪主体—— 计算机为罪犯提供了犯罪的场所和环境,替犯罪分子执行了犯罪活动。

(3)犯罪工具—— 计算机是罪犯的犯罪工具。

(4)犯罪象征—— 罪犯利用计算机进行诈骗或者进行恐怖活动。总之,计算机犯罪的目标、作案方法和工具都与计算机技术有着密切的关系,其表现形式也多种多样。

3.计算机犯罪有哪些类型?

当前，计算机犯罪主要有以下类型：

(1)程序、数据、存储介质的物理性破坏；

(2)窃取或转卖信息资源；

(3)盗用计算机机时；

(4)利用网络通信线路进行非法活动；

(5)操作员利用值班时间进行非法活动；

(6)利用信息系统中存在的程序或数据错误，进行非法活动；

(7)非法对程序进行修改；

(8)信用卡方面的计算机犯罪。

4.计算机犯罪的手段有哪些?

根据目前对计算机犯罪案例的分析，大多数计算机犯罪活动采取以下手段：

(1)数据欺骗(data diddling)

在计算机系统下，非法篡改输入/输出数据，其中包括在数据输入计算机前和输入过程中更改原始数据。有的采取假造或冒充的文件，利用软磁盘或计算机磁带进行互换(调包)以篡改原始数据。

从信息流和传输界面的角度来讲，在每一个已装备了计算机系统的企事业部门，都存在着用于可以接触或从事生成、记录、传送、编辑、检查、变更和转换送入系统中的数据，并能够在数据生成过程中进行修改。非法篡改输入/输出数据是最普通、最常见的犯罪活动。

(2)特洛伊木马(Trojan horse)

这种方法是在程序中暗存秘密指令，使计算机在仍能完成原先指定任务的情况下，执行非授权的功能。

特洛伊木马的关键是采用潜伏机制来执行非授权的功能。计算机病毒包括了特洛伊木马的功能。此外，计算机病毒还具有很强的非授权的再生机制。

(3)意大利香肠战术(Salami techniques)

色拉米(Salami)是指意大利式的香肠。意大利香肠战术是迫使对方作出一连串的细小让步，最后达到原定目标的一种战术。这是从大宗财产中偷盗小额财产的一种计算机犯罪形式，形象地比喻如同取走一小片香肠，而人们并没有感到或发现盘子中香肠数量的减少。

意大利香肠战术的关键是采用不易察觉的手段来进行非法活动。

(4)超级冲杀(Super zapping)

超级冲杀是由于大多数 IBM 计算机中心使用宏公用程序 Superzap 而得名的。这是一个当计算机停机，出现故障或其它需要人为干预时的系统程序，它是一个有效的工具，相当于系统的一把总开关钥匙。如果被非授权用户使用，就构成了对系统的一种潜在威胁。

超级冲杀的关键是非授权使用特殊情况下的计算机系统干预程序。

(5)活动天窗(Trap doors)

活动天窗通常是指故意设置的入口点，通过入口点可以进入大型应用程序或操作系统。在输入、修改和重新启动时，可以通过这些窗口访问有关程序。

活动天窗的关键是利用人为设置的窗口侵入系统。

(6)逻辑炸弹(Logic bombs)

在系统程序中插入特定的程序编码，这些编码仅在特定时

刻或特定条件下被激活，所以又称为定时炸弹或逻辑炸弹。逻辑炸弹是对系统的潜在威胁和隐患，可以造成严重危害。

逻辑炸弹的关键是特定条件下的程序激活。计算机病毒的可激发特征，实际上就是逻辑炸弹。

(7)清理垃圾(Scavenging)

这是从计算机系统或机器周围的废弃物中获取信息的一种方法。例如，当系统没有清除临时输入或输出信息的缓冲存储器，或者没有清除磁盘或磁带上存储的信息，从而造成这些信息被人为地窃取和利用。

清理垃圾是有目的或有选择地进行工作现场或废弃物中的信息搜索。

(8)浏览(Browsing)

在系统或终端设备上，利用合法使用手段在存储区搜索某些有兴趣或潜在价值的东西，也有利用合法访问系统某一指定部分文件的机会，趁机访问非授权文件，这些活动都是在正常操作掩护下的非法活动。

浏览是在合法外衣掩护下进行的非法活动。

(9)数据泄露(Data leakage)

不管计算机犯罪的手段多么高明，直接从计算机系统中窃取数据是要冒很大风险的。为此，有的作案者将一些关键数据渗漏在一般性的报表之中，有的计算机间谍在计算机系统中央处理机上安装了微型无线电发射机，将计算机处理的内容传送给几公里外的接收机。

数据泄露是有意转移或窃取信息的手段。

(10)顺手牵羊(Piggy backing)

在分时操作系统管理下的用户终端，当一个用户在使用自

己的口令进入工作状态之后，他可能临时有事暂时离开或去接电话，此时可能被他人利用，在没有授权的情况下，以人家的身份从中获取信息或数据。在数据处理中心，用户程序和打印结果往往被人冒领或代领，有的发现磁带存放位置移动；有的软磁盘丢失，这是被人钻了管理上出现的漏洞。

顺手牵羊是被人利用管理上的漏洞，从而造成文件或信息的丢失。

(11)冒名顶替(Imptrsonation)

当用户使用口令(Password)时，被他人发觉并随后利用，趁机窃取重要信息。因此，用户的口令要注意更新和保密。

(12)蠕虫(Worm)

使用未定义过的处理器来执行运算，在一个分布式网络系统中，可以通过网络来传播错误，进而造成网络服务要求被拒绝并发生死锁。通常需要重新启动才得以排除蠕虫对系统的恶性作用。

蠕虫是通过网络来扩散错误，进而危害整个系统的。

(13)核心大战(Cove Wars)

两个相互破坏对方的程序，实际运行中，可能造成对系统的破坏。

计算机系统中应该严格禁止核心大战之类的程序体之间的相互攻击。在一定意义上，计算机病毒是一个程序体(病毒载体)对计算机系统和其它用户文件(尚未感染该病毒的程序体)的主动攻击，计算机病毒的蔓延是合法的名义下(系统和其它用户文件的合法使用)进行的非授权程序加载。

5.计算机犯罪主要发生在哪些方面?

目前各国计算机犯罪主要集中在两个方面，即：机密信息系

统和金融系统。机密信息系统主要涉及具有重要政治、军事、经济价值的信息系统，也包括类似产品研制、销售和具有商业价值的非公开的信息系统。金融系统主要涉及通过计算机管理金融市场和电子货币。

6．计算机犯罪有哪些特点？

尽管计算机犯罪形式千姿百态，手段也多种多样，但其有很多共同点和趋势：

(1)计算机犯罪属于高技术犯罪，具有瞬时性和随机性，并且，人们难于对犯罪者取证。

(2)计算机犯罪是伴随现代化进程产生的，已成为当今世界各国面临的严重威胁和重大社会问题。

(3)计算机病毒是计算机犯罪的一种新的衍化形式，它们对系统的破坏亦是随编写者的目的而定的。它们可以利用现有计算机犯罪手段，这种手段又比以往的计算机犯罪手段高明得多。

(4)计算机系统的脆弱性是计算机病毒产生的基础，计算机系统的信息共享又是计算机病毒传播的首要条件。

(5)计算机科学技术的发展，特别是微型计算机的普及，硬件和软件知识的透明度以及计算机使用方法的通用性等，是计算机病毒产生的实际环境和传播途径。

(6)计算机病毒是一个国际性问题，真正要消除计算机病毒，有待于国际间的合作。

(7)罪犯趋向年轻化。在已发现的计算机罪犯中年龄范围为18—46岁，其平均年龄为25岁。

(8)罪犯往往是最熟练和有知识的技术人员，往往是掌握核心机密的人，其犯罪的破坏性也往往是相当严重的。

(9)在计算机犯罪中共谋作案远比其它类型的案件更为多