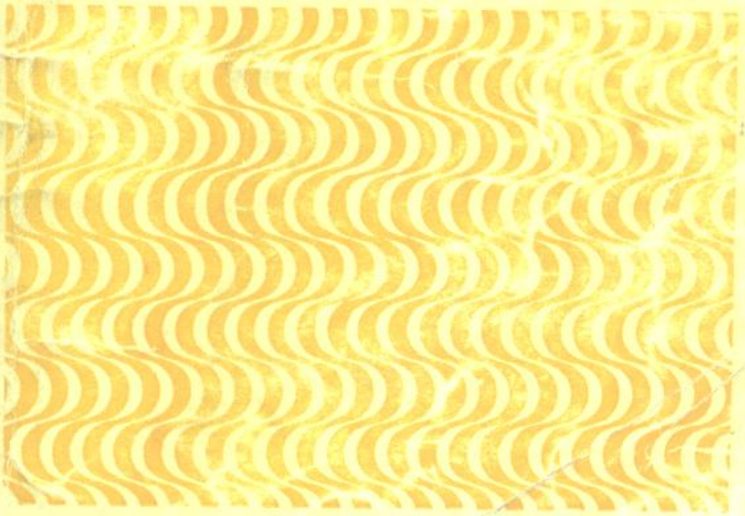
张汉亭 编著

计算机病毒的诊断治疗和预防



青岛出版社

计算机病毒的诊断治疗和预防

张汉亭 编著

青岛出版社

责任编辑　樊建修
封面设计　王　文

计算机病毒的诊断治疗和预防

张汉亭 编著

*

青岛出版社出版
（青岛市徐州路77号）
新华书店总店北京发行所发行
青岛新华印刷厂照排
山东临朐县印刷厂印刷

*

1991年7月第1版　　1991年7月第1次印刷
32开(787×1092毫米)　6.625印张　　125千字
印数1—10230
ISBN 7-5436-0644-5/TP・42
定价：3.50元

序　言

近代工业的发展曾经走过一段弯路。

工业生产技术本应与工业污染的治理同步发展，但是由于认识上的局限，人们着力于前者，忽视了后者。当近代工业经历了一段高速发展以后，人们尝到了自己种下的苦果——工业污染造成的社会公害。

工业废气污染了大气，工业污水污染了江河湖海，工业废弃物特别是带有核辐射的废弃物使人们惶惶不安。工业污染使我们的地球出现了许多陌生的令人畏惧的事物。诸如带毒的雾、美国的酸雨、日本的水俣病、南极上空臭氧层的空洞、饮水中超量砷引起的慢性中毒，镉导致的癌症等等。

物质财富的生产过程严重威胁着物质财富生产者本身的生存。在生态学家发出的"救救地球！"呼吁声中，人们被迫回过头来致力于工业污染的治理和研究。

很不幸，在计算机科学的发展过程中，又出现了极为相似的情景。

计算机应用技术本应与计算机安全技术同步发展。但是，在计算机科学发展的前期，受到计算机科学当时水平的限制，计算机是极为昂贵的系统，使用计算机必须依赖于计算机专家的介入。一般用户甚至不能亲手触摸计算机，当然就谈不上广泛的信息共享。因此，计算机的安全问题似乎不那么紧迫，不那么重要。

当着微机广泛普及，网络技术蓬勃兴起，数据库技术有了长足的进步之后，伴随广泛的信息共享出现了计算机犯罪。

计算机犯罪是一种崭新类型的犯罪。此类罪犯的特点是具有较高层次的知识能量和利用计算机安全漏洞的机遇。

计算机犯罪可以造成重大的经济、政治危害。由于这种犯罪可以瞬间进行，其发生又具随机性，所以在侦破、取证甚至审判中都会遇到种种困难。

传统的计算机犯罪的危害范围，一般局限于犯罪预定的目标，局限在相对狭小的范围内。一般人常常难于体会到计算机犯罪对自身的威胁。

但是，现在当计算机病毒——一种更高技术层次的计算机犯罪问世以后，迫使我们不得不面对病毒的威胁。

我们是无辜的。对计算机病毒的研制者，我们从未伤害过他们，我们从未欠他们的情，可是我们却频繁地受到病毒无端的攻击，我们宝贵的信息财富时时刻刻处于病毒攻击的威胁之中。

如果在计算机病毒的世界里，你是一个文盲，那么你可能受到双重伤害：一方面你最容易遭受病毒的攻击，从而造成惨重损失；另一方面你可能在不知不觉中成为病毒的"窝主"，可以使某种病毒在被扑灭几个月甚至几年后，经由你的手偶然地使之死灰复燃。

一位美国计算机安全专家指出："高素质的用户仔细观察系统的异常现象，就可以检测出病毒或蠕虫的存在。"

只有发现病毒，才能做剖析、消毒和免疫研究。要做这些工作，要求具有相当层次计算机系统知识和有关病毒的种种信息。

为普及有关病毒的基本知识，谨将此书献给读者，如果能对诸位有所帮助，笔者将感到欣慰。

限于笔者的水平，书中必定有错误和不当之处，敬请批评指正。

在本书编写过程中，樊建修、徐诚和朱巧生同志曾给予极大支持和鼓励，谨向他们致以深切谢意。

张汉亭

1990 年 9 月

目　录

第一章　计算机病毒概论

1.1　计算机病毒简史

1. 蠕虫事件

1988年11月2日下午5时1分59秒，美国康奈尔大学的计算机科学研究生，23岁的莫里斯(Morris)将其编写的蠕虫程序输入计算机网络。在几小时内导致 Internet 网络堵塞。这个网络连结着大学、研究机关的155000台计算机，这些机器用于与美国军方交换和搜集非保密数据。

莫里斯的蠕虫程序感染了约6000台计算机，使网络堵塞，运行迟缓。莫里斯因计算机欺诈和滥用罪，成为被地方法院依据1986年制定的计算机安全法起诉的第一个计算机犯罪者。如果起诉有效，他将被判处五年监禁和250000美元罚款。

美国当局对莫里斯的起诉果断而迅速，是有原因的。首先，这一事件导致了国家的大计算机网络堵塞，成为报纸的头版新闻，轰动了美国社会。其次，受到美国一些国会议员的政治压力，他们自信在两年前刚刚通过了一个有效的计算机安全法。最后是来自某些计算机专家的歇斯底里的义愤。

而最主要的原因可能是莫里斯的父亲是美国高级情报和安全机关——国家安全局(NSA)的高级计算机专家。他有能力为儿子求情以使之逃避起诉。

莫里斯的蠕虫像是计算机世界的一次大地震，引起巨大

反响，震惊了全世界，引起了人们对计算机病毒的恐慌，也使更多的计算机专家重视和致力于病毒研究。

美国的一些计算机专家在事件发生后，仔细剖析了莫里斯的蠕虫程序，对其性质和行为做了深入研究。对蠕虫事件的后果做了比较全面公正的评价。在指出其危害的同时，认为蠕虫程序揭露了国家计算机网络存在的漏洞，并引起了计算机界对病毒构成的潜在威胁的普遍重视。

莫里斯的蠕虫程序在全世界刮起了一场旋风，激起舆论界和科技界对计算机病毒的普遍关注。

2. 事实

莫里斯不是计算机病毒的始创者，美国的计算机专家 B. Meeks 指出：计算机病毒可能已有二十多年的历史了，美国军方研究计算机病毒已经十多年了。只是最近，病毒才被公开，成为受人关注的问题。

B. P. Zajac 指出：计算机病毒不是一个新问题，它不过是攻击计算机的陈旧策略的新翻版。

美国著名的计算机安全专家 Frederick B. Cohen 在加利福尼亚大学做博士论文时，就研制了计算机病毒，以求寻找一种方法防御能自身繁殖的程序。Cohen 发现防御它们几乎不可能。Cohen 使用了 DEC VAX 计算机和 Univac 1108计算机，他发现在关键的几分钟内病毒就可在计算机内传播。

Cohen 关于病毒的研究成果于1984年首次在国际计算机安全会议上发表。

1986年 Rudiger Dierstein 等人在法国巴黎召开的计算机安全会议上发表了论文“计算机病毒：潜在的威胁”。

有关计算机病毒的研究报告，自 Cohen 第一次发表以来，

人们可在历次学术会议上的有关报告中寻迹查询，而美国军方在那样长的时间内与计算机病毒的接触和有关研究，却是一片空白。病毒发展的历史，像浮存于大海的一座冰山，只能看到水面上的轮廓，对被隐藏的未知部分，没有任何资料说明其经纬，要弄清计算机病毒发展史的全貌，也许要寄希望于未来。

1.2 计算机病毒的起因

国际标准化委员会对计算机安全的定义提出如下建议："为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭破坏、更改、显露"。

计算机系统的安全可能受到三方面的威胁：

(1)自然灾害

(2)意外事故

(3)人为破坏

本书不准备讨论广义上的计算机安全问题，仅限于与计算机病毒有关的因素。

1. 脆弱的计算机系统

设计计算机系统时，主要考虑下述因素：

(1)安全性

(2)易操作性

(3)性能价格比

这三个因素互相关联互相制约，设计者必须统观全局，妥善处理，不能把某个因素强调过分，又不可忽视另一因素。最后设计的系统总是三个因素妥协的结果。从不同角度看，总可

以发现某些不得已的缺欠和漏洞。

2. 安全性

安全性在多用户系统中显得尤其重要，在信息共享的多用户系统中，安全性差的系统是危险的，常常是用户不能接受的。

例如 IBM PC 机的 MS-DOS 操作系统是一个单任务单用户系统，用户占有全部资源，可以为所欲为，做其欲做的任何事情。

80286和80386 CPU 芯片在设计时，考虑到多用户多任务的运行环境，硬件上考虑了如下因素：

(1)将各任务的信息区隔开

(2)将用户程序与操作系统隔开

前者在不同用户任务之间建立“防火墙”，防止用户之间数据的非法访问和修改。也防止了用户代码之间的相互干扰。

后者将操作系统与用户代码进行了隔离，防止用户代码扰乱操作系统的工作。用户不仅不能修改操作系统，甚至不能读操作系统的重要代码。

为实现上述目标，80286和80386采用了四个特权级、设置段特权、监督段长度、I/O 特权、特权指令、不可读的段描述符寄存器等手段，大大增强了安全性，同时给用户以种种限制，使用户感到不便。芯片结构变复杂，成本上升。

3. 易操作性

计算机系统对用户应友好，提供用户方便、友好的界面服务。一般用户使用汇编语言编写种种外围设备控制程序往往是困难的。因此，操作系统常常将内部的功能模块向用户开放。用户只需设置几个接口参数，只用几条命令调用操作系统

的功能模块，就能以极小的开销做很复杂的动作，例如读写软盘或硬盘。

4. 性能价格比

物美价廉是轰开市场的重炮。预防不安全因素所付的代价愈大，效果相对较好。在某一投资阈值之前，投资与效果一般成正比。超过阈值，过大的投资可能给用户以不能忍受的经济负担。因此必须寻找适当的安全措施和可承受的经济投资，使系统既安全而投资又不太大，保持好的性能价格比，使系统具有强的市场竞争能力。

5. 脆弱的 MS-DOS

综上所述，系统的安全性与易操作性两者互相矛盾。为了安全必将使系统趋向孤立和封闭。为了使用方便，要求系统透明和开放，顾及前者必损及后者，难于两全。

众所周知 MS-DOS 是西文操作系统，经我国计算机专家的改造，产生了 CCDOS 汉字操作系统。CCDOS 修改了 MS-DOS 中断矢量表，用新开发的常驻程序补充了 INT 16H、INT 10H 等有关键盘、屏幕、打印机等中断功能，采用“打补丁”的方法使 MS-DOS 维持西文处理全部功能的同时，增添了汉字处理功能。这证明了两点：

(1)从对用户友好的角度看，MS-DOS 是一个相当好的系统，它赋予用户以很大的权力，可以对 MS-DOS 大刀阔斧地进行改造，便于用户扩展系统功能。

(2)从安全角度看，MS-DOS 几乎没有自我保护意识，像一座不设防的城，用户如入无人之地，为所欲为。它极易受到攻击，是很脆弱的系统。

MS-DOS 的 FAT 表、文件目录、中断矢量表等对用户都