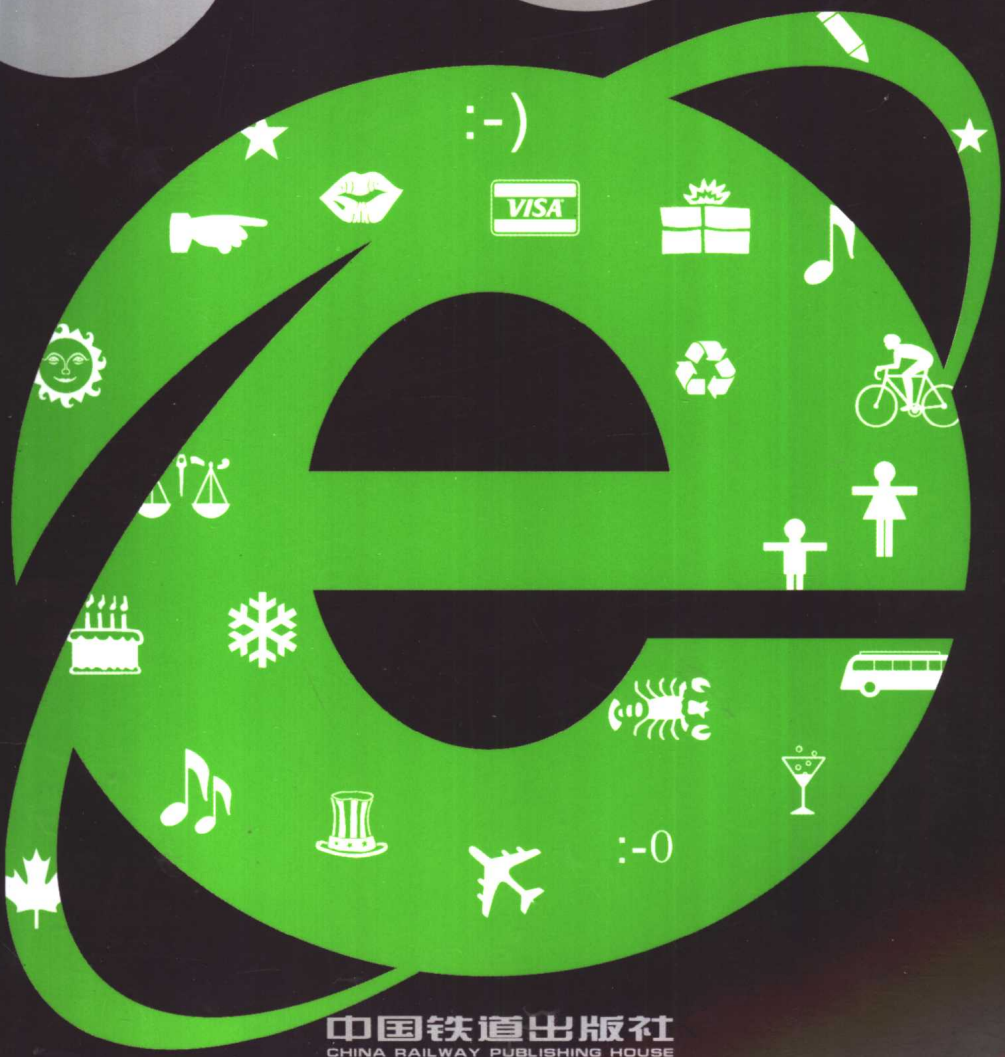
健莲科技　编著

电脑防毒、防黑、防窥百事通



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

电脑防毒、防黑、防窥百事通

健蓬科技　编著

中国铁道出版社

2003·北京

（京）新登字 063 号

内 容 简 介

本书从应用的角度出发，以实现安全使用计算机为目的，辅助读者合理配置自己的系统，安装相应的软件，最终达到安全地使用计算机的目的。您只需要按照本书介绍的步骤一步一步的安装并配置软件，就可以将已知的病毒清除，防范未知的病毒，阻止黑客的攻击，加密用户的机密数据，让您能够面对计算机安全性问题高枕无忧。

此外，本书还附录了书中介绍的防毒、防黑和防窥软件的下载地址，如果您手头没有这些软件，只需从网上 Download 就可以了。

图书在版编目（CIP）数据

电脑防毒、防黑、防窥百事通/健莲科技编著. —北京：中国铁道出版社，2002.11
ISBN 7-113-04991-5

（电脑应用百事通）

Ⅰ.电… Ⅱ.健… Ⅲ.① 计算机病毒—防治 ② 计算机网络—安全技术
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2002)第 085305 号

书　　名：电脑防毒、防黑、防窥百事通
作　　者：健莲科技
出版发行：中国铁道出版社（100054，北京市宣武区右安门西街 8 号）
责任编辑：苏　茜
封面设计：孙天昭
印　　刷：北京市彩桥印刷厂
开　　本：880×1230　1/32　印张：13.125　字数：392 千
版　　本：2003 年 1 月第 1 版　2003 年 1 月第 1 次印刷
印　　数：1～6 000 册
书　　号：ISBN 7-113-04991-5/TP·806
定　　价：19.00 元

《百事通》系列丛书编委会

《百事通》系列丛书

前 言

随着网络时代的到来，人们越来越深切地体会到计算机在日常工作和生活中所起到的重要作用，学习计算机的浪潮被一次又一次地掀起，从幼小的儿童到白发苍苍的老人都加入到了学习计算机的行列中。越来越多的职业需要具备相当水平的计算机应用技能，掌握计算机几乎已经成为个人事业发展的前提。

从最普遍的办公自动化，到网络的高级应用，以及操作系统的使用技巧等，这些技能都是在使用计算机和解决问题的过程中所必须掌握的。学会了优化系统性能，才能使自己的爱机跑得更快；学会了网络的设置技巧，才能更加随心所欲地畅游网海；学会了刻录光盘的各种技巧，才能将自己喜欢的音频、视频制成 VCD。这些技能，不仅能大幅提高工作效率，也能让自己的生活变得更加丰富多彩。

为了实现广大计算机用户的愿望，中国铁道出版社特别推出了《百事通》系列丛书，帮助读者快速掌握各种计算机的应用技能和技巧，为读者提供一条学习计算机的捷径。《百事通》系列丛书首批推出的共八种：《Windows XP 百事通》、《泡网百事通》、《光盘刻录百事通》、《宽带应用百事通》、《电脑防毒、防黑、防窥百事通》、《局域网架构、维护、排困百事通》和《当机拯救百事通》等。这些图书的内容都与计算机的日常应用紧密结合，可以帮助读者真正解决实际应用中的难题。

《百事通》丛书采用新颖的版式，案例丰富，在详细讲解的同时配合必要的操作步骤，读者只要按照书中的步骤进行操作，就可以达到所要的效果。本套丛书将知识和实例紧密结合，并提供了许多小技巧、小秘诀，不仅让读者受益，也提高了阅读的趣味性。

《百事通》系列丛书题材实用、内容超值，希望广大读者能够通过本套丛书掌握各种知识和技巧，真正成为计算机应用的高手。

由于时间有限，书中难免存在不尽人意之处，还望广大读者批评指正。

编 者

目 录

百事通

电脑防毒、防黑、防窥基础知识

Chapter 1

- 计算机防毒基础
- 防黑基础
- 防窥基础

1.1 计算机防毒基础

1.1.1 认识计算机病毒

1.计算机病毒的定义

计算机病毒其实就是一个程序，它和我们平常所使用的 IE,Word,OutLook 这些软件一样，都是属于计算机软件，只不过这种程序拥有和细菌一样独特的“寄生”、“感染”、“繁殖”、“破坏”等特性，所以我们称它为病毒。

简单来说，病毒就是一段非常小的程序（通常只有几 K 字节或者几百字节），它会不断地自我复制、隐藏、感染其他的软件程序或电脑，然后伺机执行一些（破坏）动作。

2.计算机病毒的起源

计算机病毒的起源最早在 1987 年，有一对巴基斯坦的兄弟，为自己开发的软件写了一段保护代码，这段保护程序在发现有人非法拷贝软件的时候，会自动复制到非法复制的软盘上，并将磁盘的卷标改为“(C)Brain”，以警告那些非法软件使用者。当初“(C)Brain”的出现其实并没有什么破坏行为，纯粹是警告使用者不要非法拷贝软件。不过后来研究这类会自我复制的程序的人，纷纷加入了一些破坏性行为，使得大家目前看到的计算机病毒，或多或少的都会破坏感染电脑中的数据，使大家谈毒色变。

3.计算机病毒产生的背景

计算机病毒的产生是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物。它产生的背景是：

(1) 计算机病毒是计算机犯罪的一种新的衍化形式

计算机病毒是高技术犯罪，具有瞬时性、动态性和随机性。不易取证、风险小破坏大，从而刺激了犯罪意识和犯罪活动。是某些人恶作剧和报复心态在计算机应

用领域的表现。

(2) 计算机软硬件产品的脆弱性是根本的技术原因

计算机是电子产品。数据从输入、存储、处理、输出等环节，易误入、篡改、丢失、作假和破坏；程序易被删除、改写；计算机软件设计的手工方式,效率低下且生产周期长；人们至今没有办法事先了解一个程序有没有错误，只能在运行中发现、修改错误，并不知道还有多少错误和缺陷隐藏在其中。这些脆弱性就为病毒的侵入提供了方便。

(3) 微机的普及应用是计算机病毒产生的必要环境

1983 年 11 月 3 日美国计算机专家首次提出了计算机病毒的概念并进行了验证。几年前计算机病毒就迅速蔓延,到我国才是近年来的事。而这几年正是我国微型计算机普及应用热潮。微机的广泛普及，操作系统简单明了，软、硬件透明度高，基本上没有什么安全措施,能够透彻了解它内部结构的用户日益增多，对其存在的缺点和易攻击处也了解得越来越清楚，不同的目的可以做出截然不同的选择。目前，在 IBM PC 系统及其兼容机上广泛流行着各种病毒就很说明这个问题。

4.计算机病毒的感染途径

计算机病毒因为拥有高度传染性,所以使用者常常在莫名其妙的情形下就感染上了病毒，和细菌一样，大家都知道病从口入是病毒的传染方式，计算机病毒的传播途径也是有一定规律可循的，就目前已知的计算机病毒而言，它们的传播途径无非是以下两类：

(1) 软盘或者光盘传播

a. 不小心使用了含有病毒的软盘或者光盘启动，你的电脑就感染了开机型病毒。

b. 不小心执行了感染了磁盘或者光盘中感染病毒的文件，你的电脑就感染了文件型病毒。

c. 电脑系统已经感染了病毒，在你访问磁盘或者将已经感染病毒的文件刻录到光盘内时，这些病毒就乘机感染了磁盘和光盘，然后再以前两种方法传播。

(2) 通过网络传播

这里所谓的网络是广义的网络，包括企业内的局域网和大家通常使用的互联网。当你从网络中获取一个感染病毒的软件，或是收到的电子邮件中含有病毒，在不经意间浏览或者打开它们后，病毒就会感染你的系统。根据统计，目前通过网络感染的病毒已经比通过磁盘和光盘感染的病毒高出 100 倍，可见，网络已经成为最大的病毒传播途径。图 1.1 就是笔者收到的一封可疑的电子邮件，附件中很可能就是染毒的文件。

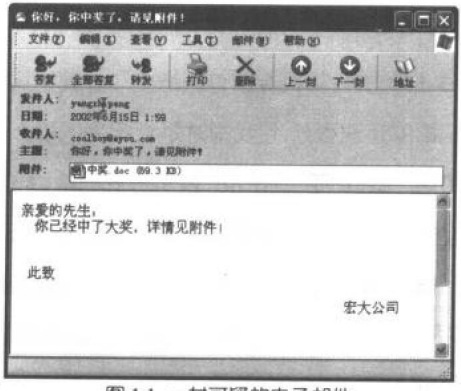


图 1.1 一封可疑的电子邮件

5.计算机病毒的危害

计算机病毒会对电脑系统的软件或者硬件造成破坏，根据目前电脑病毒的破坏程度，我们大致分为以下几种情况：

(1) 系统速度变慢甚至死机

电脑病毒因为要在后台进行自我复制、感染的工作，所以它必须要驻留在内存中伺机执行，因此，你的电脑速度会被病毒这些额外的工作占用大量的资源，使得速度变慢，情况严重的话，甚至死机。

(2) 硬盘容量减小

电脑病毒既然是电脑程序的一种，所以它一定也需要占用磁盘空间，因此，电脑病毒大量自我复制，感染其他文件的结果，会造成硬盘空间的急剧减小，例如 Nimda 病毒。

(3) 网络系统崩溃

自从梅丽莎病毒出现以后，目前许多新的电脑病毒（如 Nimda,求职信病毒等）都开始利用网络系统的漏洞大量地复制和传播，这些病毒大多利用系统漏洞和电子邮件，把病毒大量地寄给感染者，一传十，十传百，这样大量的电子邮件就涌入了服务器，造成网络拥塞，甚至崩溃。

(4) 数据破坏和电脑无法使用

电脑病毒最令人发指的就是破坏数据，例如，前几年比较流行的 CIH 病毒，就是将用户的硬盘的分区表破坏，让用户的电脑无法启动。更有甚者的是，CIH 病毒还可以利用主板 BIOS 的一个设计缺陷，在 BIOS 中写入空数据，使用户的电脑陷入一片黑屏的状态，不得不送入厂家进行维修。

6.计算机病毒的实质

相信读者中对病毒程序了解的应该不太多，所以在本小节最后，我将带大家来看看计算机病毒里面到底是什么样子？本章一开始就曾提到：“计算机病毒其实就是一个程序”，所以病毒实际就如图 1.2 所示：

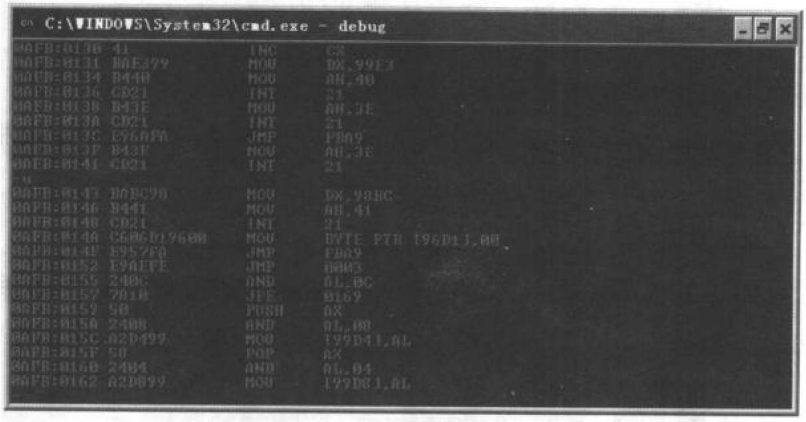


图 1.2 一个病毒在计算机中的代码形式

上面是我们获取的病毒的一段代码，很显然，这是一段汇编程序，也就是最接近机器执行的程序，关于汇编语言，不是本书的讨论范围，有兴趣的读者可以参阅有关书籍来了解更多有关病毒的知识。

1.1.2 计算机病毒的分类

计算机病毒的分类有不同的标准。

1.按破坏性可分为：

(1) 良性病毒：仅仅显示信息、奏乐、发出声响，自我复制的，除了传染时减少磁盘的可用空间外，对系统没有其他影响。

(2) 恶性病毒：封锁、干扰、中断输入输出、使用户无法打印等正常工作，甚至电脑中止运行。这类病毒在电脑系统操作中造成了严重的错误。

(3) 极恶性病毒：死机，系统崩溃、删除普通程序或系统文件，破坏系统配置导致系统死机，崩溃，无法重启。这些病毒对系统造成的危害，并不是本身的算法中存在危险的调用，而是当它们传染时会引起无法预料的和灾难性的破坏。

(4) 灾难性病毒；破坏分区表信息、主引导信息、FAT、删除数据文件，甚至格式化硬盘等。

2.按传染方式可分为：

(1) 文件型病毒：

一般只传染磁盘上的可执行文件(COM，EXE)。

文件型病毒特点是附着正常程序文件，成为程序文件的一个外壳或部件。根据传染方式的不同，又可以分为非常驻型，常驻型，千面人和隐性四类：

a. 非常驻型病毒

非常驻型病毒在你执行中毒的程序时，马上去搜索其他磁盘文件，然后立即传染给它。

b. 常驻型病毒

常驻型病毒在执行完中毒的程序后，会隐藏在系统内存中，此时只要执行任何可执行程序，就会感染病毒，常驻型病毒的传播效果要比非常驻型显著。

c. 千面人病毒

千面人病毒实际上是常驻型病毒的一种，不过它运用了特殊的编程技巧，使它

每次感染别的文件以后都会改变自己的结构，这样做的目的是干扰查毒软件的视线，以增强病毒的传播性。

d. 隐性文件型病毒

隐性文件型病毒有点类似千面人病毒，也是常驻型病毒的一种。隐性文件型病毒的原理和千面人病毒刚好相反，千面人是感染病毒后的文件千变万化，而隐性文件型病毒却让感染后的文件看起来和没感染一样。

(2) 引导扇区病毒：改变每一个用 DOS 格式来格式化的磁盘的第一个扇区里的程序。

通常引导扇区病毒先执行自身的代码，然后再继续 PC 机的启动进程。大多数情况，在这台感染有引导型病毒的机器对可读写的软盘进行读写操作，那么这个软盘也就会被感染。引导扇区病毒感染的原理如图 1.3 所示：

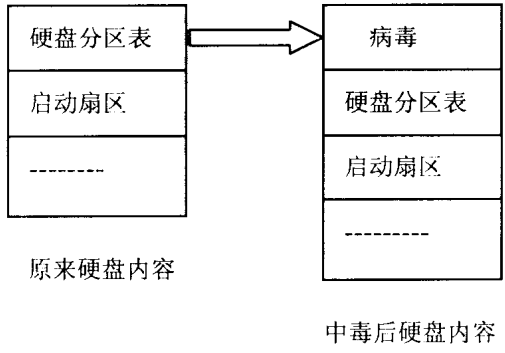


图 1.3 引导扇区病毒原理

(3) 混合型病毒：兼有以上两种病毒的特点，既感染引导区又感染文件，因此扩大了这种病毒的传染途径。

(4) 宏病毒

宏病毒是一种伴随文件一起传播的，最有名的宏病毒，就是前一段闹得满城风云的梅丽莎病毒，它可以造成许多公司局域网系统崩溃。宏病毒是目前最热门的话题之一，因为它跟我们常用的 MS Office 软件息息相关，主要是利用软件本身所提供的编程手段来设计的，所以凡是提供了宏编程的软件都有宏病毒存在的可能，如