

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

健達科技 編著

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

版权所有 侵权必究

凡购买铁道版的图书，如有缺页、倒页、脱页者，请与本社计算机图书批销部调换。

《百事通》系列丛书编委会

张瀚文	姚 辉	姬宪军
刘淑兰	杨松鹤	张 茜
张 英	陈 曦	曾 卓
杨 静	刘振中	刘 翰
刘 稚	张美丽	姚玉英
姚继忠	姚春杰	陈 悅
张淑萍	张淑惠	

《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

第 1 章 电脑防毒、防黑、防窥基础知识	1
1.1 计算机防毒基础	2
1.1.1 认识计算机病毒	2
1.1.2 计算机病毒的分类	6
1.1.3 应有的防毒观念	10
1.2 防黑基础	15
1.2.1 黑客的定义	15
1.2.2 黑客入侵的目的	16
1.2.3 黑客入侵常用的方法	18
1.2.4 防范黑客入侵安全准则	29
1.3 防窥基础	36
1.3.1 加密学基础	36
1.3.2 用密码破解方法	37
1.3.3 从密码心理学看如何保护自己的密码	38
本章小结	40
第 2 章 如何查杀病毒	41
2.1 培养自我查毒的习惯	42
2.1.1 电脑中毒可能征兆	42
2.1.2 如何自我查毒	44
2.2 沉着冷静应对病毒	54
2.2.1 电脑中毒了怎么办	54
2.2.2 流行病毒的特征及清除方法	56
2.3 其他相关问题	73
2.3.1 如何更新病毒数据库	73
2.3.2 数据破坏如何恢复	75
2.4 本章小结	80

本章小结.....	80
-----------	----

第3章 防患于未然——使用防毒软件..... 81

3.1 话说防毒软件	82
3.1.1 防毒软件是否真那么重要	82
3.1.2 如何选择防毒软件	82
3.1.3 常用的防毒软件	84
3.2 使用金山毒霸防护你的系统	90
3.2.1 安装金山毒霸	90
3.2.2 使用金山毒霸查杀病毒	95
3.2.3 使用金山毒霸的嵌入工具	106
3.2.4 使用金山毒霸的实用工具	111
3.2.5 升级金山毒霸	129
3.3 使用其他防毒软件防护你的系统	131
3.3.1 瑞星杀毒软件	131
3.3.2 Norton Antivirus	137
本章小结.....	139

第4章 最佳防毒策略——备份..... 142

4.1 备份的重要性	142
4.2 备份 Windows 系统重要数据	142
4.2.1 WinRescue 软件介绍	142
4.2.2 安装 WinRescue	143
4.2.3 使用 WinRescue 备份 Windows 系统重要数据	145
4.2.4 使用 WinRescue 还原 Windows 系统重要数据	148
4.2.5 WinRescue 的其他功能	152
4.3 制作紧急还原光盘	153
4.3.1 获取 Symantec Ghost	153
4.3.2 安装 Symantec Ghost	156
4.3.3 使用 Symantec Ghost 制作启动磁盘	160
4.3.4 使用 Symantec Ghost 备份硬盘数据	164
4.3.5 开始刻录紧急还原光盘	166

4.3.6 使用 Symantec Ghost 还原硬盘数据	169
本章小结	171

第 5 章 网络防黑基本功 173

5.1 黑客常用的攻击手段	174
5.2 配置 Windows 系统防范黑客入侵	178
5.2.1 安全配置 Windows 系统	178
5.2.2 使用本地安全策略增强系统的安全性	179
5.2.3 升级 Windows 系统防堵漏洞	185
5.3 特洛伊木马大揭秘	191
5.3.1 特洛伊木马的原理	191
5.3.2 实战特洛伊木马	199
5.3.3 特洛伊木马终结者—Trojan Remover	200
本章小结	209

第 6 章 使用防火墙防范黑客入侵 211

6.1 防火墙简介	212
6.1.1 防火墙概览	212
6.1.2 防火墙软件的选择	213
6.2 天网个人防火墙	214
6.2.1 天网防火墙简介	214
6.2.2 天网防火墙下载,安装和注册	215
6.2.3 天网防火墙设置	221
6.2.4 天网安全检测修复系统	230
6.3 ZoneAlarm	232
6.3.1 安装 ZoneAlarm	232
6.3.2 ZoneAlarm 使用说明	235
6.4 Norton 个人防火墙	241
6.4.1 Norton 个人防火墙简介	241
6.4.2 Norton 个人防火墙的获取和安装	242
6.4.3 Norton 个人防火墙的配置	246
本章小结	255

第7章 初级防窥秘笈 257

7.1 BIOS 加密	258
7.1.1 BIOS 的基本功能和加密原理	258
7.1.2 BIOS 加密方法	259
7.1.3 BIOS 密码的破解与保护	262
7.2 Windows 系统加密	266
7.2.1 Windows 98 系统的加密功能	266
7.2.2 Windows 2000 系统的加密功能	269
7.2.3 使用超级兔子魔法设置加密 Windows	278
7.3 常用软件的加密	281
7.3.1 办公软件的加密	281
7.3.2 压缩软件的加密	288
7.3.3 常用网络工具的加密	294
本章小结	297

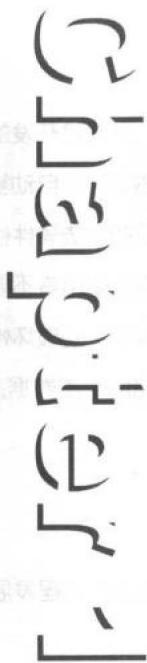
第8章 高级防窥大法 299

8.1 文件加密	300
8.1.1 密码大师	300
8.1.2 iProtect Portable	305
8.1.3 文件加密利器 Fedt	308
8.1.4 其他文件加密工具	311
8.2 光盘加密	313
8.2.1 刻录加密光盘	313
8.2.2 光盘加密保护	316
8.3 专业加密	320
8.3.1 给你的文件加把锁——WinXFiles	320
8.3.2 让你的邮件更安全——PGP	328
本章小结	338
本章涉及的软件下载地址	339
防病毒软件下载地址	339
防黑软件下载地址	339

防窥软件下载地址	339
第9章 三防技巧FAQ.....	341
9.1 防毒FAQ	342
9.1.1 病毒知识FAQ	342
9.1.2 反病毒FAQ	349
9.1.3 金山毒霸.NET	367
9.2 防黑FAQ	375
9.2.1 黑客常用的攻击方法有哪些	375
9.2.2 网络防黑到底有哪些策略	380
9.2.3 个人上网需注意什么	380
9.2.4 为什么要经常修改上网密码	382
9.2.5 如何有效阻断拒绝服务攻击	383
9.2.6 混客绝情病毒说明与解决方案	385
9.2.7 网吧上网应注意什么	386
9.2.8 怎样防止QQ被黑	390
9.2.9 恶意网页烦人怎么办	395
9.3 防窥FAQ	399
9.3.1 怎样设置安全的密码	399
9.3.2 加密文件一般使用什么工具	400
9.3.3 Office系列文件密码忘记怎么办	400
9.3.4 Zip,Rar文件忘记密码怎么办	401
9.3.5 BIOS密码忘记怎么办	402
9.3.6 忘记Windows 2000密码怎么办	407

百事通

电脑防毒、防黑、防窥 基础知识



- 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，目前通过网络传播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。

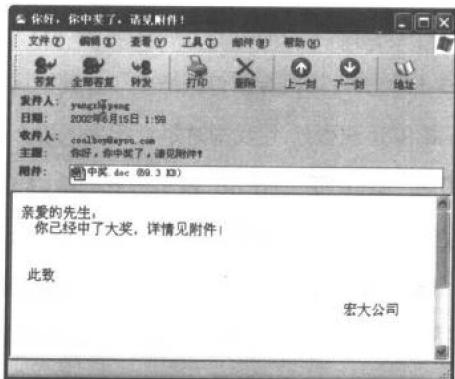


图 1.1 一封可疑的电子邮件

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，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：

```

C:\WINDOWS\System32\cmd.exe - debug
00401700: 41      INC    DS
00401701: B0E999    MOU    BX,99E9
00401702: B440      MOU    BH,40
00401703: C02        INT    21
00401704: C021      INT    21
00401705: B41E      MOU    BH,1E
00401706: C024      INT    21
00401707: B430      MOU    BH,30
00401708: C026      INT    21
00401709: E960F0    JMP    F009
0040170A: B431      MOU    BH,31
0040170B: C021      INT    21
0040170C: B432      MOU    BH,32
0040170D: C021      INT    21
0040170E: B433      MOU    BH,33
0040170F: C021      INT    21
00401710: B434      MOU    BH,34
00401711: C021      INT    21
00401712: B435      MOU    BH,35
00401713: C021      INT    21
00401714: B436      MOU    BH,36
00401715: C021      INT    21
00401716: B437      MOU    BH,37
00401717: C021      INT    21
00401718: B438      MOU    BH,38
00401719: C021      INT    21
0040171A: B439      MOU    BH,39
0040171B: C021      INT    21
0040171C: B43A      MOU    BH,3A
0040171D: C021      INT    21
0040171E: B43B      MOU    BH,3B
0040171F: C021      INT    21
00401720: B43C      MOU    BH,3C
00401721: C021      INT    21
00401722: B43D      MOU    BH,3D
00401723: C021      INT    21
00401724: B43E      MOU    BH,3E
00401725: C021      INT    21
00401726: B43F      MOU    BH,3F
00401727: C021      INT    21
00401728: B440      MOU    BH,40
00401729: C021      INT    21
0040172A: B441      MOU    BH,41
0040172B: C021      INT    21
0040172C: B442      MOU    BH,42
0040172D: C021      INT    21
0040172E: B443      MOU    BH,43
0040172F: C021      INT    21
00401730: B444      MOU    BH,44
00401731: C021      INT    21
00401732: B445      MOU    BH,45
00401733: C021      INT    21
00401734: B446      MOU    BH,46
00401735: C021      INT    21
00401736: B447      MOU    BH,47
00401737: C021      INT    21
00401738: B448      MOU    BH,48
00401739: C021      INT    21
0040173A: B449      MOU    BH,49
0040173B: C021      INT    21
0040173C: B44A      MOU    BH,4A
0040173D: C021      INT    21
0040173E: B44B      MOU    BH,4B
0040173F: C021      INT    21
00401740: B44C      MOU    BH,4C
00401741: C021      INT    21
00401742: B44D      MOU    BH,4D
00401743: C021      INT    21
00401744: B44E      MOU    BH,4E
00401745: C021      INT    21
00401746: B44F      MOU    BH,4F
00401747: C021      INT    21
00401748: B450      MOU    BH,50
00401749: C021      INT    21
0040174A: B451      MOU    BH,51
0040174B: C021      INT    21
0040174C: B452      MOU    BH,52
0040174D: C021      INT    21
0040174E: B453      MOU    BH,53
0040174F: C021      INT    21
00401750: B454      MOU    BH,54
00401751: C021      INT    21
00401752: B455      MOU    BH,55
00401753: C021      INT    21
00401754: B456      MOU    BH,56
00401755: C021      INT    21
00401756: B457      MOU    BH,57
00401757: C021      INT    21
00401758: B458      MOU    BH,58
00401759: C021      INT    21
0040175A: B459      MOU    BH,59
0040175B: C021      INT    21
0040175C: B45A      MOU    BH,5A
0040175D: C021      INT    21
0040175E: B45B      MOU    BH,5B
0040175F: C021      INT    21
00401760: B45C      MOU    BH,5C
00401761: C021      INT    21
00401762: B45D      MOU    BH,5D
00401763: C021      INT    21
00401764: B45E      MOU    BH,5E
00401765: C021      INT    21
00401766: B45F      MOU    BH,5F
00401767: C021      INT    21
00401768: B460      MOU    BH,60
00401769: C021      INT    21
0040176A: B461      MOU    BH,61
0040176B: C021      INT    21
0040176C: B462      MOU    BH,62
0040176D: C021      INT    21
0040176E: B463      MOU    BH,63
0040176F: C021      INT    21
00401770: B464      MOU    BH,64
00401771: C021      INT    21
00401772: B465      MOU    BH,65
00401773: C021      INT    21
00401774: B466      MOU    BH,66
00401775: C021      INT    21
00401776: B467      MOU    BH,67
00401777: C021      INT    21
00401778: B468      MOU    BH,68
00401779: C021      INT    21
0040177A: B469      MOU    BH,69
0040177B: C021      INT    21
0040177C: B46A      MOU    BH,6A
0040177D: C021      INT    21
0040177E: B46B      MOU    BH,6B
0040177F: C021      INT    21
00401780: B46C      MOU    BH,6C
00401781: C021      INT    21
00401782: B46D      MOU    BH,6D
00401783: C021      INT    21
00401784: B46E      MOU    BH,6E
00401785: C021      INT    21
00401786: B46F      MOU    BH,6F
00401787: C021      INT    21
00401788: B470      MOU    BH,70
00401789: C021      INT    21
0040178A: B471      MOU    BH,71
0040178B: C021      INT    21
0040178C: B472      MOU    BH,72
0040178D: C021      INT    21
0040178E: B473      MOU    BH,73
0040178F: C021      INT    21
00401790: B474      MOU    BH,74
00401791: C021      INT    21
00401792: B475      MOU    BH,75
00401793: C021      INT    21
00401794: B476      MOU    BH,76
00401795: C021      INT    21
00401796: B477      MOU    BH,77
00401797: C021      INT    21
00401798: B478      MOU    BH,78
00401799: C021      INT    21
0040179A: B479      MOU    BH,79
0040179B: C021      INT    21
0040179C: B47A      MOU    BH,7A
0040179D: C021      INT    21
0040179E: B47B      MOU    BH,7B
0040179F: C021      INT    21
004017A0: B47C      MOU    BH,7C
004017A1: C021      INT    21
004017A2: B47D      MOU    BH,7D
004017A3: C021      INT    21
004017A4: B47E      MOU    BH,7E
004017A5: C021      INT    21
004017A6: B47F      MOU    BH,7F
004017A7: C021      INT    21
004017A8: B480      MOU    BH,80
004017A9: C021      INT    21
004017AA: B481      MOU    BH,81
004017AB: C021      INT    21
004017AC: B482      MOU    BH,82
004017AD: C021      INT    21
004017AE: B483      MOU    BH,83
004017AF: C021      INT    21
004017B0: B484      MOU    BH,84
004017B1: C021      INT    21
004017B2: B485      MOU    BH,85
004017B3: C021      INT    21
004017B4: B486      MOU    BH,86
004017B5: C021      INT    21
004017B6: B487      MOU    BH,87
004017B7: C021      INT    21
004017B8: B488      MOU    BH,88
004017B9: C021      INT    21
004017BA: B489      MOU    BH,89
004017BB: C021      INT    21
004017BC: B48A      MOU    BH,8A
004017BD: C021      INT    21
004017BE: B48B      MOU    BH,8B
004017BF: C021      INT    21
004017C0: B48C      MOU    BH,8C
004017C1: C021      INT    21
004017C2: B48D      MOU    BH,8D
004017C3: C021      INT    21
004017C4: B48E      MOU    BH,8E
004017C5: C021      INT    21
004017C6: B48F      MOU    BH,8F
004017C7: C021      INT    21
004017C8: B490      MOU    BH,90
004017C9: C021      INT    21
004017CA: B491      MOU    BH,91
004017CB: C021      INT    21
004017CC: B492      MOU    BH,92
004017CD: C021      INT    21
004017CE: B493      MOU    BH,93
004017CF: C021      INT    21
004017D0: B494      MOU    BH,94
004017D1: C021      INT    21
004017D2: B495      MOU    BH,95
004017D3: C021      INT    21
004017D4: B496      MOU    BH,96
004017D5: C021      INT    21
004017D6: B497      MOU    BH,97
004017D7: C021      INT    21
004017D8: B498      MOU    BH,98
004017D9: C021      INT    21
004017DA: B499      MOU    BH,99
004017DB: C021      INT    21
004017DC: B49A      MOU    BH,9A
004017DD: C021      INT    21
004017DE: B49B      MOU    BH,9B
004017DF: C021      INT    21
004017E0: B49C      MOU    BH,9C
004017E1: C021      INT    21
004017E2: B49D      MOU    BH,9D
004017E3: C021      INT    21
004017E4: B49E      MOU    BH,9E
004017E5: C021      INT    21
004017E6: B49F      MOU    BH,9F
004017E7: C021      INT    21
004017E8: B4A0      MOU    BH,A0
004017E9: C021      INT    21
004017EA: B4A1      MOU    BH,A1
004017EB: C021      INT    21
004017EC: B4A2      MOU    BH,A2
004017ED: C021      INT    21
004017EE: B4A3      MOU    BH,A3
004017EF: C021      INT    21
004017F0: B4A4      MOU    BH,A4
004017F1: C021      INT    21
004017F2: B4A5      MOU    BH,A5
004017F3: C021      INT    21
004017F4: B4A6      MOU    BH,A6
004017F5: C021      INT    21
004017F6: B4A7      MOU    BH,A7
004017F7: C021      INT    21
004017F8: B4A8      MOU    BH,A8
004017F9: C021      INT    21
004017FA: B4A9      MOU    BH,A9
004017FB: C021      INT    21
004017FC: B4AA      MOU    BH,A0
004017FD: C021      INT    21
004017FE: B4AB      MOU    BH,A1
004017FF: C021      INT    21
004017C0: B490      MOU    BH,90
004017C1: C021      INT    21
004017C2: B491      MOU    BH,91
004017C3: C021      INT    21
004017C4: B492      MOU    BH,92
004017C5: C021      INT    21
004017C6: B493      MOU    BH,93
004017C7: C021      INT    21
004017C8: B494      MOU    BH,94
004017C9: C021      INT    21
004017CA: B495      MOU    BH,95
004017CB: C021      INT    21
004017CC: B496      MOU    BH,96
004017CD: C021      INT    21
004017CE: B497      MOU    BH,97
004017CF: C021      INT    21
004017D0: B498      MOU    BH,98
004017D1: C021      INT    21
004017D2: B499      MOU    BH,99
004017D3: C021      INT    21
004017D4: B49A      MOU    BH,9A
004017D5: C021      INT    21
004017D6: B49B      MOU    BH,9B
004017D7: C021      INT    21
004017D8: B49C      MOU    BH,9C
004017D9: C021      INT    21
004017D0: B49D      MOU    BH,9D
004017D1: C021      INT    21
004017D2: B49E      MOU    BH,9E
004017D3: C021      INT    21
004017D4: B49F      MOU    BH,9F
004017D5: C021      INT    21
004017D6: B4A0      MOU    BH,A0
004017D7: C021      INT    21
004017D8: B4A1      MOU    BH,A1
004017D9: C021      INT    21
004017D0: B4A2      MOU    BH,A2
004017D1: C021      INT    21
004017D2: B4A3      MOU    BH,A3
004017D3: C021      INT    21
004017D4: B4A4      MOU    BH,A4
004017D5: C021      INT    21
004017D6: B4A5      MOU    BH,A5
004017D7: C021      INT    21
004017D8: B4A6      MOU    BH,A6
004017D9: C021      INT    21
004017D0: B4A7      MOU    BH,A7
004017D1: C021      INT    21
004017D2: B4A8      MOU    BH,A8
004017D3: C021      INT    21
004017D4: B4A9      MOU    BH,A9
004017D5: C021      INT    21
004017D6: B4AA      MOU    BH,A0
004017D7: C021      INT    21
004017D8: B4AB      MOU    BH,A1
004017D9: C021      INT    21
004017D0: B490      MOU    BH,90
004017D1: C021      INT    21
004017D2: B491      MOU    BH,91
004017D3: C021      INT    21
004017D4: B492      MOU    BH,92
004017D5: C021      INT    21
004017D6: B493      MOU    BH,93
004017D7: C021      INT    21
004017D8: B494      MOU    BH,94
004017D9: C021      INT    21
004017D0: B495      MOU    BH,95
004017D1: C021      INT    21
004017D2: B496      MOU    BH,96
004017D3: C021      INT    21
004017D4: B497      MOU    BH,97
004017D5: C021      INT    21
004017D6: B498      MOU    BH,98
004017D7: C021      INT    21
004017D8: B499      MOU    BH,99
004017D9: C021      INT    21
004017D0: B49A      MOU    BH,9A
004017D1: C021      INT    21
004017D2: B49B      MOU    BH,9B
004017D3: C021      INT    21
004017D4: B49C      MOU    BH,9C
004017D5: C021      INT    21
004017D6: B49D      MOU    BH,9D
004017D7: C021      INT    21
004017D8: B49E      MOU    BH,9E
004017D9: C021      INT    21
004017D0: B49F      MOU    BH,9F
004017D1: C021      INT    21
004017D2: B4A0      MOU    BH,A0
004017D3: C021      INT    21
004017D4: B4A1      MOU    BH,A1
004017D5: C021      INT    21
004017D6: B4A2      MOU    BH,A2
004017D7: C021      INT    21
004017D8: B4A3      MOU    BH,A3
004017D9: C021      INT    21
004017D0: B4A4      MOU    BH,A4
004017D1: C021      INT    21
004017D2: B4A5      MOU    BH,A5
004017D3: C021      INT    21
004017D4: B4A6      MOU    BH,A6
004017D5: C021      INT    21
004017D6: B4A7      MOU    BH,A7
004017D7: C021      INT    21
004017D8: B4A8      MOU    BH,A8
004017D9: C021      INT    21
004017D0: B4A9      MOU    BH,A9
004017D1: C021      INT    21
004017D2: B4AA      MOU    BH,A0
004017D3: C021      INT    21
004017D4: B4AB      MOU    BH,A1
004017D5: C021      INT    21
004017D6: B490      MOU    BH,90
004017D7: C021      INT    21
004017D8: B491      MOU    BH,91
004017D9: C021      INT    21
004017D0: B492      MOU    BH,92
004017D1: C021      INT    21
004017D2: B493      MOU    BH,93
004017D3: C021      INT    21
004017D4: B494      MOU    BH,94
004017D5: C021      INT    21
004017D6: B495      MOU    BH,95
004017D7: C021      INT    21
004017D8: B496      MOU    BH,96
004017D9: C021      INT    21
004017D0: B497      MOU    BH,97
004017D1: C021      INT    21
004017D2: B498      MOU    BH,98
004017D3: C021      INT    21
004017D4: B499      MOU    BH,99
004017D5: C021      INT    21
004017D6: B49A      MOU    BH,9A
004017D7: C021      INT    21
004017D8: B49B      MOU    BH,9B
004017D9: C021      INT    21
004017D0: B49C      MOU    BH,9C
004017D1: C021      INT    21
004017D2: B49D      MOU    BH,9D
004017D3: C021      INT    21
004017D4: B49E      MOU    BH,9E
004017D5: C021      INT    21
004017D6: B49F      MOU    BH,9F
004017D7: C021      INT    21
004017D8: B4A0      MOU    BH,A0
004017D9: C021      INT    21
004017D0: B4A1      MOU    BH,A1
004017D1: C021      INT    21
004017D2: B4A2      MOU    BH,A2
004017D3: C021      INT    21
004017D4: B4A3      MOU    BH,A3
004017D5: C021      INT    21
004017D6: B4A4      MOU    BH,A4
004017D7: C021      INT    21
004017D8: B4A5      MOU    BH,A5
004017D9: C021      INT    21
004017D0: B4A6      MOU    BH,A6
004017D1: C021      INT    21
004017D2: B4A7      MOU    BH,A7
004017D3: C021      INT    21
004017D4: B4A8      MOU    BH,A8
004017D5: C021      INT    21
004017D6: B4A9      MOU    BH,A9
004017D7: C021      INT    21
004017D8: B4AA      MOU    BH,A0
004017D9: C021      INT    21
004017D0: B4AB      MOU    BH,A1
004017D1: C021      INT    21
004017D2: B490      MOU    BH,90
004017D3: C021      INT    21
004017D4: B491      MOU    BH,91
004017D5: C021      INT    21
004017D6: B492      MOU    BH,92
004017D7: C021      INT    21
004017D8: B493      MOU    BH,93
004017D9: C021      INT    21
004017D0: B494      MOU    BH,94
004017D1: C021      INT    21
004017D2: B495      MOU    BH,95
004017D3: C021      INT    21
004017D4: B496      MOU    BH,96
004017D5: C021      INT    21
004017D6: B497      MOU    BH,97
004017D7: C021      INT    21
004017D8: B498      MOU    BH,98
004017D9: C021      INT    21
004017D0: B499      MOU    BH,99
004017D1: C021      INT    21
004017D2: B49A      MOU    BH,9A
004017D3: C021      INT    21
004017D4: B49B      MOU    BH,9B
004017D5: C021      INT    21
004017D6: B49C      MOU    BH,9C
004017D7: C021      INT    21
004017D8: B49D      MOU    BH,9D
004017D9: C021      INT    21
004017D0: B49E      MOU    BH,9E
004017D1: C021      INT    21
004017D2: B49F      MOU    BH,9F
004017D3: C021      INT    21
004017D4: B4A0      MOU    BH,A0
004017D5: C021      INT    21
004017D6: B4A1      MOU    BH,A1
004017D7: C021      INT    21
004017D8: B4A2      MOU    BH,A2
004017D9: C021      INT    21
004017D0: B4A3      MOU    BH,A3
004017D1: C021      INT    21
004017D2: B4A4      MOU    BH,A4
004017D3: C021      INT    21
004017D4: B4A5      MOU    BH,A5
004017D5: C021      INT    21
004017D6: B4A6      MOU    BH,A6
004017D7: C021      INT    21
004017D8: B4A7      MOU    BH,A7
004017D9: C021      INT    21
004017D0: B4A8      MOU    BH,A8
004017D1: C021      INT    21
004017D2: B4A9      MOU    BH,A9
004017D3: C021      INT    21
004017D4: B4AA      MOU    BH,A0
004017D5: C021      INT    21
004017D6: B4AB      MOU    BH,A1
004017D7: C021      INT    21
004017D8: B490      MOU    BH,90
004017D9: C021      INT    21
004017D0: B491      MOU    BH,91
004017D1: C021      INT    21
004017D2: B492      MOU    BH,92
004017D3: C021      INT    21
004017D4: B493      MOU    BH,93
004017D5: C021      INT    21
004017D6: B494      MOU    BH,94
004017D7: C021      INT    21
004017D8: B495      MOU    BH,95
004017D9: C021      INT    21
004017D0: B496      MOU    BH,96
004017D1: C021      INT    21
004017D2: B497      MOU    BH,97
004017D3: C021      INT    21
004017D4: B498      MOU    BH,98
004017D5: C021      INT    21
004017D6: B499      MOU    BH,99
004017D7: C021      INT    21
004017D8: B4A0      MOU    BH,A0
004017D9: C021      INT    21
004017D0: B4A1      MOU    BH,A1
004017D1: C021      INT    21
004017D2: B4A2      MOU    BH,A2
004017D3: C021      INT    21
004017D4: B4A3      MOU    BH,A3
004017D5: C021      INT    21
004017D6: B4A4      MOU    BH,A4
004017D7: C021      INT    21
004017D8: B4A5      MOU    BH,A5
004017D9: C021      INT    21
004017D0: B4A6      MOU    BH,A6
004017D1: C021      INT    21
004017D2: B4A7      MOU    BH,A7
004017D3: C021      INT    21
004017D4: B4A8      MOU    BH,A8
004017D5: C021      INT    21
004017D6: B4A9      MOU    BH,A9
004017D7: C021      INT    21
004017D8: B4AA      MOU    BH,A0
004017D9: C021      INT    21
004017D0: B4AB      MOU    BH,A1
004017D1: C021      INT    21
004017D2: B490      MOU    BH,90
004017D3: C021      INT    21
004017D4: B491      MOU    BH,91
004017D5: C021      INT    21
004017D6: B492      MOU    BH,92
004017D7: C021      INT    21
004017D8: B493      MOU    BH,93
004017D9: C021      INT    21
004017D0: B494      MOU    BH,94
004017D1: C021      INT    21
004017D2: B495      MOU    BH,95
004017D3: C021      INT    21
004017D4: B496      MOU    BH,96
004017D5: C021      INT    21
004017D6: B497      MOU    BH,97
004017D7: C021      INT    21
004017D8: B498      MOU    BH,98
004017D9: C021      INT    21
004017D0: B499      MOU    BH,99
004017D1: C021      INT    21
004017D2: B49A      MOU    BH,9A
004017D3: C021      INT    21
004017D4: B49B      MOU    BH,9B
004017D5: C021      INT    21
004017D6: B49C      MOU    BH,9C
004017D7: C021      INT    21
004017D8: B49D      MOU    BH,9D
004017D9: C021      INT    21
004017D0: B49E      MOU    BH,9E
004017D1: C021      INT    21
004017D2: B49F      MOU    BH,9F
004017D3: C021      INT    21
004017D4: B4A0      MOU    BH,A0
004017D5: C021      INT    21
004017D6: B4A1      MOU    BH,A1
004017D7: C021      INT    21
004017D8: B4A2      MOU    BH,A2
004017D9: C021      INT    21
004017D0: B4A3      MOU    BH,A3
004017D1: C021      INT    21
004017D2: B4A4      MOU    BH,A
```

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. 按传播方式可分为：

(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：

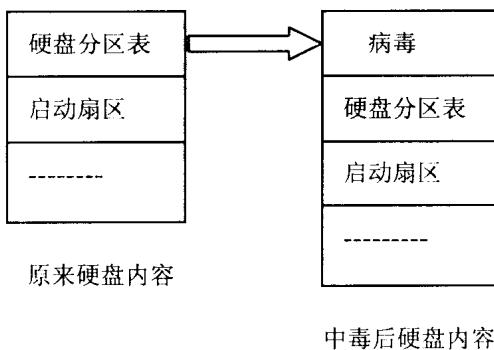


图 1.3 引导扇区病毒原理

(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