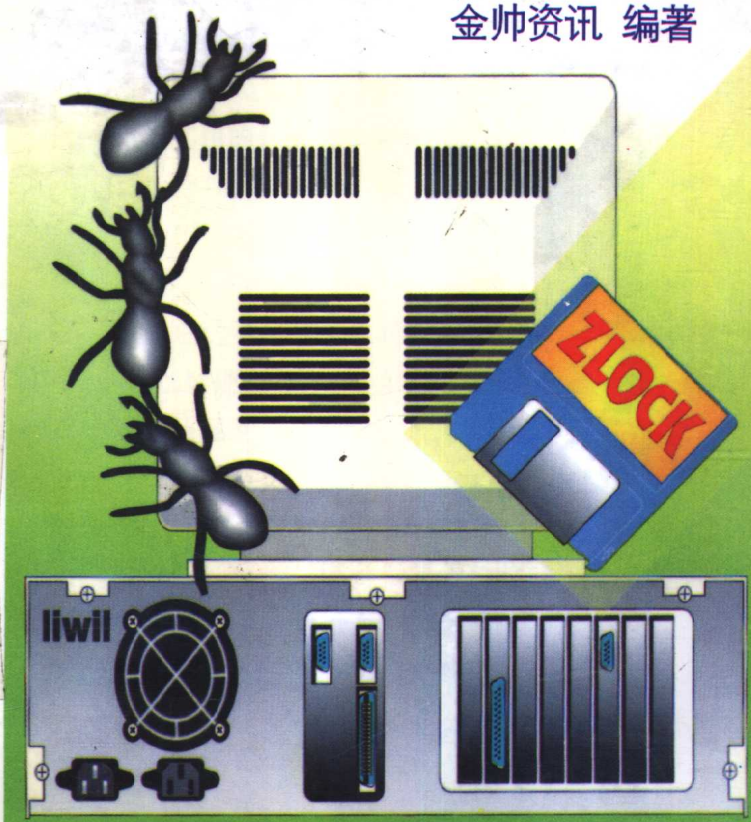
电脑随身系列

病毒急救站

金帅资讯 编著

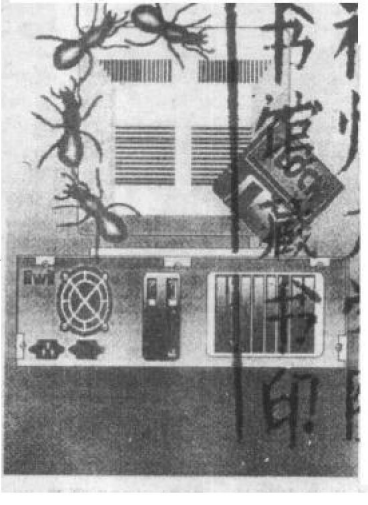


吉林科学技术出版社

电脑 身系列

病毒急救站

金帅资讯　编著



吉林科学技术出版社
台湾立威出版股份有限公司

【吉】新登字 03 号

电脑随身系列
病毒急救站

金帅资讯 编著

责任编辑：赵玉秋 王玉峰　　封面设计：汤士伦

出版　吉林科学技术出版社　787×1092 毫米 32 开本　6.25 印张
　　台湾立威出版股份有限公司　108，000 字
　　1996 年 3 月第 1 版　1996 年 3 月第 1 次印刷
发行　吉林科学技术出版社　印数：1—10000 册　定价：含软盘 20.00 元
印刷　辽宁金城印刷厂　ISBN 7-5384-1615-3/TP·44

序

电脑病毒-电脑发明之后的破坏性副产物，DOS系统下的病毒虽然层出不穷，Windows下的病毒也陆续出笼，伴随互连网络、BBS的快速发展，更直接的带动病毒传播的速度及区域，病毒的种类也愈来愈复杂、刁钻。所以，只要您有使用电脑，对于电脑病毒最好就要有基本的认识。

本公司提供多年的防毒经验，为您从电脑病毒的起源谈起，循序渐进的帮您建立起对于病毒的基本概念。有了这些了解，再告诉大家如何预防病毒的感染；最后，则是使用本书所附的GSAFE扫毒、BVK解毒程序，让您的电脑有初步的防御能力，在遇到病毒时，也可以有个解毒实战的经验。

本书对于近期的Windows病毒另有专章详细剖析，您千万不要错过了！

《病毒急救站》一书的诞生，金帅BBS总站长薛宇智先生孜孜不倦的撰稿是一定要感谢的，立威出版社对于本书的插图以及编排也是颇多费心，最重要的是，我们都有一块“努力防毒的心”，同时希望，读者您也能从本书中获益，这将是我们最大的喜悦。

金帅资讯科技有限公司

1995年11月

商标声明

BVK版权为金帅资讯科技有限公司所有

GSAFE版权为金帅资讯科技有限公司所有

ZLOCK版权为金帅资讯科技有限公司所有

MS-DOS版权为**Microsoft Corp.**所有

Microsoft Word版权为**Microsoft Corp.**所有

windows 3.1版权为**Microsoft Corp.**所有

Windows 95版权为**Microsoft Corp.**所有

其余所提到之产品、软件版权均隶属于各该公司所有

目录

1

何谓电脑病毒

本章内容

自从“电脑病毒”这个名词问世以来，就一直是信息界的内忧，它的肆虐与破坏不绝于耳，常造成电脑使用者的不安与厌恶……所以在这信息爆炸的时代，如何有效防毒，实是您不得不重视的事情。而防毒的最基本条件，就是要先了解何谓电脑病毒。

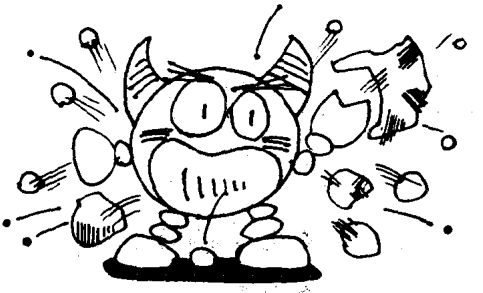
读完本章后，您将会知道：

- ◆ 电脑病毒的起源
- ◆ 何谓电脑病毒
- ◆ 电脑病毒的分类
- ◆ 电脑病毒的剖析

1-1 电脑病毒的起源

(C)BRAIN原本是巴基斯坦的两位兄弟，为了保护自己创作的软件，而写的一段保护程序。它会把磁盘的标名(VOLUME LABLE)改为“(C)BRAIN”，以防别人的盗拷，除此之外，它并不具任何破坏性。

但类似这种技术的发展，有越来越多的人使用，而其目的也和防拷相形渐远，这就是现在人人闻之色变的电脑病毒。



开机型病毒开山祖师(C)BRAIN

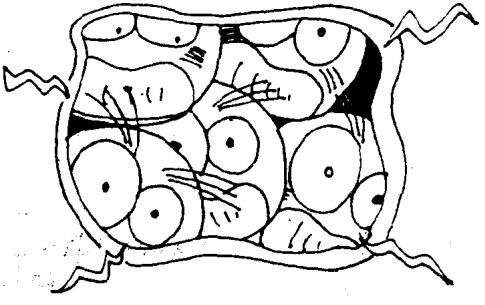
1-2 何谓电脑病毒

电脑病毒就是利用一段小程序，通过一个简单的原则，使自己能不断的散播到各个有电脑的地方，进而造成电脑的操作失灵、系统故障、甚至破坏电脑磁盘中的资料。

而上述所提到的简单原则，则可以分为下列三种：

1. 不断复制自己，造成系统超载。

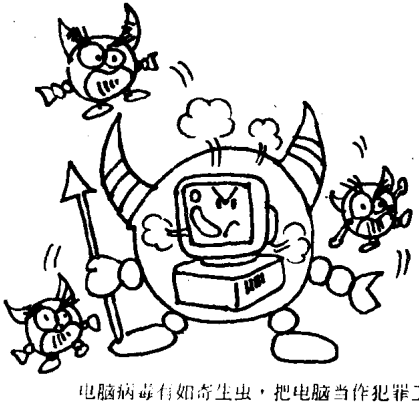
如：美国研究生MORRIS在网络上执行一个不断复制自己的小程序，造成网络上的超载死机。



电脑病毒有如再生虫要把电脑网络挤爆了。

2. 将自己复制并附在正常程序中。

如：NATAS会将自己复制在别的正常程序中或磁盘的启动程序，自己可不断的散播。



电脑病毒有如寄生虫，把电脑当作犯罪工具。

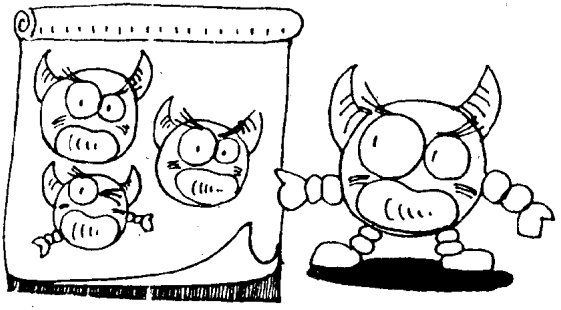
3. 具备某种功能，借以在使用者使用时，发生破坏式干扰的动作。

如：美国情报局在与伊拉克战争中，将干扰飞弹发射的程序植入打印机的芯片中，当打印机被打开时，电脑就失去了控制飞弹的能力。

电脑病毒真是无孔不入，就连飞弹都没辄。

1-3 电脑病毒分类与剖析

日益增加的病毒种类繁多，其技术更是变化多端令人无法捉摸，要以何种方式来防范各种不同类型的病毒，实在是一门高深的学问。在谈防治病毒之前，要先了解时下病毒的特性及其感染的方式，方能对症下药。



各种电脑病毒的分门别类。

◆ 传统开机型病毒

纯粹的开机型病毒多利用软盘开机时侵入电脑系统，然后再伺机感染其他的软盘或硬盘，例如：DISK KILLER、STONED 3（米开朗基罗）、HARD ELEVEN。

三月六日开机时中**stoned 3**的**pc**硬盘会被**format**，屏幕无动作，但硬盘的灯一直在亮。

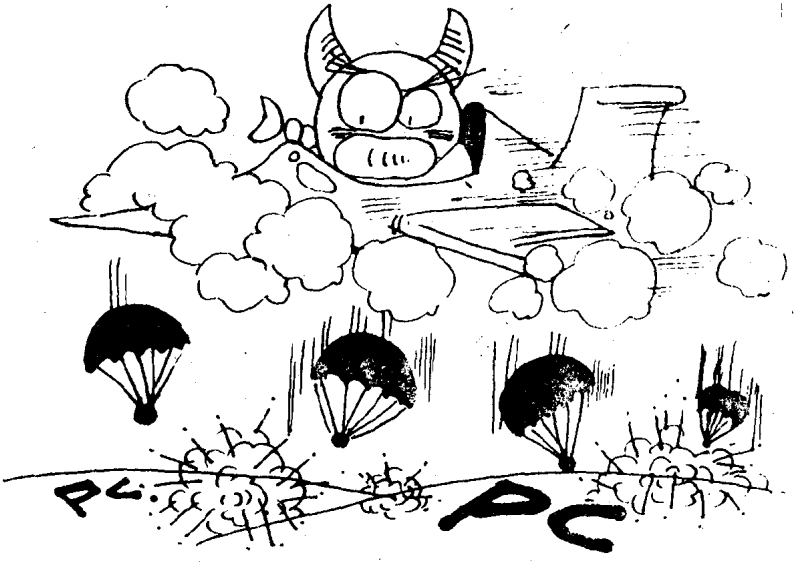
目前市面上大多数的防毒、扫毒程序均可预防此类病毒，一般USER对于此类病毒最好的预防方式，即是避免使用外来磁盘开机。

以1990年以后出品的AMI BIOS而言，就已经提供了设定由硬盘开机的功能，足可令USER避开此类病毒的侵扰。使用者于电脑开机时，按**Del**或**Esc**键即进入BIOS的设定，其中选择ADVANCED BIOS SETUP将光标移至SYSTEM BOOT UP SEQUENCE选项，设定<C: A:>，即完成了由硬盘开机的设定。

◆ 隐形开机型病毒

凡是被“隐形”开机型病毒感染的系统，当您检查Partition Table 及BOOT Sector时，病毒会将正常的扇区资料还原，就好象没有中毒一般，此型病毒较不易为一般扫毒软件所查觉，而防毒软件对于未知的此型病毒，必须具有辨认扇区资料真伪的能力。

此类病毒已出现的有FISH、NOVEMBER 4、MONKEY、GOLDEN CICADA。

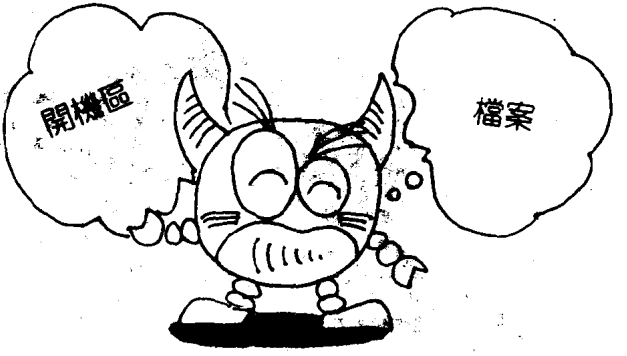


隐形病毒轰炸机，正对陆上的PC进行轰炸(感染)。

◆ 文件感染型兼开机型病毒

尽管防毒观念中强调，避免使用外来的软盘开机，但是仍仅能预防上述两种开机型病毒，文件感染型兼开机型病毒则是利用文件感染时伺机感染开机区，因而具有双重的行动能力。

此型较著名的病毒有CANCER、HAMMER V、MACGYVER 2.0、NATAS，目前市面上的防毒扫毒软件多能检测出此类病毒。



具备双重身份的电脑病毒，正沾沾自喜。