从零开始学电脑

接祖华 编著

病毒防范

海洋出版社

从零开始学电脑

病毒防范

接祖华　编著

海洋出版社

图书在版编目(CIP)数据

病毒防范 / 接祖华编著. — 北京:海洋出版社, 2003.6
(从"零"开始学电脑)
ISBN 7-5027-5738-4

Ⅰ.病… Ⅱ.接… Ⅲ.计算机病毒—防治—基本知识 Ⅳ.TP309.5

中国版本图书馆 CIP 数据核字(2003)第 000314 号

策划编辑:申果元
责任编辑:杨海萍
责任印制:刘志恒

从零开始学电脑
病毒防范

海洋出版社 出版发行
http://www.oceanpress.com.cn
(邮编:100081 北京市海淀区大慧寺路 8 号)
北京市美通印刷有限公司印刷 新华书店经销
2003 年 6 月第 1 版 2003 年 6 月北京第一次印刷
开本:850mm×1168mm 1/32 印张:45
字数:100 千字 印数:6500 册
定价:150.00 元(全套 15 册)

目　次

人们通过电脑处理文稿、图片和收发 E-mail 进行信息交流；程序员们利用电脑编制各种各样的应用软件等等。电脑的应用使社会空前的进步和发展，但是电脑病毒也给社会带来了巨大的麻烦和破坏。电脑一旦遇到破坏性的病毒，不但使多日苦熬制作的数据毁于一旦，而且还会导致电脑硬件的损坏。

那么，到底什么是电脑病毒？它的传播途径有哪些？如何判断电脑是否感染病毒？什么是杀毒软件？有哪几种常用杀毒软件？如何利用杀毒软件保护系统和查杀病毒？这都是本书要告诉你的。

简述病毒

一. 什么电脑病毒？

电脑病毒不是活的细菌，而是由某些程序员设计的专门用来破坏电脑数据的程序。这种程序具有再生能力，它会自动地通过修改他人的程序，偷偷地把自己嵌入其中，或者隐藏到他人电脑的存储器中，从而“感染”程序。当满足一定条件时，该程序就会干扰电脑正常工作，搞乱或破坏已存储信息，甚至导致整个电脑系统瘫痪。

二. 电脑病毒传染的途径

病毒侵入有许多途径，最常见的是使用了被“感染”病毒的程序文件软盘。这些病毒可能是你从朋友那里拷贝文件得到的，也许是从因特网上下载的，或者是接收到的电子邮件中含有的病毒等等。

三. 如何判断您的电脑已经感染了病毒

电脑一旦感染病毒，会出现一些异常的现象。通过对这些异常现象分析，就可以初步判断电脑是否感染了病毒。这些异常现象通常表现为以下几种方式。

1. 电脑突然无法启动

这时，除了硬盘发生故障外，感染病毒的可能性极大。

2. 系统的运行速度明显下降

如果电脑系统的运行速度突然减慢，也是一种较为明显的感染病毒的症状。

3. 打开文件时的速度比以前慢

如果发觉打开文件的时间越来越长，除了内存容量不够大、硬盘数据碎块太多没有整理以外，极有可能是因为电脑“中毒”了。

4. 电脑经常死机

电脑经常死机或程序运行时出现错误信息，甚至运行到一半就死机。这表明文件已经损坏，也可能是病毒所引起的，因为某些病毒会覆盖文件的数据，所以会造成文件损坏。

5. 文件夹被莫名其妙地删除

文件突然莫名其妙地就从硬盘里消失了，如果不是自己误删，那就有可能是病毒引起的。

6. 电脑显示异常

当电脑显示异常时，则有可能是病毒发作的症状。例如

- 电脑屏幕异常滚动，而与显示器的质量无关；
- 电脑屏幕上出现异常信息显示；
- 电脑屏幕上的英文字符出现滑落；

☞电脑屏幕上显示的汉字不全；

☞电脑自己突然演奏音乐等等。

四. 防止电脑感染病毒的方法

防止电脑病毒的感染，除了靠杀毒软件，更要靠养成良好的工作习惯，来预防电脑病毒。

☞使用正版软件。目前市场上的盗版软件猖獗，不法盗版者有意、无意之间成为电脑病毒的主要传播者。拒绝使用盗版软件，可以减少感染病毒的机会。

☞制作一张干净的启动盘，而且不要随便使用来历不明的启动盘。

☞不要打开来路不明的文件。

☞不要随便打开电子邮件的附加文件。因特网的日益发展壮大，电脑病毒自然也不甘寂寞，利用电子邮件的附加文件传染病毒，给人们带来了巨大灾难。

☞从网上下载的文件，必须先用杀毒软件检查。

KV3000 杀毒王

KV3000 杀毒王是北京江民新科技术有限公司最新推出的一套优秀的国产计算机杀毒软件。它在原 KV3000 版基础上新增了邮件监视和清除功能。可以实时监控传送邮件中发现的病毒、黑客程序文件等，它能防杀 DOS、Windows、宏、网络蠕虫、黑客有害程序、网络炸弹、恶性 CIH 等病毒。

- 在线式“实时监测”病毒，可时时刻刻查杀外来软盘、光盘和因特网的病毒。
- 可以查杀隐藏在 ZIP、ARJ、RAR、CAB、LZH 等多种压缩文件和电子邮件中的病毒，它还提供了更加完善的硬盘救护箱、清除病毒向导、自动定时扫描、详细的病毒检查报告等功能。

一. 安装 KV3000 杀毒王

首先，将 KV3000 杀毒王的光盘放在光驱中，KV3000 杀毒王会自动运行，出现安装界面（见图 1-1）；

图 1-1

提示单击“下一步”，就可以将 KV3000 杀毒王安装在默认的 C：KVW3000 目录下；

最后根据提示信息重新启动计算机，有关详细安装 KV3000 杀毒王的方法见购买说明书，这里不再赘述。

二. KV3000 杀毒王使用步骤

1. 运行

安装成功后，在计算机的桌面上显示的是 KV3000 杀毒王的图标（见图 1-2），直接双击该图标；

图 1-2

接着出现的 KV3000 杀毒王的主界面（见图 1-3），在这个界面下用户可以完成病毒的查、杀、实时监视、恶意网页的实时监视、注册表被恶意修改的恢复、智能升级、邮件病毒的查、杀、实时监视等功能。除了实时监视外，在查杀病毒时用户必须先选择目标，然后才能对其查杀。

2. 主界面的使用

首先要在主界面上选择查杀的目标，在“查杀目标”下的“我的电脑”下可以选择要查杀的驱动器、盘符、目录或者直接选择单个的文件夹来查杀（见图 1-4）。可以在这里控制实时监视的各种功能的开启或者关闭，可以查看查杀病毒引擎的版本以及使用的病毒库的日期等信息。

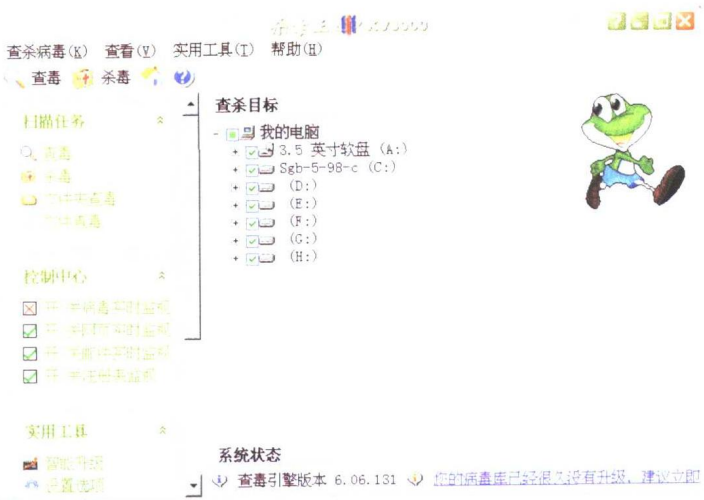

查杀病毒(K) 查看(V) 实用工具(T) 帮助(H)
查毒 杀毒
扫描任务
控制中心
实用工具
查杀目标
我的电脑
3.5 英寸软盘 (A:)
Sgb-5-98-c (C:)
(D:)
(E:)
(F:)
(G:)
(H:)
系统状态
查毒引擎版本 6.06.131
欢迎使用杀毒王

图 1-3

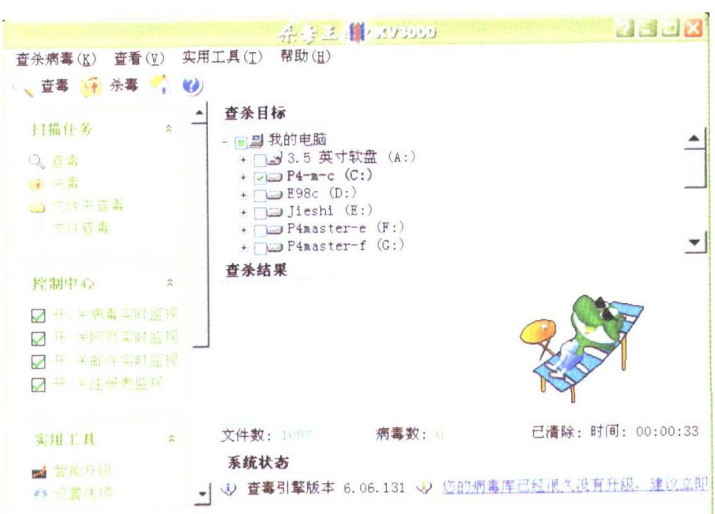

查杀病毒(K) 查看(V) 实用工具(T) 帮助(H)
查毒 杀毒
扫描任务
控制中心
实用工具
查杀目标
我的电脑
3.5 英寸软盘 (A:)
P4-m-c (C:)
E98c (D:)
Jieshi (E:)
P4master-e (F:)
P4master-f (G:)
查杀结果
已清除：时间：00:00:33
系统状态
查毒引擎版本 6.06.131

图 1-4

3. 检查病毒

当在“查杀目标”下选择目标后，点“查毒”按钮会出现查病毒窗口（见图 1-5）。

图 1-5

可以使用三种方式来执行查病毒操作。典型的查病毒窗口中可以看出检查的文件数，检查出的病毒数量以及所用的时间。在窗口的最下面显示的是正在扫描的文件。检查病毒的过程可以点击“暂停”或者“停止”按钮，暂停或停止检查病毒的工作。在“查杀结果”下显示的是发现病毒的信息包括发现病毒的文件、路径、病毒名称等。检查病毒可以检查出普通文件和信箱中的病毒、网络蠕虫等。

4. 杀病毒

杀病毒和查病毒一样，必须先选择要杀病毒的目标，然后再杀，同时杀病毒也可以使用三种途径来执行。杀病毒的过程也可以暂停

或者终止，其他的显示信息和查病毒一样（见图 1-6）。

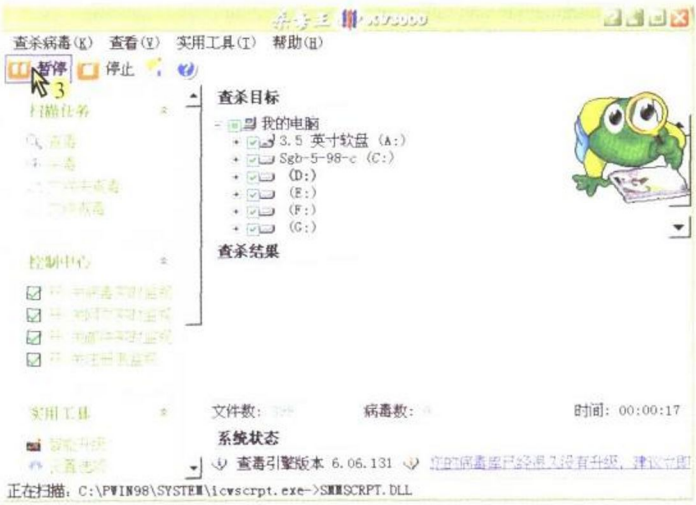


图 1-6

所不同的是杀完病毒后，病毒隔离系统会自动接管被杀病毒的备份信息，通过使用病毒隔离系统可以恢复或者彻底删除感染病毒的文件。这里的杀病毒还可以直接杀掉在各种信箱中的网络蠕虫或者病毒等，这是 KV3000 杀毒王新增强的功能。

5. 实时监视病毒

☞病毒实时监视

可以通过单击控制中心的“开/关病毒实时监视”来控制病毒实时监视功能的开启与关闭。状态的显示是使用对号和叉号来表示的（见图 1-7）。

图 1-7

☞网页实时监视

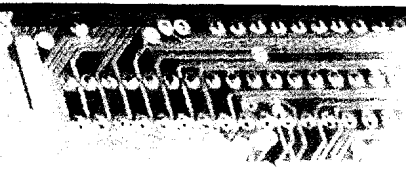
网页实时监视功能的开启和关闭是通过单击控制中心下的“开/关网页实时监视”来实现。

☞邮件实时监视

邮件实时监视信息可以通过控制中心的“开/关邮件实时监视”来实现该功能的开启与关闭。当在收邮件遇到病毒时，KV3000 杀毒王的邮件监视会自动报警，并提示用户可以删除或者清除病毒。当然被清除的病毒是由病毒隔离系统备份的。用户可以通过病毒隔离系统来实现邮件的恢复或者彻底删除。

☞注册表实时监视

注册表实时监视同样可以通过控制中心的“开/关注册表监视”来实现该功能的开启与关闭。当 KV3000 杀毒王监测到注册表关键区域被修改后，会立即报警提示用户注册表修改的地方，只有在用



户确认该修改是允许的情况下，该注册表项才能被修改。该注册表监视功能可以防止很多的黑客程序对系统注册表的修改、自动运行等。

- 智能升级

为了保持 KV3000 杀毒王的查杀实时监视病毒的功能，必须及时升级查杀病毒的功能。建议用户上网使用智能升级功能来实现版本和文件的更新。当然，用户可以选择多种的升级方式，除了直接上江民公司的网站升级外，还可以通过局域网络、FTP 等方式来升级，详细的设置方法，用户可查看“实用工具”中的“设置选项”下的“升级”。

- 设置选项

在“实用工具”的“设置选项”下有“KV3000 防毒设置”显示框，一共有 7 个设置选项。更详细的其他功能选项可以选择相应的功能项目来处理，完整的功能项目包括扫描目标、处理方法、扫描选项、处理结果、在线监控、升级、IE 安全等 7 项。

- 病毒隔离

病毒隔离系统记录了所有 KV3000 杀毒王杀过了的病毒的原始信息，包括杀毒名称、发现该病毒的原始文件路径信息等。用户通过病毒隔离系统可以十分方便地恢复原始的清除病毒前的文件。需要注意的是如果显示的要恢复到的目标是 Windows 的临时目录的话，该文件可能就是在信箱中发现的病毒的原始信息，是查杀邮件病毒的备份，实际的文件格式是 E-mall 格式。

- 引导区备份

通过该功能用户可以十分方便地备份或者恢复系统的主引导区和引导区（见图 1-8）。建议用户将这些系统的关键区域备份在软盘上并妥善保存。请注意恢复系统区域的操作是非常危险的，请确认

你的操作，并尽可能在有经验的人员指导下进行。更详细的信息可以参看 KV3000 杀毒王的说明文件。

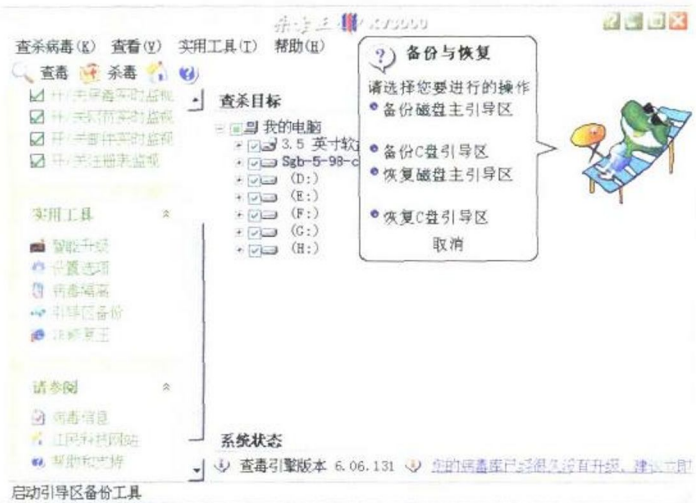


图 1-8

☞ IE 修复王

本功能可以恢复被恶意网页修改的各种 IE 设置和一些基本的 Windows 桌面、窗口、运行功能等，对于一些被恶意网页侵害的系统非常实用。

图 1-9

四. KV3000 杀毒王查杀病毒实例

1. 查杀“CMOS 设置破坏者”病毒

“CMOS 设置破坏者”(CMOS Destroyer) 是一种引导区病毒。它主要感染硬盘主引导区和软盘 BOOT 区。并且，它不论在 DOS、WINDOWS、WINDOWS NT、UNIX 等操作系统中，统统都可以感染硬盘的引导区！因为它的传染方式是专门覆盖计算机硬盘的主引导区上的数据记录。

当病毒发作时，病毒把计算机的 CMOS 中的软驱和硬盘类型及参数全部修改设置为 **“0”**，使计算机不能引导。

查杀病毒的方法：

第一步，先用干净的系统启动软盘重新启动计算机。

第二步，退出系统软盘，把 KV3000 杀毒王 A 盘插入软驱。在 A:\>盘符下输入 KV3000，按回车。进入 KV3000 杀毒王在 DOS 下的界面。

当进入 KV3000 杀毒王在 DOS 查杀界面后按 **“F6”** 功能键，可以百分之百的观察到硬盘分区表，即物理扇区 0 面 0 道 1 扇区是否有病毒。如果发现病毒，请您按照画面提示彻底杀毒。

2. 查杀 Pretty Park、SUB7GOLD 和 WINDOS 病毒

Pretty Park、SUB7GOLD 和 WINDOS 是一种很可怕的病毒。当您用 KV3000 杀毒王查找到它时，如果轻易将其删除，那么，C 盘里所有可执行文件就无法启动了！原因是它在文件注册表里秘密实施了连锁装置，锁住了硬盘。

查杀 Pretty Park、SUB7GOLD 和 WINDOS 类病毒的方法是：

第一步，先手工解除连锁装置。先用干净的系统启动软盘重新启动计算机。

再退出系统启动软盘，插入 KV3000 杀毒王 A 盘。将 A 盘中的 FILES32.vxd病毒文件拷贝到您的计算机C盘\WINDOWS\SYSTEM 下。然后退出 KV3000 杀毒王 A 盘，同时按下 “Ctrl+Alt+Del “三键，使用硬盘重新启动计算机。

第二步，进入 WINDOWS 后，用鼠标在 “开始” \ “运行” 窗口输入 :REGEDIT, 将注册表打开。在 HKEY_CLASS_ROOT\exefile\shell\open\command 中将 FILES32. VXD 串删除！

第三步，然后用系统启动盘再次重新启动。插入 KV3000 杀毒王 A 盘，查杀 FILES32. VXD 病毒即可。

如果查毒软件查出的是 SUB7GOLD 黑客有害程序，就请您用系统软盘启动计算机后，退出系统盘换上 KV3000 杀毒王 A 盘，请将 MUEEXE.EXE 或 WINDOWS.EXE 病毒文件拷贝到 WINDOWS 的系统 SYSTEM 目录下，然后用硬盘启动计算机。

第四步，重新回到 WINDOWS 环境，用鼠标单击 “开始”、“运行”。在 “运行” 窗口里输入：“REGEDIT”，将注册表 HKEY_CLASS_ROOT\exefile\shell\open\command 中将 MUEEXE. EXE 或 WINDOS. EXE 串删除！

第五步，再次同时按下 “Ctrl+Alt+Del” 三键，用 KV3000 系统启动软盘重新启动计算机。再插入 KV3000 硬盘救护王 A 盘，在 DOS 下杀除 MUEEXE. EXE 或 WINDOS. EXE 黑客病毒。

(注意 :必须先将注册表中的该字符串删除后，才能使用KV3000 硬盘救护王杀除病毒。)

注册表中病毒路径：

HKEY_CLASS_ROOT\exefile\shell\open\command 中的 FI LE-S32. VXD (必须删除！)。

HKEY_CLASS_ROOT\exefile\shell\open\command 中的 mu-