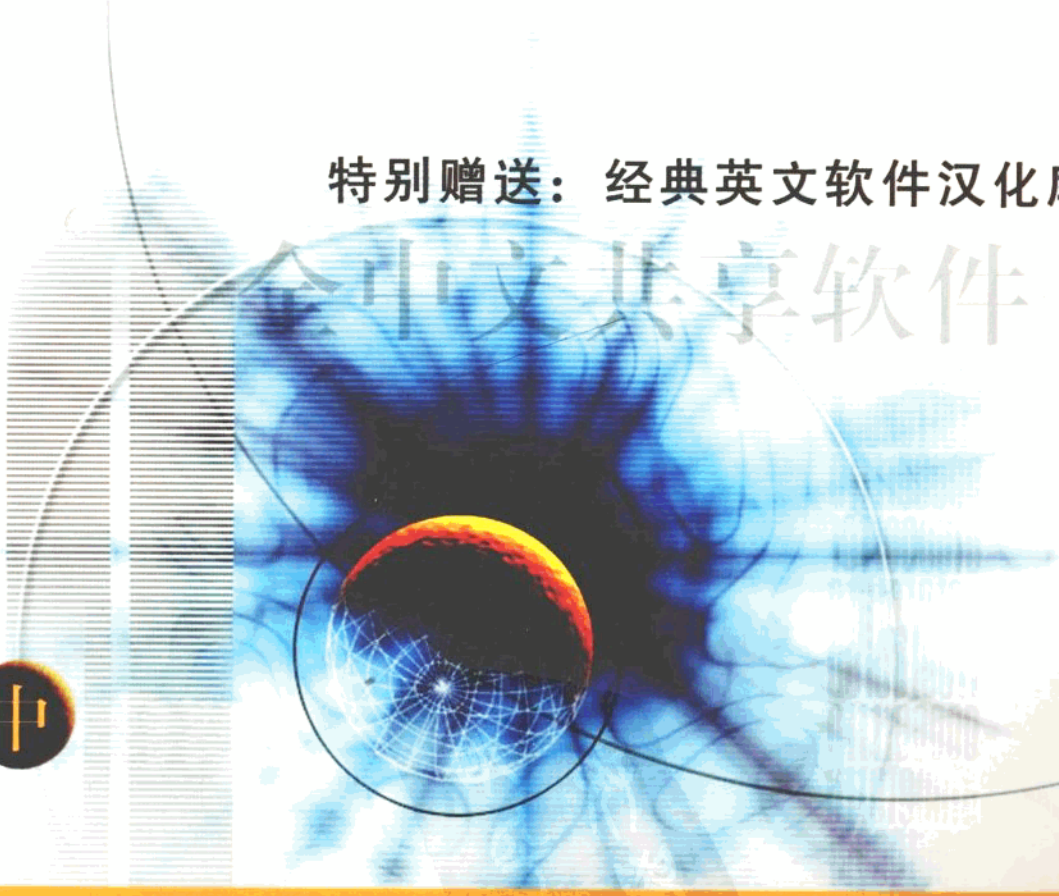
软件世界出品之软件酷秀系列

定价：16 元

全中文共享软件

中国人用中文软件

特别赠送：经典英文软件汉化库



中

目录

病毒防护

光盘说明

相关资讯

磁盘工具

光盘说明

相关资讯

多媒体类

光盘相关

音频视频播放

多媒体编辑制作

相关资讯

光盘工具

光盘说明

相关资讯

加密软件

光盘说明

相关资讯

商务软件

光盘说明

相关资讯

图形图像

光盘说明

编辑、制作

获取、捕捉

浏览察看

相关资讯

网络相关

FTP 软件

MODEM 加速

拨号工具

常用工具

传真软件

电话相关

电子邮件

计费软件

离线浏览

浏览器

网页编辑

下载软件

寻呼软件

远程登录

相关资讯

文字相关

光盘说明

相关资讯

系统优化

光盘说明

相关资讯

压缩工具

光盘说明

相关资讯

病毒防护

新事物产生后总会有这样那样的问题，不光是来路不明的各种文件，网络也不例外，带给你方便的同时造成难以想像的危险，不可避免的问题我们真对待，不仅是OICQ、浏览器、电子邮件和你下载的文件，随着计算机水平的整体提高，以后肯定还会有其他形式的危险在等待着你，你是否做好准备应付它们了？请随时保持一颗警惕的心。

功能强劲的杀毒软件PC-cillin 2000

杀毒软件一直是广大用户关注的热点之一，KV300、KILL、AV95、瑞星等软件的“喊杀”声正此起彼伏，上演了一幕精彩的“世纪之战”，相比之下PC-cillin则显得不那么起眼。其实作为趋势公司精心推出的一款优秀杀毒软件，PC-cillin的功能丝毫不比上述杀毒软件差，甚至在很多地方都是有过之而无不及，鉴于许多用户对这样一个优秀软件还不太了解，现将其有关功能向大家做一个简要介绍：

一、可直接对压缩文件和电子邮件附件进行扫描

某国内著名媒体的配套光盘可能是国内第一张带有CIH病毒的正版光盘，尽管该光盘在面世之前曾经某杀毒软件严格检测，但仍有“漏网之鱼”的原因就在于配套光盘全部采用ZIP压缩包的形式，而该杀毒软件却不具备直接查解压缩包中文件是否带有病毒的功能，从而导致了这一严重事件，这就充分说明了直接查解压缩包中病毒的重要性。正因为如此，PC-cillin特意向广大用户提供了直接查解压缩包及电子邮件附件中是否附带有病毒的功能，它无需要打开压缩文件或电子邮件附件，即可对它们附带的所有文件进行病毒扫描，从而杜绝了那些“披着羊皮的狼”可能对我们造成的危害。具体来说，PC-cillin可直接对PKZIP、ARJ、LHA、TAR、GNU-ZIP、UNIX compress、MS-compress、PKLITE、LZEXE、DIET、Cabinet等12种压缩格式以及Uuencode、MIME、Bin Hex等3种编码格式的文件进行查解，并且它可对压缩文件进行两层扫描，也就是说即使病毒经过两层不同方式的压缩之后，PC-cillin仍可将它们“挖”出来，效果可是相当不错的哦！

二、速度快、体积小

由于PC-cillin 98可将即时扫描的病毒监控部分与手动进行的文件扫描部分分开进行存储，其中病毒监控部分常驻内存，而手动进行的文件扫描部分与磁盘病毒扫描部分则只在调用时才载入内存，因而大大降低了对内存的需求，同时也减少了所占用的系统资源。不仅如此，整个PC-cillin的程序运行方式也进行了重新设计，从而大幅度提高了运行速度及工作效率。

三、可通过Active Channel获取最新病毒信息

为方便用户获取最新的病毒信息，PC-cillin特意

向用户提供了活动桌面功能，我们只需利用这一功能即可直接订阅 Internet Explorer 4.0 的 Active Desktop 和 Active Channel，从而实现了自动在第一时间获取最新的病毒信息以及病毒代码文件更新信息的目的，确保了系统的安全性。当然，除了活动桌面功能之外，PC-cillin 还提供了其它许多系统更新的方式，用户可通过 Internet 按预先设定的时间自动更新病毒扫描引擎，也可手动更新病毒代码和扫描引擎，还可通过 BBS、磁盘或 CD-ROM 等方式来更新病毒代码文件，使用非常方便。

四、Web Trap 可阻止 Internet Java Applet 及 ActiveX 病毒

为防止 Internet Java Applet 及 ActiveX 等病毒可能对用户造成的危害，PC-cillin 特意向用户提供了用于对这些病毒进行防范的 Web Trap 功能。启动该功能后，PC-cillin 就会随时对 Internet Explorer 或 Netscape Navigator 等 Web 浏览器进行监视，从而防止了用户遭受到恶意的 Java Applet 及 ActiveX 等程序的侵害，效果非常好。

五、同时提供了“手动扫描”、“预设扫描”和“即时扫描”等多种不同的病毒扫描方式

为满足用户在不同条件下的需要，PC-cillin 一共提供了“手动扫描”、“预设扫描”和“即时扫描”等三种不同的病毒扫描方式（见左图），我们既可利用“手动扫描”方式实现手工启动扫描程序，并对所选驱动器或文件夹进行扫描的目的；又可利用“预设扫描”方式实现自动定时激活 PC-cillin 对系统进行扫描的目的；同时我们还可利用“即时扫描”方式实现将病毒扫描引擎常驻于内存，随时对输入 / 输出的文件进行扫描，确保系统达到“百毒不侵”的境界。需要说明的是，这三种扫描方式的适用范围并不一样，其中“手动扫描”方式主要用于在安装那些有疑问的软件之后使用，“预设扫描”方式主要是用于指定由系统定时自动查毒，这两种扫描方式耗时较长，但范围较为全面，可将任何病毒“置之于死地”，而“即时扫描”则是随时监视系统文件的变化，防止病毒入侵，其速度快，但它仅仅监视一些比较常见的病毒，范围不太全面，广大用户应加以配合使用。

六、对检测到的病毒提供了多种不同的处理方式

不同的用户在碰到病毒后将会采用不同的方式，如绝大多数用户在发现病毒之后都希望立即将其清除，不过对于那些高级用户来说，它们往往并不需要直接清除病毒，而可能需要将病毒保存下来以供研究、分析！为此，PC-cillin 特意向用户提供了五种不同的病毒处理方式，即“拒绝访问（检测到病毒之后只向用户显示有关信息，而不对被感染文件进行任何处理）”、“清除病毒（清除被感染文件中的病毒代码）”、“删除文件（删除感染有病毒的文件）”、“更改扩展名（更改被感染文件的扩展名，使文件无法运行、打开，以防止病毒激活和蔓延）”、“移动文件（将被感染文件移至指定目录，隔离起来）”，广大用户可根据需要加以选择。

另外，PC-cillin 还具有可在屏幕保护状态下从事后台病毒扫描以节省时间、可任意指定扫描的文件类型、清除带毒文件时自动制作备份、允许对指定类型的文件或指定文件夹中的文件不予扫描、可记录详细的病毒日志以供用户日后参考、提供了详细的病毒信息等众多优秀功能，限于篇幅，这里不可能详细介绍，望读者见谅……

病毒克星 — 金山毒霸

金山毒霸可查杀超过 2 万多种病毒家庭和近百种黑客程序，除传统的病毒外，还能查杀最新的 access，PowerPoint，Word2000，Java，Html，Javascript，VBScript 等病毒。

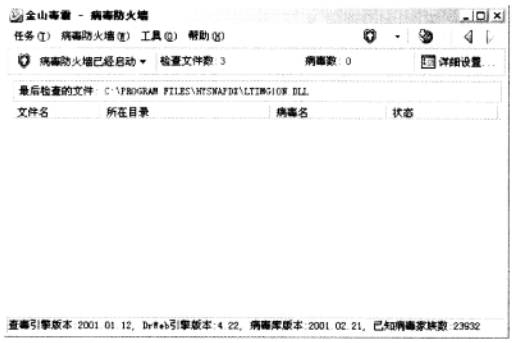
使用说明：

用金山毒霸查杀病毒：

您可以在金山毒霸“控制中心”的“目录选择窗口”选择要检查的驱动器和目录，按下“开始查毒”按钮即可自动进行查毒。当金山毒霸提示发现病毒时，选择“清除病毒”或“删除文件”按钮

即可清除病毒，详情请参阅联机帮助文件。

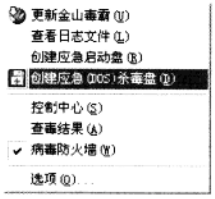
金山毒霸病毒防火墙：



金山毒霸的病毒防火墙可以过滤操作系统当前的文件操作，实时检测病毒，以保证在病毒试图感染您的系统前发现病毒并报警。您也可设置为发现病毒时自动清除病毒，实现全自动的防毒杀毒。

制作应急杀毒盘和应急启动盘：

为了避免 Windows 被某些病毒破坏而无法正常启动，也为了清除某些需要在干净的DOS 环境下才能清除的病毒，请您务必制作一张应急启动盘和应急杀毒盘。



在使用金山毒霸的应急杀毒盘前，请用干净的 Windows 启动盘启动计算机。 您可以用金山毒霸的应急盘制作程序制作一张应急启动盘，注意不要在带毒环境中制作应急启动盘。

金山毒霸的应急杀毒盘包含金山毒霸的命令行版本程序 KAVDX.EXE 和硬盘修复程序 KAVFIX.EXE。KAVDX 的使用说明请参阅 KAVDX.TXT 文件。 建议您用金山毒霸硬盘修复程序备份您的硬盘分区表数据到软盘上，操作方法可参阅 KAVFIX.TXT 文件。

处理引导区病毒出现的故障：

引导区部分是计算机磁盘上最为重要的数据区域，为了避免金山毒霸在处理引导区病毒时由于一些特殊的不可预知的因素造成故障，导致您的机器无法正常启动。金山毒霸在清除引导区病毒前总会要求您制作一份备份文件。正确地使用金山毒霸可以将您的机器恢复到清除病毒前的状态，保证您的数据不致丢失。如果不幸中招，请您参照以下步骤进行恢复工作：

1、使用一张干净的软盘启动您的机器；

2、执行KAVFIX.EXE；

3、选择第3号功能：Restore Process Sectors

4、KAVFIX.EXE 为保障正确无误的工作而不是您的误操作，需要您在此确认恢复动作；

5、然后KAVFIX.EXE 会提示输入您所备份的文件名；

6、接着KAVFIX.EXE 会自动根据您所备份的文件结构类型来进行判断。

一是如果备份文件中含有主引导区信息。KAVFIX 会要求您输入物理硬盘盘号，这里的盘号指的是您的物理硬盘的顺序号，从0 开始。比如您要恢复第一个物理硬盘的主引导区，则输入0；要恢复第二个物理硬盘则输入1....依此类推；

二是备份文件中只是纯粹的分区引导区信息。KAVFIX 则会要求您输入您所希望恢复的分区盘号，这里的盘号是指包括软驱在内的A、B、C、D、E 等等的逻辑分区盘号；

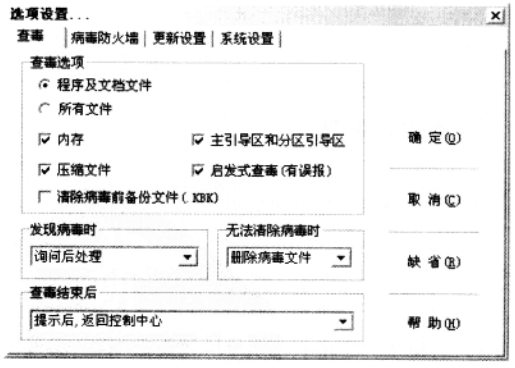
三是备份文件是由2 号功能Backup Process Sectors 所创建的，KAVFIX 也会要求您输入物理硬盘盘号，同情况一。此处一定要谨慎，不要错覆盖了其他的盘。

7、KAVFIX.EXE 恢复引导区成功后，将报告 SUCCESSFUL 信息，否则将报告 fail。

8、选择 'Q' 退出KAVFIX.EXE，如果是恢复硬盘的数据，请您重新启动机器。

启发式查毒：

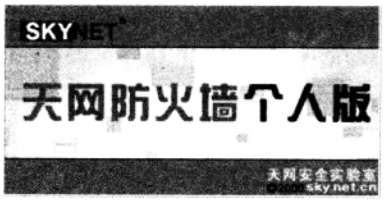
启发式查毒是采用虚拟机的方式让程序在软件仿真的机器环境中虚拟执行，并在执行过程中判断程序是否有非法内存驻留，异常磁盘操作等等类似病毒的操作，



通过综合的方式确定是否含有可疑代码，一般是以Unknown. 开头的病毒名。由于正常的程序有时会有其中的一些行为，因此有时会有误报的情形，一般遇到这种情形，请通过技术支持途径向开发商反馈。

电脑卫士 — 天网防火墙个人版

天网防火墙个人版是一套给个人电脑使用的网络安全程序，它可以帮你抵挡网络入侵和攻击，防止信息泄露，并可其网站（WWW.SKY.NET.CN）相配合，根据可疑的攻击信息，来找到攻击者。天网防火墙个人版把网络分为本地网和互联网，可以针对来自不同网络的信息，来设置不同的安全方案，它适合于在拨号上网的用户，也适合通过网络共享软件上网的用户。



使用说明：

请先设置好本软件，否则可能会影响您的使用。第一次启动防火墙启动后，会提示用户注册，您可到网站上（WWW.SKY.NET.CN）免费获得注册密码，然后输入到注册界面中，要注意大小写。注册成功后，以后将不再提示注册。

天网防火墙个人版可根据不同的网络状况，灵活的设置不同的安全方案，最大限度的保护你的电脑受网络上的攻击：如果你不熟悉网络，那你可以采用其帮您制定的方案；如果你是网络专家，那么你也可以自己直接定制自己的安全规则，安全规则的设定是在《普通设置》或《高级设置》中完成的，其中《普通设置》是给不熟悉网络的用户使用；《高级设置》是给比较了解TCP/IP协议的用户使用。

《普通设置》

对普通用户提供了如下方案，用户使用时，只需拖动跟踪条，直到调整到自己所需的方案。

安全方案说明：

1、安全级别：极高

这种安全方案是最安全的，但也是限制最多的，因为在此方案中，您的个人电脑与网络完全断开了，没有人可通过网络访问到您，但是您也无法访问网络。当你由于要离开电脑一段时间，但又不想关机时，你就可以通过这种方案保护你的电脑。

2、安全级别：高：

这种安全方案很安全，你可以用浏览器访问WWW，但ICQ、OICQ等软件无法使用，类似于FTP的服务程序也无法使用的。应为这时所有端口的服务都关闭了，别人无法通过端口的漏洞来入侵你的电脑。而且就算是你的机器中有某种特洛依木马的客户端程序，也由于不会受到入侵者的控制而激活。

3、安全级别：中：

这种安全方案也比较安全，别人无法用端口扫描器来扫描你的机器是否有什么端口处于开放状态，您可以使用Mirc、ICQ、QICQ等软件，可以防止别人通过冰河、BO等特洛依木马的客户端程序控制你的机器，并且阻挡了某些常用的蓝屏攻击和信息泄露问题。不会影响其他网络软件的使用。

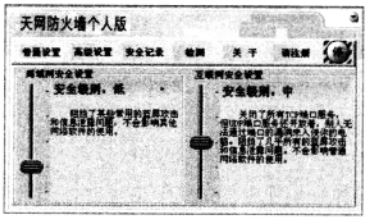
4、安全级别：低：

这种安全方案是限制最小的，代价是可能会受到某些端口攻击，但还是阻挡了某些常用的蓝屏攻击和信息泄露问题，别人无法用PING命令来探测你的机器，不会影响其他网络软件的使用。你可以在这种方案下使用各种网络工具。

5、用户自己定义

这种安全方案是最灵活的，但要求使用者对TCP/IP协议有相当的了解，你可以自己针对局域网和互联网来指定不同的安全方案，具体说明见《高级设置》。

如果你只是用拨号网络上网，那么，您只需调整《互联网安全设置》。



对拨号网络上网用户的建议：您可以根据您在互联网中的日常操作来设置。

您的操作	互联网安全设置	局域网安全设置
访问WWW和mirc	高	低
使用ICQ或OICQ	中	低
FTP等服务器	低	低

《高级设置》

对TCP/IP协议有一定了解的用户可在这里定制自己的安全方案。

《高级设置》页面中分为本地网和互联网两块，每块中包含了一些TCP/IP协议的复选框：

与网络联接：正常时表示与网络之间保持着连接，

但网络操作受到其他规则限制。关闭时表示与网络之间的连接已经完全断开，就好象拔下了网线，所有的网络操作都不可进行。

ICMP：关闭时，即别人无法用 PING 的方法来确定你的存在。但不影响你去 PING 别人。由于ICMP协议现在也被用来作为蓝屏攻击的一种方法，而且该协议对于普通用户来说，是很少使用到的，建议关掉此功能。

IGMP：IGMP是用于组播的一种协议，对于WINDOWS的用户是没有什么用途的，但现在也被用来作为蓝屏攻击的一种方法，建议关掉此功能，关闭后不会对用户造成影响。

TCP监听：关闭时，你机器上所有的TCP端口服务功能都将失效。这是一种对付特洛依木马客户端程序的有效方法，因为这些程序也一种服务程序，由于关闭了TCP端口的服务功能，外部几乎不可能与这些程序进行通讯。而且，对于普通用户来说，在互联网上只是用于WWW浏览，关闭此功能不会影响用户的操作。但要注意，如果你的机器要执行一些服务程序，如FTP SERVER，HTTP SERVER 时，一定要使该功能正常，而且，如果你用ICQ来接受文件，也一定要将该功能正常，否则，你将无法收到别人的文件。另外，关闭了此功能后，也可以防止许多端口扫描程序的扫描。

UDP监听：关闭时，你机器上所有的UDP服务功能都将失效。不过好象通过UDP方式来进行蓝屏攻击比较少见，但有可能会被用来进行激活特洛依木马的客户端程序。注意，如果你使用了ICQ或OICQ，就不可以关闭此功能，否则，你将无法收到别人的ICQ信息。

NETBIOS：失效时，你机器上所有共享服务功能都将关闭，，别人在资源管理器中将看不到你的共享资源。注意：如果在失效前，别人已经打开了你的资源，那么他仍然可以访问那些资源，直到他断开了这次连接。注意，如果你在局域网中，而且您的网络设置中还有IPX，NETBUEI网络协议，那么局域网中的其他机器还是可以用这些协议来访问你的机器。

《紧急按钮》

如果按下了按钮，那么与网络之间的连接将马上完全断开，在怀疑受到某些不明攻击时，比如好象有人在控制您的机器，你可以通过这种保护你的电脑，在确认没有问题后，再开放网络。

当防火墙收到你在安全规则中拒绝接受的数据包时，屏幕右下角的图表会闪动，（防火墙会根据您设置的安全级别来判断数据包的可疑性，并拦截掉这些可疑的数据包），并且防火墙还会把这些数据记录下来，您可以双击闪动的图标，进入《安全记录》的界面中。如果您对这些数据不了解，可以按《客户服务中心》键去网站得到解释和建议。注意，被拦截掉的数据包不一定是攻击数据包，而且，就算是攻击数据包，你也可以放心使用，因为它们已经被拦截掉了，不会对您的机器有什么影响。

熊猫卫士 6.0 中文铂金版

熊猫卫士6.0铂金版集成了所有的Internet保护功能，具有智能、强大和便于使用的特点，并提供全面的技术支持及服务。熊猫卫士铂金版是第一个专门为Windows 98开发的病毒防护软件。它也可为Windows 95、Windows NT Workstation 3.51和4.0、Windows 2000 Professional、Windows 3.x、MS-DOS和OS/2提供保护，因此无论您使用何种操作系统，熊猫卫士都能保证您计算机的安全。

熊猫卫士铂金版能有效地保护计算机所有可能的病毒入口，包括E-mail、新闻组和Internet访问。它可高效地扫描和清除病毒，无论它们藏身于何处；同时它能最大限度地确保数据的完整性。熊猫卫士铂金版不仅能保护所有病毒侵入点，也能防止病毒从您的计算机发送出去而感染其它用户。

熊猫卫士将强大的功能和易于使用集于一身。其艺术级的界面、丰富的设置选项、发现病毒后的动作设置、集中式的管理、极为方便的多语言切换一定令您爱不释手。它将完全扭转人们心中反病毒程序复杂、难以掌握的印象。

它提供最完善的服务。一个防毒软件没有一套完整的服务来支持它就将失去活力。熊猫卫士铂金版能在激烈的市场竞争中保持不败的原因就在于此。因为它拥有智能更新（业界唯一的每日自动更新病毒特征文件）、一年365天，一天24小时的个人在线技术支持、总部24小时的SOS病毒解决方案、全球最新病毒新闻等各种服务。

完全质量保证。熊猫卫士铂金版保持着一项世界纪录，同时拥有ICSA和Checkmark这两个权威安全认证组织的认证，它们授予熊猫卫士的证书比任何其它同类产品都要多。

ICSA认证：该认证由美国著名的国际计算机安全协会向防毒产品颁发，证明该防毒产品能定期100%地侦测出所谓的Wild病毒（即在任何时候传播最广泛的病毒），并能侦测出90%以上的Zoo Collection（传播不很广泛的病毒）。

Checkmark认证：由英国专门撰写有关电脑安全文章的杂志——“安全电脑”（Secure Computing）杂志颁发的著名认证。

目前国内杀病毒软件市场诸侯割据，国内和国外的各种防病毒软件充斥着整个市场。消费者在选择该类软件时，往往不知道该如何入手，是不是选择一个能杀病毒数最多的软件或是一个占用内存最低的软件就是最佳的方案。在这里笔者推荐一个刚进入中国市场不久的优秀的防病毒软件—熊猫卫士6.0，也借这样一个机会，向消费者介绍一下如何客观的评判一个防病毒软件。

首先简单地介绍一下熊猫卫士，熊猫卫士是世界上第四大防病毒软件厂商熊猫软件公司(Panda Software)的荣誉产品，熊猫软件在全世界范围内三十多个国家设有分支机构，它来自欧洲，100%的欧洲自有技术，在欧洲的市场占有率一直名列第一。虽然进入美国市场才不到两年时间，但也在美利坚闯出了名堂，现在市场占有名列第三。

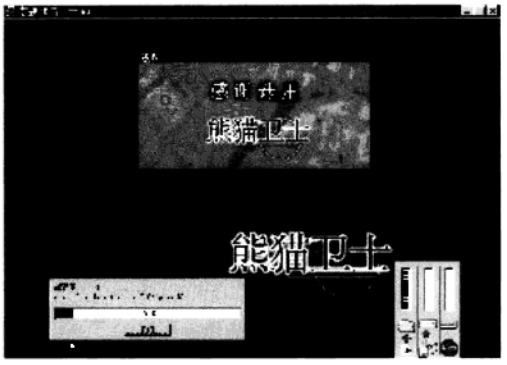
使用说明：

1．安装过程

熊猫卫士6.0的安装过程非常简单且用户界面友好，即使是一个对防病毒软件没有任何了解的人，软件的安装也可以说是轻而易举。

安装程序提供三种安装方式：智能安装、完全安装和自定义安装。这里需要着重介绍的是熊猫卫士的智能安装：它是一个为方便安装设置熊猫卫士6.0而专门设计的工具。通过详细分析安装在电脑上的软硬件及一套简单的问卷，智能安装将最大程度地优化熊猫卫士6.0的安装设置。例如你已经有互联网络的连接，熊猫卫士会自动将客户连接的方式加入到软件更新设置中。

整个软件占硬盘空间为31MB，在安装完毕后，安装

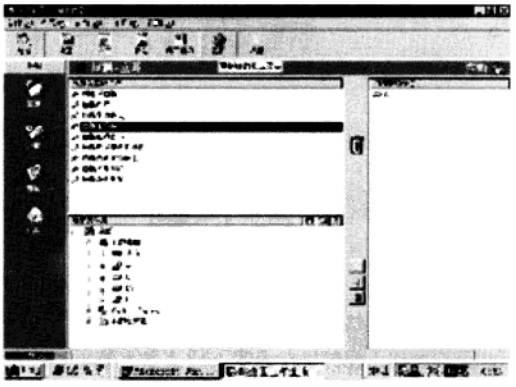


程序会提示你重启动系统，在系统重启动后，在系统托盘处会出现一个熊猫图标，表示整个系统受到了熊猫卫士的保护，无论病毒来自互联网络或者是局域网络，还是本地入口（磁盘、ZIP驱动器），它们都会受到常驻哨兵的痛击。

2．图形界面

熊猫卫士6.0的图形界面堪称优秀，熊猫卫士内置一个浏览器，用户可以在服务、杀毒工具和内置帮助文件中任意遨游。

熊猫卫士提供了4种扫描方式：即刻扫描、定期扫



描、启动扫描和常驻扫描。你可以轻松地在这些扫描方式中切换，在图形界面的左下角，熊猫卫士动态地以天数告诉你当前病毒特征文件的新旧。30天就表示你已经一个月没有更新软件，这样的设计恐怕也只有提供每日

更新的防病毒产品才敢放吧。熊猫提供两种操作模式：为了使熊猫卫士6.0适合不同的用户，我们的防病毒软件提供两种操作模式：常规模式和高级模式。两者的区别是，在保证提供相同保护程度的前提下，常规模式仅显示最常用的扫描选项，不需用户设置任何复杂选项，因此，操作极其简单。高级模式则允许用户设置任何扫描选项。

3．设置选项

你可以选择扫描何种类型的文件、是否扫描压缩文件（熊猫卫士支持多重压缩）、发现病毒采取何种措施（自动杀毒、通知用户、重命名文件、发电子邮件给系统管理员等等，见上图）。

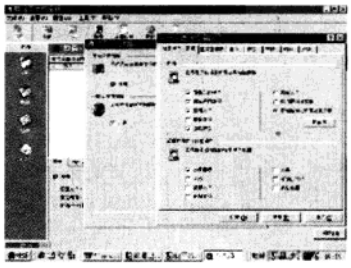
4、扫描和杀毒能力

扫描和杀毒能力对于一个防病毒软件并不是唯一决定其优劣的因素。但是作为一个消费者，当然希望自己的杀毒工具的查杀能力越强越好。熊猫卫士在这一点上可以说是毫不逊色。目前它的已知病毒库中包括大约48000种病毒。同样，熊猫卫士独有的hoax技术，对于未知病毒也可以同样查杀。

熊猫卫士同时通过最权威的安全认证组织国际计算机安全协会（ICSA）和黄金海岸的Checkmark的二级安全认证。当然国内的业界人士对于这些认证可能较为陌生，他们更关心的是针对国内病毒的查杀能力，大家完全可以放心，在去年底由公安部病毒检验站主持的一个防毒软件对比测试中，熊猫卫士网络版在所有十二种允许在中国销售的防毒产品中，在查毒、杀毒两项指标上都名列第一。无论一个病毒是来自传统的病毒入口，还是新兴的互联网络，它们都进不了用户的电脑。

5．实时监控能力

熊猫卫士提供两种类型的实时监控：哨兵监控和互联网监控。哨兵监控实时监视当前系统中所有正在运行或打开的文件，任何病毒代码或可疑操作都会激活哨兵，哨兵交自动采取一系列预定义的措施或通过消息框的方式告知用户。



除了当前打开的文件，熊猫卫士的互联网监控还实时防范来自互联网的病毒和黑客程序的威胁。要知道，除了传统的病毒，现在新兴出现的病毒多来自互连网络，ActiveX；Java等一系列恶意程序都可能在你网上冲浪时对你的系统进行攻击。熊猫卫士能完全监控这些端口。

6．系统资源占用

对于大多数电脑用户，系统资源的占用情况是是否选择一个软件的重要因素。特别是对于那些长期驻留内存的程序更是这样。我们使用Windows98内置的系统信息，在安装前后，试验用电脑的整体系统资源占用减少了3%~6%，对于这样的系统资源占用，用户完全是可以接受的。毕竟电脑系统受到了最全面的安全防护。

7．软件更新

熊猫卫士产品也是业界唯一提供病毒特征文件每日更新的防病毒软件。要知道，每天全世界范围内有大约15种新病毒产生，换句话说，一个月软件不更新，防毒程序就不能对付大约500种新病毒，防病毒技术发展到今天，针对某一个病毒能不能写出清除代码已不是问题，关键是响应速度，能否在最快时间内更新客户的程序。当然，除了病毒特征文件的更新，程序本身查毒能力的升级也是非常重要。

8．因特网病毒防范能力

随着通过国际互联网的交流日益频繁，用户感染病毒的机率也越来越大。熊猫卫士防病毒软件正是基于此发展起来的新一代防毒软件，除具有常规杀毒软件的性能外，还是一款针对Internet应用设计的防护软件，支持最多的Internet使用协议，可以防护所有的病毒入口。

9．服务

熊猫软件中国有限公司是国内唯一一家提供24小时S.O.S服务的电脑安全公司，24小时S.O.S服务即熊猫软件承诺在24个小时内提供客户送达的病毒文件的解决方案。熊猫卫士独有的这项服务在业界可以说是独一无二。当然无论用户在何时对产品产生疑问，都可以质询熊猫卫士的技术工程师。

相关资讯

常见邮件病毒的症状和解毒方法

国际计算机安全权威机构发布最新病毒公告称，发现了一种新型的名为“W97M/Melissa”的宏病毒（美丽杀手），该病毒能传染Word 97和Word 2000。第一天便有60000台以上机器被感染，短短的一个星期，互联网便经历了一场罕见的“电子邮件病毒”的风暴！“电子邮件病毒”真这么厉害吗？有没有方法可以解毒呢？下面让我们来看看这些病毒的发作症状及解毒方法。看完后，你就可以对“它们”说“不”。

美丽杀手

根据KILL98反病毒技术人员对W97M/Melissa病毒进行的分析，确定该病毒传染的对象是Word 97和Word 2000文件。当用户打开已感染有该病毒的文件时，美丽杀手便传染用户系统，同时，病毒通过用户收发带毒的电子邮件互相传染，而且传染方式非常隐蔽。美丽杀手病毒的具体表现症状是：

1．当用户打开的文件感染有该病毒时，病毒首先检查注册表中是否有美丽杀手的注册信息，若有则表明系统已被传染，否则，在注册表中创建一条注册项如下：HKEY_CURRENT_USER\Software\Microsoft\Office\“Melissa?” = “... by Kwyjibo”

2．利用Visual Basic指令建立一个OutLook对象，从OutLook的全域地址表中获取成员地址信息，将下列信息以电子邮件方式，自动发送到地址表中的前50个邮箱(一次发送50封邮件)。其中：邮件主题为:“Important Message From —”

正文为:“Here is that document you asked for ... don’t show anyone else :—)”。之后，病毒将已感染有该病毒的文件作为附件发送出去。目前较为流行的一种附件的文件名为“list.DOC”(注意附件的文件名并不只有这一种)。

3．当用户接收到带毒的邮件并打开时，用户的Word系统中所有打开的文件将被传染。当机器时钟的时间数值与日期的数值相同时，如4月27号的4点27分，病毒将打开一个被传染的文件，在当前的光标位置插入下列信息：“Twenty — two points, plus triple — word — score, plus fifty points for using all my letters. Game’s over. I’m outta here.”

4．值得注意的是美丽杀手在传染Word 2000时，首先从注册表中检查其安全保护级别，如果注册表中HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security\“Level”的值不为0，将禁用菜单中的“MACRO/SECURITY”选项。如果用户使用的系统是Word 97，则禁用菜单中“TOOLS/MACRO”选项。

“怕怕”病毒

美丽杀手病毒余威尚存，作为美丽杀手病毒的发现者，Network Associates公司又发现了一种与它类似但危害更大的电子邮件病毒Copycat。这种被昵称为“Papa”(怕怕)的新病毒是一种Excel病毒，跟Melissa一样，它可以自动复制自己并发送给用户地址簿中的前60个人。此外，Papa每次被激活时都向外发送电子邮件，而Melissa只在第一次被激活时才发送邮件。Papa也向IP地址为207.222.214.225或者24.1.84.100的服务器随机发出“拒绝服务类型的攻击”。

“辛迪加”病毒

“Syndicate.A”(辛迪加)，是基于Word 8(Office 97)病毒的一个变种，与美丽杀手病毒非常相近，但比美丽杀手的危害性大。它驻留在ThisDocument模块中，被感染的机器在使用Outlook时，病毒从地址簿中每一个地址列表中挑选前69个地址，然后把已感染的文档作为附件发送给这些地址。主题行为：“Fun and games from Username”，正文信息为：“Hi! Check out this neat doc I found on the Internet!”发送完毕后，Syndicate.A还将发送E—mail给另一接收者：project1@nym.alias.net，主题为：“Guess who’s infected: UserName”(猜猜又有谁中毒了)，正文信息为“Infected!”

解毒方法：最新发布的KILL98和Network Associates的Mcafee Virusscan等国内外杀毒软件已经能够杀除美丽杀手及其变种了，已经中毒的赶快去下载啊。

Happy99 病毒

看着现在横行江湖的美丽杀手，如果你记性还好的话，也许还记得曾经风光一时的“Happy99”吧，Happy99对硬件和数据均没有大的影响，惟一的只是默默地耗费着时间和资源，减缓网络运行的速度，直至导致公司邮件服务的瘫痪。同样地，该程序也是通过电子邮件，向被感染用户所使用的新闻组和邮件地址发送几百份自身的拷贝。

如果你收到一封E-mail，带有一个名为happy99.exe（注意，可能不是这个文件名）的附件，而你去执行了它，你的屏幕上就会自动打开一个窗口，以黑色为底色的满天烟火，此后，只要你发信夹带附件就死机。重新启动后，还是不能发送夹带附件的信。如果不夹带附件，可以发信，但是Happy99会悄悄附在信中，对方如果运行，即被感染。然后，happy99就潜伏下来，如有机会，会赠送下一个收信人一个自身的拷贝。

解毒方法：如果你收到带有Happy99.exe的邮件，并且已经运行了happy99.exe，恭喜你，你将有机会看到下面的解毒方法（如果没有运行，那我要祝贺你，因为你是一个聪明人）。

通过更新病毒库，最新的PC－Cillin或Norton防毒程序可以将happy99查解。另外，国内的冠群金辰、瑞星、信源等杀病毒厂商已推出清除happy99的软件。当然你还可以用手工进行检测和处理：打开Windows的System目录，如果发现有ska.exe、ska.dll与wsock32.ska等三个文件，那就说明你的电脑已经中毒了！你可以将前两个文件删除，再把wsock32.ska重新命名为wsock32.dll，然后，再将邮件中的happy99.exe删除即可。

对症下药 查杀病毒

在节日里，人们相互祝福是很平常的事。随着因特网的普及，在网上相互祝贺也成为时尚。在你发出自己的祝福时，要谨防通过电子邮件传播的电脑病毒。

随着I Love You（爱虫）病毒日渐远离我们，岁末，网上邮件病毒又活跃起来。首先是I_WORM.MTX病毒、Funlove.4099病毒、ktiz.8192病毒的泛滥，这几种计算机病毒，主要通过网络邮件传播、感染，通常具有感染PE格式的Windows系统文件、系统文件以及各种普通格式的PE文件。

“I-Worm.Naridad” 圣诞节病毒

接踵而来的是I-Worm.Naridad（圣诞节病毒）网络蠕虫程序，其传播机制不同于一般的网络蠕虫程序，具有较大的迷惑性：用户通过Outlook Express收到一封自己曾经发送过的邮件的回复信件，内容与发送的完全一致，邮件主体、正文都一样，只是增加了一个电子邮件的附件，名称是Navidad.exe文件，大小为32768字节。该附件就是网络蠕虫、程序的主体文件，该邮件只是在微软的Outlook Express邮件系统下自动传播，它会自动地给您的收件箱的所有人发送一份该网络蠕虫程序。由于该网络蠕虫程序存在Bug（错误），因此该附件执行后，会导致Windows系统不能正常启动。

“I_Worm.Blebla.B” 罗密欧与朱丽叶

然后又出现了I_Worm.Blebla.B（罗密欧与朱丽叶）网络蠕虫程序。同其它网络蠕虫程序一样，它也是通过电子邮件的附件来发送的，文件的名称是Xromeo.exe和Xjuliet.chm，该蠕虫程序的名称由此而来。和其他蠕虫程序不同的是，它能自动地执行附件文件xjuliet.chm，然后由该附件来调用可执行文件xormeo.exe，该蠕虫程序正是利用该可执行程序来实现自动传播的，这些文件被自动存放在Windows的临时文件夹TEMP中。用户在使用OE阅读信件时，这两个附件自动被保存、运行。运行该附件后，该蠕虫程序将自身发送给Outlook地址薄里的每一个人。

这些网络蠕程序都带有不同程度的破坏性，用户在使用邮件系统时应特别留意附件中的程序，即使是熟悉的人发送的附件程序也应该先下载，然后采用最新版本的杀毒软件来查杀。笔者通常采用最新推出的金山毒霸，它采用了实时监控、自动解压缩、反病毒技术，在DOS、Windows平台都可以彻底预防和杀除这些网络蠕虫程序。

“COMS 设置破坏者” 病毒

CMOS DESTROYER（CMOS设置破坏者）病毒是引导区病毒，有A、B、C三个变种，在国外称为ANTICMOS（反CMOS）病毒。

该病毒感染硬盘的主引导记录和软盘的BOOT区，并且该病毒不分是什么DOS、WINDOWS、NT、UNIX等操作系统，都可以统统感染硬盘的引导区，因为它采用的是覆盖主引区记录的传染方式。

其中A类型，它发作时破坏CMOS的设置，将其软驱和硬盘的参数全置为0，导致硬盘不能引导，需手工重新设置参数。B类型不破坏CMOS设置，但使机器发出一种颤动的声音，并使机器死循环。C类型也不破坏CMOS设置，但连续发出一种怪叫，所以B、C两种也称“TRILL颤动”病毒。

我们所说的“CMOS设置破坏者”病毒，不等于说躲藏在CMOS里面的病毒。由于此病毒可以将CMOS设置改变成加密，从此有人误认为CMOS内有CMOS病毒。

清除方法是使用干净系统软盘起动计算机，再用KV3000等杀毒软件来查杀该病毒。

其实病毒并不可怕，只要我们能够了解它的特征并在使用过程中多加注意，就完全可以避免它。

病毒防治三例

BO黑洞

现在有很多病毒都是通过E-mail传播的，还有一些恶意邮件要提醒用户注意，这类信件往往是不怀好意的，经常夹带一些具有恶意的附件程序。

Back Orifice（简称BO）就是这样一类程序。它是一个基于Windows的远端控制软件。它的工作原理是：首先把服务（Server）程序给欲攻击方，并且执行它。攻击者自己就运行客户（Client）程序来控制欲攻击方。当用户运行了Boserve.exe之后，Windows的注册表会被BO修改，并把自己复制到system目录下面，再把原来的Boserve.exe文件删除掉。以后每次启动Windows时，它都会根据注册表自动加载System目录下面的Boserve.exe服务程序。此时表面上来看Windows没有任何的变化，而实际上Boserve.exe服务程序正在悄悄地运行，接受从网络客户端传来的控制命令。

BO软件是一个名叫Cut of the Dead Cow的黑客组织开发的。此软件包总共有8个文件，其中Boclient文件总共有11组命令。这些操作包括搜索服务端IP地址，进入欲攻击方计算机，DIR、CD、RD、MD操作，拷贝、删除文件、从客户端发送文件到服务端和从服务端得到所需要的文件，还有显示被控制计算机的系统信息（包括CPU的类型、内存数量、各个驱动器的资料）及重启计算机等操作。

堵住BO黑洞的办法：可以利用江民公司KV300+（X++）原盘启动机器，执行KV300，即可查出或删掉潜藏在系统中的网络黑客程序BO。用户也可用KV300自我升级的方式扩充代码，即可查出机器中的BO黑客程序。

不打开附件就安全了吗？

近来互连网上频繁出现的各种电子邮件病毒，使人们对自己信箱中的附件既向往，又不敢随便亲近。于是就有好心的网友总结出一条经验：不要随意打开陌生邮件的附件，即使是朋友的邮件，在打开附件之前也要进行一项确认仪式：打电话问问他们是否真的给你发了信。但是面对每月第一个下午发作的Kak病毒，这些最保守的经验也只会被打得落花流水。

Kak病毒一种伴随HTML文件出现的病毒，全名“Wscript/Kak”，又称为“野蛮小子”、“泡沫小子第二”。其感染性与BubbleBoy（泡沫小子）病毒相同，利用微软程序中ActiveX控件scriptlet.typelib中存在的缺陷编写，通过IE 5浏览器将病毒代码写到Windows的开始目录中，并在System目录中创建一个自己的拷贝，然后就能够附在每个Outlook发出的电子邮件中向其他机器传播。凡是安装了IE5或Office 2000的电脑都有可能被感染。

美国在线电脑零售商Shoppingplanet.com就曾经一不小心，把带有KAK电脑病毒的产品广告电子邮件发给了5万多客户。值得庆幸的是眼下KAK病毒本身并无恶意，不会删除电脑中的文件。只是显示这样一行文字：Kagou-Anti-Kro$oft says not today! 然后它就会试图关闭Windows。如果用户的安全等级设定较高，也有可能看到这样的警告：你希望ActiveX控件插件运行吗？这时，应当回答：“否”。

幸好“爱虫”病毒没有利用Kak的特性，否则的话，后果真是不堪设想。所以，面对邮件蠕虫病毒，光是不打开附件是远远不够的。由于“野蛮蠕虫”病毒传播速

度快，感染方式特殊，因此，最好选用具备实时监控的反病毒软件，如KV300才能达到预防目的。当然，一种杀病毒软件只能截取它所知道的病毒，如果你至少一星期没有升级你的杀毒软件了，就要小心Kak病毒的入侵哦！

如何“自治”CIH

陈盈豪真是个天才，他编制的一个不足2K的小程序居然可以令几十万的电脑用户叫苦不迭，以至于偌大个中国，竟然在每个月的26日之前都要播出警告提示，以防用户的电脑受到CIH的骚扰。可是它有一个“漏洞”，那就是它无法令主板BIOS芯片中那块ROM内容也同时更改，而只是往EEPRAM中增加了1个字节，从而令BIOS损坏的。所以，我们完全可以通过自己的双手，来摆平这个CIH。下面，笔者就介绍给大家一种方法。（本例使用的是AWARDBIOS芯片）

正如上面提到的，主板BIOS中最重要的BLOCK模块并没有受到CIH的攻击，而这一模块本身就具有开机的功能，因此我们就可以通过编辑可执行文件，达到恢复BIOS的目的了。

1）制做一张DOS系统盘，将该损坏主板型号的BIOS文件和驱动刷新BIOS的文件（一般都由AWARD提供，多数名称就是AWARD．EXE）拷贝到该软盘上。

2）在根目录下编辑一个AUTOEXEC．BAT文件。在这个文件中，写下如下几行命令：@echo off a:\AWARD.exe X.bin；X为该损坏主板的BIOS文件名

3）将电脑开机，插入该系统盘到软驱中，只要你的软驱不是损坏的，那么一般都能够完成主板的BIOS修复工作。

这种方法，其实是利用了主板上CMOS芯片中除BIOS程序以外的BLOCK模块的功能。根据IBM在1980年推出PC时制定的规则，电脑的主板在由BLOCK模块引导开机时，必须由ISA显卡驱动才能显示出图像。而且，BLOCK作为一个固定模块，存储在ROM中。由于CIH只能破坏EPRAM，因此对BLOCK无能为力，当然也就可以令我们轻松搞定恢复BIOS了。

记得编辑部的阿周曾深有感触的告诉我，他现在觉得他的硬盘是这世界上最重要的东西，因为几乎所有的重要文件，包括新写的稿件、记录的备份、朋友的来信等全部被储存在硬盘里。CPU烧了，内存坏了都关是不大，而万一硬盘不幸乘鹤而去，简直比费他的命还痛苦……

文件更新至尊 — 同步大师

一个软件开发人员，在公司和家里各有一台电脑，另外还有一部便携机（应该很多人都有相似的情况），常常同一源代码文件或字处理文档在三台机器上都有，不幸的是，几乎不太可能使它们总是保持一致并且是最新的版本，尤其是文件数量很多的时候，要花很多时间来找出每台电脑上最新的文件。于是着手写了这个软件，解决了这个问题，后来又增加了一些资源管理器的常用功能，最主要的特性是能在同一窗口界面上处理不同目录中文件的拷贝、移动等操作，相当方便，再也不用打开两个“我的电脑”或在资源管理器中不断地切换目录、Ctrl+C、Ctrl+V了！目前最新版本是1.0Beta2，主要功能如下：

一、 提供两个目录间文件的同步功能，目前支持四种同步方式：

1、同步检查－仅进行同步检查，列出两个目录中不完全相同的文件清单

2、原始同步－保证原始目录中文件的最新版本都存在于比较目录中

3、比较同步－删除比较目录中多余的文件，保证与原始目录中的文件完全一致

4、完全同步－不删除文件，保证两个目录中的文件完全一致

二、 目录文件比较，支持以下比较方式：

1、列出所有文件

2、列出相同文件－两个目录中都存在且长度和修改时间都相同的文件

3、列出相似文件－两个目录中都存在且长度相同但修改时间不同的文件

4、列出不同文件－另一个目录中不存在或文件长度不同并且文件修改时间不同的文件

5、列出较旧文件－修改时间较早的文件 6、列出较新文件－修改时间较晚的文件

三、 全功能目录浏览，包括：

1、树状目录导航

2、ListView方式文件详细内容（文件名、类型、大小、修改时间、创建时间、访问时间）显示

3、支持按文件名、类型、大小、时间等排序显示及多重排序显示

4、显示目录统计信息（目录数、文件数、文件大小总和）

5、支持文件通配符过滤显示

四、 支持常见文件操作。

包括拷贝、移动、删除、改名等，操作在同一界面双目录下进行，非常直观、简便。

五、 支持双击启动文件缺省相关程序。以后版本预期功能：

1、全面支持带子目录同步操作

2、更多的同步方式

3、支持文件查找

4、支持鼠标拖放操作

5、透明支持ftp操作（可用于网站智能更新）

6、支持文件内容比较

7、使用者提出的更多的功能……

操作说明：

启动“开始菜单”中的同步大师，出现以下界面（图1）：

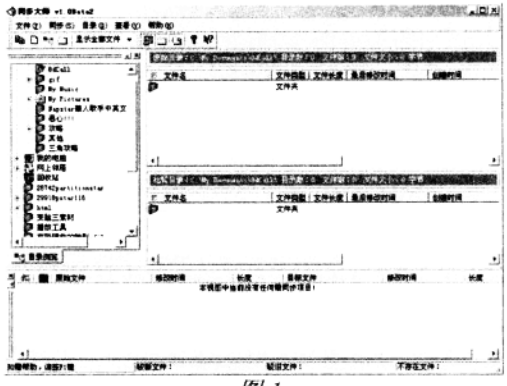


图1

三个主要的操作区域：目录浏览区、原始目录区、比较目录区。

这里要先介绍两个专用名词：激活目录区和非激活目录区。在任何时候，原始目录区和比较目录区只能有一个是当前操作目录区－称为激活目录区，标志是目录区标题栏的文本颜色为黄色，另一个目录区就称为非激活目录区，标志是目录区标题栏的文本颜色为白色。

dirbrowse目录浏览区：在界面的左侧部份，用来选择操作目录。可以显示本机所有硬盘驱动器目录、网络邻居共享目录及一些特殊的系统目录（我的文档、我的公文包等）。选择某一目录将引起当前激活目录重新刷新成该目录下目录和文件。

dirsource原始目录区：在界面的右上侧部分，用来显示指定目录下的子目录和文件，进行主要的文件操作和同步操作。双击子目录将进入该子目录，并刷新目录浏览区。点击鼠标右键将弹出可用操作的菜单。该区与比较目录区的唯一区别在于同步操作时，该区的被选择文件是“源”文件。

dirdest比较目录区：在界面的右下侧部分，用来显示指定目录下的子目录和文件，进行主要的文件操作和同步操作。双击子目录将进入该子目录，并刷新目录浏览区。点击鼠标右键将弹出可用操作的菜单。该区与原始目录区的唯一区别在于同步操作时，该区的被选择文件是“目标”文件。