网络安全

安全工具（二）

狄登峰 主编

目　录

PortReporter 助你上网更安全.....1
打造系统的安全防线.....11
利用 IRIS 学习 TCP/IP 15
用瑞星 2004 版进行游戏保护 48
用“百艺程序锁定器”加密电脑.....52
在家当一回“黑客” 58
IDS 的自防护原则与技术途径 63
用木马克星保护系统安全 68
配置功能齐全的诺顿网络安全特警 70
QQ 病毒的克星—QQAV.....78
超越网管的七“剑客” 80
中小学网络安全问题之反黄篇.....83
反黑精英——TrojanEnder.....90
Linux 系统安全工具介绍 97
局域网安全好工具-DeviceLock.....119
我的安全工具箱 121
如何用 PGP 加密 131
密码设置的秘诀 132

PortReporter 助你上网更安全

不要以为只有专业的大软件才可以追踪木马的踪迹，微软的工具软件 PortReporter 就可以完成对本机网络通讯进行记录和分析的功能，她不仅扫描计算机目前正在打开的 TCP 和 UDP 端口，而且可以跟踪记录 TCP 和 UDP 端口变化过程，比如木马悄悄打开的端口或者其他用户远程登录你的计算机上传一些乱七八糟的文件，所做的一切都被 PortReporter 详细的记录下了，通过分析日志就一目了然了。即使你使用不同的帐号登录计算机，PortReporter 依然忠实的记录所有使用者的帐号和登录后所有网络通讯作为。日志是以文本文件的格式保存的，用记事本就可以打开。

一、安装和卸载 PortReporter

PortReporter 可以安装在 MicrosoftWindowsServer2003,MicrosoftWindowsXP,orMicrosoftWindows2000 操作系统上，不要提 Windows98，微软公司已经不再提供对 Windows98 的技术支持，虽然微软公司依然提供对 Windows2000 的技术支持，但是 PortReporter 在 2000 上不能充分发挥她的效能。在 WindowsServer2003 和基于 WindowsXP 内核技术的计算机上，这个服务可以提供多种功能：监视正在使用的端口，端口对应的进程，这个进程是应用程序还是系统的服务，已经该进程打开的模块，还有使用者的帐号等，而在 2000 系列操作系统上，这个服务只记录什么时候哪些端口被使用。这个只有 153K 大的软件可以从微软的网站上免费下载：

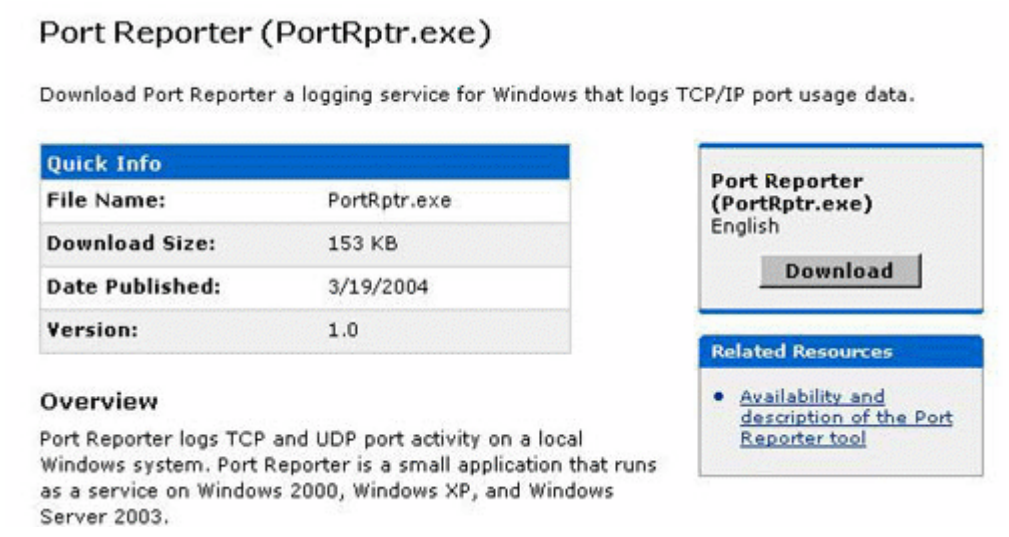

图 1

下载下来的是一个自解压的 EXE 文件，还原后得到 4 个文件如图 2 中显示。

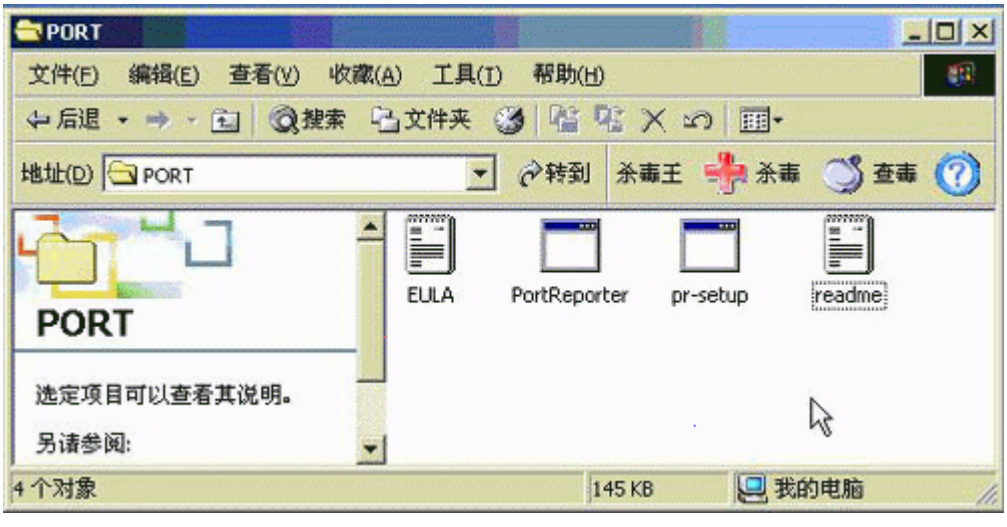

图 2

安装时只需要执行其中的 Pr-Setup.exe 文件就可以了，通过这个程序来安装 PortReporter 服务，Pr-Setup.exe 安装过程重要做了两项工作：

一是增加下面的注册表项:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\PortReporter

再是安装 PortReporter 服务，使用户在控制台中能够控制该服务的启动和停止。

Pr-Setup.exe 有 2 个参数-D 和-U

-D

允许用户把 PortReporter 安装到指定目录，比如你可以将 PortReporter 安装到 d:\tools\portreporter\下就使用这个参数。如果不带任何参数直接允许 Pr-Setup.exe 那么 PortReporte 安装在 drive:\ProgramFiles\PortReporter 目录中。

图 3 显示的是默认安装时的过程

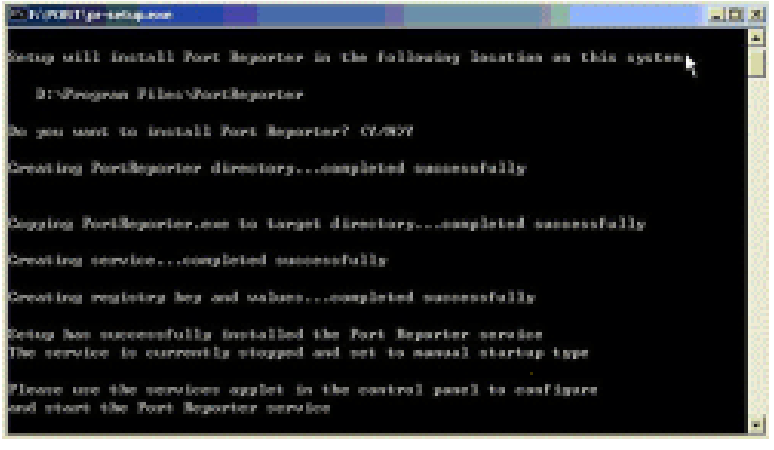

图 3

- -U

执行 pr-setup.exe-u 就可以卸载 PortReporter。

二、配置 PortReporter 服务

安装完成后 PortReporter 服务并不立即起作用，要运行它就必须手工启动这个服务。打开管理工具中的服务对话框，如图 4 所示启动服务，服务启动之后没有任何的提示，其实这个时候它已经在记录了。

图 4

2 个小技巧：启动服务时，如果不使用任何参数，日志文件被放在%systemroot%\System32\LogFiles\PortReporter 目录中，如果没有这个目录，启动服务时会自动新建该目录。

第一个技巧就是使用参数-ld 可以指定日志保存目录，如果你的计算机有多人同时用，把日志保存到你的个人目录不是更安全吗。比如可以这样输入参数：-ld ‘c:\programfiles\portreporter’。这样你的日志就被保存到 c:\programfiles\portreporter 目录了。

第二个技巧是修改日志文件大小，默认启动时日志最大为 5M，超过 5M 后，就建新的日志文件。使用-ls 参数可以设置日志文件大小（1M-100M），比如设置日

志文件大小为 8M：-ls8000，注意这里的单位是 KB。图 5 设置启动参数。

图 5

不过在 WindowsXP 中文版下用-ld 时不成功，显示错误如图 6

图 6

三、日志的浏览

打开保存日志文件的目录，默认是%systemroot%\System32\LogFiles\PortReporter，如果你使用-LD 修改了保存位置打开相应的目录，进入这个目录，我们可以看到三个文件：

PR-INITIAL-*.log

PR-PORTS-*.log

PR-PIDS-*.log

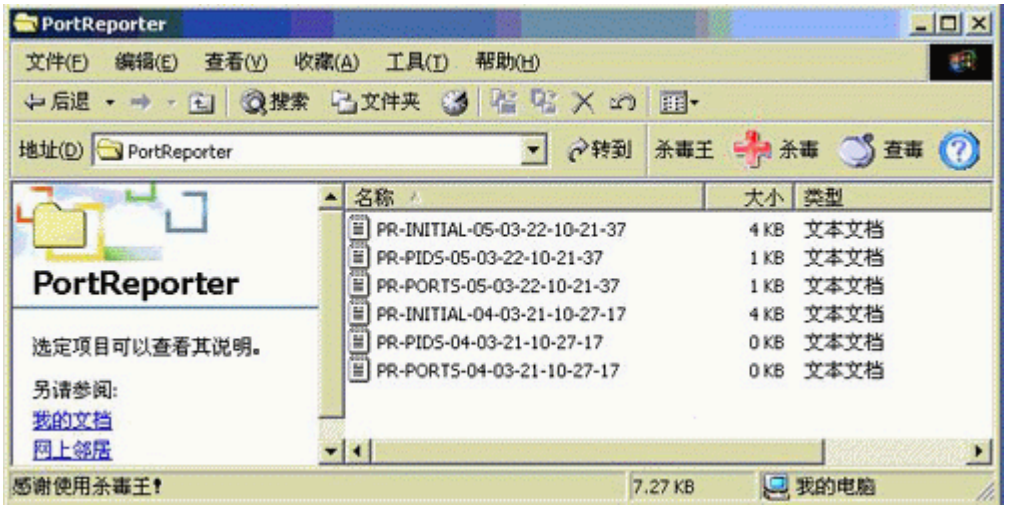

图 7

其中*代表日志文件创建时间，格式是 year-month-day-hour-minute-second 比如图中文件的创建时间是 2004 年 3 月 21 日 10 时 27 分 17 秒。图中有 6 个文件是因为我修改了系统时钟造成的，PortReporter 忠实的记录了这一过程。

PR-INITIAL-*.log 文件

这个文件主要记录了服务启动初始化的时候整个系统里面所有进程对网络的使用情况。具体每个人计算机不同，花费的时间不同，当然记录的内容也不同。

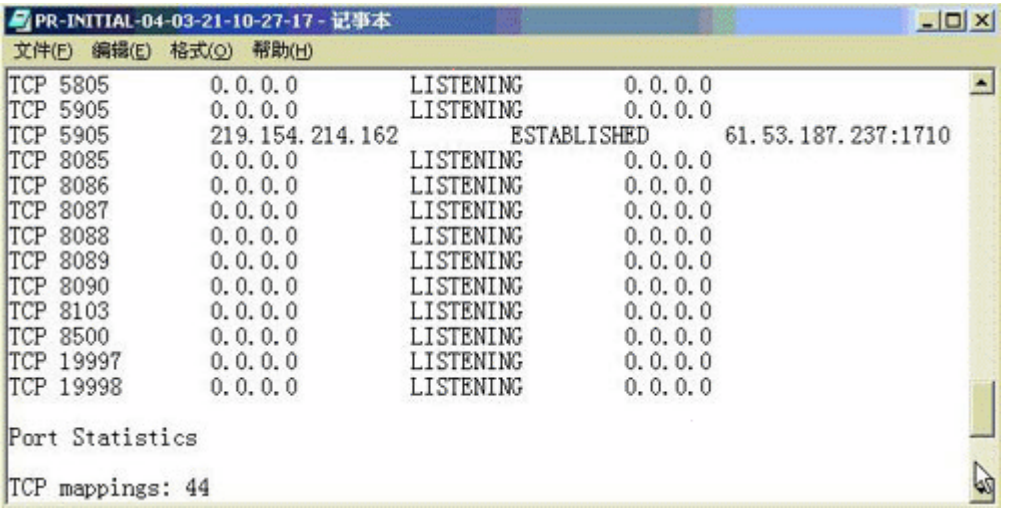

图 8

上图显示的是在 2000 启动服务得到的日志，其中的表头含义是：PID:Process（进程号）Port（端口）Local IP（本地 IP）State（状态）RemoteIP:Port（远程 IP 和端口）。图中显示我打开了 WINVNC 的服务端口 5905/5805，并且有一台 IP 为 61.53.187.237 的远程计算机正在连接（ESTABLISHED/活动连接状态）我的计算机（本地 IP219.154.214.162）；图中还显示我打开了 8085-8093 端口，这几个端口是提供 WWW 服务打开的端口（LISTENING/侦听状态），不是默认的 80。

如果日志文件比较大，浏览起来就费力了，这一点不如有些专业软件直观，如果能有树型结构就更方便阅读了，不过这个软件毕竟才 153K，功能奢侈不到那去。另外，PID 也可以通过任务管理器看到：单击进程选项卡，如果没有 PID 列，请单击查看、选择列，然后单击选中"PID"（进程标识符）复选框。单击标为"PID"的列标题，按进程的 PID 对进程进行排序。这样，就可以轻

易找到进程 ID。netstat-ano 命令可用来确定哪个进程（程序）侦听给定的端口。

PR-PIDS-*.log 文档

它针对每个 PID 都做了记录，也就是端口对应的进程。如果有新的程序被安装并且使用了新的 UDP 端口，那么这个文件将记录有关变化。

PR-PORTS-*.log 文件

这个文件记录了当前所有侦听端口，并且记录了每个端口所对应的应用程序（也许其中就有木马）。如果你浏览了网页比如 WWW.163.COM，或者打开了应用程序（QQ），该文件都做了详细的记录，包括通讯时间，两端 IP 和端口等信息，是不是有点被监视的感觉，显然木马也逃脱不了监视。PR-PORTS 的格式是这样的

date,time,protocol,localport,localIPaddress,remoteport,remoteIPaddress,PID,module,usercontext

04/3/21,10:27:9,TCP,4522,219.154.214.162,8080,61.53.187.157,1036,MyIE.exe,<MIE\PPOPE>

图 9 显示的是浏览 163 网站时的记录

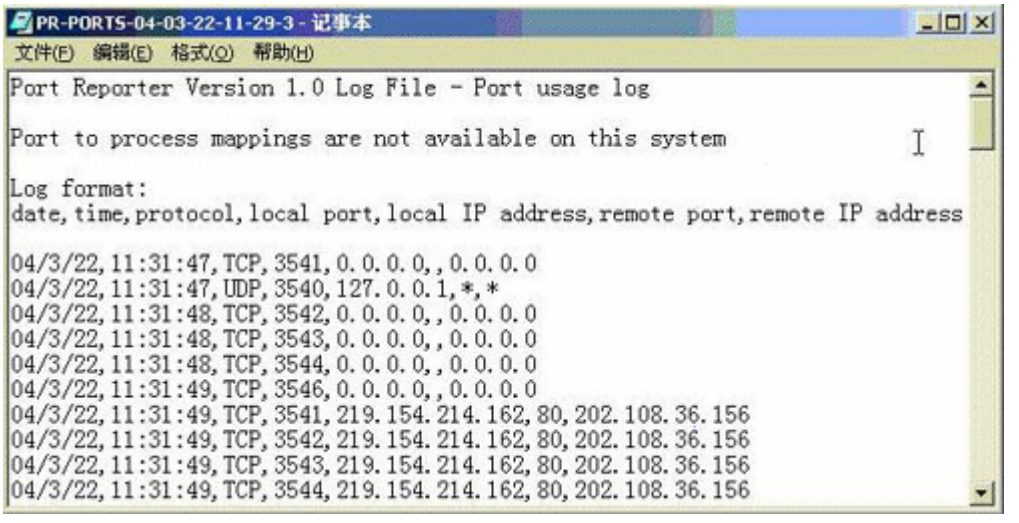

图 9

图 10 显示的是使用 WINVNC 时的通讯记录

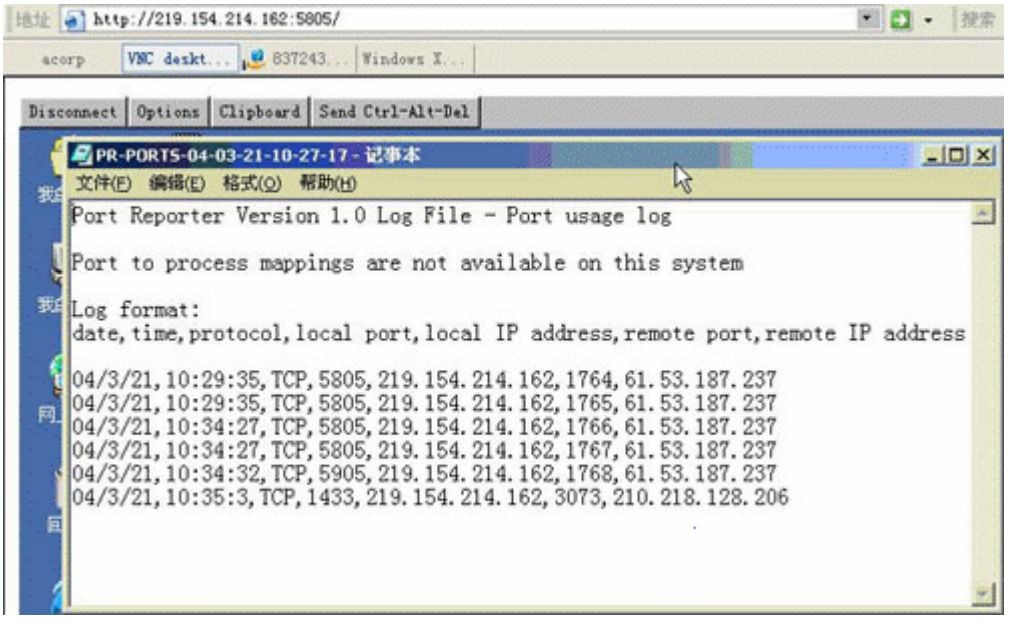

图 10

四、几个典型用途

1、**检查木马悄悄打开的端口**

一般中木马的计算机都会被木马打开一个或多个端口，等待远端连接该端口，通过这个端口，不怀好意的网客可以轻易获取重要信息甚至直接控制被中了木马的计算机。通过分析 portreporter **日志文件，对比知名的木马端口，你可以立即发现木马的行踪，有了** PID **可以查找到木马相对应的应用程序，接下来就是消灭木了。**

常见的木马端口可以在网上查到。

2、**关闭不必要的端口**

Windows **安装有许多的服务，他们大多会打开很多端口，这些端口直接暴露在外网中是很危险，通过分析过分析** portreporter **日志文件可以知道已经打开了哪些端口，如果确实需要就保留，不希望暴露的端口就坚决关闭。比如** 80 **是提供** WWW **服务的端口，如果你不提供** WWW **服务就没有必要开放** 80 **端口，一个危险的端口是** 23 **不是特别需要就关闭它。关闭端口的方法包括关闭相应的服务或使用网络防火墙。**

3、**谁动你的奶酪**

如果有人趁你不在的机会偷偷登录你的计算机，或者使用的是公共的计算机，而其中某个人下载安装了不该安装的软件或浏览恶意网页而中毒，通过分析 portreporter **日志文件可以查询具体登录的网址，并且能发现恶意网页的** IP **和端口以及相应的应用程序，屏蔽或清除恶意代码也就有了线索。**

4、**谁登录了共享目录**

如果要监视谁正在使用的共享目录，可以通过 Windows **的有关组件看到，比如在** Windows98/Me **中使用“网**

络监视器”可以查看目前谁在使用你的计算机上的资源，在 Windows2000/XP 中，网络监视器不再监测访问本机的连接及来访者的访问信息，但来可以通过下面的方法监视：控制面板-管理工具-计算机管理，在右边的目录树中双击展开“共享文件夹”，下面共有三个选项：“共享”、“会话”和“打开文件”等。但是你不能 24 小说盯着屏幕，也许有人上传了乱七八糟的文件，这时使用 portreporter 服务 24 小时动态监视，通过日志就能查出谁使用了你的共享目录，包括时间和 IP 等信息都在日志中有详细的记载。

总结

PortReporter 是以后台服务的方式运行的，只要你启用她，她就默默的监视并记录网络通讯过程。显然，日志中的信息对发现木马和解决网络问题都非常有用，通过分析日志对提高你的计算机安全性能也大有帮助。而且这个软件是微软发布的，毕竟是自家的东西，应该和 Windows 结合更紧密，让用户更有安全感。

打造系统的安全防线

提到 HackerEliminator 你可能还很陌生，但是如果提到风靡一时的 LockDown2000，想必大家就不会陌生了。HackerEliminator 其实就是 LockDown2000 的新版本。通过 HackerEliminator 我们可以实时监视系统所有正在运行的进程，当发现异常的进程就会及时报警，防止骇客和木马程序的攻击，只需 5 分钟就可打造系统的安全防线。

软件基本信息

软件名称：HackerEliminator

软件大小：2598KB

软件语言：**简体中文**

软件类别：**共享版**

运行环境：Win9X/Me/NT/2000/XP

下载地址：http://www.mydown.com

一、把木马“揪’出来

1.扫描病毒

运行 HackerEliminator，在左侧的功能窗口中选择“扫描器”(图 1)，接着在右侧的窗口中通过文件夹图标按钮来选择要扫描的路径，可以是某个磁盘或者某个文件夹，注意不能选择“我的电脑”。之后点击“扫描”按钮就可以对磁盘或文件夹进行全方位的扫描。如果发现木马程序，会将它们“揪”出来，显示在窗口中。右键单击该木马，还可以通过快捷菜单中的命令删除该文件、删除该文件所在的文件夹以及浏览文件夹等。

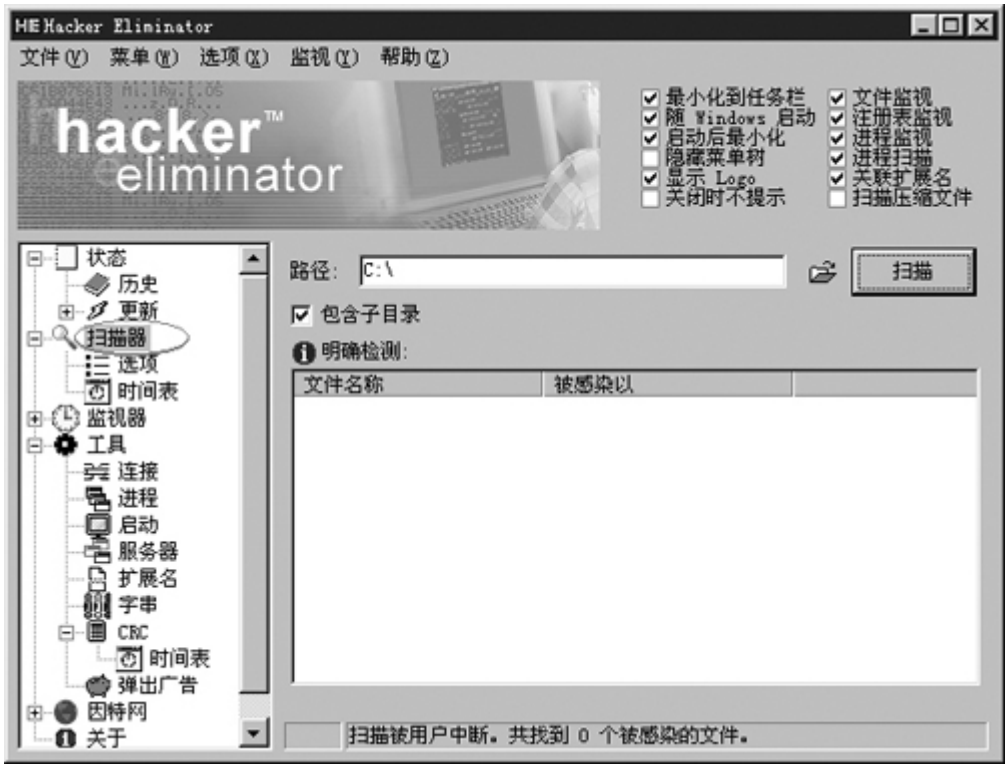

图 1

2.**扫描设置**

在默认的情况下，“HackerEliminator”**可以扫描包括** BAT、COM、EXE、DLL、VBS、VXD **等扩展名的文件。其实，很多木马病毒程序都是隐藏在压缩文件中的，有的病毒还可以使用其它的扩展名来伪装自己。这时，为了让扫描更加彻底，你可以在主界面左侧选择“扫描器→选项”(图** 2)，**在打开的窗口中选中“扫描压缩文件”，在窗口下方点击“添加扩展名”按钮来添加其它扩展名，比如** JS、WSH、HTT **等。这样就不会放过任何一个病毒。**

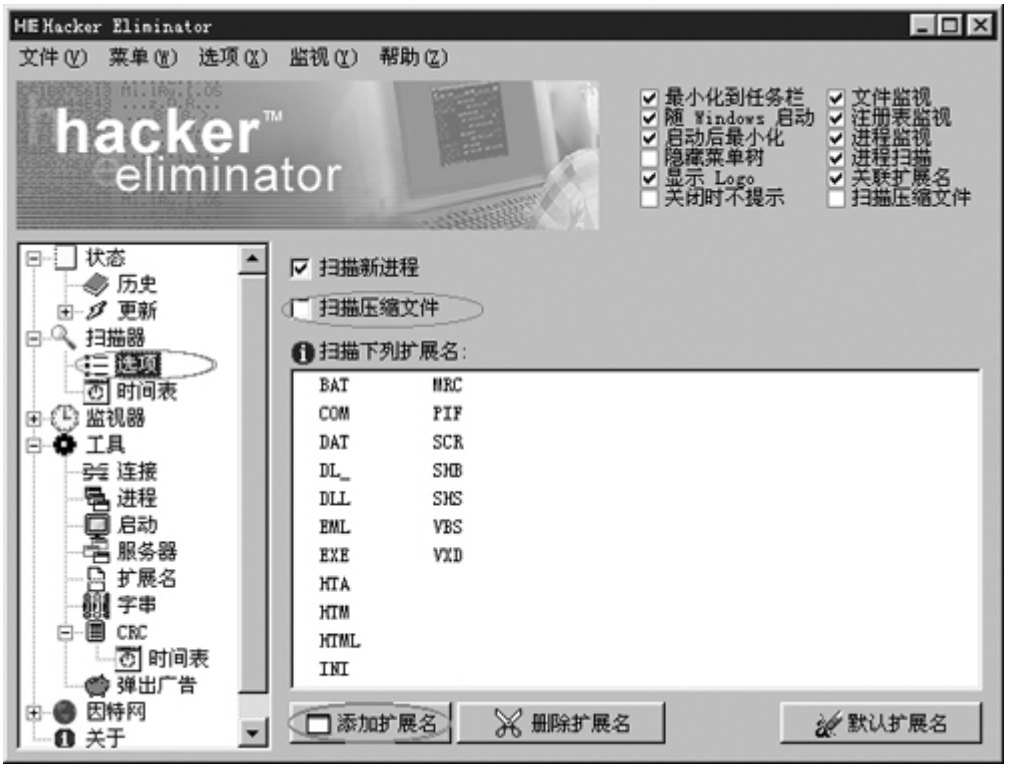

图 2

另外，通过“时间表”功能，你可以为某个文件或文件夹设置定时扫描。

二、打造安全防线

1.设置监视的对象

除了扫描功能外，HackerEliminator 可以实时对系统文件、注册表文件以及系统进程进行监视。如果发生异常，比如运行新的应用程序，它就会自动弹出进程窗口来报警。如果发现并没有运行该程序，可以点击“关闭进程”，打开相应的文件夹查看详细的情况。如果要监视更多的内容，可以点击相应的项目，比如你还想监视其它的文件，可以在左侧的窗口中选择“文件”，接着在窗

口右下方点击“添加文件”按钮来添加其它要监视的文件，可以是任何类型的文件。

2.活用监视工具

HackerEliminator 还提供了连接、进程、启动、服务器、扩展名等工具，通过“连接”工具你可以了解到当前网络所有数据包的情况，包括对 TCP、UDP 监听，提供 IP 地址、本地端口、远端端口、监听状态信息，通过这些你可以分析当前数据包发送和接收情况，防止骇客的攻击。通过“进程”工具，你可以查看当前运行的所有进程情况，提供是否联网、进程路径等非常有用的功能列表。通过这些，你可以了解到某个进程是否访问网络，比如常见的木马程序就会自动连网。通过“启动”工具，还可以轻松管理系统的启动项目，点击窗口下方的“从启动项删除”按钮可以轻松删除不需要启动的项。

现在，个人安全防线已经打造完毕，你可以在新春之际安心地上网了。

利用 IRIS 学习 TCP/IP

一、前言

目前，网络的速度发展非常快，学习网络的人也越来越多，稍有网络常识的人都知道 TCP/IP 协议是网络的基础，是 Internet 的语言，可以说没有 TCP/IP 协议就没有互联网的今天。目前搞网络的人非常多，许多人就是从一把夹线钳，一个测线器联网开始接触网络的，如果只是联网玩玩，知道几个 Ping 之类的命令就行了，如果想在网络上有更多的发展不管是黑道还是红道，必须要