用户使用说明

1. **产品简介：**

软件名称：PcGuard。

我开发的PcGuard安全系列工具包含四大模块：进程管理模块、注册表监控模块、文件监控模块、病毒查杀软件模块。

进程管理，进程管理模块可以对本机的进程进行列表，并且可以查看所有进程的映像名称以及PID，当前占用内存大小，已运行时间，以及文件映像的路径。并且在程序右上角用户可以单击显示模块信息按钮，显示进程模块信息。用户还可以对指定的项进行右键弹出用户。单击菜单项中进行相应的操作，其中包括了刷新，终止进程，暂停进程，恢复进程，文件所在，百度一下，复制进程路径，调用注册表监视。（进程管理程序的外观在不同时间启动是不同的，程序采用随机数动态产生皮肤）

注册表监视模块，对用户所有程序进行注册表监视，主要监视子键创建，子键删除，键值设置，键值删除，键值查询等。此程序主界面有两个一级菜单，用户可以在监视设置里进行相应的动作的监视设置。此外用户还可以在工具菜单里调用注册表编辑器,进程管理工具进行编辑和对特定程序进行监视设置。并且用户可以保存监视记录。监控的核心主要利用HOOK及Detours技术，拦截系统的API。

病毒查杀模块，可以进行磁盘上文件的扫描，能够查杀内存中的病毒进程，并对扫描出的病毒进行查杀，主要运行流程：选择扫描目标——开始扫描硬盘——把文件加入扫描队列——按多线程病毒库对比（照特征码识别出病毒文件）——查找病毒进程——结束病毒进程——把可疑文件加入可疑文件队列中——删除病毒启动设置——列出可疑文件——其余清理。杀毒引擎核心用Window API编程和多线程编程，保证杀毒的速度及效率。

文件监控模块可以对指定的文件夹进行监控，并且可以通过单击设置按钮，弹出设置对话框可以设置各种监控选项，并且可以把用户此次的设置保存在配置文件.ini里，下次启动程序时程序按照上次设置进行相应的监控。对文件的监控可以获得目录中文件的行为、并记录是哪个文件，以及文件行为的精确时间。此外用户可以在监控到的选项上单击右键弹出菜单，用户可以在菜单中选择转到相应文件的操作。此外用户可以选择保存监视到得文件修改记录，还可以导出记录到相应的路径中。监控的核心部分用Window API编程和多线程编程，保证软件的运行效率。

1. **系统要求**：

操作系统： Windows 2000， XP， Vista或Windows 7

处理器： Pentium II processor 以上

内存： 64M以上

硬盘： 需要至少5M可用空间

显示器： 分辨率1024x768或以上，32位真彩色

外设： 鼠标、键盘。

1. **软件安装及设置：**

本软件为绿色软件，不需要安装驱动文件，不会修改任何注册表键值。解压Bin压缩包直接运行PcGuard.exe即可。

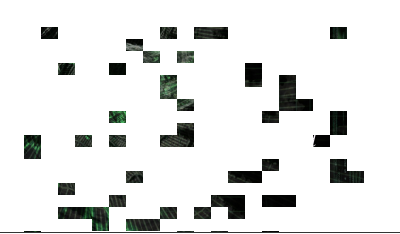
软件主程序为PcGuard.exe，四个模块分别为独立的可执行文件，分别为ProcessManage.exe, RegMonitor.exe, FileMonitor.exe , VirusKiller.exe。运行时需要将这五个个程序放在Bin文件夹下。其中杀毒软件FileMonitor.exe ，VirusKiller.exe还分别需要配置Config.ini文件，病毒库文件virus.ini，这几个文件需要在同一个目录下。

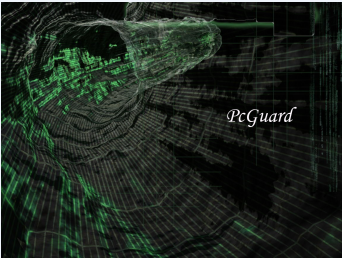
1. **软件使用：**

主界面

1. 软件解压后，应该有一个可执行文件PcGuard.exe，此为安全工具主文件，在文件夹Tools目录下，文件夹中有各个子模块程序。
2. 打开PcGuard.exe即看到主界面如下图，分四个模块：注册表监控，杀毒软件模块，文件监控模块，进程管理模块。

3.刚开始的动画界面显示，





最后界面：



4.程序主界面的上半面主要是四个按钮单击按钮可以启动相应的程序。

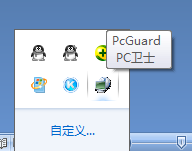
程序中间相应的显示对应的程序有没有启动如下图：



5.程序左下角滚动显示文字 Virus-free PC, enjoy the Internet of life!

6.右下角 鼠标放在联系作者框上是鼠标会变成手指形状，表示这是超链接 ，用户单击此图标可以进入我的博客和我联系。

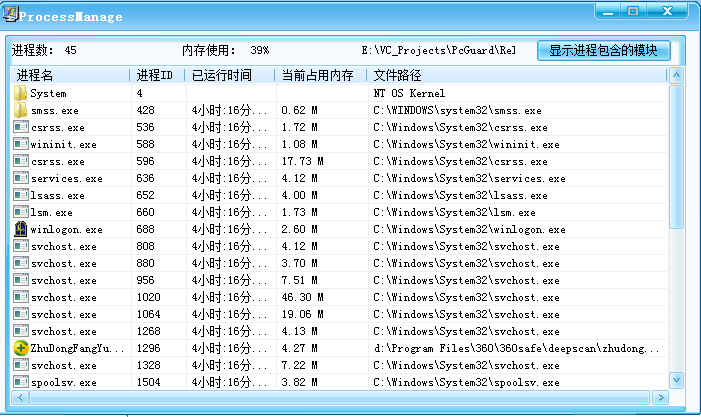
7. 当程序最小化是可以任务托盘

双击托盘图标可以显示程序主界面。右键托盘图标可以显示托盘菜单可以选择显示界面和退出程序。

进程管理模块

8.在安全工具中，进程管理工具必不可少。在主界面点击“进程管理”即可打开进程管理模块。主界面如下：

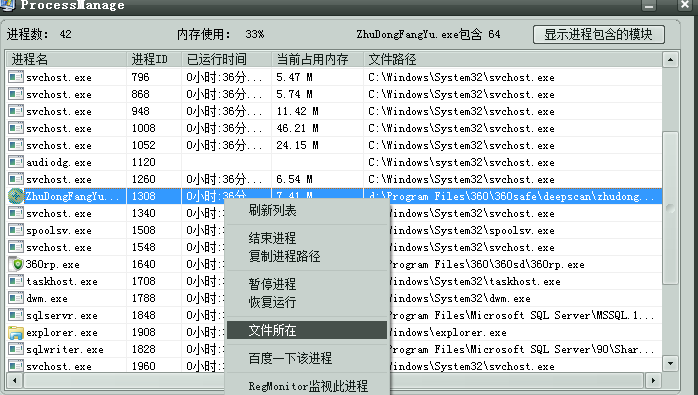


显示模块信息如图：



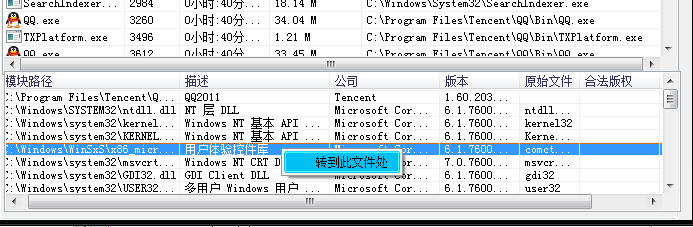
9.进程管理，进程管理模块可以对本机的进程进行列表，并且可以查看所有进程的映像名称以及PID，当前占用内存大小，已运行时间，以及文件映像的路径。并且在程序右上角用户可以单击显示模块信息按钮，显示进程模块信息。用户还可以对指定的项进行右键弹出用户。单击菜单项中进行相应的操作，其中包括了刷新，终止进程，暂停进程，恢复进程，文件所在，百度一下，复制进程路径，调用注册表监视。（进程管理程序的外观在不同时间启动是不同的，程序采用随机数动态产生皮肤）

右键弹出菜单根据需要来进行操作。



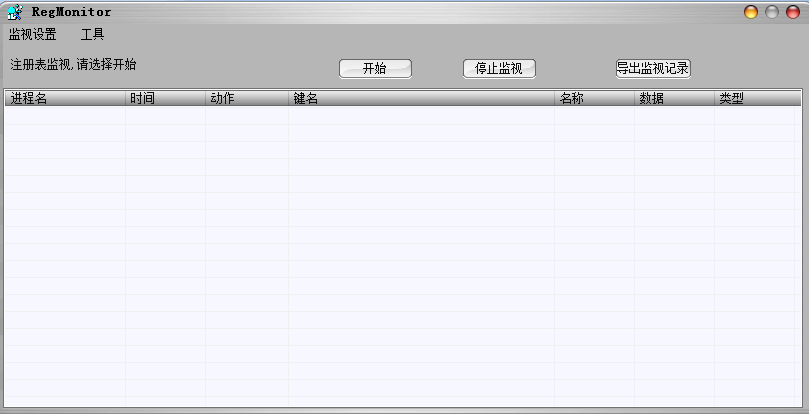
10. 进程管理器的RegMonitor监视此进程主要利用了进程间通信机制，但要注意进程间权限问题。

11. 进程模块显示部分主要显示此进程的一些调用模块信息。可以显示每个dll模块的路径，描述，公司，版本，原始文件，合法版权，修改时间等信息。用户可以有有右键弹出菜单，转到此文件处.



**注册表监视模块**

主界面上点击“文件监视”即可打开文件监控模块，界面如下图：



12.注册表监视模块主要利用hook技术及Detours 技术来实现对指定的程序或者所有程序进行注册表行为拦截。

13 .注册表监视模块，对用户所有程序进行注册表监视，主要监视子键创建，子键删除，键值设置，键值删除，键值查询等。此程序主界面有两个一级菜单，用户可以在监视设置里进行相应的动作的监视设置。此外用户还可以在工具菜单里调用注册表编辑器,进程管理工具进行编辑和对特定程序进行监视设置。并且用户可以保存监视记录。

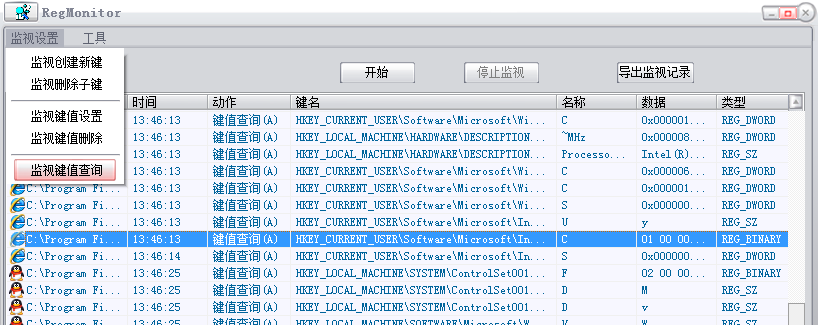
如图：拦截结果。



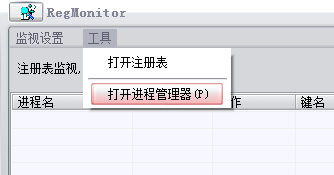
点击监控设置弹出菜单，选择相应的监视行为，如下图：



指定监视特定的行为如下图(只监视键值查询)：



用户可以单击工具菜单弹出相应的菜单，用户可以根据所需打开注册表编辑，或选择进程管理器查看进程，监视指定的进程。



用户可以保存监视的结果到指定的路径中如下图：



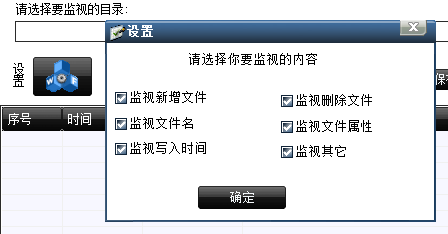
文件监控模块

主界面上点击“文件监视”即可打开文件监控模块，界面如下图：



14.首先在要监视的目录中输入相应的目录，或点击右侧的浏览按钮进行选择。然后可以点击设置按钮监视选项（默认情况下调用以前的监控设置），比如是否监视新增文件，是否监视文件属性的改变、文件大小的改变等。

监视设置如下图：

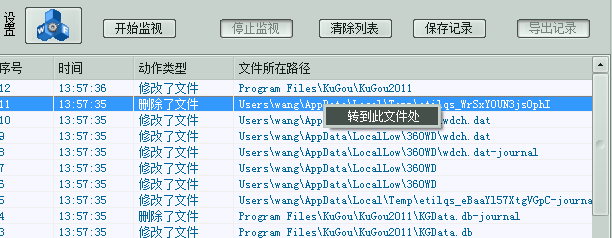


设置完毕后，点击“开始监视”软件即开始监视。期间被监视对象相应的改动会显示在下面的列表中，项目包括事件的高精度事件、文件路径以及文件产生的动作。

15点击“停止监视”可以停止对目录的监视。点击“清除列表”可以对列表中的日志进行清除，重新开始监视。

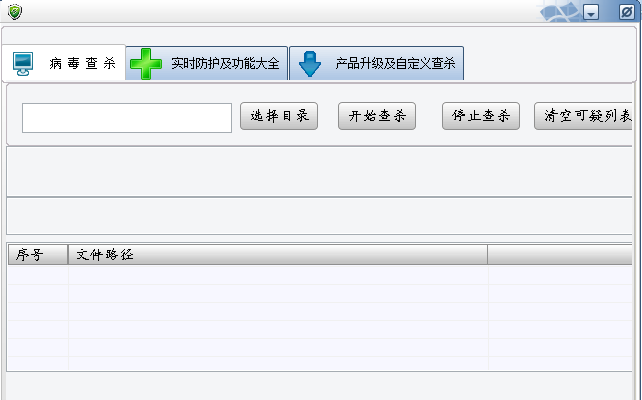
16.在监视过程中，不能够对监视选项进行设置，目录路径的改变也无效。但是可以对日志进行清除。监视完成后用户更具需要保存监视记录。

用户可以单击右键弹出菜单 转到变化文件处。如下图：

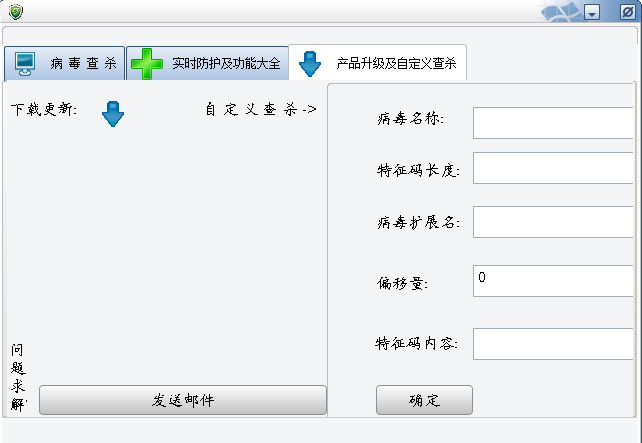


病毒查杀模块

16.点击“病毒查杀”，即进入病毒查杀模块，此模块又包含三个Tab。软件界面如下：

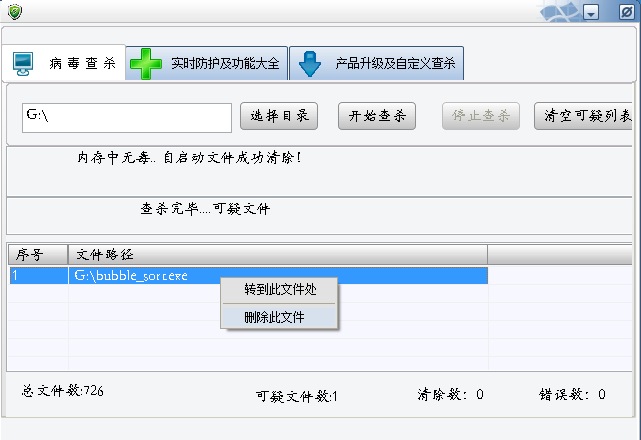






17.点击选择目录，其中可以选择本地计算机上所有的盘符或者文件，选择一个，然后点击“开始查杀”即可对相应的分区进行杀毒。

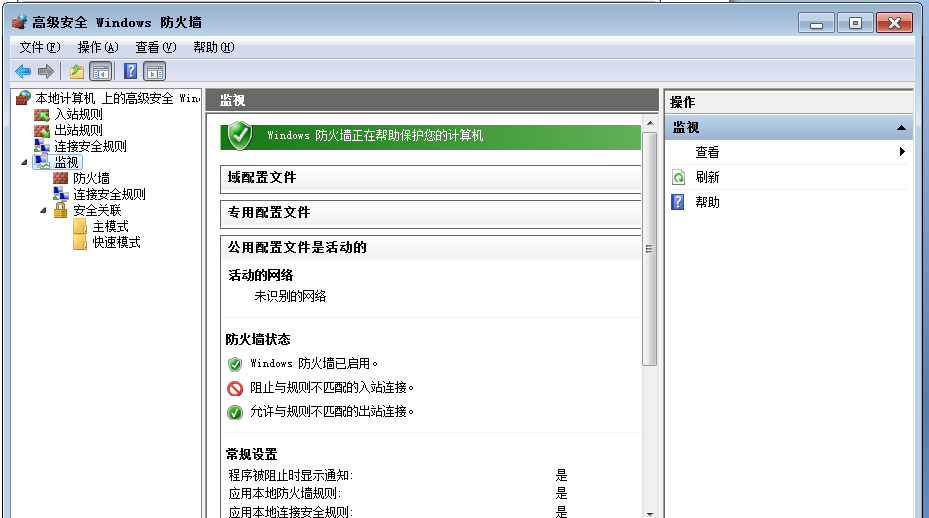
在软件扫描磁盘的过程中，会显示文件扫描进度。若发现病毒，则会尝试对病毒进行查杀以及内存（进程）查杀加入可疑文件列表，最后清楚所有磁盘下的autorun.inf文件。查杀过程会显示此文件是否安全。最后会将病毒文件、病毒详情及查杀结果显示出来。文件扫描完毕后，会出现总结，总结共扫描了多少文件、查杀了多少病毒，查杀错误等信息。



如下图显示扫描结果：

18. 实时防护及功能大全模块。主要调用windows系统自带的安全相关的工具

用户可以在这样的工具里设置防火墙，出入站等非常详细的设置如下图：

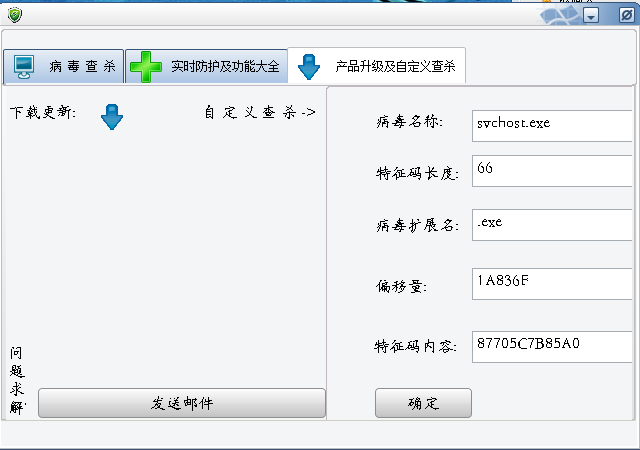


18. 产品升级及自定义查杀 Tab 页

主要可以进行病毒库的升级 单击 下载小图标可以下载到最新的病毒库。

左下角是问题求解，单击发送邮件按钮可以给作者发送邮件进行问题探讨和交流。（这需要用户的电脑有OutLook邮件软件）

程序右边是自定义查杀。



1. **具体特性：**

此面向系统安全的软件设计工具都是本人自己独立开发（其中遇到的问题主要通过论坛求解和向学长求解），其中引入了Skin#（一个可以美化程序界面的库）进行了相应的美化（采用运行期间动态装载减少软件启动时间和防止库丢失软件不能运行）,并且编写了相应的动态链接库进行系统监控，提高程序性能。编程语言使用C++，采用windows系统底层API，效率高；编译软件使用Visual C++ 6.0，这个编译器比较经典所以所以选用它，此外需要安装较新的Platform SDKMicrosoft （Platform SDK for Windows 2003（注意安装好了一定要把 include lib 路径重新排好序）,微软detours库等）。核心部分都是直接调用操作系统的API函数，保证了高效率的运行。部分程序能够多线程运行，使在多核CPU上更大的提升效率。整个安全工具小巧易用能够满足用户的多数需求。

**6、常见问题解答**

Q：为什么在主界面打开模块时，提示“皮肤库加载失败”？

A: SkinH.dll模块需要放置在Bin文件夹下，若此模块丢失，或放置位置不正确，则主界面中不能够加载此模块。查看是否把SkinH.dll 放置在Bin目录下。

Q：为什么没有提示“皮肤库加载失败”但软件运行界面没有被美化？

A：请注意查看你的Bin文件夹下包含skin子文件项吗，如没有可以重新加压Bin压缩包或者到作者博客上下载此文件。

Q：为什么软件单击监视按钮，但仍不能监视到动作？

A:应该是权限问题，请右键以管理员身份重新运行此软件。

Q：打开病毒查杀软件时为什么会提示"病毒库文件加载失败，无法进行病毒查杀工作!"？

A：毒查杀软件需要与病毒库Virus.ini在同一个目录，而且不能够随便更改文件名。若文件名被更改，或文件丢失，则会出现找不到病毒库的现象。若找不到此文件可以下载更新或者在 产品升级及自定义查杀Tab页中重新定义查杀方法。

Q：现在的病毒库完善吗，怎样使用病毒查杀软件？

A：还不完善，只包含了软件测试用的几个模拟病毒样本，还不能够真正用于杀毒。软件包自带了几个模拟病毒样本，是几个小程序，并不是病毒，对计算机没有任何危害。病毒库需要以后进一步更新。

测试时将压缩包内的几个程序解压出来，为了更快速的测试，可以放到文件数量比较少的磁盘分区上。然后打开病毒查杀软件，选择放有模拟病毒样本的分区，点击“开始查杀”，等扫描到模拟病毒样本时，就会将其作为病毒对待，会显示病毒信息，并进行查杀内存，并把结果列在可疑文件序列中。

Q：怎样与作者交流？

A：可以用QQ：840450770或 E-mail：[wangdanit@126.com](mailto:wangdanit@126.com)