



# 计算机安全与维护

## 第五章 **Windows** 系统安全维护与加固基础



## 本章内容提要

- 第三方安全软件介绍与使用
- 组策略编辑器
- 注册表安全
- 访问控制加固
- UAC



## 第三方安全软件介绍与使用

- 本节介绍两款第三方安全软件
- SREng
  - System Repair Engineer, 简称 SREng, 是 KZTechs.COM 网站站长 Smallfrogs 开发的一款计算机安全辅助和系统维护辅助软件
  - <http://weibo.com/smallfrogs> 2005年起至今就职于金山
- IceSword
  - 冰刃是一款功能强大的杀毒辅助软件, 号称专门针对功能强大的内核级后门而设计, 但是仅仅支持Windows 2000/XP/2003操作系统, 不支持Windows 7及之后版本的操作系统
  - 作者已于2007年正式加入360, 参与360安全卫士及相关产品的研发



- 该软件主要用于发现、发掘潜在的系统故障和大多数由于计算机病毒造成的破坏，并提供一系列的修改建议和自动修复方法
- 可以自己诊断操作系统可能存在的普遍性问题，即使是计算机的初学者，也可以使用 System Repair Engineer (SREng) 的智能扫描功能将您系统的概况生成一份简要的日志，然后将该日志传送给对操作系统熟悉的朋友或网友，在他们的帮助下解决您系统可能存在的问题
- 最新版本2.8.4.1331，更新于2011年1月16日



- SREng软件的特点

- 提供一个能够较快诊断出系统常见故障的工具
- 能够修复大多数常见的故障
- 能够生产一个扫描报告
- 能够运行于多种操作系统平台下，支持多语言界面
- 具备一定的自动检测修复能力
- 便于扩充且能够以最小的代价进行扩充



- SREng的功能划分为四大部分
- 启动项目的编辑
  - 启动项允许/禁用/删除/编辑;启动配置文件配置;服务配置;驱动配置;系统配置/修复
- 系统配置/修复
  - 常见文件关联自动修复;系统关键数据修复;浏览器加载项管理;HOSTS文件管理;Winsock Provider 修复/重置;安全模式重置等



- 智能扫描/诊断

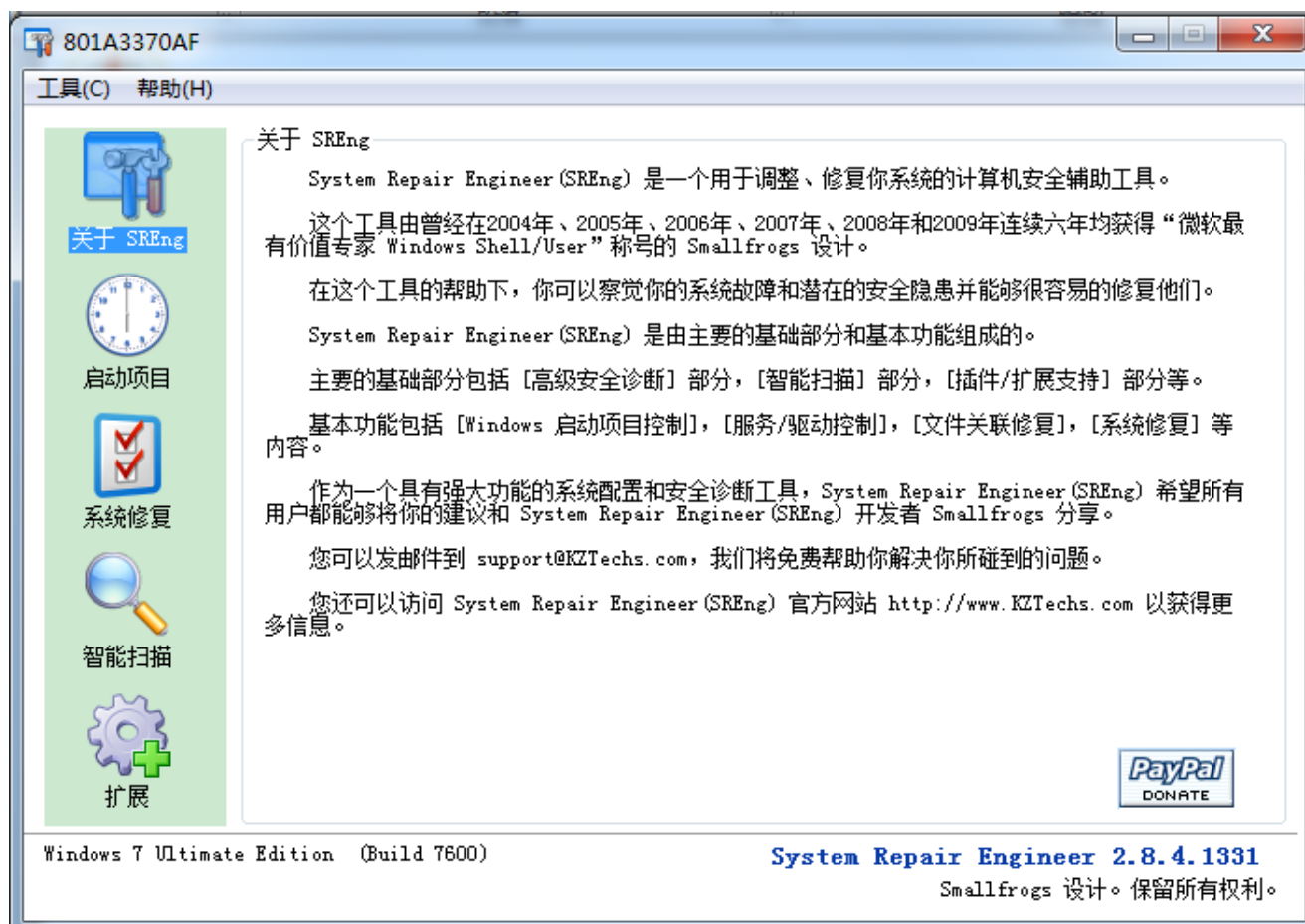
- 基于数字签名认证的高级安全诊断组件;API HOOK 警告提示/修复;隐藏进程检测;扫描报告提供;可疑文件自动提取等等

- 扩展插件

- 第三方插件支持;自定义扩展批处理数据支持



- SREng的主界面，最新版本为2.8.4.1331

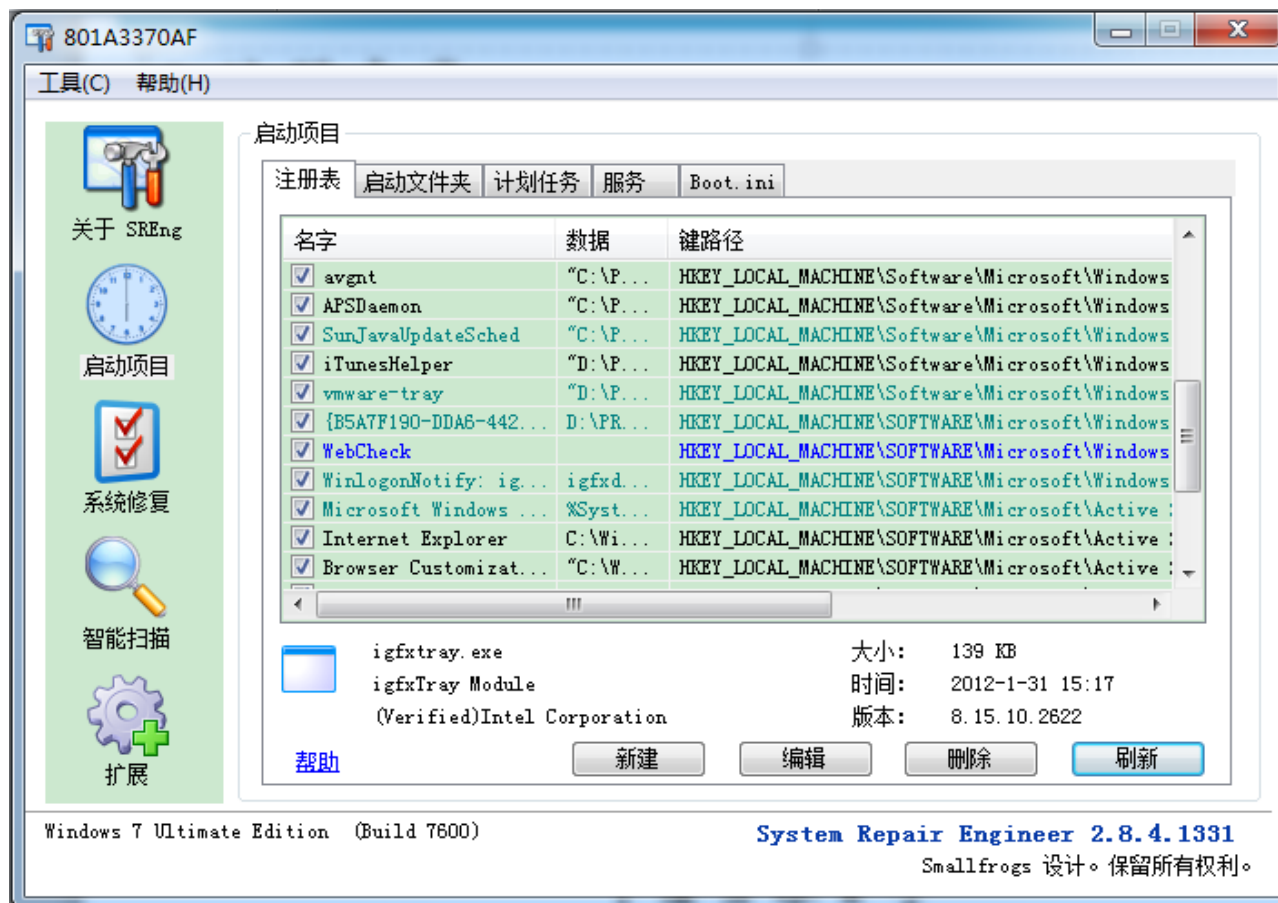






# SREng

## • 注册表类

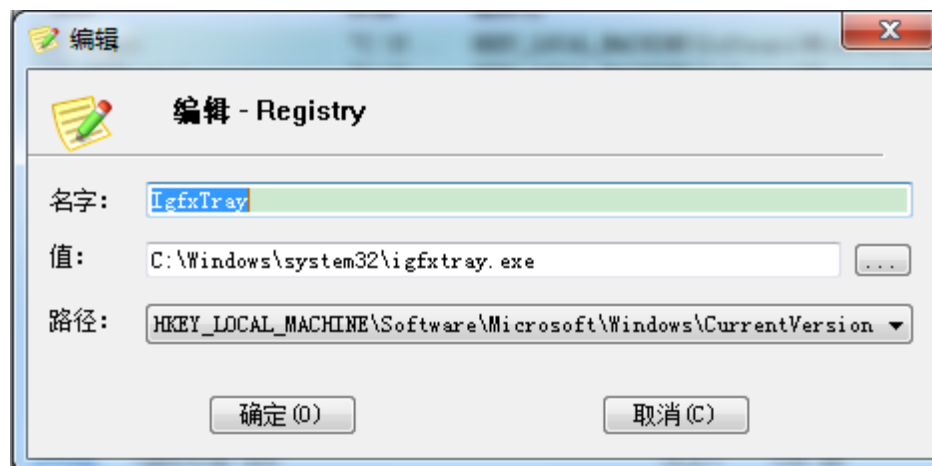




- 注册表类的启动项目由十多个注册表键值所含数据组成。包括常见的  
HKLM\Software\Microsoft\Windows\CurrentVersion\Run、  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run 等
- 如果 System Repair Engineer 发现默认的键值被修改成非默认值，且这个键值经常被计算机病毒修改，那么会弹出一个警告提示提醒用户注意

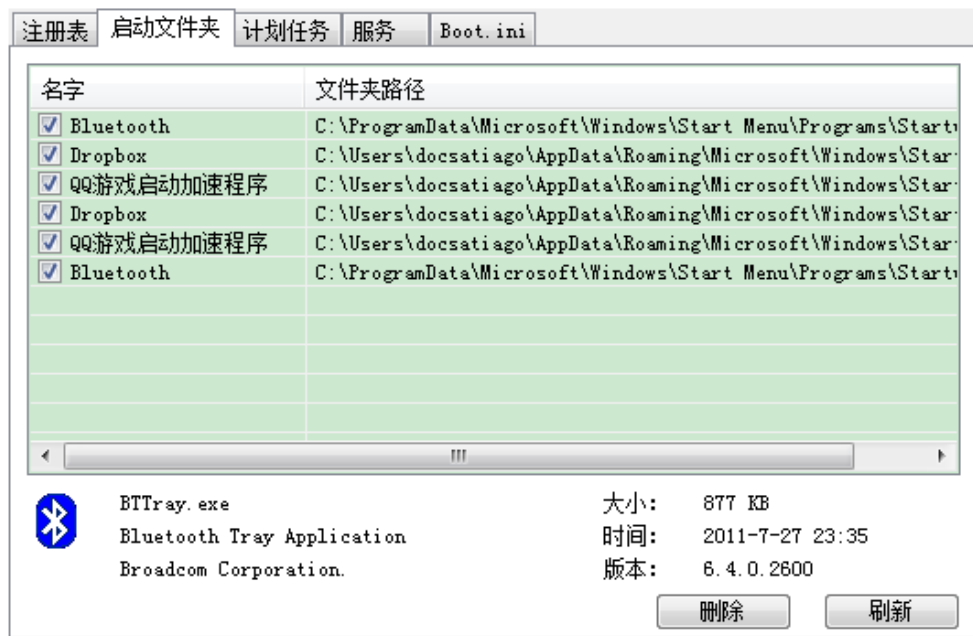


- 如果 SREng 发现一个可疑的项目，那么会以颜色高亮显示  
高危项目：红色  
未知安全等级项目：蓝色  
安全项目：绿色
- 可以对注册表值进行修改



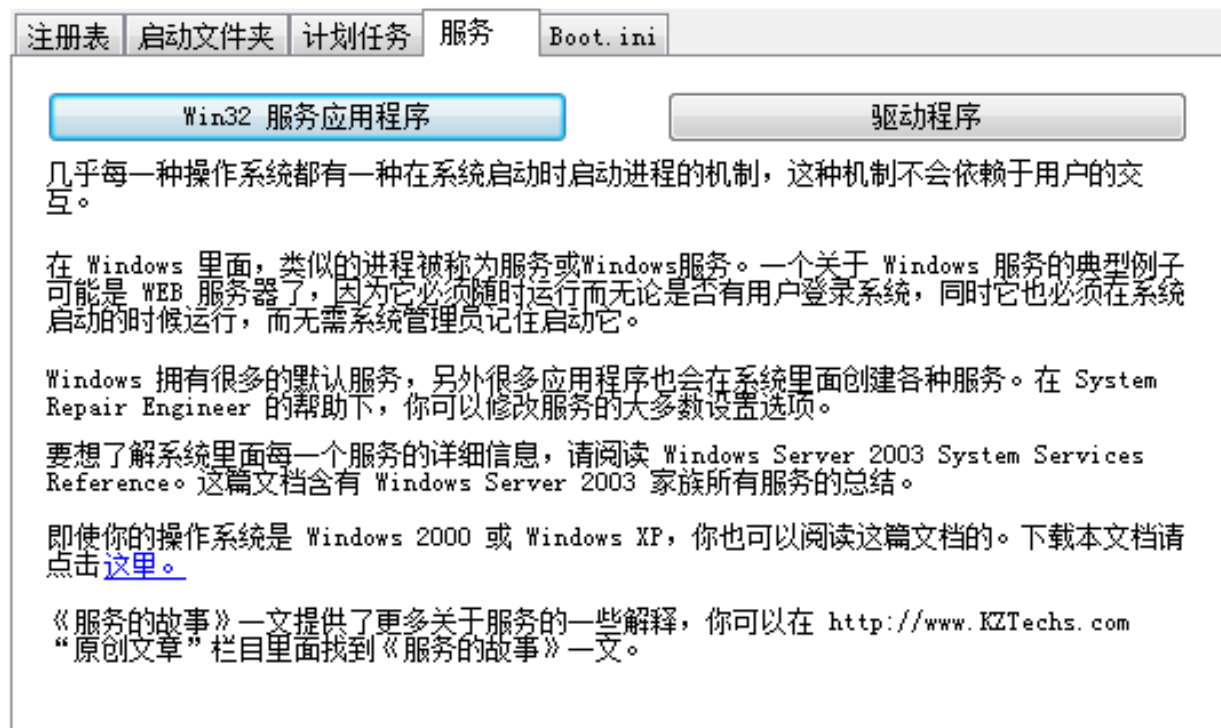


- 启动文件夹分作公用启动文件夹和私有启动文件夹。公用启动文件夹里面的启动快捷方式对所有用户均有效，而私有启动文件夹里面的快捷方式仅对当前用户有效



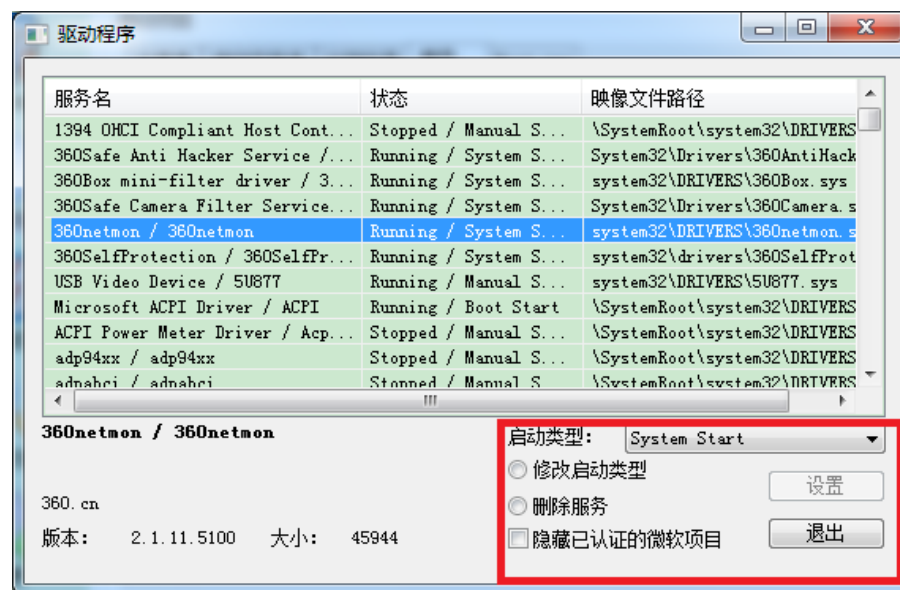
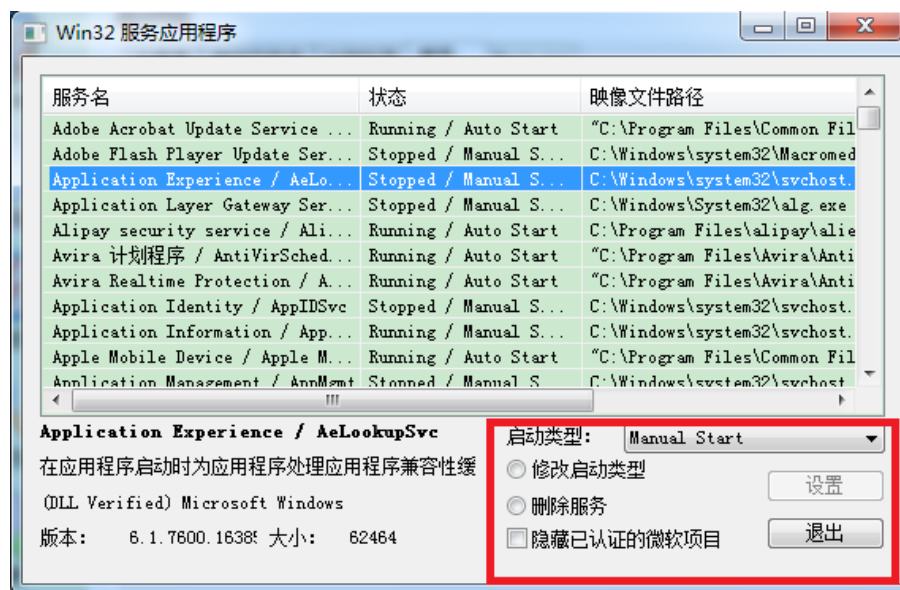


- Win32服务配置模块被分为两类：Win32服务应用程序和驱动程序



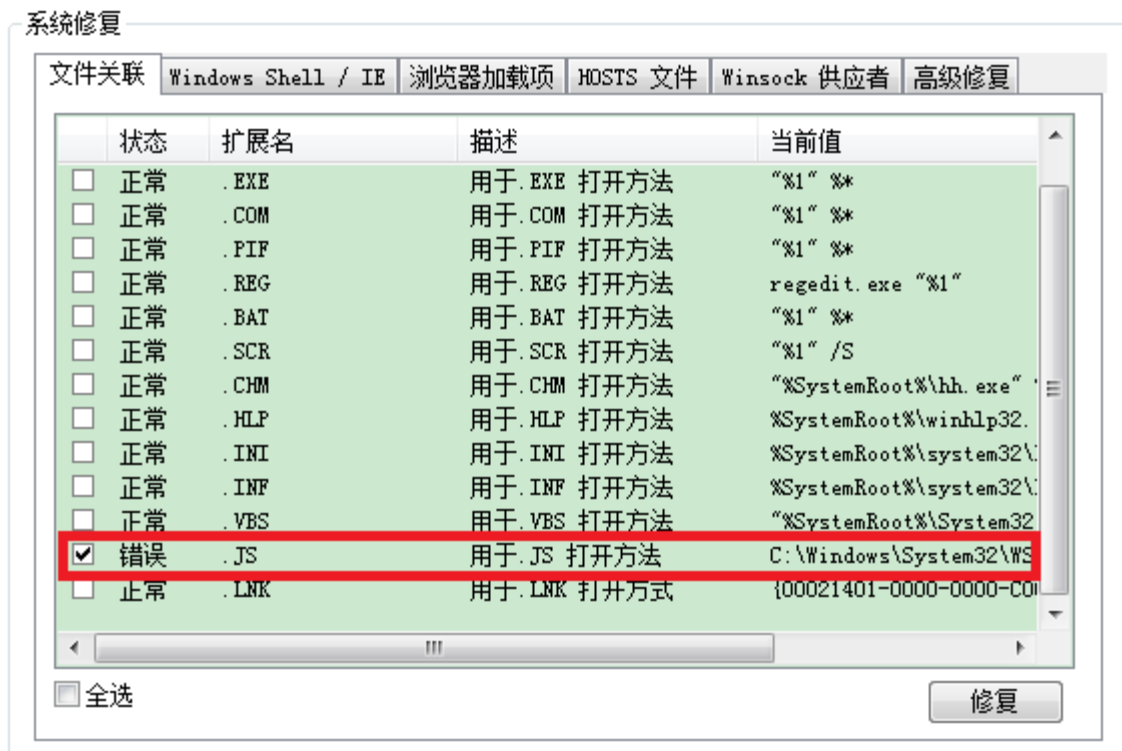


- 列表中是对应的服务项，想改变一个服务的启动类型，点击“修改启动类型”，点击“设置”即可，也可删除服务



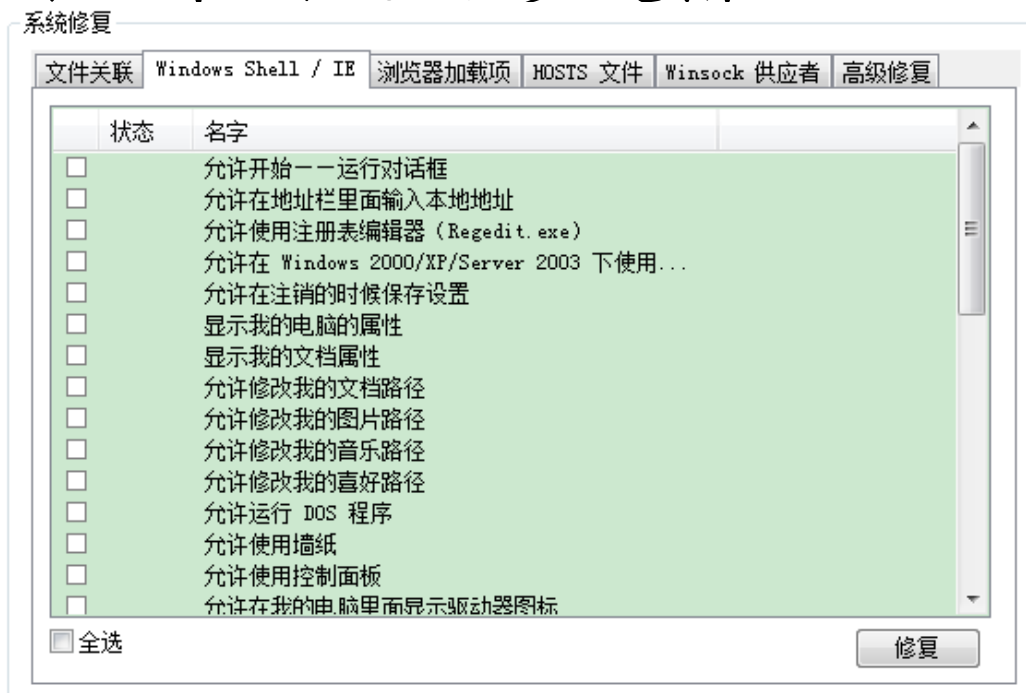


- 文件关联部分在原有基础上增加了自动侦测功能，对于非默认文件关联值会显示一个错误标示并且自动选中修复复选框





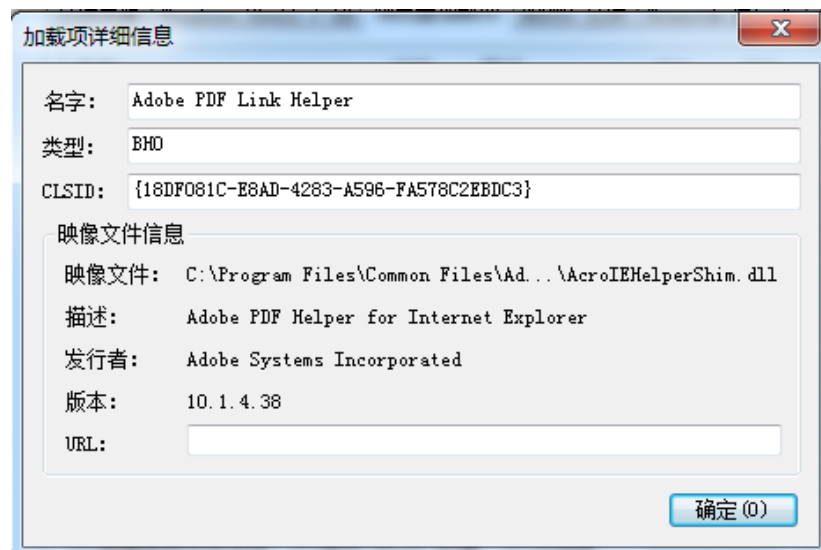
- Windows Shell 主要指 Windows 外壳程序，包括资源管理等。在 SREng 里面，重新对 Windows Shell 和 IE 进行了归类处理，合并了一些针对同一个问题的修复措施





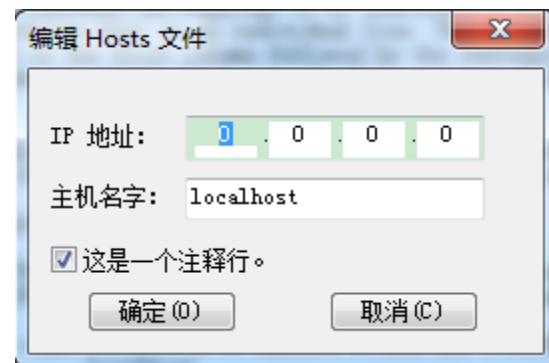
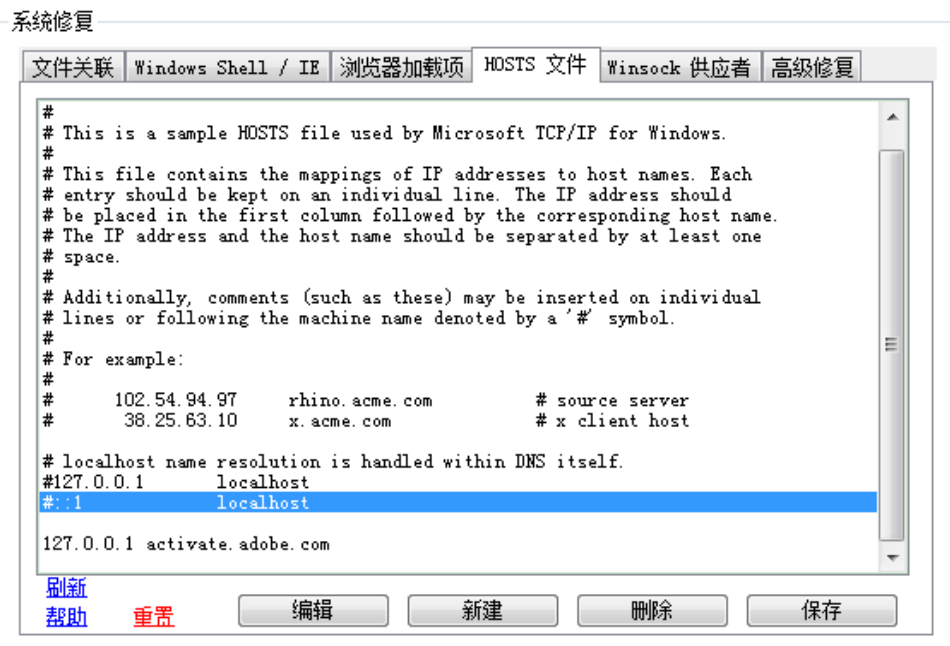


- 浏览器加载项是目前大多数“流氓软件”使用的一种自我加载方法。增加了浏览器加载项管理功能。提供了删除/禁用/查看浏览器加载项等功能。另外，还额外提供了显示 Shell 扩展内容的功能





- HOSTS文件是一个用于将主机名和IP地址对应起来的文件。目前被很多计算机病毒用作限制用户进行升级或限制访问某些网站。提供了对HOSTS文件的配置、管理功能



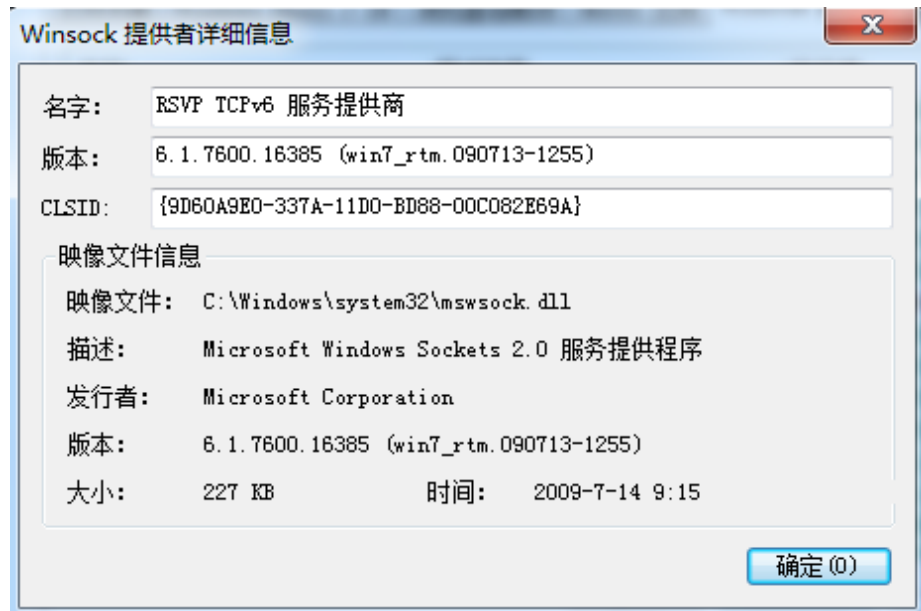


- Winsock Provider 用于提供系统网络访问，如果 Winsock Provider 出现问题，将导致不能使用网络功能，包括ICMP协议、TCP 协议等
- 重置功能用于将 Winsock Provider 重置为系统初始的默认值。此功能用于解决由于 Winsock Provider 被破坏导致的网络访问异常



- 重置功能把所有的winsock provider恢复到系统默认初始值状态
- 此操作可能会导致一些添加自定义winsock provider的软件工作失效或不正常

系统修复





- 高级修复类包括推荐修复级别和高强修复级别。
- 推荐修复级别针对常见、已知的非正常修改进行修复
- 而高强修复级别则针对所有的修改进行修复，而不管这种修改是否是正常的
- 在特殊的情况下才建议使用高强修复级别



- 高级手动修复包括重置winsock, 修复安全模式, API HOOK 检查





- 智能扫描功能是扫描系统信息，包括文件关联、启动组、正在运行的进程等，并产生一个报告，用于提供给别人分析使用的一项功能

## 智能扫描

智能扫描将产生一个和你系统有关的详细报告。这个报告能够帮助你解决你系统中存在的问题。更多信息请阅读帮助内容。

- ☒ 所有的启动项目（包括注册表、启动文件夹、服务等）
- ☒ 浏览器加载项
- ☒ 正在运行的进程（包括进程模块信息）
- ☒ 文件关联
- ☒ Winsock 提供者
- ☒ Autorun.inf
- ☒ HOSTS 文件
- ☒ 进程特权扫描
- ☒ 计划任务
- ☒ Windows 安全更新检查

☒ 检查进程模块的数字签名

☐ 自动将可疑文件复制到 SuspiciousFiles 子目录里面

扫描



- 对进程模块进行数字签名检查会提高安全检查级别，但是会减慢扫描速度
- 支持自动将扫描日志里面涉及的文件放到 SuspiciousFiles 子目录里面并支持分类存放



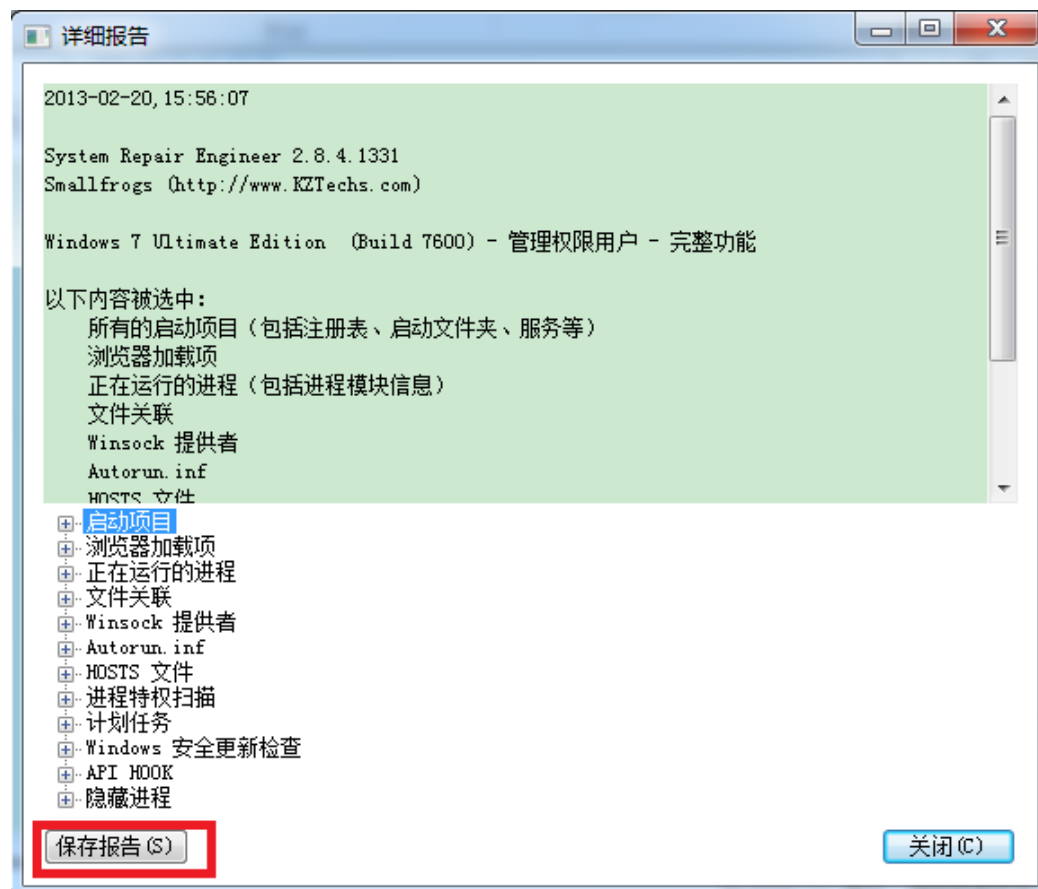




- 扫描完成以后进度条将自动关闭，并出现一个报告窗口
- 为了减少报告的体积，智能扫描功能将把发行者是 Microsoft 的项目过滤掉，并不会出现在报告里面



- 点击“保存报告”，以文本形式保存



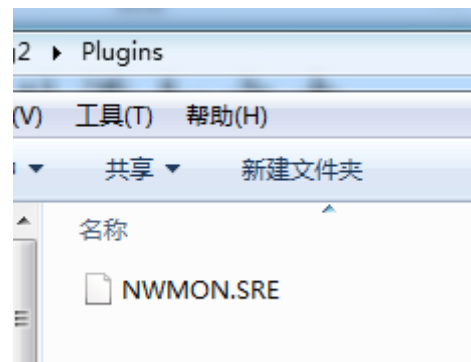
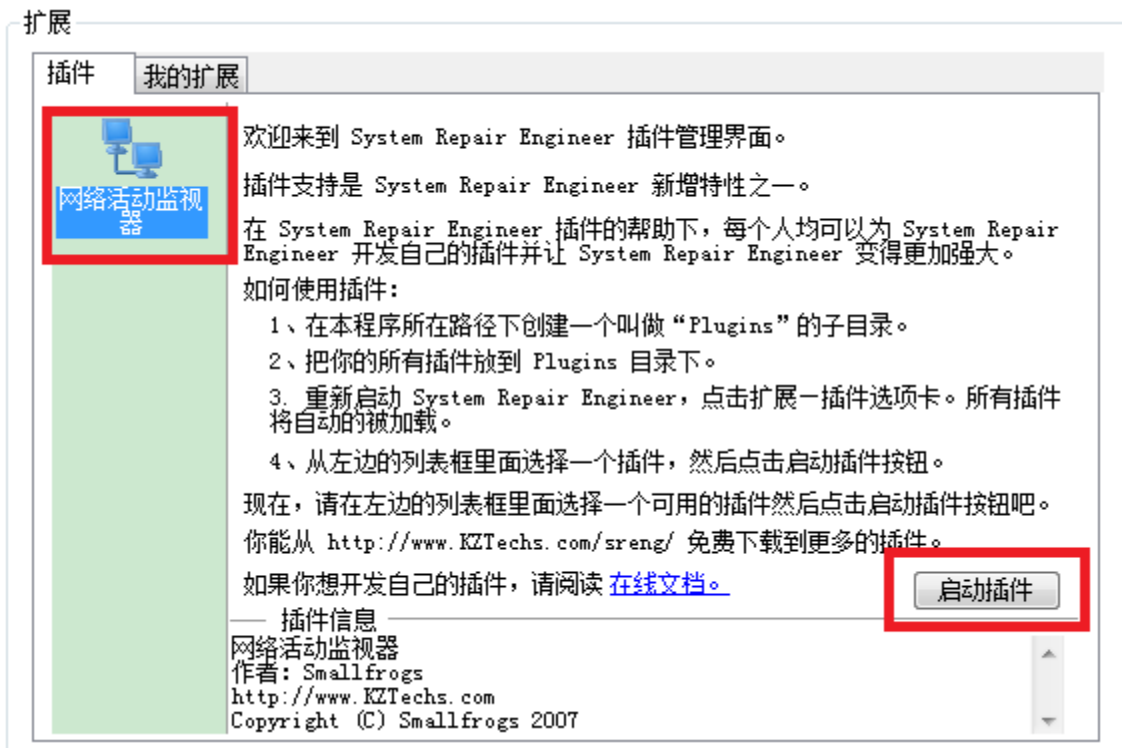


- 从 KZTechs.COM 网站下载所需要的插件
- 将插件解压缩，插件文件扩展名一定是.SRE
- 在SREng主程序所在目录下方建立子目录：  
Plugins
- 将解压缩以后产生的 .SRE 文件复制到 Plugins  
目录里面

启动 SREng，如果先前下载的插件能够被支持，则会在“插件”管理页左边看到插件列表和插件图标，选择插件，然后点击“启动插件”按钮以后就使用插件了。



- 插件文件路径，添加插件后重启软件就可以使用了



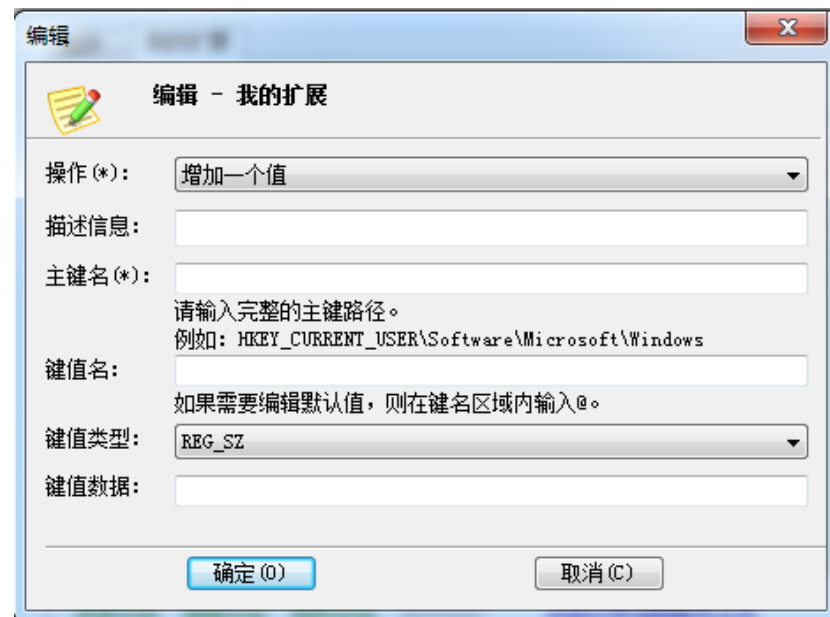
下载地址: <http://www.kztechs.com/sreng/plugins.html>



- 我的扩展功能通过提供外部的一个配置文件，让用户把自己的配置信息保存下来，而且随时可以进行编辑、新建、删除操作，SREng根据配置文件的记录信息，执行特定的操作
- 我的扩展的应用范围，只提供了注册表键值的删除/新建/编辑，注册表主键的删除/新建功能
- 我的扩展功能使用扩展名为SRE的文件作为规则储存文件，默认的规则库文件名是：  
SREngExt.SRE



- 如果需要加载其他的规则文件，点击界面中蓝色字体的文字可以让用户自己选择需要加载的规则文件

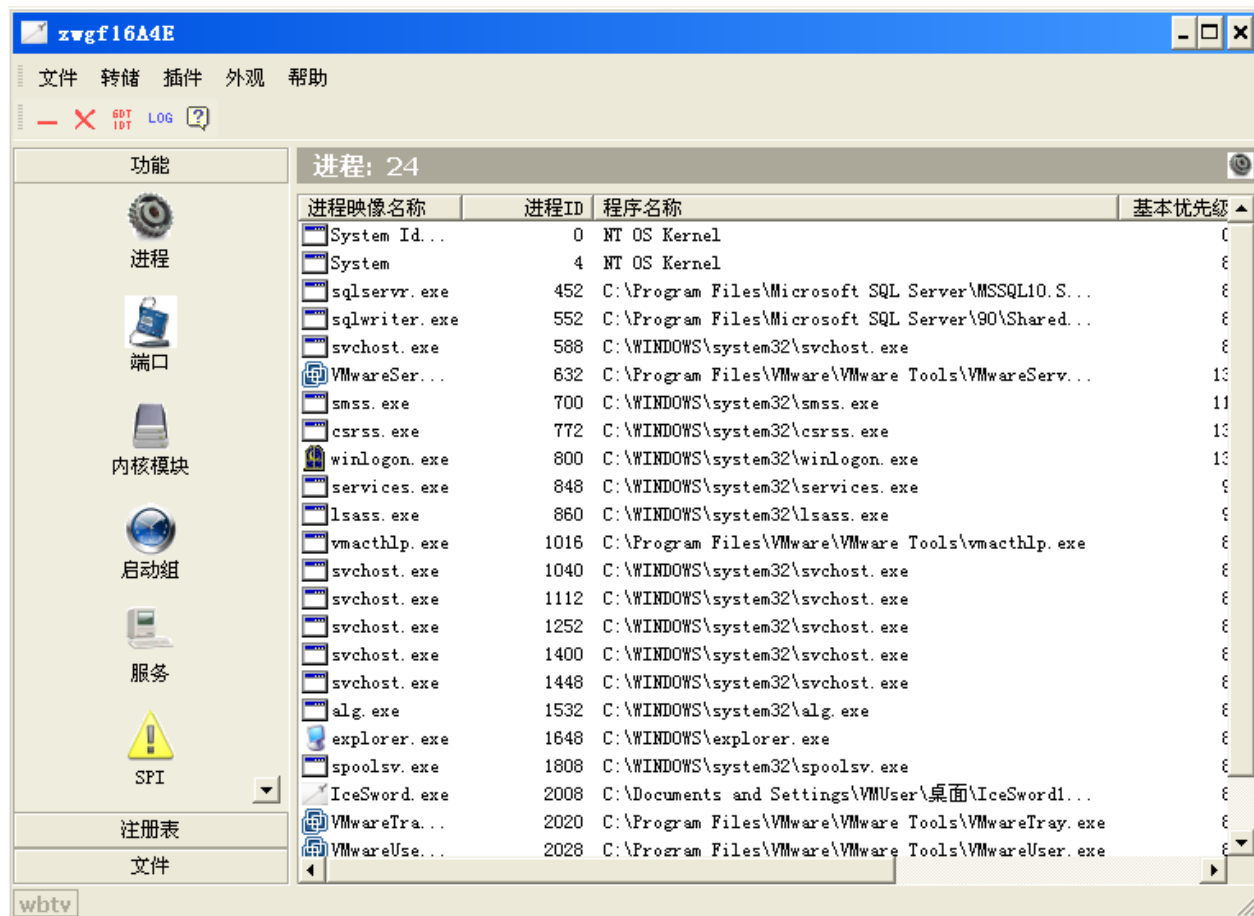




- IceSword工具最大的特点就是采用了很多新颖的内核级的方法和手段，使得检测和清除效果得到提升
- 显示所有的隐藏进程，隐藏文件，隐藏端口，隐藏服务，并且可以轻松杀掉相关的进程，禁用服务
- 可以直接的删除已经加载的驱动文件，受保护的注册表和流氓软件中无法正常删除的文件



- 软件主界面，目前最新版本1.22，更新于2007年





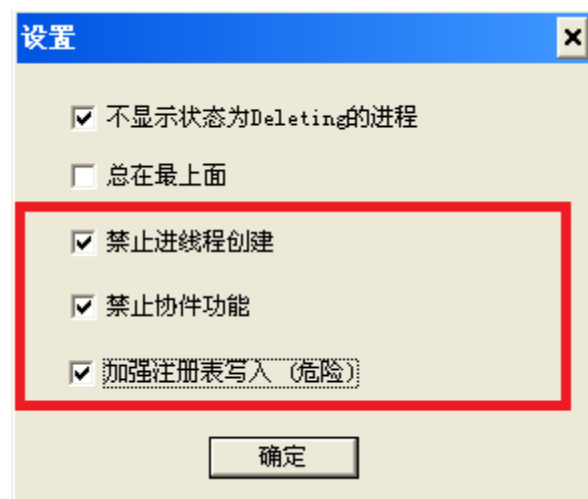
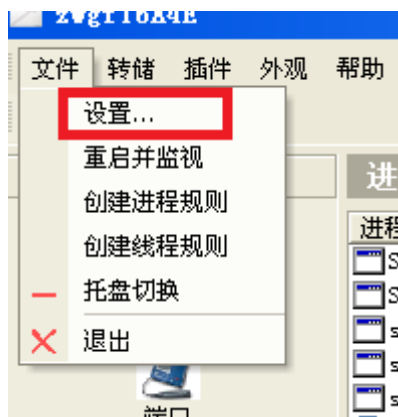


- 打开软件，显示在系统任务栏或软件标题栏的都只是一串随机字符串，而不是常见的程序名，这是IceSword独有的随机字符串标题栏
- 每次打开出现的字符串都是随机生成，这样那些通过标题栏来关闭程序的木马和后门就无用了



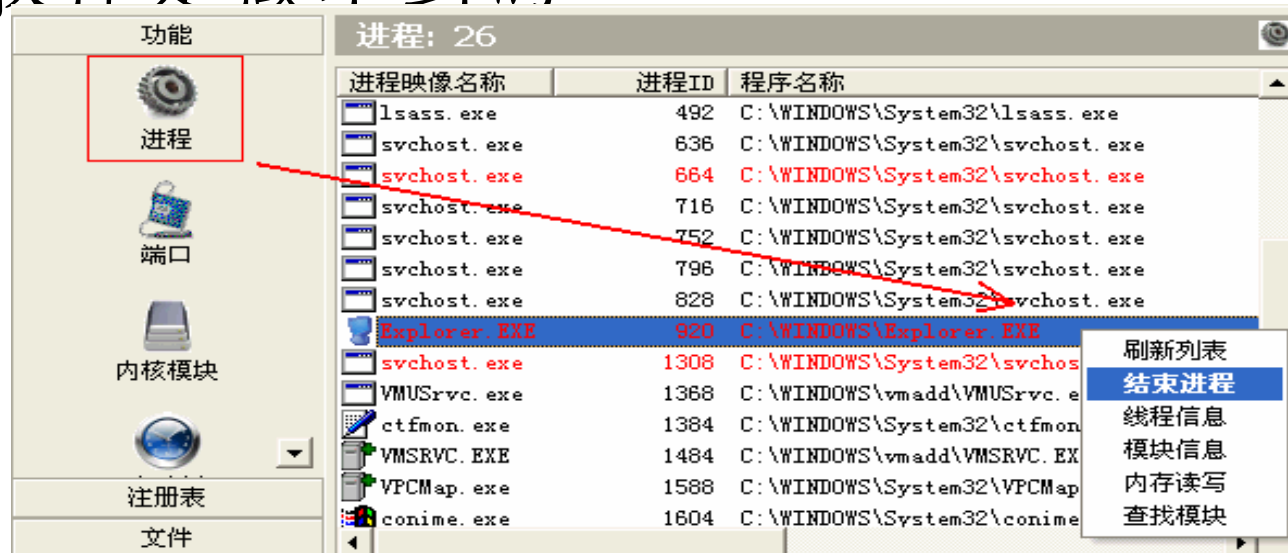


- 运行IceSword.exe。如果无法运行，可以试着将文件名改成随即名字
- 选择“文件-设置”，勾选最下面的三项，这样设置后无法再打开任何新的程序，方便检测



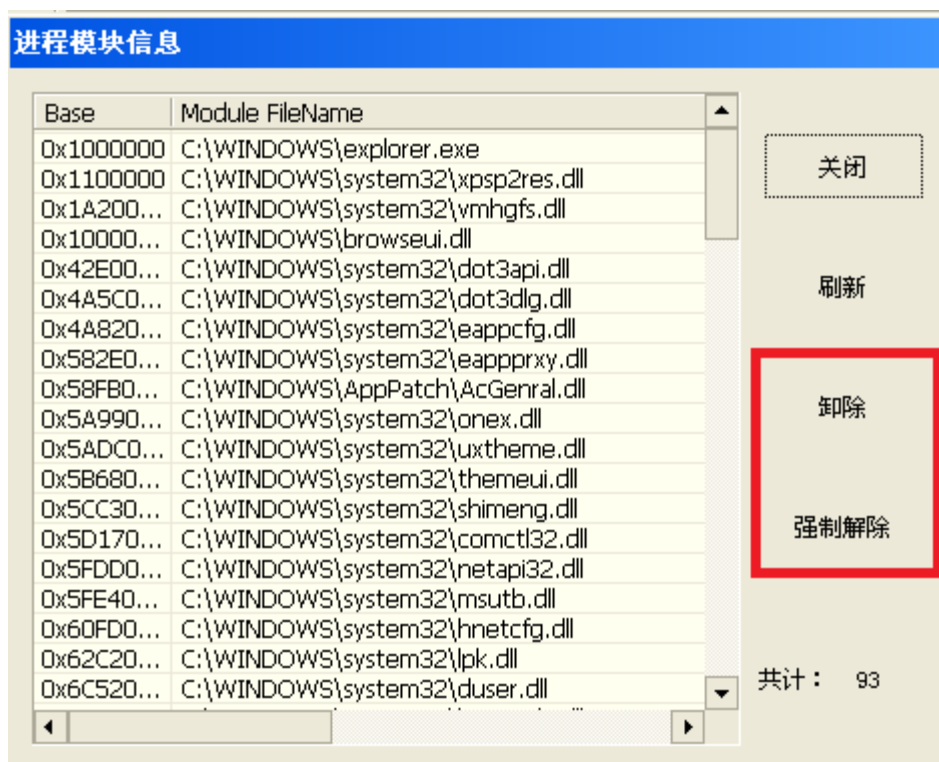


- 查看系统当前进程。显示为红色的为隐藏进程，系统默认是没有的，红色项应全部结束
- IceSword可结束除Idle进程、System进程、csrss进程这三个进程外的所有进程，这一点，很多同类软件是做不到的





- 很多木马程序喜欢插入DLL模块到进程中，找到病毒模块，点击卸载或者强制解除





- 可以查看到隐藏的端口，但是不会像进程一样以红色显示，需要自己对照查看

功能

进程

端口

内核模块

启动组

服务

端口: 17

| 协议  | 本地地址                 | 远程地址        | 状态        | 进程ID | 进程程序名称                          |
|-----|----------------------|-------------|-----------|------|---------------------------------|
| TCP | 127.0.0.1 : 1028     | 0.0.0.0 : 0 | LISTENING | 1532 | C:\WINDOWS\system32\alg.exe     |
| TCP | 0.0.0.0 : 445        | 0.0.0.0 : 0 | LISTENING | 4    | NT OS Kernel                    |
| TCP | 0.0.0.0 : 135        | 0.0.0.0 : 0 | LISTENING | 1112 | C:\WINDOWS\system32\svchost.exe |
| TCP | 192.168.0.104 : 139  | 0.0.0.0 : 0 | LISTENING | 4    | NT OS Kernel                    |
| UDP | 192.168.0.104 : 123  | * : *       |           | 1252 | C:\WINDOWS\system32\svchost.exe |
| UDP | 0.0.0.0 : 500        | * : *       |           | 860  | C:\WINDOWS\system32\lsass.exe   |
| UDP | 192.168.0.104 : 1900 | * : *       |           | 1448 | C:\WINDOWS\system32\svchost.exe |
| UDP | 127.0.0.1 : 123      | * : *       |           | 1252 | C:\WINDOWS\system32\svchost.exe |
| UDP | 127.0.0.1 : 1035     | * : *       |           | 1252 | C:\WINDOWS\system32\svchost.exe |
| UDP | 192.168.0.104 : 137  | * : *       |           | 4    | NT OS Kernel                    |
| UDP | 0.0.0.0 : 1026       | * : *       |           | 1400 | C:\WINDOWS\system32\svchost.exe |
| UDP | 127.0.0.1 : 1900     | * : *       |           | 1448 | C:\WINDOWS\system32\svchost.exe |
| UDP | 0.0.0.0 : 4500       | * : *       |           | 860  | C:\WINDOWS\system32\lsass.exe   |
| UDP | 0.0.0.0 : 445        | * : *       |           | 4    | NT OS Kernel                    |
| UDP | 192.168.0.104 : 138  | * : *       |           | 4    | NT OS Kernel                    |
| RAW | ---                  | ---         | ---       | 4    | NT OS Kernel                    |
| RAW | ---                  | ---         | ---       | 860  | C:\WINDOWS\system32\lsass.exe   |

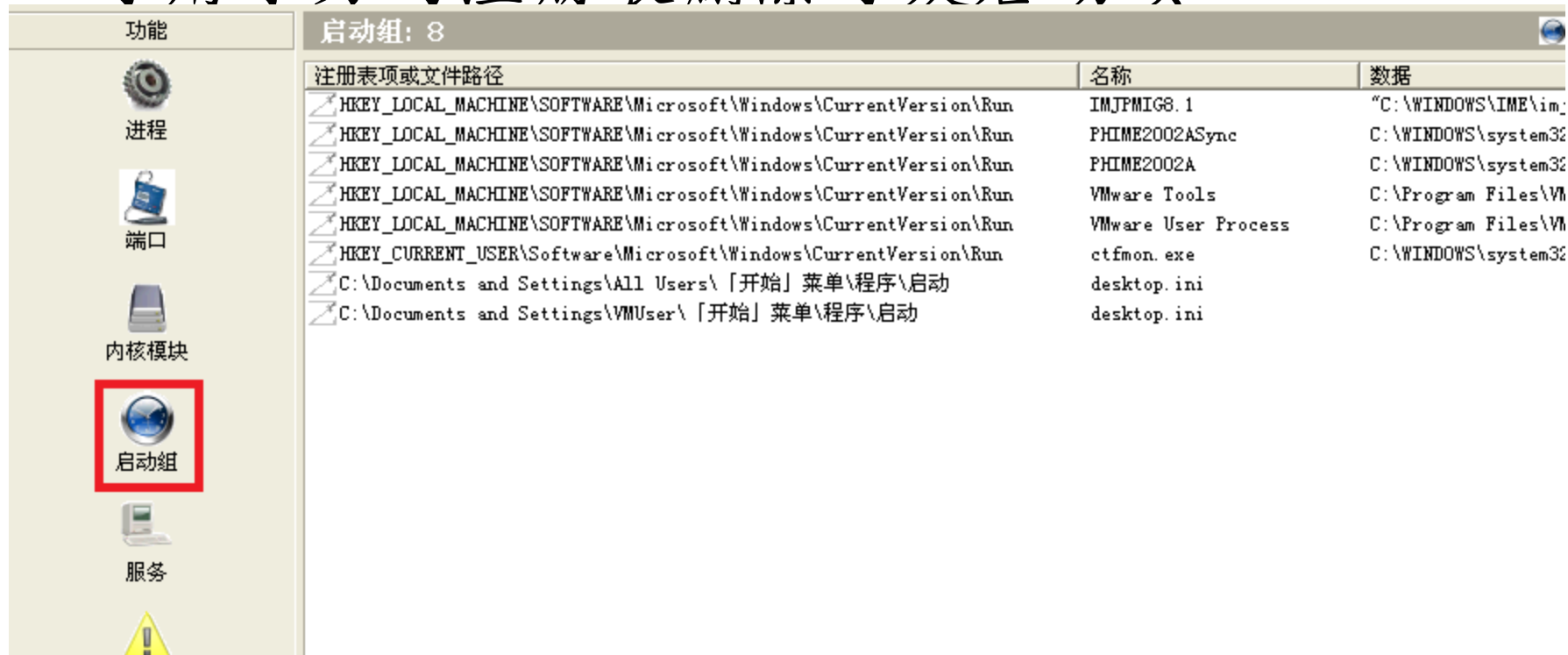


- 冰刃中的内核模块只能察看简单的内核信息，需要通过与其他工具的结合分析来定位有问题的模块

| 文件名           | 基址         | 映像大小       | 标志         | 加载顺序 | 名称                                      |
|---------------|------------|------------|------------|------|---|
| ntkrnlpa.exe  | 0x804D8000 | 0x001F8480 | 0x0C004000 | 0    | \WINDOWS\system32\ntkrnlpa.exe          |
| hal.dll       | 0x806D1000 | 0x00020300 | 0x0C004000 | 1    | \WINDOWS\system32\hal.dll               |
| KDCOM.DLL     | 0xF8B9A000 | 0x00002000 | 0x09004000 | 2    | \WINDOWS\system32\KDCOM.DLL             |
| BOOTVID.dll   | 0xF8AAA000 | 0x00003000 | 0x09004000 | 3    | \WINDOWS\system32\BOOTVID.dll           |
| ACPI.sys      | 0xF856B000 | 0x0002E000 | 0x09004000 | 4    | ACPI.sys                                |
| WMILIB.SYS    | 0xF8B9C000 | 0x00002000 | 0x0D004000 | 5    | \WINDOWS\system32\DRIVERS\WMILIB.SYS    |
| pci.sys       | 0xF855A000 | 0x00011000 | 0x09004000 | 6    | pci.sys                                 |
| isapnp.sys    | 0xF869A000 | 0x00009000 | 0x09004000 | 7    | isapnp.sys                              |
| compbatt.sys  | 0xF8AAE000 | 0x00003000 | 0x09004000 | 8    | compbatt.sys                            |
| BATTC.SYS     | 0xF8AB2000 | 0x00004000 | 0x0D004000 | 9    | \WINDOWS\system32\DRIVERS\BATTC.SYS     |
| intelide.sys  | 0xF8B9E000 | 0x00002000 | 0x09004000 | 10   | intelide.sys                            |
| PCIIDEX.SYS   | 0xF891A000 | 0x00007000 | 0x0D004000 | 11   | \WINDOWS\system32\DRIVERS\PCIIDEX.SYS   |
| MountMgr.sys  | 0xF86AA000 | 0x0000B000 | 0x09004000 | 12   | MountMgr.sys                            |
| ftdisk.sys    | 0xF853B000 | 0x0001F000 | 0x09004000 | 13   | ftdisk.sys                              |
| dmload.sys    | 0xF8BA0000 | 0x00002000 | 0x09004000 | 14   | dmload.sys                              |
| dmio.sys      | 0xF8515000 | 0x00026000 | 0x09004000 | 15   | dmio.sys                                |
| PartMgr.sys   | 0xF8922000 | 0x00005000 | 0x09004000 | 16   | PartMgr.sys                             |
| VolSnap.sys   | 0xF86BA000 | 0x0000C000 | 0x09004000 | 17   | VolSnap.sys                             |
| atapi.sys     | 0xF84FD000 | 0x00018000 | 0x09004000 | 18   | atapi.sys                               |
| vm SCSI.sys   | 0xF8AB6000 | 0x00003000 | 0x09004000 | 19   | vm SCSI.sys                             |
| SCSI PORT.SYS | 0xF84E5000 | 0x00018000 | 0x0D004000 | 20   | \WINDOWS\system32\DRIVERS\SCSI PORT.SYS |
| disk.sys      | 0xF86CA000 | 0x00009000 | 0x09004000 | 21   | disk.sys                                |
| CLASSPNP.SYS  | 0xF86DA000 | 0x0000D000 | 0x0D004000 | 22   | \WINDOWS\system32\DRIVERS\CLASSPNP.SYS  |



- 和内核程序一样，只能查看，无法作任何处理。  
只显示几个地方的启动项目，不够全面
- 可用冰刃的注册表删除可疑启动项





- 注册表中，仅包括  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run和  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run两个项目
- 文件夹包括C:\Documents and Settings\您所使用的用户名\「开始」菜单\程序\启动和  
C:\Documents and Settings\All Users\「开始」菜单\程序\启动





- 服务中可以显示隐藏服务，和进程一样，用红色表示

进程

端口

内核模块

启动组

**服务**

SPI

| 服务名          | 显示名称          | 当前状态 | 服务类型       | 服务进程ID | 启动类别 | 描述            | 服务模块      |
|--------------|---------------|------|------------|--------|------|---------------|-----------|
| Alerter      | Alerter       | 已停止  | 共享进程服务     | ----   | 已禁用  | 通知所选用...      | C:\WINDOW |
| ALG          | Applicatio... | 已启动  | 独立进程服务     | 1532   | 手动   | 为 Interne...  | C:\WINDOW |
| AppMgmt      | Applicatio... | 已停止  | 共享进程服务     | ----   | 手动   | 提供软件安...      | C:\WINDOW |
| aspnet_state | ASP.NET 状...  | 已停止  | 独立进程服务     | ----   | 手动   | 为 ASP.NET...  | C:\WINDOW |
| AudioSrv     | Windows Audio | 已启动  | 共享进程服务     | 1252   | 自动   | 管理基于 W...     | C:\WINDOW |
| baqghb       | Helper Config | 已停止  | 共享进程服务     | ----   |      |               |           |
| BITS         | Background... | 已停止  | 共享进程服务     | ----   | 已禁用  | 在后台传输...      | C:\WINDOW |
| Browser      | Computer B... | 已启动  | 共享进程服务     | 1252   | 自动   | 维护网络上...      | C:\WINDOW |
| CiSvc        | Indexing S... | 已停止  | 共享进程服务,可交互 | ----   | 手动   | 本地和远程...      | C:\WINDOW |
| ClipSrv      | ClipBook      | 已停止  | 独立进程服务     | ----   | 已禁用  | 启用“剪贴...      | C:\WINDOW |
| clr_optim... | Microsoft ... | 已停止  | 独立进程服务     | ----   | 自动   | Microsoft ... | C:\WINDOW |
| COMSysApp    | COM+ Syste... | 已停止  | 独立进程服务     | ----   | 手动   | 管理 基于C...     | C:\WINDOW |
| CryptSvc     | Cryptograp... | 已启动  | 共享进程服务     | 1252   | 自动   | 提供三种管...      | C:\WINDOW |
| DcomLaunch   | DCOM Serve... | 已启动  | 共享进程服务     | 1040   | 自动   | 为 DCOM 服...   | C:\WINDOW |
| Dhcp         | DHCP Client   | 已启动  | 共享进程服务     | 1252   | 自动   | 通过注册和...      | C:\WINDOW |
| dmadmin      | Logical Di... | 已停止  | 共享进程服务     | ----   | 手动   | 配置硬盘驱...      | C:\WINDOW |
| dmserver     | Logical Di... | 已启动  | 共享进程服务     | 1252   | 自动   | 监测和监视...      | C:\WINDOW |
| Dnscache     | DNS Client    | 已启动  | 共享进程服务     | 1400   | 自动   | 为此计算机...      | C:\WINDOW |
| Dot3svc      | Wired Auto... | 已停止  | 共享进程服务     | ----   | 手动   | 此服务在以...      | C:\WINDOW |
| EapHost      | Extensible... | 已停止  | 共享进程服务     | ----   | 手动   | 向 Windows...  | C:\WINDOW |

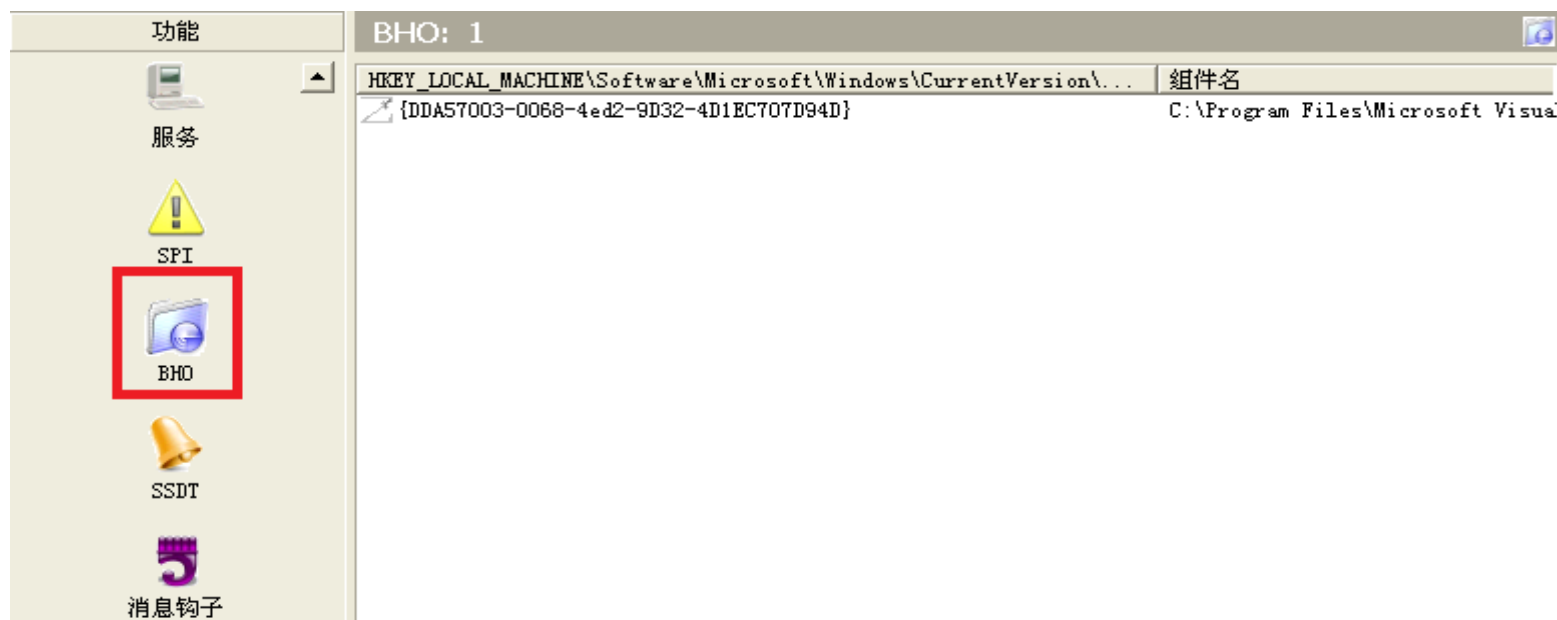


- 修改服务状态：启动，停止，暂停，恢复
- 系统的关键服务是不能停止的，否则系统会自动重新启动计算机
- 修改服务的启动类型：禁用、自动、手动

|         |               |     |             |   |
|---------|---------------|-----|-------------|---|
| nt      | Applicatio... | 已停止 | 共享进程服务      | - |
| :_state | ASP.NET 状...  | 已停止 | 独立进程服务      | - |
| rv      | Windows Audio | 已停止 | 共享进程服务      | 1 |
|         | Helper Config | 已停止 | 共享进程服务      | - |
|         | Background... | 已停止 | 共享进程服务      | - |
| er      | Computer B... | 已停止 | 共享进程服务      | 1 |
|         | Indexing S... | 已停止 | 共享进程服务, 可交互 | - |
| rv      | ClipBook      | 已停止 | 独立进程服务      | - |
| otim... | Microsoft ... | 已停止 | 独立进程服务      | - |
| sApp    | COM+ Syste... | 已停止 | 独立进程服务      | - |
| svc     | Cryptograp... | 已停止 | 共享进程服务      | 1 |
| unch    | DCOM Serve... | 已停止 | 共享进程服务      | 1 |
|         | DHCP Client   | 已启动 | 共享进程服务      | 1 |
| n       | Logical Di    | 已停止 | 共享进程服务      | - |



- IceSword 的“BHO”的功能，可以检查浏览器劫持项
- BHO是病毒常驻的一个位置，手动清除时需要在这里清除残余项

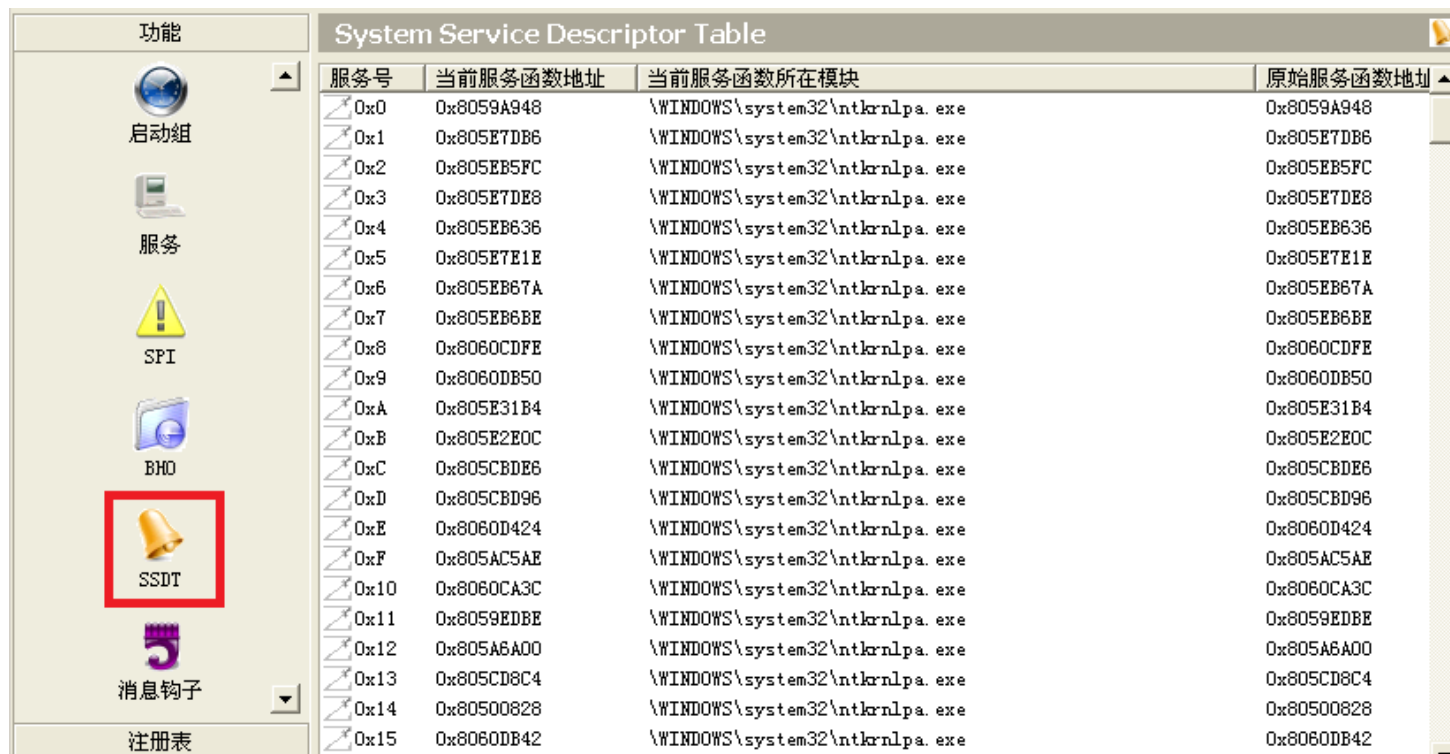




- BHO(Browser Helper Object, 浏览器辅助对象, 简称BHO)
- BHO在注册表中的位置是:  
HKEY\_LOCAL\_MACHINE\Software  
\Microsoft\Windows\CurrentVersion\Explorer  
\Browser Helper Objects
- BHO的目的是为了更好的帮助程序员打造个性化浏览器, 以及为程序提供更简洁的交互功能, 现在很多IE个性化工具就是利用BHO来实现的



- 被修改的项以红色显示
- 对修改的项右键-“恢复”即可还原初始值

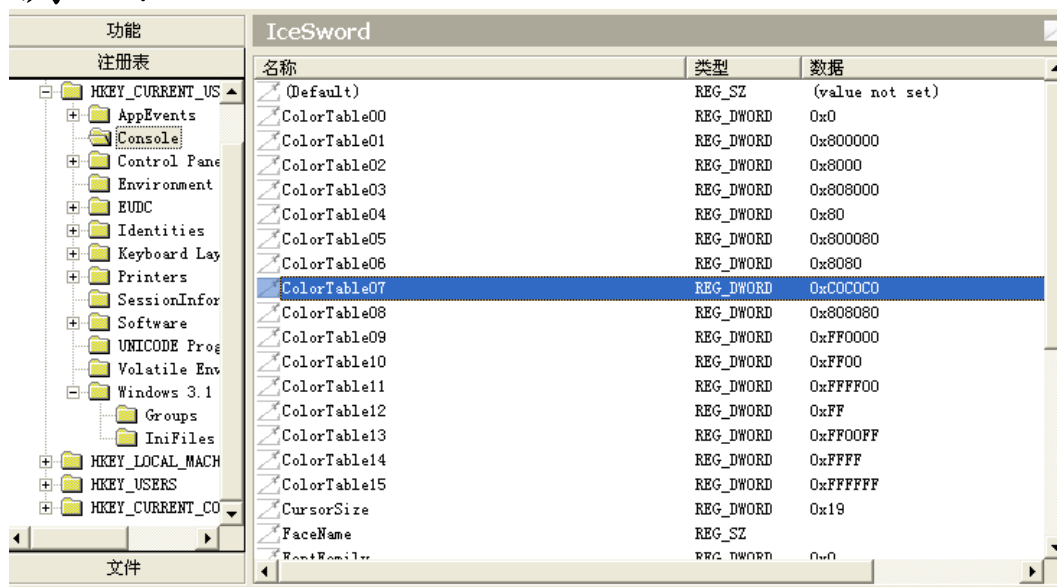




- SSDT (System Services Descriptor Table) , 系统服务描述符表
- 这个表就是一个把ring3的Win32 API和ring0的内核API联系起来
- Rootkit之类的病毒经常通过hook截获系统的服务函数调用, 以实现注册表、文件的隐藏
- 防毒软件、系统监控、注册表监控软件往往会采用此接口来实现自己的监控模块

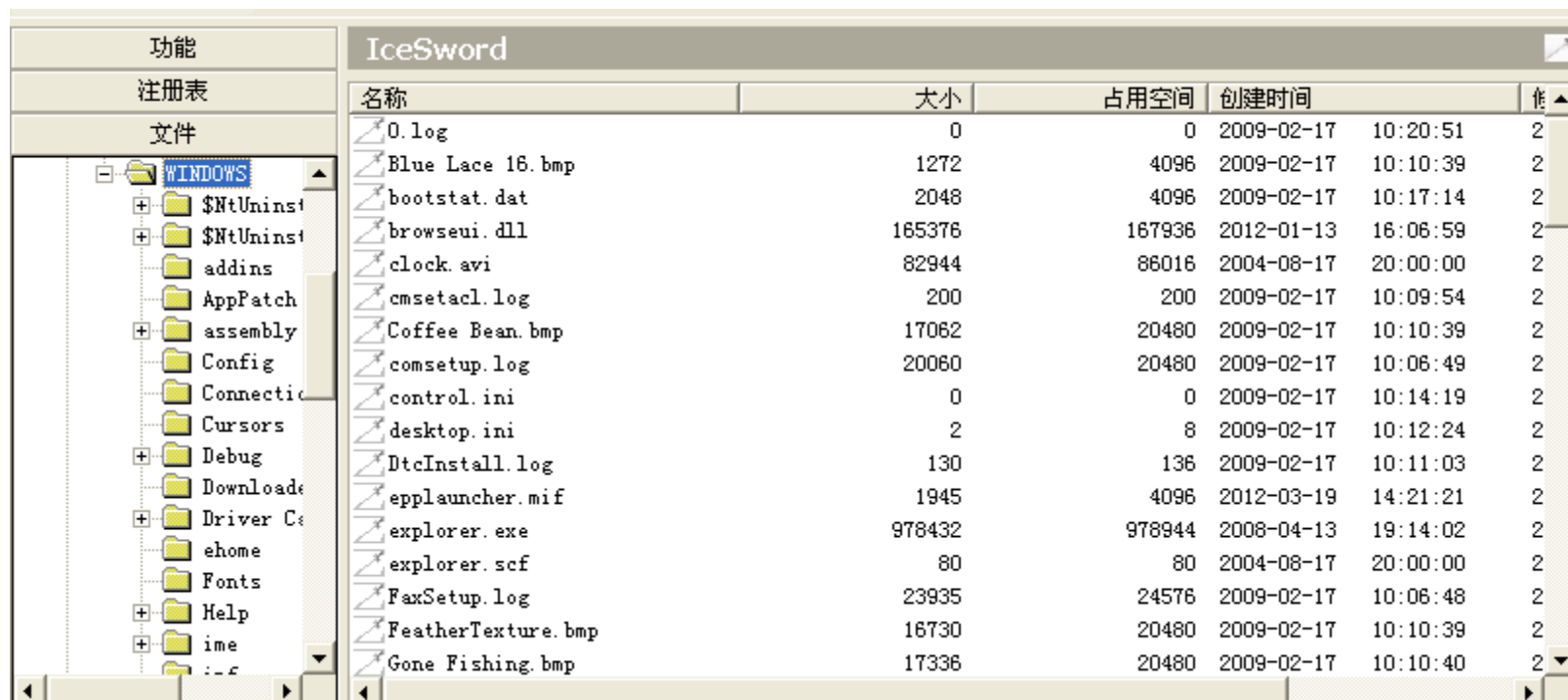


- IceSword对注册表有非常高的权限（管理员权限），可以看到某些系统注册表编辑器中不可见的项目，进行操作的时候要有十足把握，不要因为错删、错改某些系统关键项目，使计算机系统崩溃





- 文件是一个浏览计算机所有文件的地方，可以看到任何隐藏的文件，对付无法删除的文件，也可以使用强制删除等特殊方法删除



| 功能  |             | IceSword           |        |        |                     |   |
|-----|-------------|--------------------|--------|--------|---------------------|---|
| 注册表 |             | 名称                 | 大小     | 占用空间   | 创建时间                | 作 |
| 文件  |             |                    |        |        |                     |   |
| +   | [-] WINDOWS | 0.log              | 0      | 0      | 2009-02-17 10:20:51 | 2 |
|     |             | Blue Lace 16.bmp   | 1272   | 4096   | 2009-02-17 10:10:39 | 2 |
|     |             | bootstat.dat       | 2048   | 4096   | 2009-02-17 10:17:14 | 2 |
|     |             | browseui.dll       | 165376 | 167936 | 2012-01-13 16:06:59 | 2 |
|     |             | clock.avi          | 82944  | 86016  | 2004-08-17 20:00:00 | 2 |
|     |             | cmsetacl.log       | 200    | 200    | 2009-02-17 10:09:54 | 2 |
|     |             | Coffee Bean.bmp    | 17062  | 20480  | 2009-02-17 10:10:39 | 2 |
|     |             | comsetup.log       | 20060  | 20480  | 2009-02-17 10:06:49 | 2 |
|     |             | control.ini        | 0      | 0      | 2009-02-17 10:14:19 | 2 |
|     |             | desktop.ini        | 2      | 8      | 2009-02-17 10:12:24 | 2 |
|     |             | DtcInstall.log     | 130    | 136    | 2009-02-17 10:11:03 | 2 |
|     |             | epplauncher.mif    | 1945   | 4096   | 2012-03-19 14:21:21 | 2 |
|     |             | explorer.exe       | 978432 | 978944 | 2008-04-13 19:14:02 | 2 |
|     |             | explorer.scf       | 80     | 80     | 2004-08-17 20:00:00 | 2 |
|     |             | FaxSetup.log       | 23935  | 24576  | 2009-02-17 10:06:48 | 2 |
|     |             | FeatherTexture.bmp | 16730  | 20480  | 2009-02-17 10:10:39 | 2 |
|     |             | Gone Fishing.bmp   | 17336  | 20480  | 2009-02-17 10:10:40 | 2 |



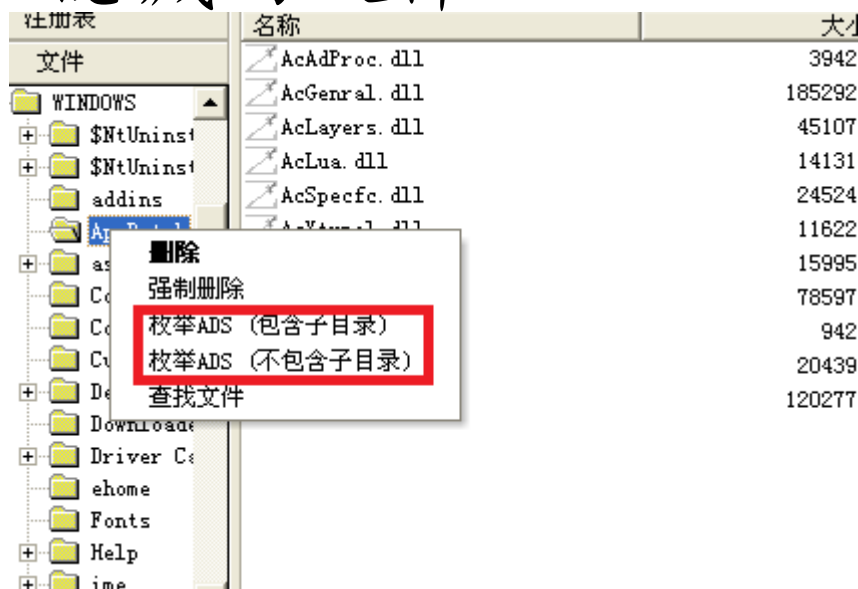


- 为完全清理文件，有时强制删除文件会失败，请先使用“删除”
- 删除后刷新一下看是否文件还存在，如果有，先结束进程





- 若你的分区格式是NTFS，在清理时请使用管理员权限帐户登陆，并右键目录，选择“枚举ADS（不包含子目录）”。这样可以揪出利用NTFS交换数据流（Alternate Data Streams，简称ADS）隐藏的文件





- 技巧一：防止冰刃进程被结束
- 以命令行形式输入：IceSword.exe /c，此时需要Ctrl+Alt+D才能关闭（使用三键前先按一下任意键），如果最小化到托盘时托盘图标又消失了，可用Ctrl+Alt+S唤出主界面



- 技巧二：用冰刃的“复制”改写文件（此方法用于强制删除无效时）
- 对一个被非共享打开的文件、或一个正运行的程序文件（如木马），你想改掉它的内容，可新建一文件，写入你想写的文件（文件名和你要替换的文件一致），然后打开冰刃文件->文件，找到该文件，右键“复制”，然后浏览到你  
想修改的文件（木马）的路径，确定即可



# 安全卫士时代的恶意代码手工检测 (1/2)

- wsyscheck
  - 最新版本更新于2008年
- XueTr / PC Hunter
  - XueTr支持32位的2000、XP、2003、Vista、2008、Win7系统，最新版本0.45更新于2012年10月
  - PC Hunter支持2000~win8.1的所有32位操作系统，还支持64位的Win7、Win8和Win8.1系统，最新版本1.32更新于2013年12月
  - <http://www.xuetr.com/>
- PowerTool
  - 持续更新维护中，支持Win 8.1和64位系统
  - 作者微博：<http://weibo.com/powertool>
- Win64AST
  - 专用于64位Windows的Anti-RootKit类工具
    - <http://m5home.blog.163.com/>



## 安全卫士时代的恶意代码手工检测 (2/2)

- 新工具越来越少
- 已有工具大部分均停止更新
- 商业化公司支持的傻瓜化桌面终端安全软件成熟度越来越高
- 恶意代码手工检测的基本思路和方法是基本的信息安全分析能力
  - 思路+工具



## 本章内容提要

---

- 第三方安全软件介绍与使用
- 组策略编辑器
- 注册表安全
- 访问控制加固
- UAC



## 组策略编辑器

- 组策略是管理员为计算机和用户定义的，用来控制应用程序，系统设置和管理模版的一种机制
- 组策略就是介于控制面板和注册表之间的一种修改系统，设置程序的工具
- 组策略高于注册表，组策略使用更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，远比手工修改注册表方便，灵活，功能也更强大





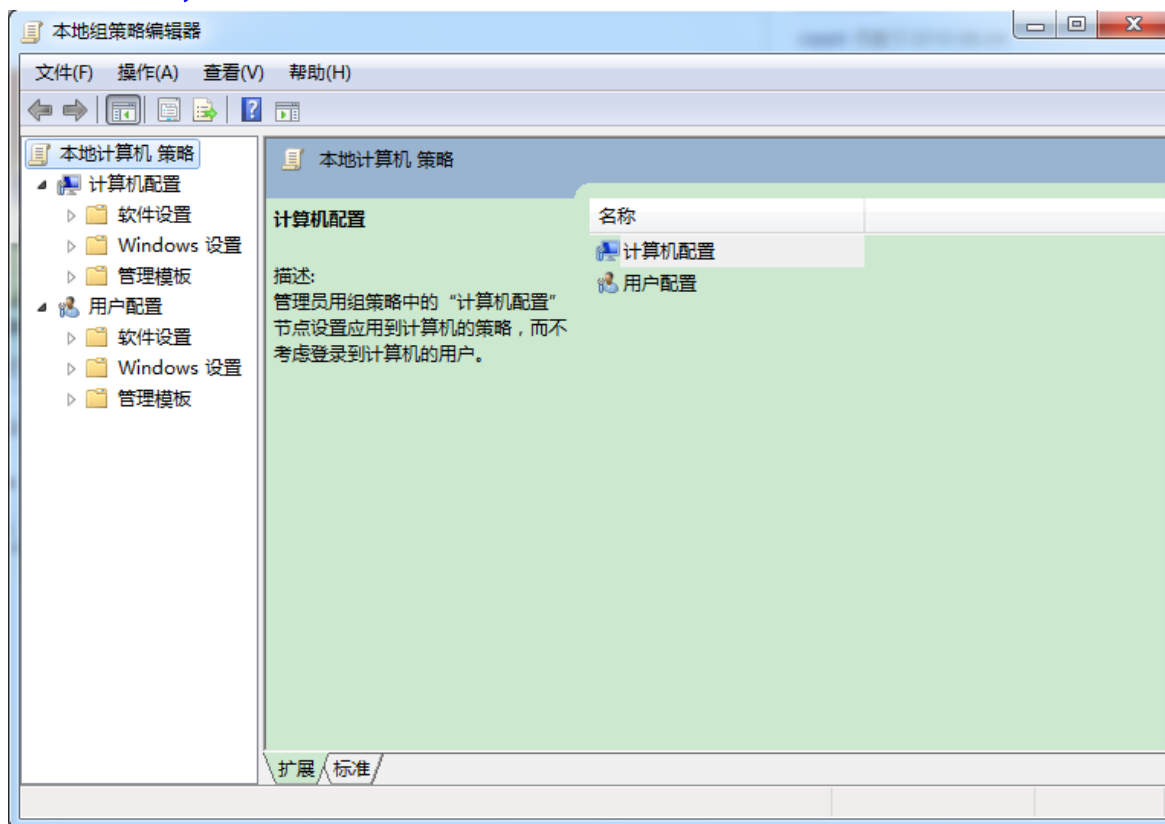
## 组策略编辑器

- 使用组策略可以实现的功能
  - 帐户策略的设定
  - 本地策略的设定
  - 脚本的设定
  - 用户工作环境的定制
  - 软件的安装与删除
  - 限制软件的运行
  - 文件夹的转移
  - 其他系统的设定



# 组策略编辑器

- 启动组策略的方法1  
——开始-运行，输入gpedit.msc

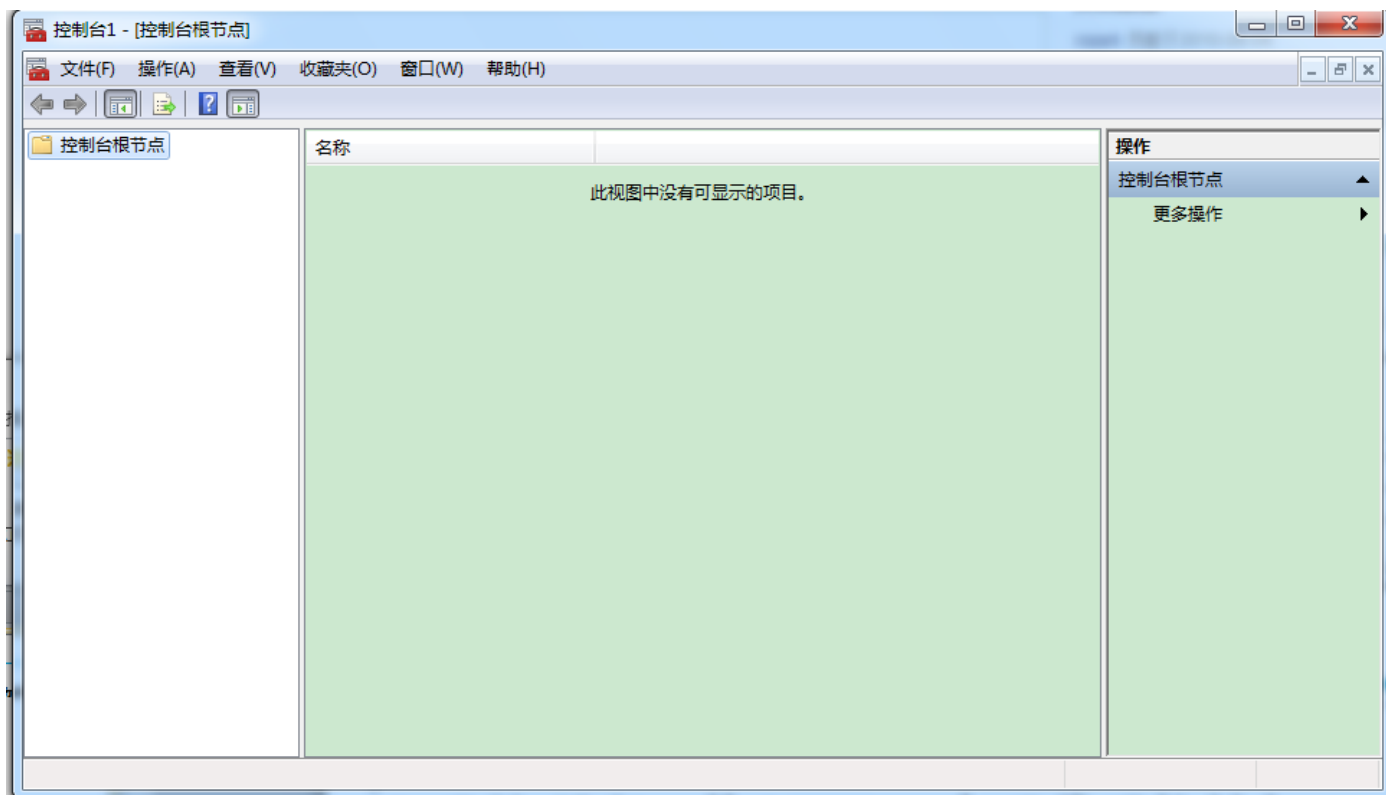




# 组策略编辑器

- 启动组策略的方法2

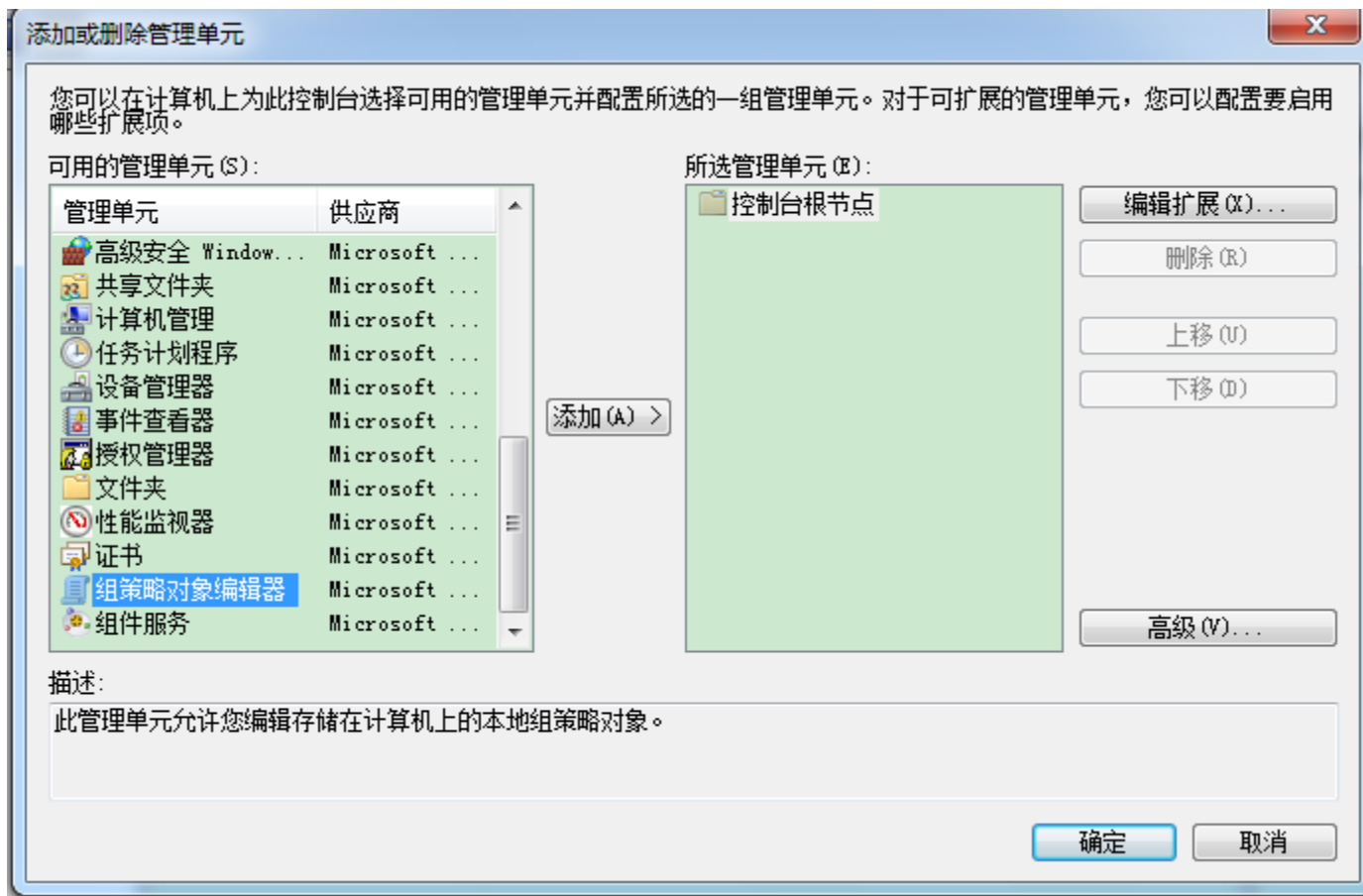
—开始-运行，输入mmc，打开管理控制台





# 组策略编辑器

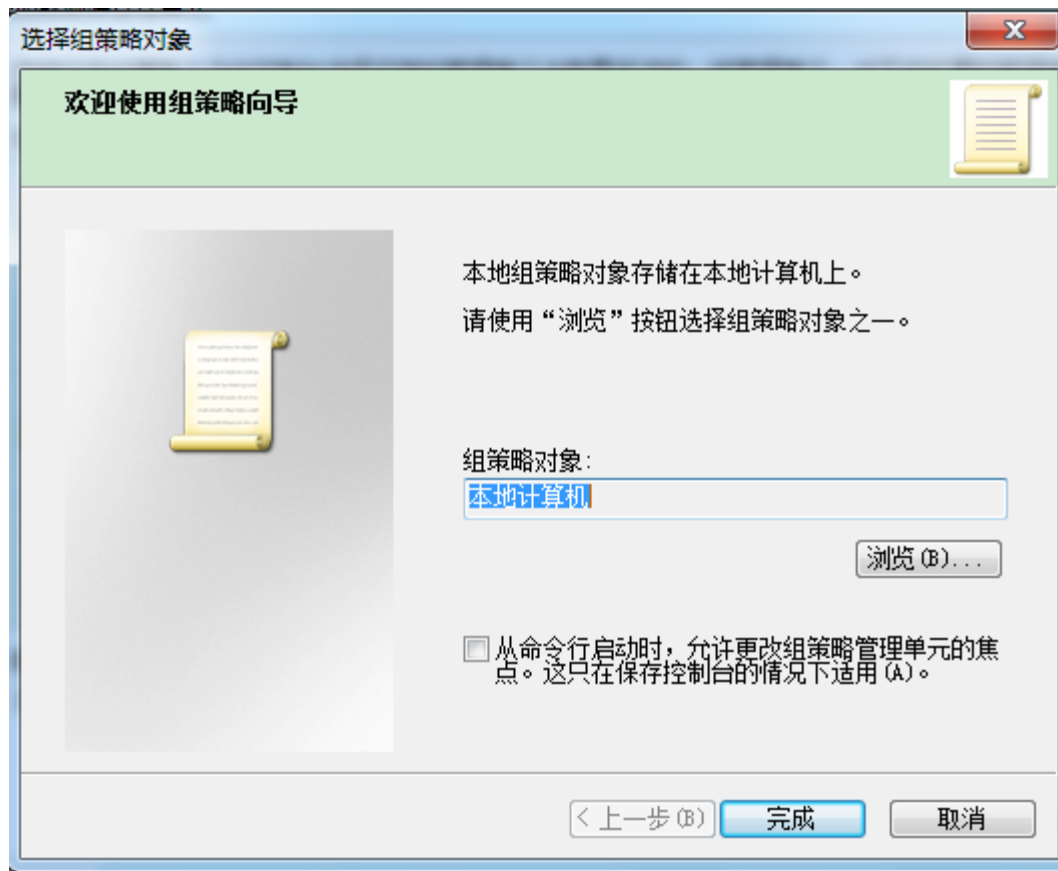
- 添加组策略编辑器





# 组策略编辑器

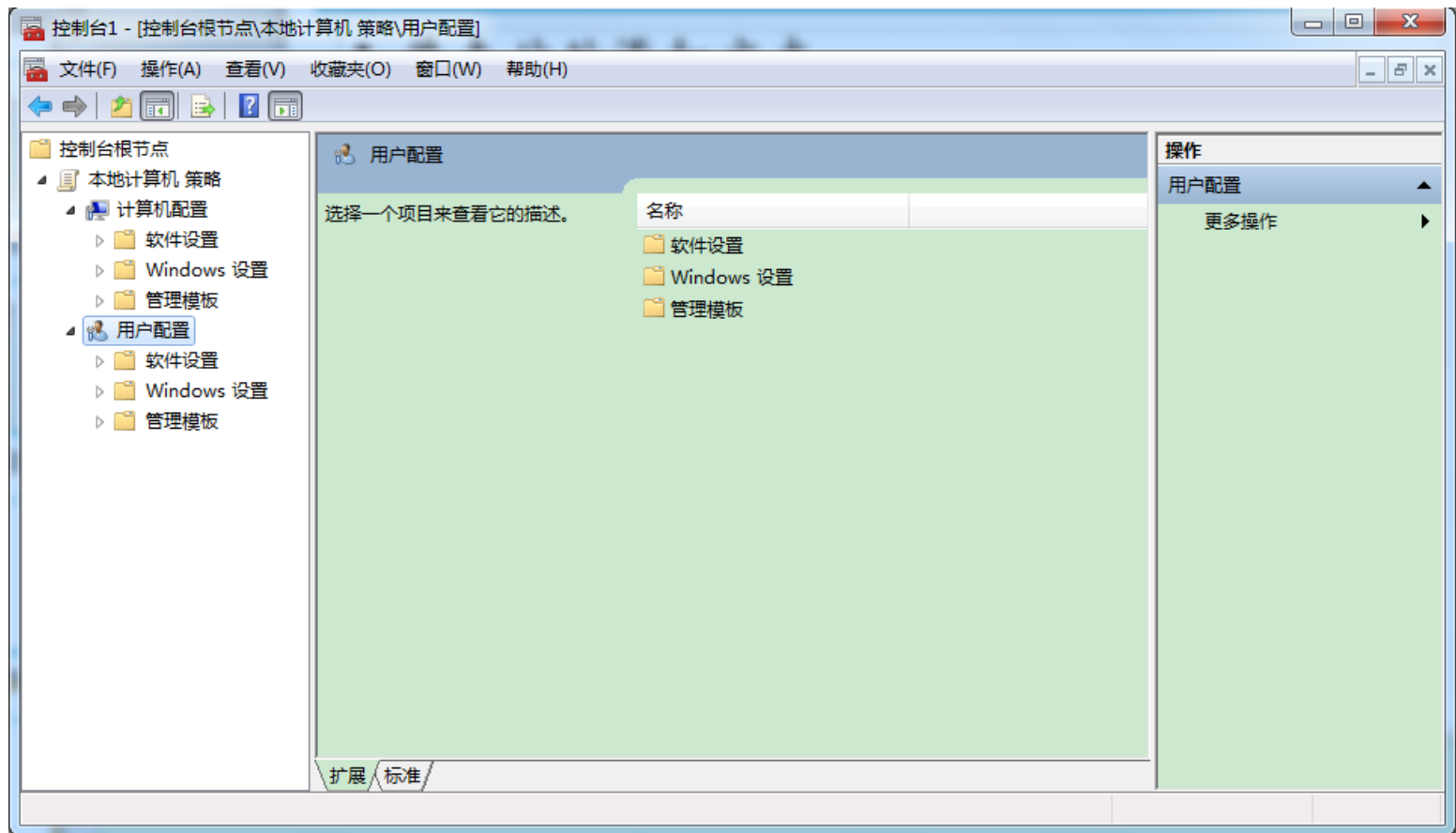
- 选择组策略对象





# 组策略编辑器

- 控制端添加组策略编辑器





- 计算机配置

—计算机配置包括所有与计算机相关的策略设置，他们用来指定操作系统行为，桌面行为，安全设置，计算机开机与关机脚本，指定的计算机应用选项以及应用设置

- 用户配置

—用户包括所有与用户相关的策略设置，它们用来指定操作系统行为，桌面设置，安全设置，指定和发布的应用选项，应用设置，文件夹重定向选项，用户登录与注销等



# 组策略编辑器

- 组策略插件扩展

- 软件设置

- Windows 设置

- 帐号策略，本地策略，事件日志，受限组，系统服务，注册表，文件系统，IP安全策略，公钥策略

- 管理模版





# 组策略编辑器

- 组策略对象

- 组策略的基本单元是组策略对象GPO，它是一组设置的组合

- 有两种类型的组策略对象

- 本地组策略对象

- 非本地组策略对象

- 组策略作用范围

- 由它们所链接的站点，域或组织单元启用



## 组策略编辑器

- 组策略的应用时机

- 计算机配置

- 计算机开机时自动启用
    - 域控制器默认5分钟自动启用
    - 非域控制器默认每隔90-120分钟自动启动
    - 不论策略是否有变动系统每隔16小时自动启动一次



## 组策略编辑器

- 组策略的应用时机

- 用户配置

- 用户登录时自动启用
    - 系统默认每隔90分钟自动启动
    - 不论策略是否有变动系统每隔16小时自动启动一次

- 手动启动组策略的命令是

- gpupdate /target: computer /force



## 组策略编辑器

- 组策略的处理顺序
  - 组策略的配置是累加的
  - 应用顺序
    - 本地组策略对象
    - 站点的组策略对象
    - 域的组策略对象
    - 组织单元的组策略对象
  - 后面的策略覆盖前面的策略



## 本章内容提要

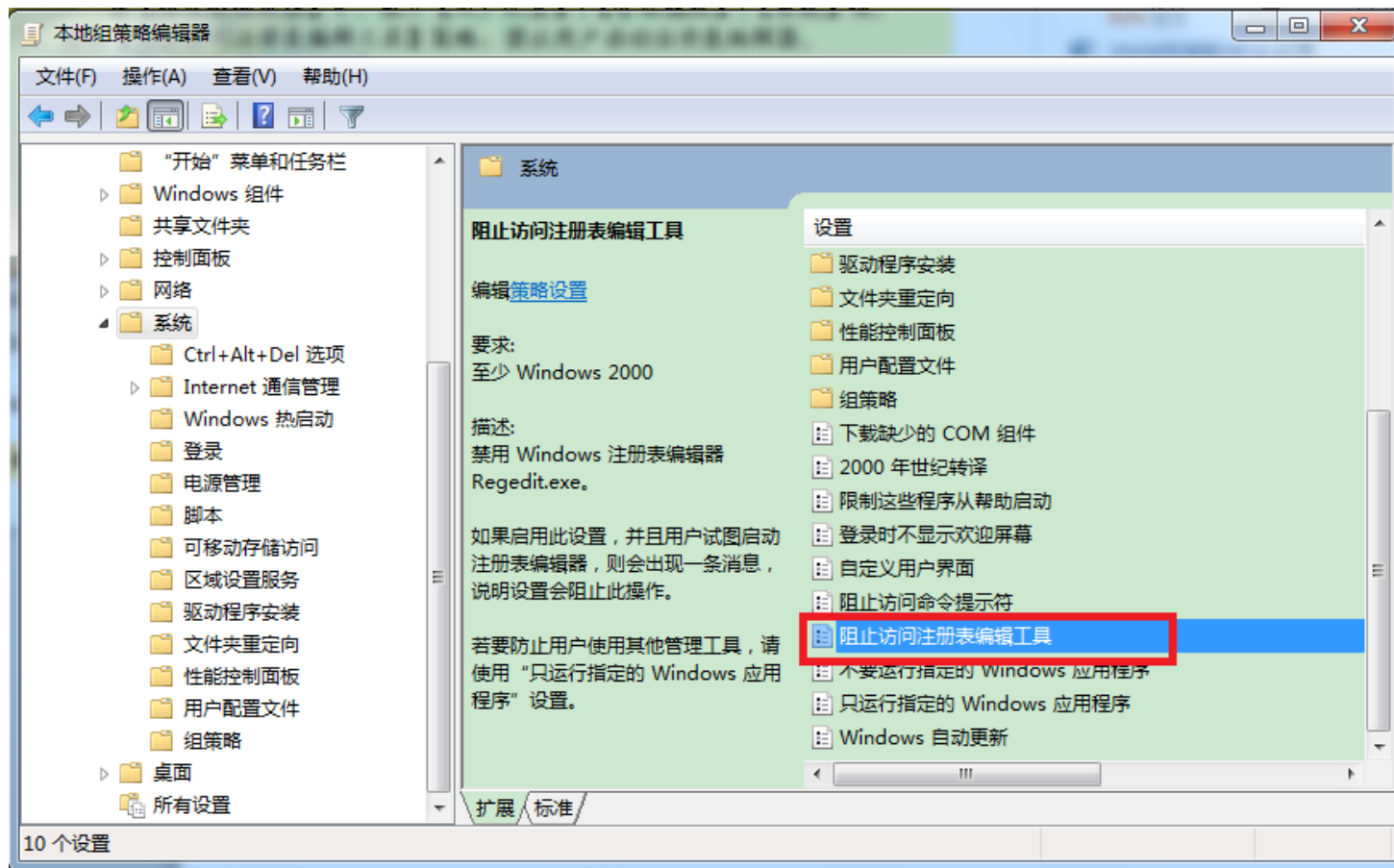
---

- 第三方安全软件介绍与使用
- 组策略编辑器
- 注册表安全
- 访问控制加固
- UAC



# 注册表安全

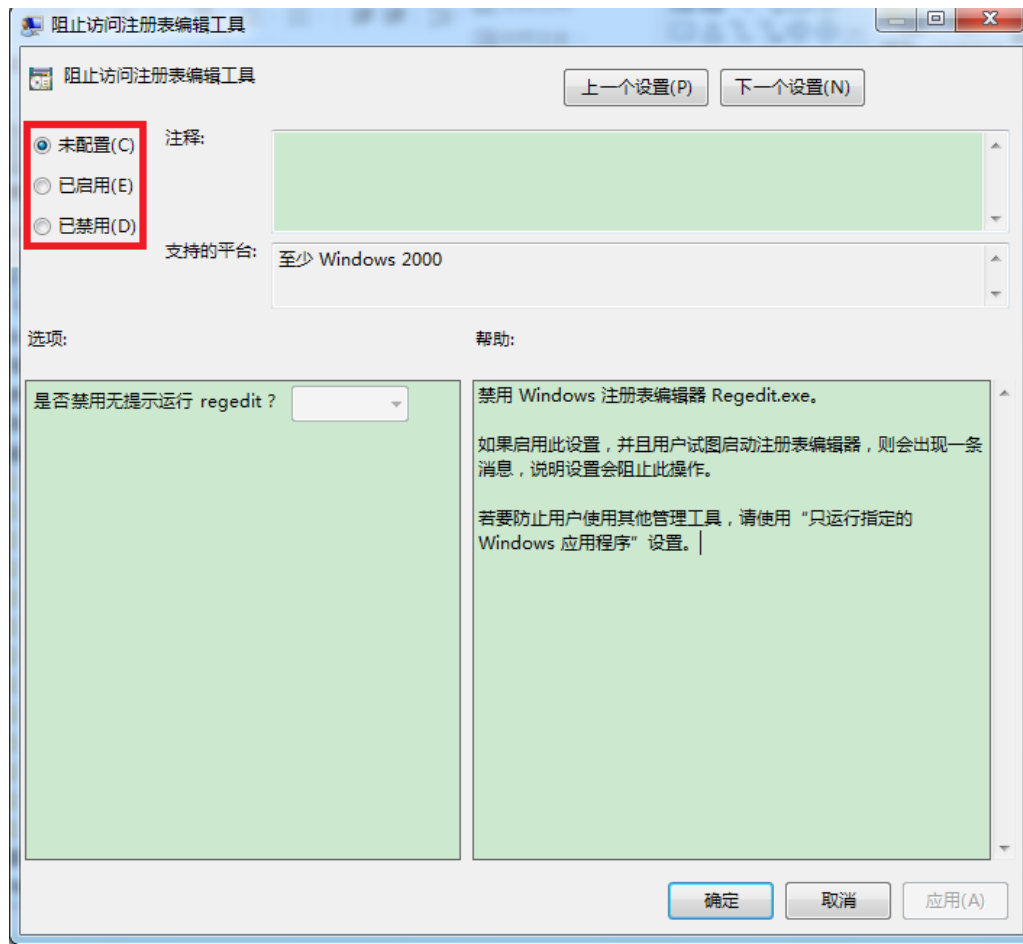
- 通过组策略编辑器禁用注册表编辑器





## 注册表安全

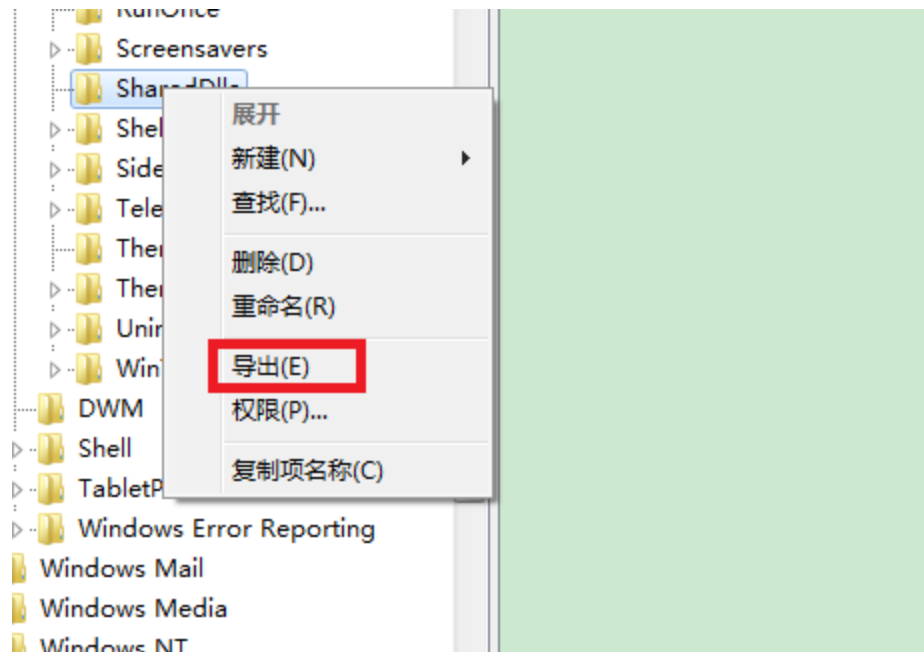
- 打开配置界面，选择“已启用”，点击“确定即可”





- 备份注册表项

—运行regedit.exe,在想要备份的注册表节点右键选择“导出”，保存文件后缀名为.reg



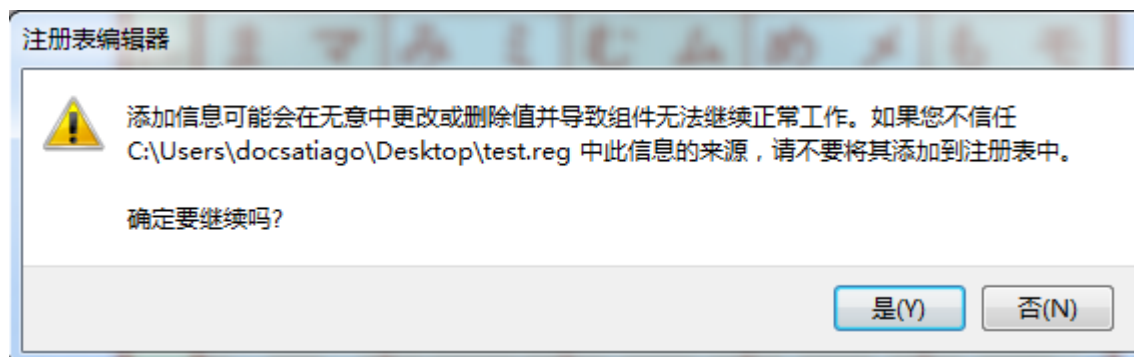




## 注册表安全

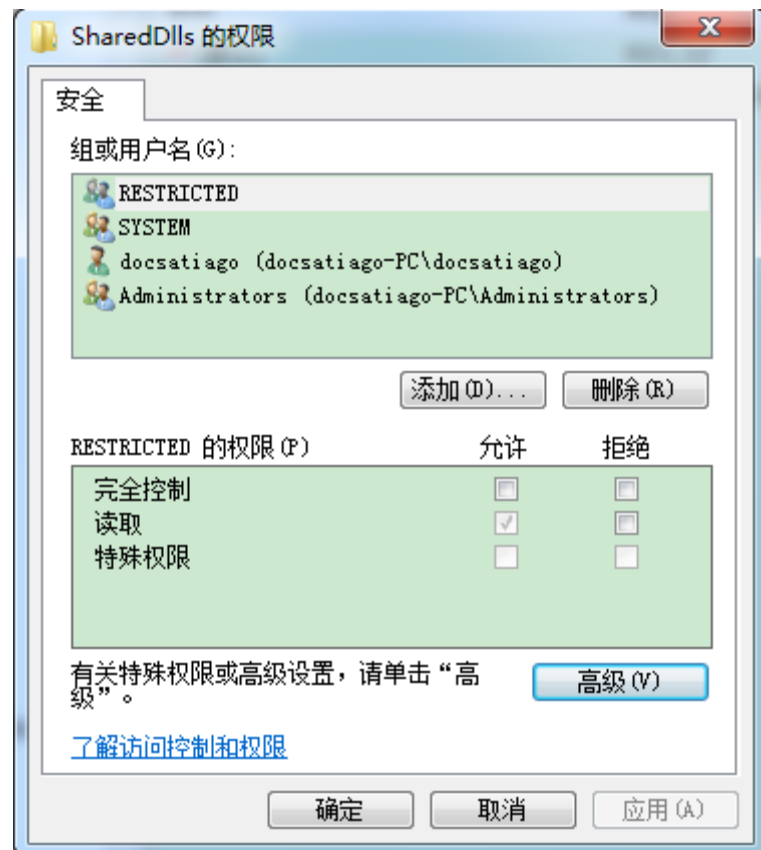
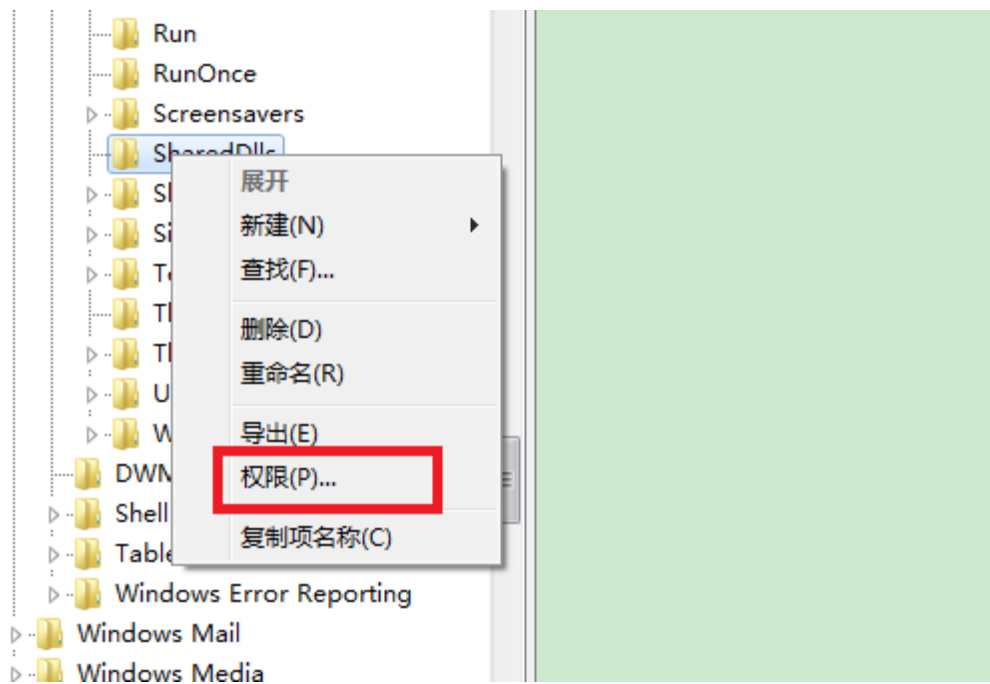
- 还原注册表项

—双击导出的注册表文件，看到提示后点击“确定”  
则自动导入





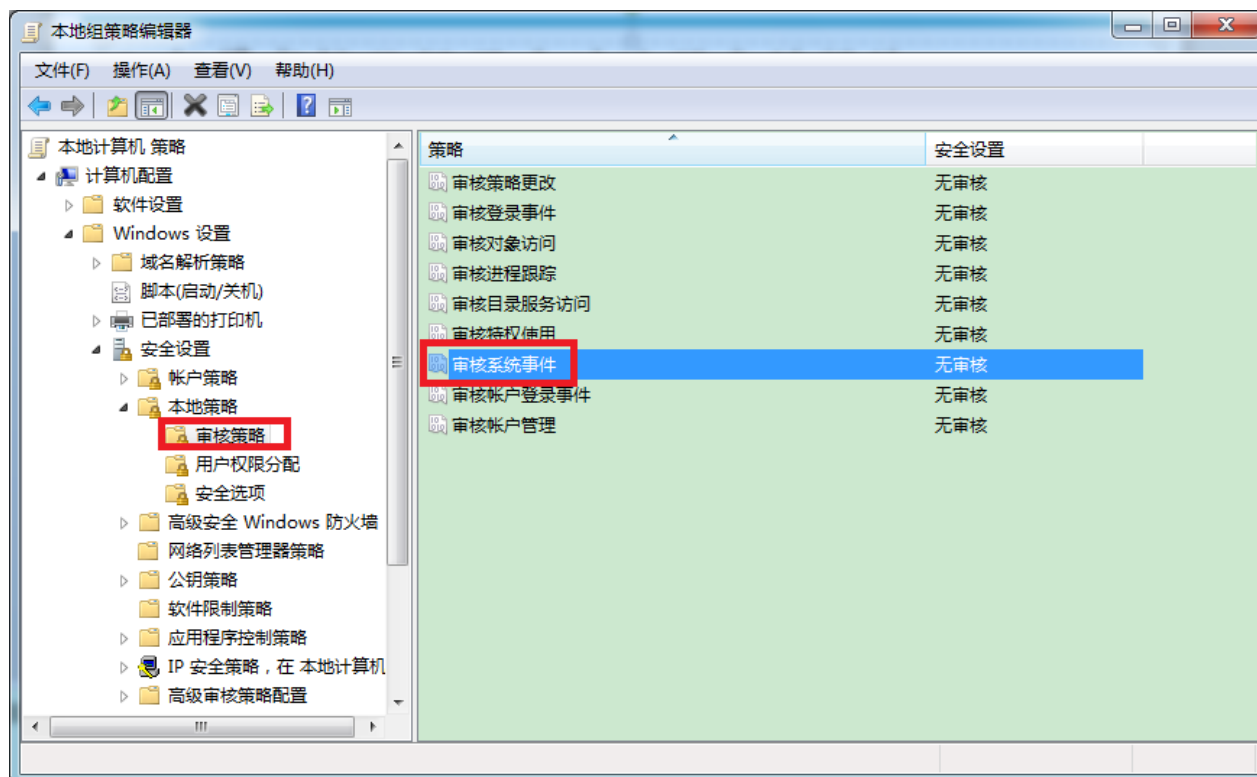
- 设置对注册表的访问权限





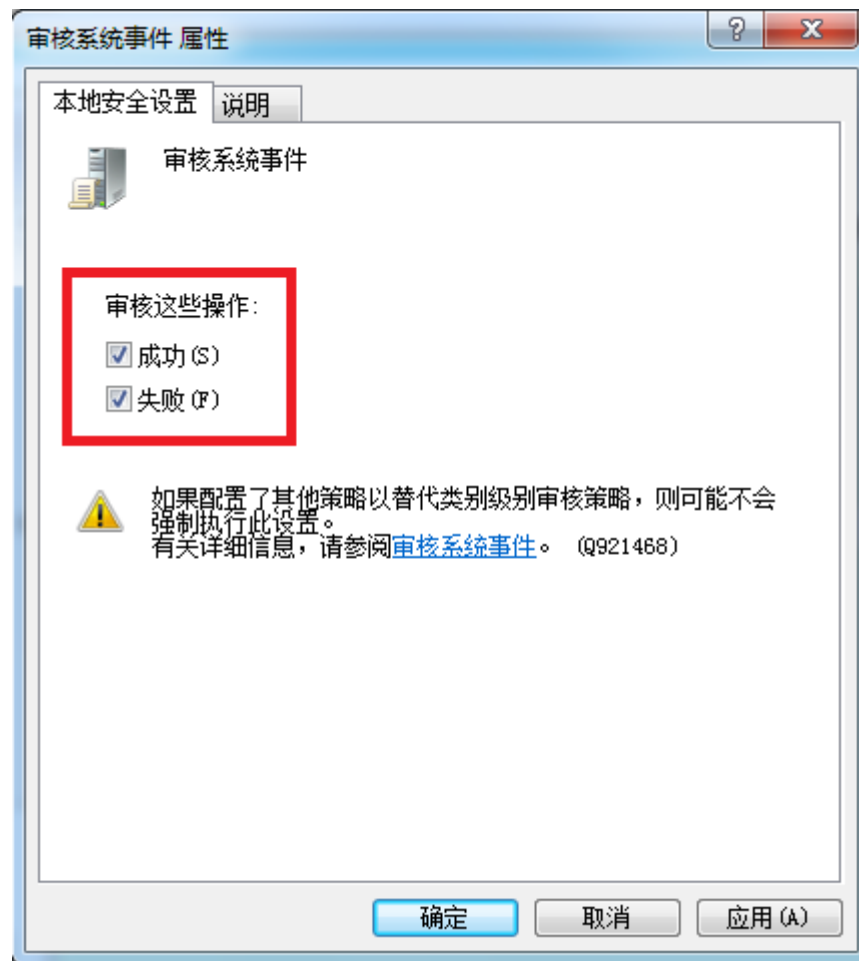
# 注册表安全

- 部署审核监视用户对注册表的操作  
—选择组策略编辑中的“审核策略”-“审核系统事件”





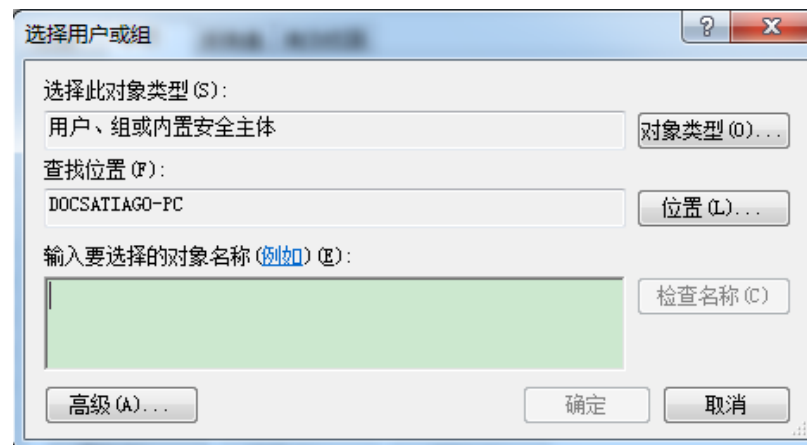
- 启用“审核系统事件”配置





## 注册表安全

- 打开对应的权限对话框，该对话框中单击“高级”-“审核”选项卡，单击“添加”按钮进入对话框，在此选择要审核的用户或组。

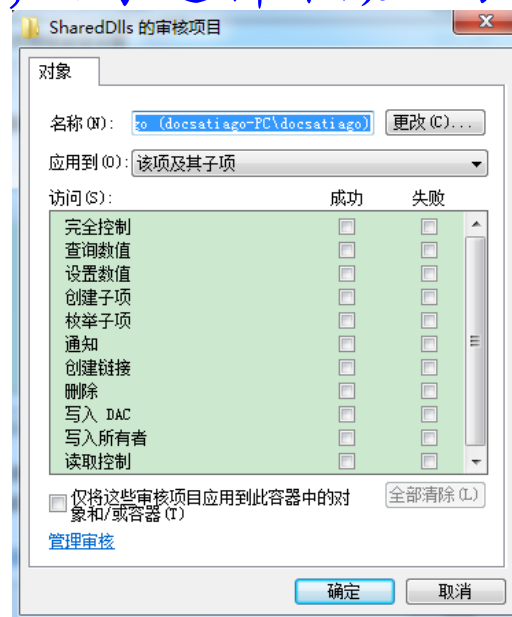




## 注册表安全

- 审核的用户或者组添加完毕后，点击“确定”进入“审核项目”对话框

—针对每个权限选择要进行的审核类型。如果希望跟踪权限的成功使用，就选择相应的“成功”选项；如果希望更正权限的失败使用，则选择相应的“失败”选项





## 本章内容提要

---

- 第三方安全软件介绍与使用
- 组策略编辑器
- 注册表安全
- 访问控制加固
- UAC



## 温故：访问控制的基本概念

- 主体

—主动的实体，是访问的发起者，它造成了信息的流动和系统状态的改变，主体通常包括人、进程和设备等

- 客体

—包含或接受信息的被动实体，客体在信息流动中的地位是被动的，客体通常包括文件、设备、信号量和网络节点等

- 访问

—是使信息在主体和客体之间流动的一种交互方式

- 读、写、执行等





## 温故：访问控制的基本概念

- 授权访问

- 主体访问客体的允许，授权访问对每一对主体和客体来说是给定的

- 安全访问策略

- 一套规则，可用于确定一个主体是否对客体拥有访问能力

- 主体对客体的操作行为集和约束条件集

- 访问控制的三要素

- 主体、客体、安全访问策略



## 温故：访问控制模型

- 访问控制的三个基本方面

- 认证

- 身份认证：客体对主体的识别认证
    - 客体和主体的身份可以随着时间、应用场景而改变

- (访问控制)策略实现：访问授权

- 授权主体对客体可以正常访问
    - 非授权主体对客体无法访问

- 访问审计

- 记录访问历史，实现不可抵赖性



## 温故：Windows的访问控制机制

---

- 主体
  - 帐户 / 用户组
- 客体
  - 文件 / 文件夹 / 注册表
- 访问控制策略
  - DACL
  - 组策略（编辑器）
    - gpedit.msc



---

由“绕过Windows系统登录认证机制”说起

Show Time!

---

中国传媒大学



## 温故：系统安全的分层模型

人

应用系统/服务

操作系统

网络基础设施

IT物理环境

- 空口令或弱口令
- 输入法漏洞直接绕过登录认证
- Windows XP默认的管理员空口令后门
  - 默认安全机制的缺陷
- 使用Windows PE光盘
  - 预置系统后门
    - 屏幕键盘：osk.exe
    - shift后门：sethc.exe
    - 放大镜：magnify.exe

物理安全是上层安全的基础



---

如何加固系统堵住这些漏洞呢?

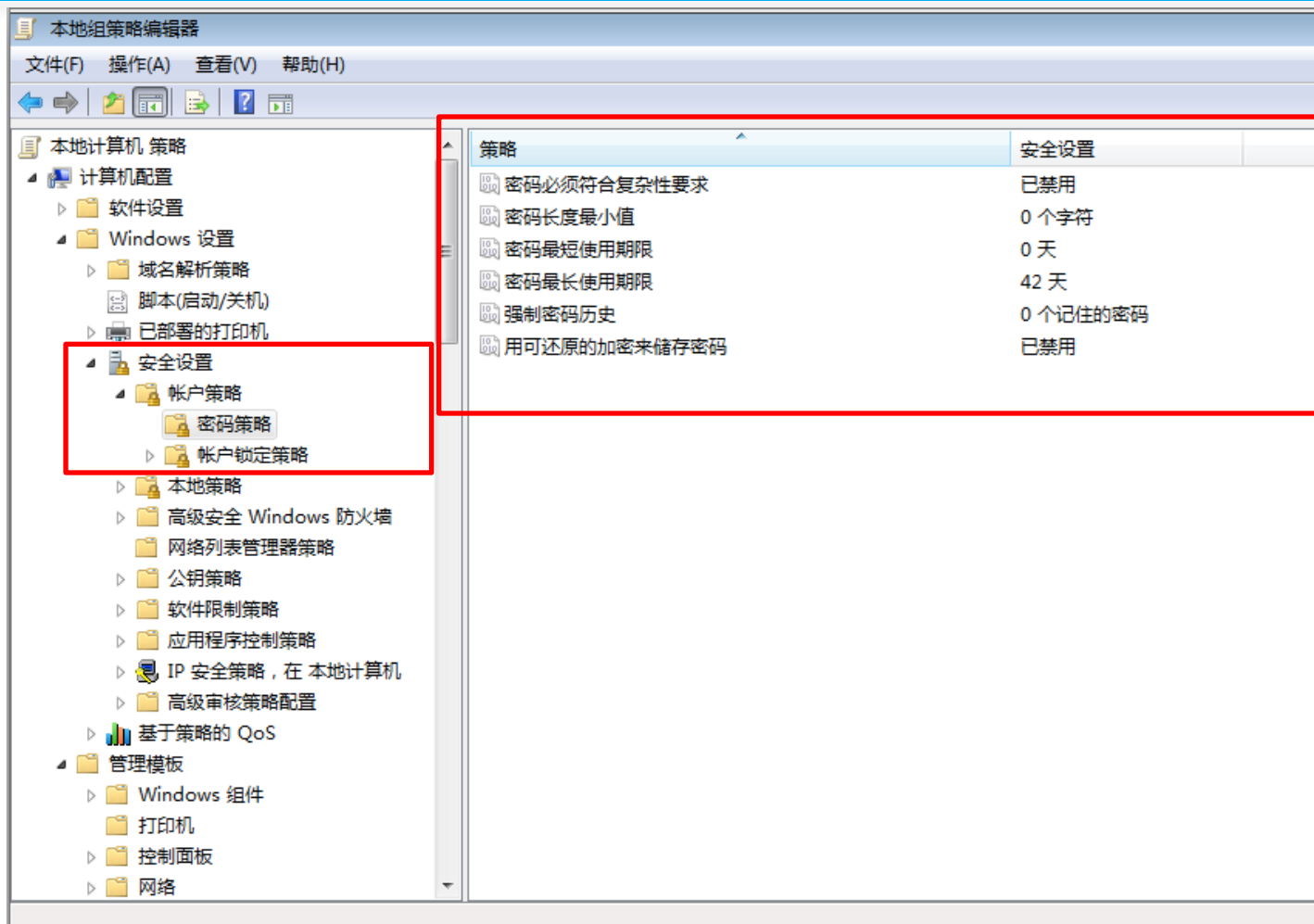


## 认证安全加固机制

- 空口令或弱口令
- 输入法漏洞直接绕过登录认证
- Windows XP默认的管理员空口令后门
  - 默认安全机制的缺陷
- 使用Windows PE光盘
  - 预置系统后门
    - 屏幕键盘: osk.exe
    - shift后门: sethc.exe
    - 放大镜: magnify.exe
- 口令强度强制要求
- 使用最新版本的软件
- 使用最新的操作系统
  - 保持自动更新
  - 勤打补丁
- 启用硬件安全机制
  - BIOS安全机制
    - 上电加密
    - 硬盘加密
  - 做好物理安保措施



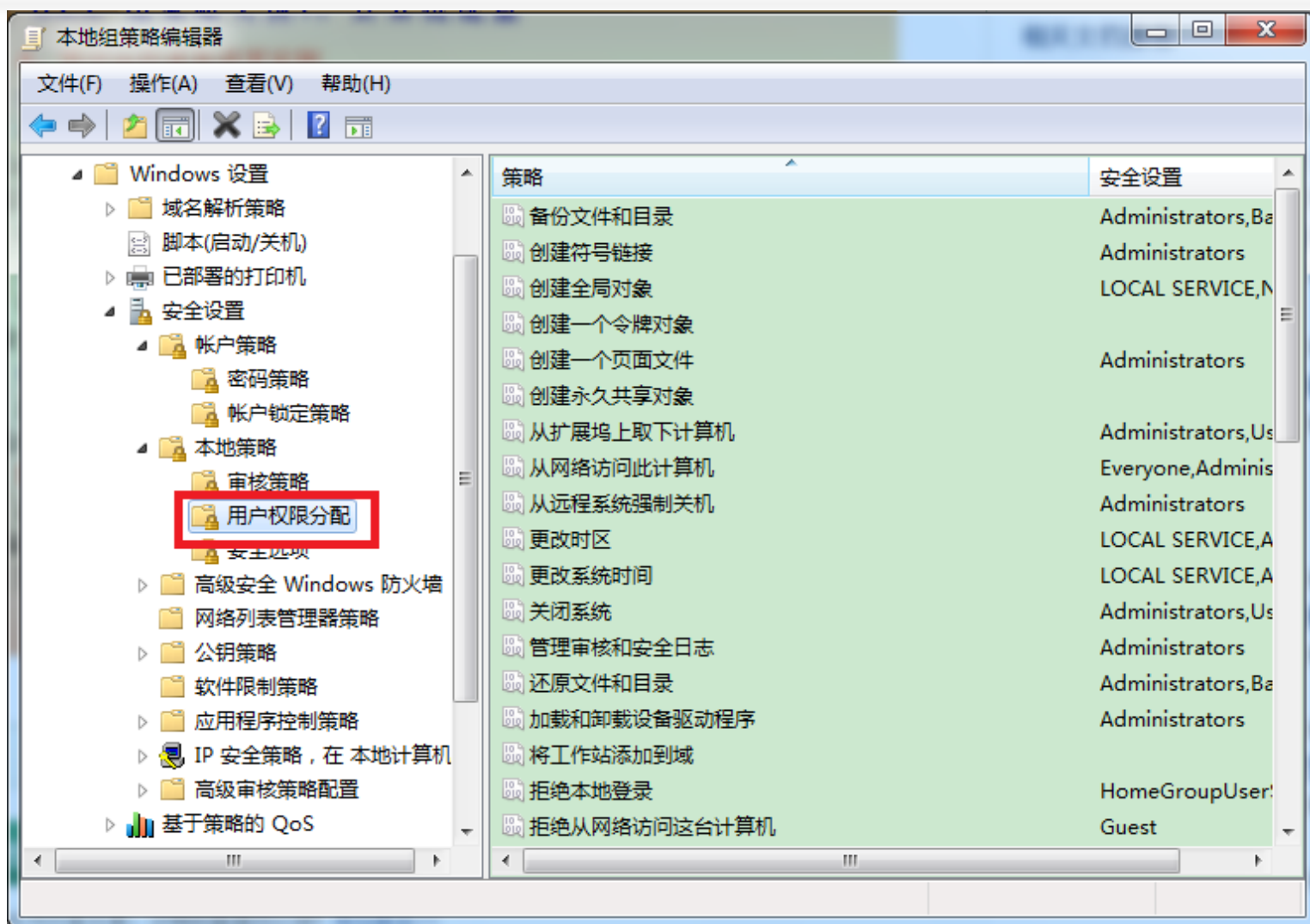
# 通过组策略编辑器来设置强制口令策略







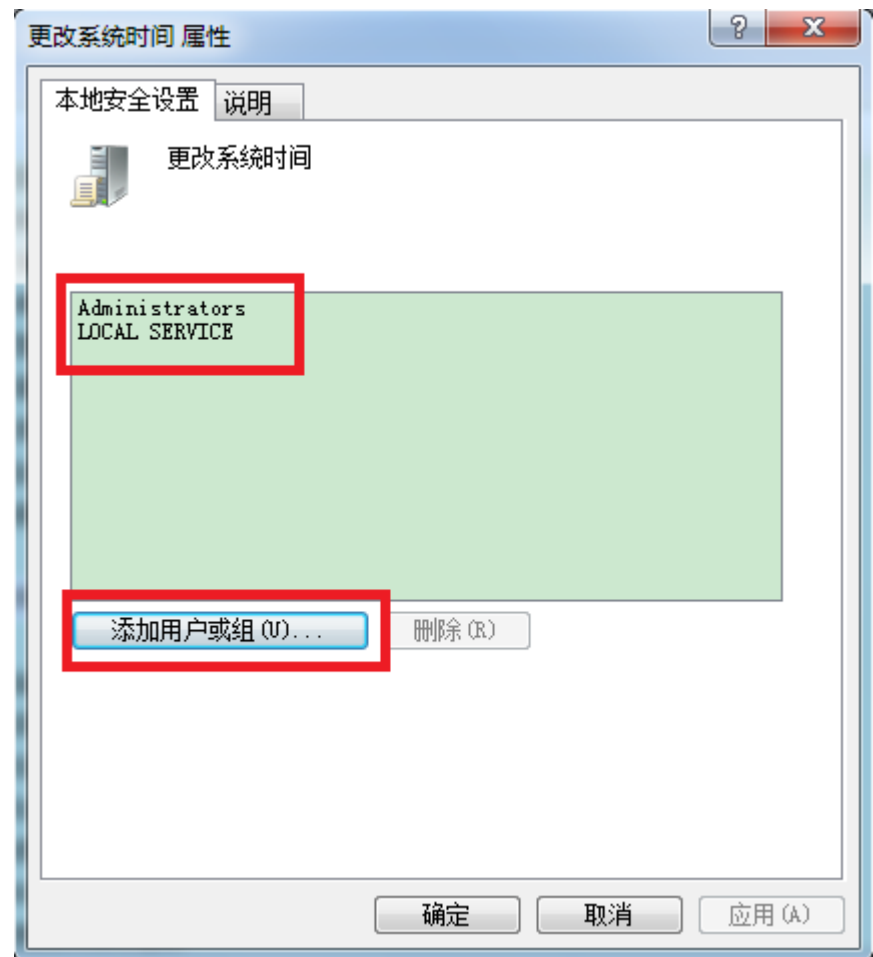
## 通过组策略编辑器来设置或者更改用户权限(1/2)





## 通过组策略编辑器来设置或者更改用户权限(2/2)

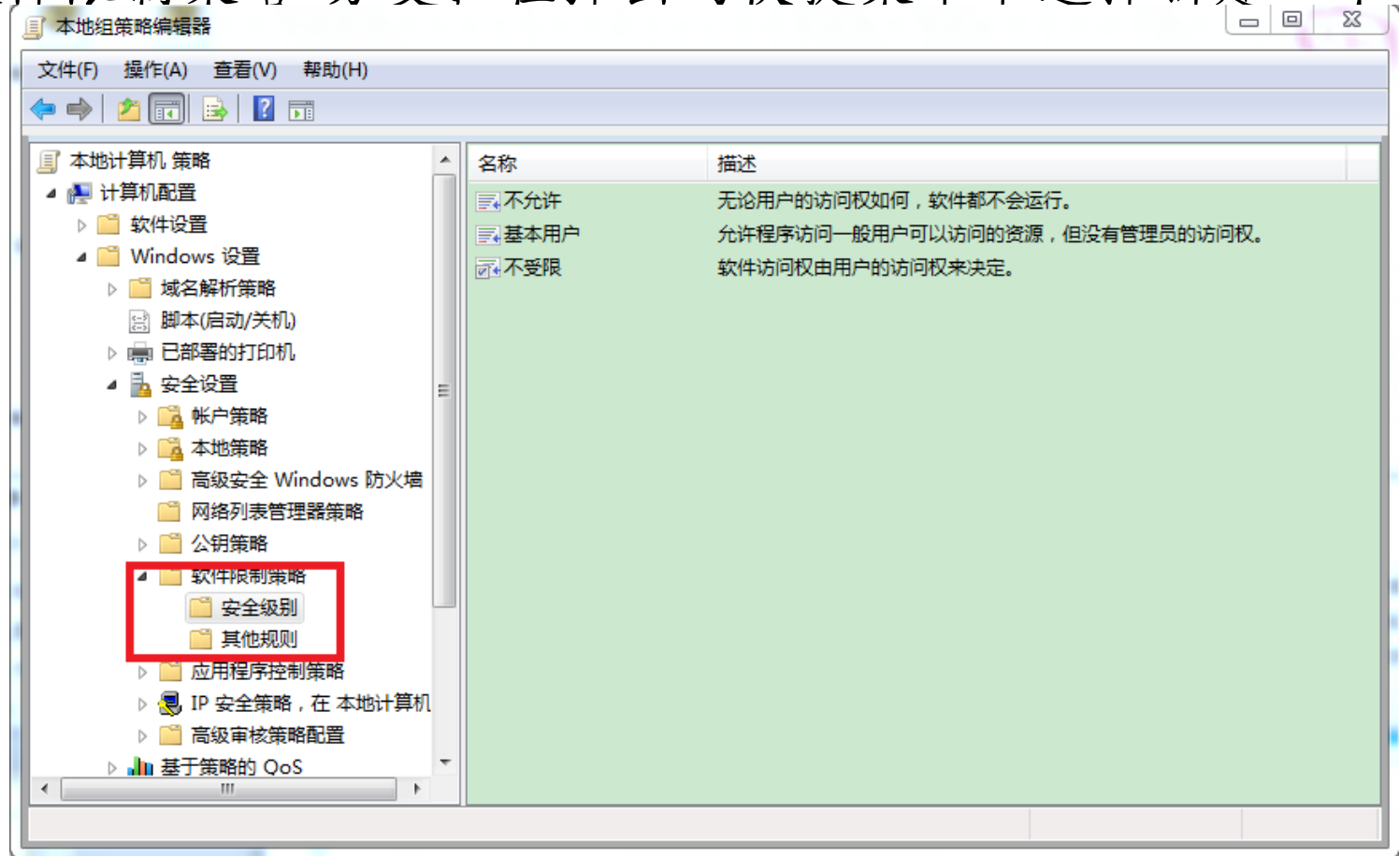
- 点击其中一项的属性菜单，即可为对应的配置添加用户或者用户组





## 软件运行限制(1/3)

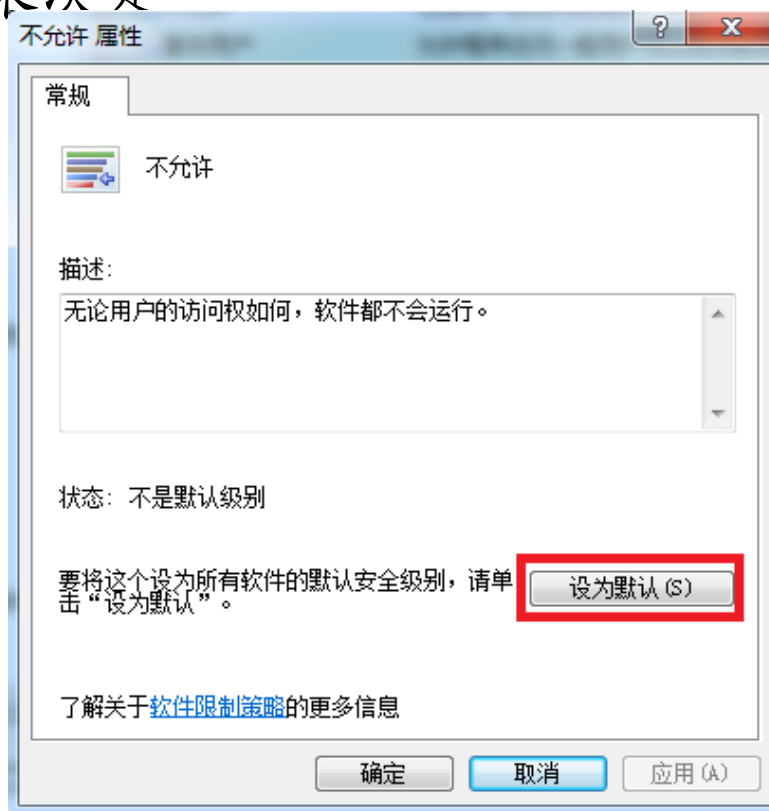
- 在"计算机配置"→"Windows设置"→"安全设置"分支中，右键选中"软件限制策略"分支，在弹出的快捷菜单中选择新建一个策略





## 软件运行限制(2/3)

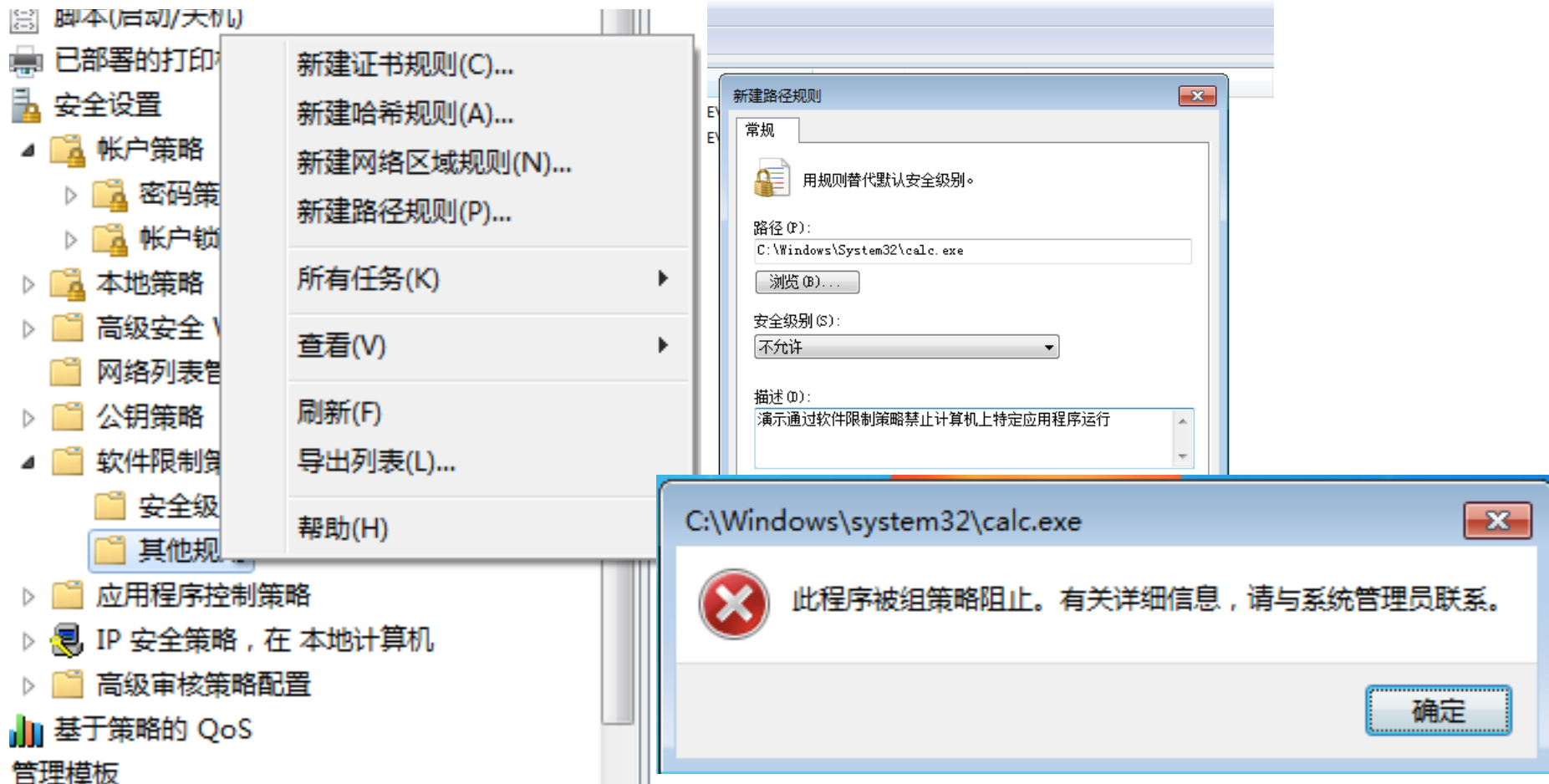
- 不允许的：无论用户的访问权如何，软件都不会运行；
- 不受限的：这是默认的安全级别，其解释为“软件访问权由用户的访问权来决定”





## 软件运行限制(3/3)

- 注销重新登录后策略才会生效





## 本章内容提要

---

- 第三方安全软件介绍与使用
- 组策略编辑器
- 注册表安全
- 访问控制加固
- UAC



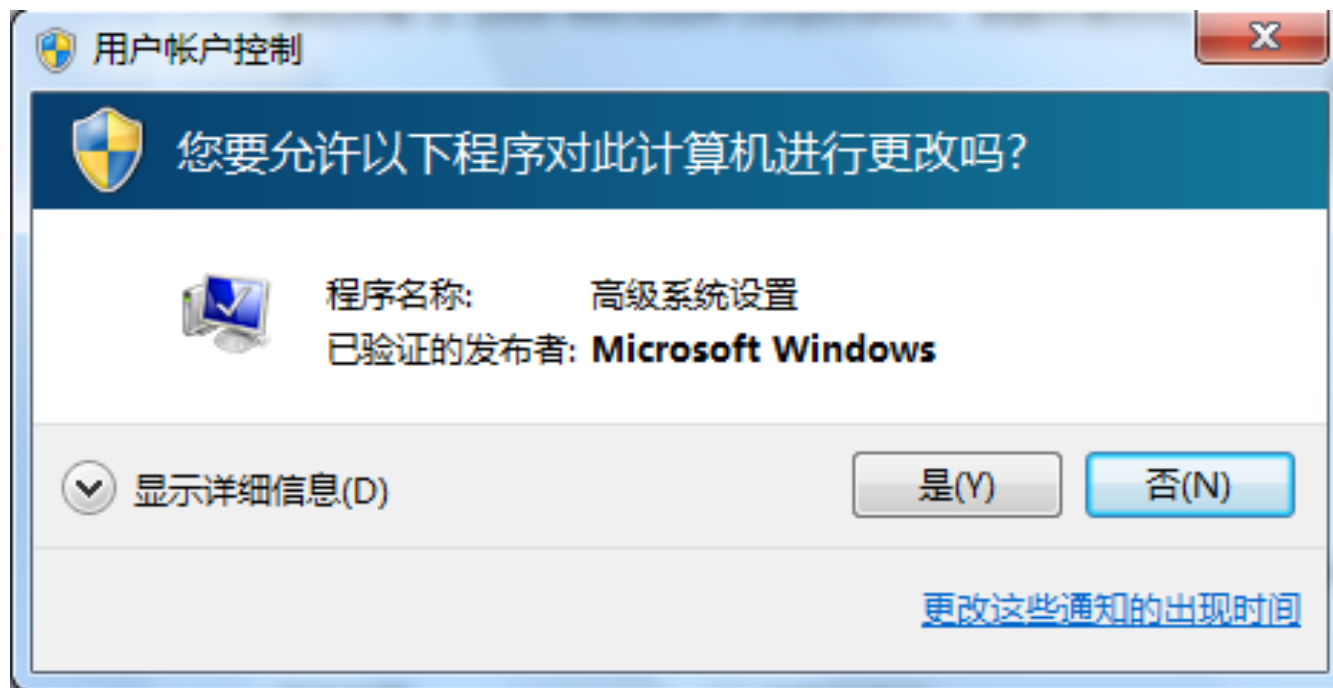
## UAC概述

- UAC(User Account Control, 用户帐户控制)是微软为提高系统安全而首先在Windows Vista中引入的新技术, 它要求用户在执行可能会影响计算机运行的操作或执行更改影响其他用户的设置的操作之前, 提供权限或管理员密码
- 通过在这些操作启动前对其进行验证, UAC可以帮助防止恶意软件和间谍软件在未经许可的情况下在计算机上进行安装或对计算机进行更改



## 修改系统设置时UAC提示

- 可能会影响本计算机其他用户的 Windows 功能或程序需要许可才能启动。请检查操作的名称以确保它正是要运行的功能或程序







## 有数字签名的程序提权时UAC提示

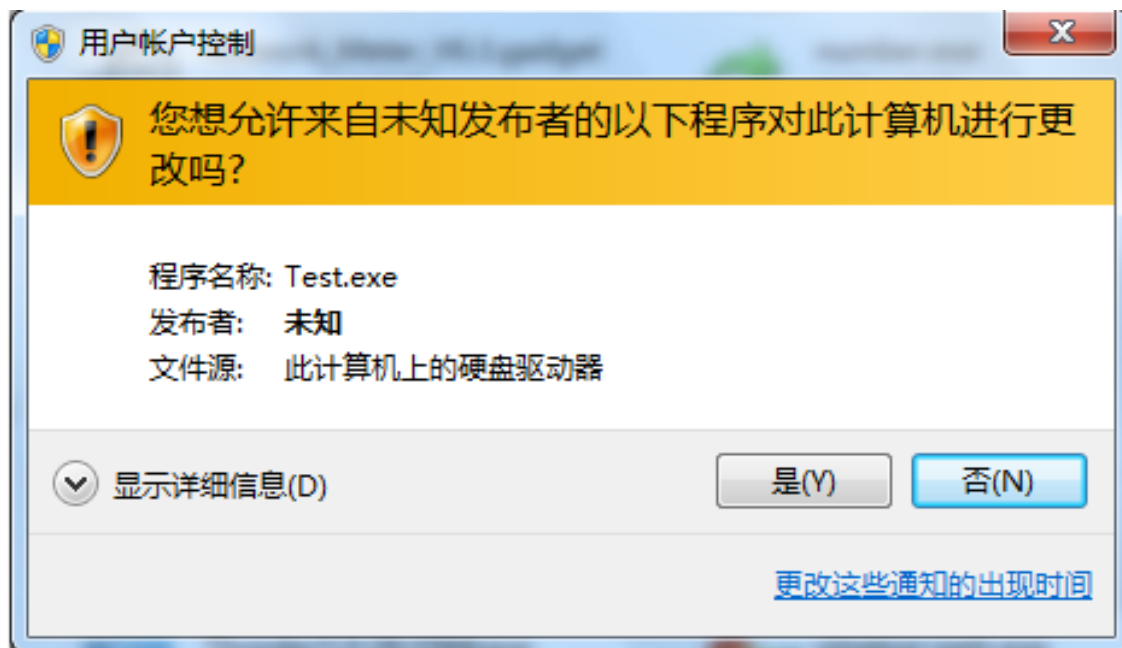
- 不属于 Windows 的的程序需要许可才能启动。它具有指明其名称和发行者的有效的数字签名，该数字签名可以帮助确保该程序正是其所声明的程序。确保该程序正是您要运行的程序。





## 没有数字签名的程序提升权限时UAC提示

- 未能识别的程序是指没有其发行者所提供用于确保该程序正是其所声明程序的有效数字签名的程序。这不一定表明有危险，因为许多旧的合法程序缺少签名。但是，应该特别注意并且仅当其获取自可信任的来源时允许此程序运行





## 需要UAC机制授权的动作

- 配置Windows Update
- 设置家长控制
- 增加或删除用户帐户
- 将文件移动或复制到Program Files或Windows目录
- 改变用户的帐户类型
- 查看其他用户文件夹
- 改变UAC 设置
- 安装ActiveX
- 安装或卸载程序
- 安装设备驱动程序

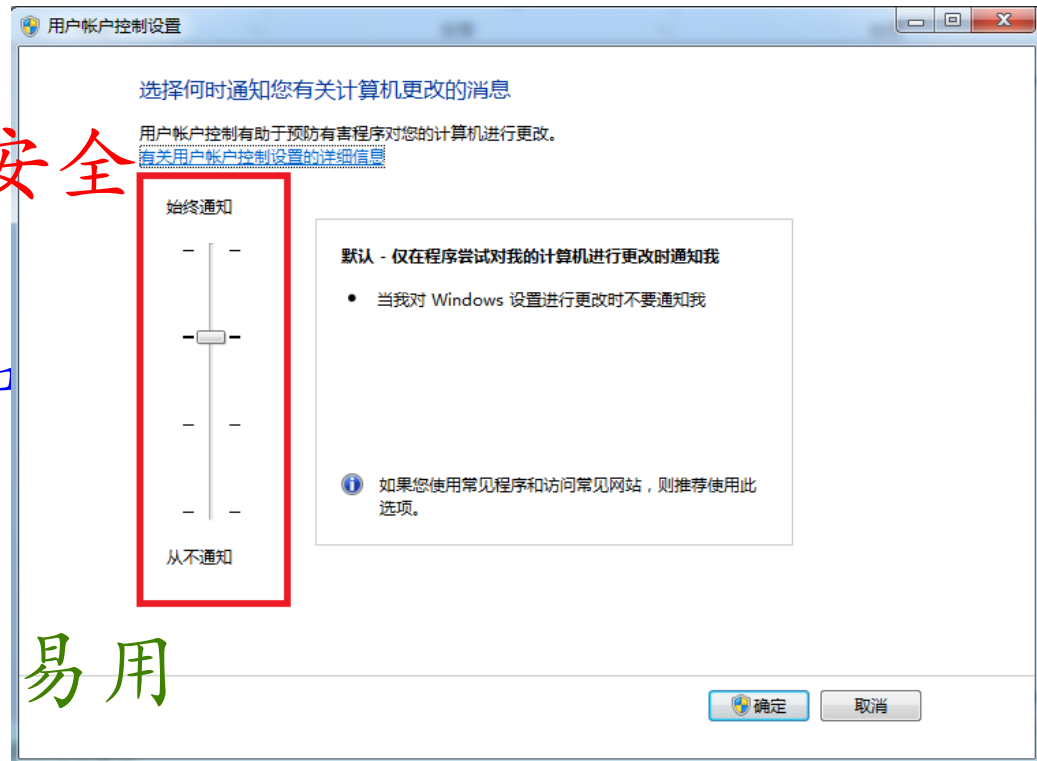


## 修改UAC的安全保护等级(1/4)

- 在“控制面板”-“用户帐户”中，选择“更改用户帐户控制设置”

—Vista的UAC只有“开启”和“关闭”两项功能设置，在Windows7的UAC里增加了四个级别的设置项

安全



易用



## 修改UAC的安全保护等级(2/4)

- 最高的级别是“**始终通知我**”，即用户安装应用软件或者对应用软件进行升级、应用软件在用户知情或者不知情的情况下对操作系统进行更改、修改Windows设置等等，都会向系统管理员汇报，同时屏幕会被锁死并降低亮度



## 修改UAC的安全保护等级(3/4)

- 第二个级别为“**仅在应用程序试图尝试改变计算机时**”通知系统管理员。这个级别是操作系统的默认控制级别。他与第一个级别的主要差异就在于用户主动改变Windows设置时不会通知系统管理员。在这个级别下，即使操作系统上有恶意程序在运行，也不会给操作系统造成多大的负面影响。因为恶意程序不能够在系统管理员不知情的情况下修改系统的配置，如更改注册表、更改IE浏览器的默认页面、更改服务启动列表等等



## 修改UAC的安全保护等级(4/4)

- 第三个级别为“**仅当应用程序试图尝试改变计算机时**”通知系统管理员，其他设置基本和第二级别一致，区别在于屏幕亮度不降低，也不锁屏
- 第四个级别就是所有都不通知即**关闭UAC**



## 课内演示实验

- 实验一 安全软件sreng2的操作视频演示
  - 视频中演示sreng2软件功能启动项目，系统修复，智能扫描等功能的操作和使用
  - 演示软件中的插件的下载
  - 演示软件中的插件的使用方法
  - 软件的相关的配置信息





## 课内演示实验

- 实验二 安全软件IceSword的操作视频演示
  - 该软件在之前的病毒分析试验中已经使用过了，对该软件也有了相应的了解
  - 在实验中对软件的各项功能做一个简单的操作演示



## 课内学生实验

- 实验 组策略编辑器的使用
  - 提升上网速率
  - 个性化任务栏和开始菜单
  - 个性化桌面设置
  - Windows 资源管理器的安全配置
  - 系统命令提示符，注册表，自动播放
  - 控制面板的配置
  - 帐户策略



## 课后作业（可选）

---

- 如何禁用移动存储设备？
- 如何绕过上述禁用机制？
- 实践你的想法，提交实验报告