病毒实验报告

- xiabee

实验目的

- 运行键盘监控木马，监控键盘，设置开机自启动
- 学习关闭流氓软件

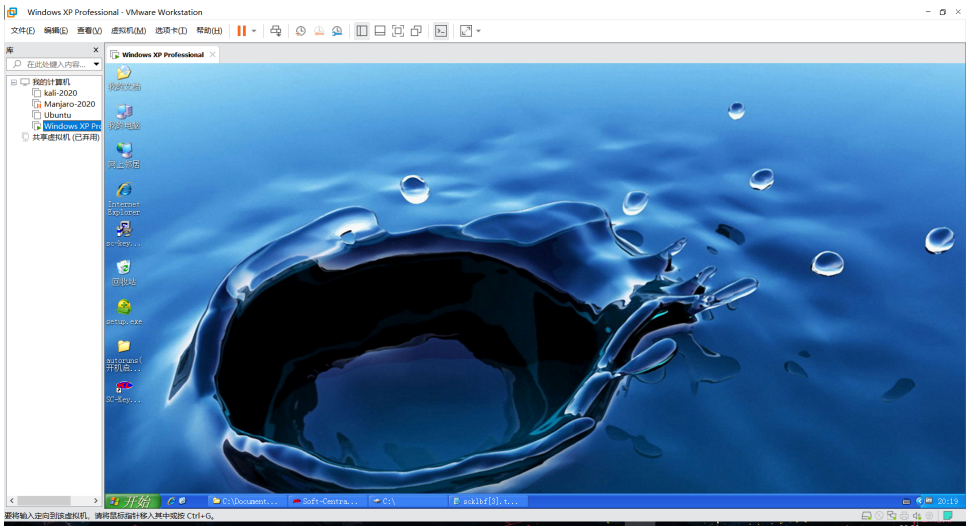
实验操作

- 安装`SC-KeyLog2`键盘监控木马
- 运行木马，观察执行结果
- 设置木马自启动
- 修改启动项，取消360等软件自启动

实验过程

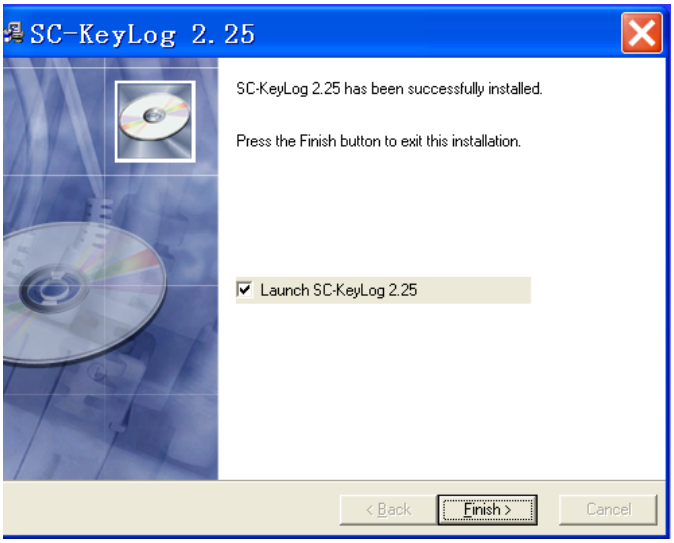
一、安装木马

0x00 安装XP虚拟机

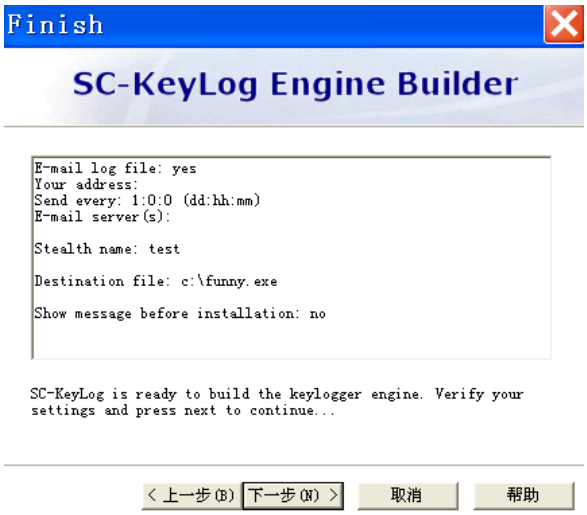


将`Windows XP`虚拟机硬盘文件解压，直接导入`VMware`中运行

0x01 安装木马

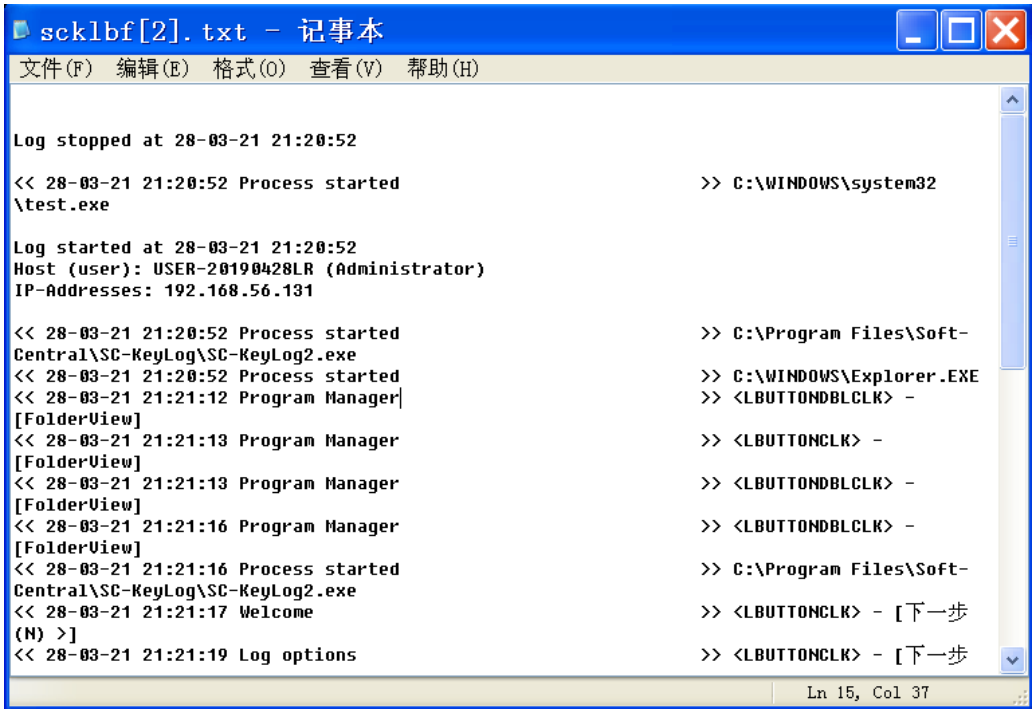


0x02 运行木马



木马名称设置为`test.exe`

0x03 观察记录

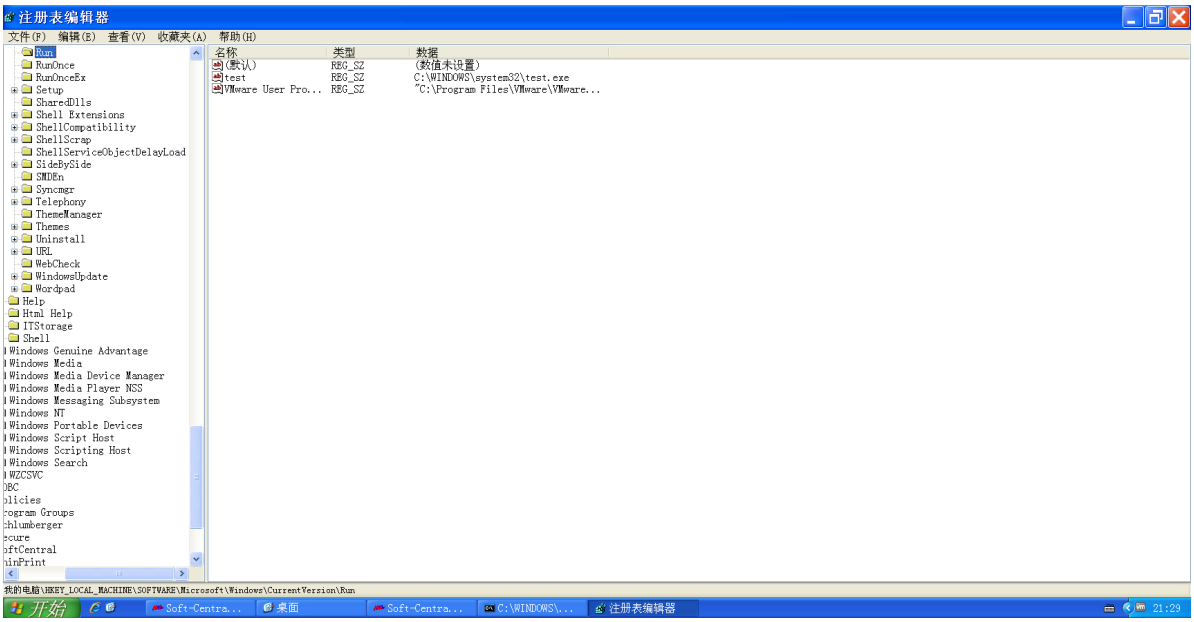


二、设置开机自启动

方法一：修改注册表

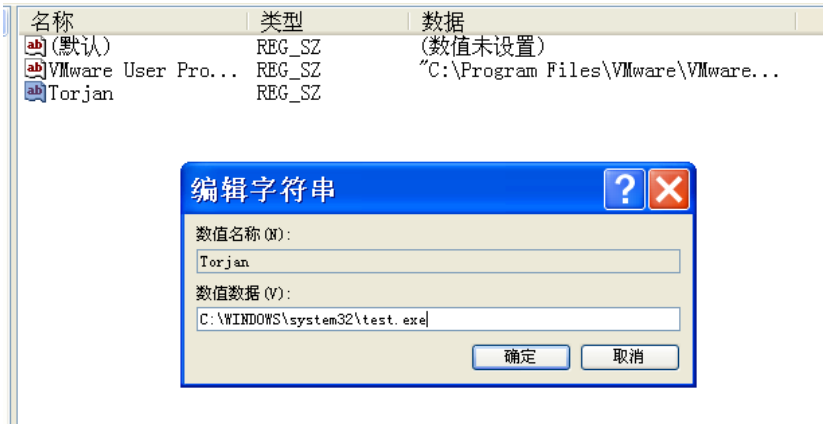
0x00 打开注册表

找到自启动路径：`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

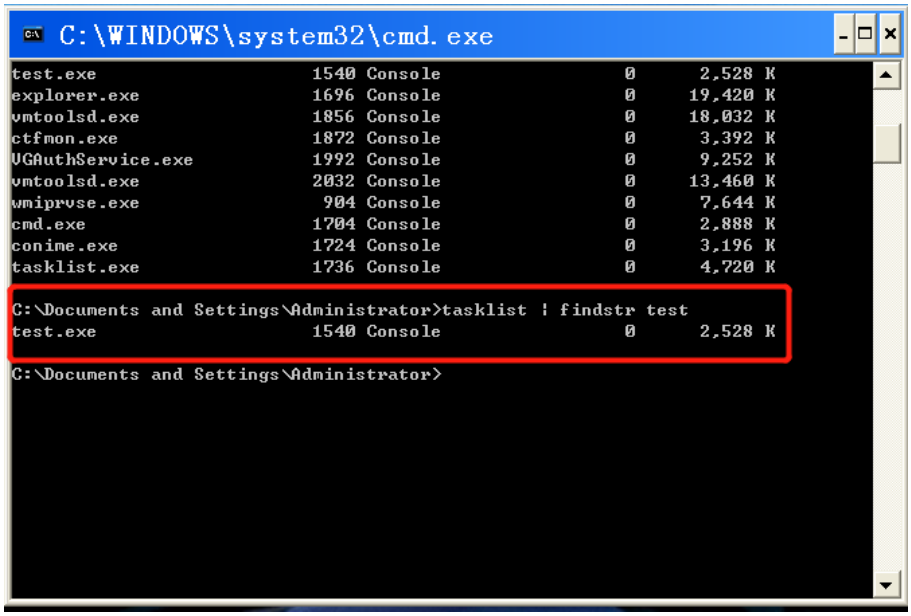


0x01 新建字符串值

创建新字串，设置数据值为木马路径：`C:\WINDOWS\system32\test.exe`

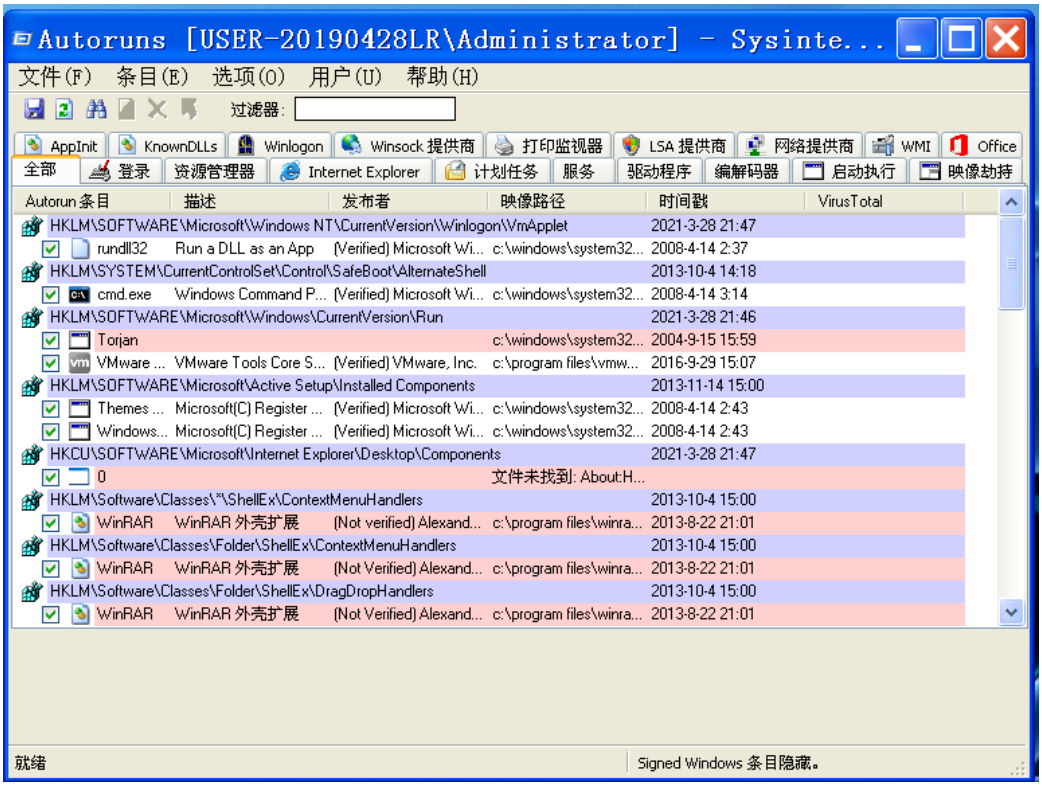


此时重启计算机，`test.exe`已自启动



方法二：启动项快捷管理

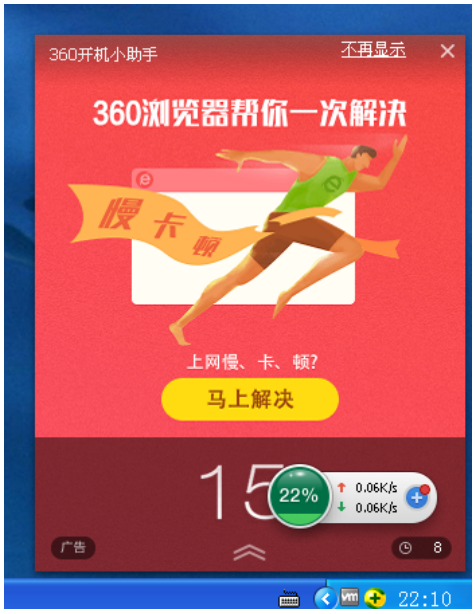
直接运行`autoruns.exe`，管理开机启动项



三、取消360等软件自启动

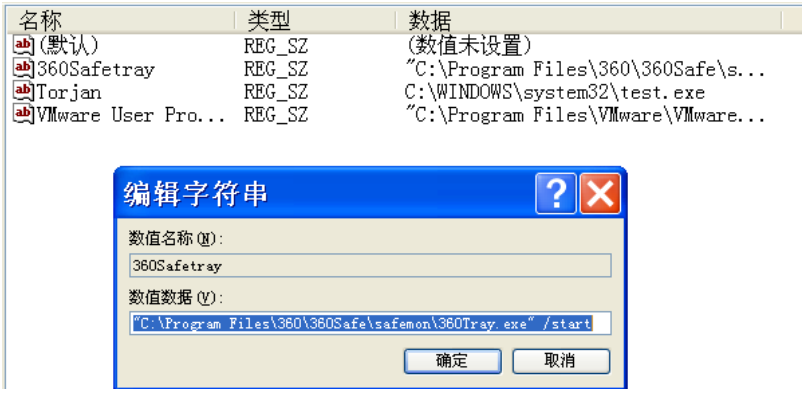
0x00 准备工作

安装360后直接开机，发现360自行启动：

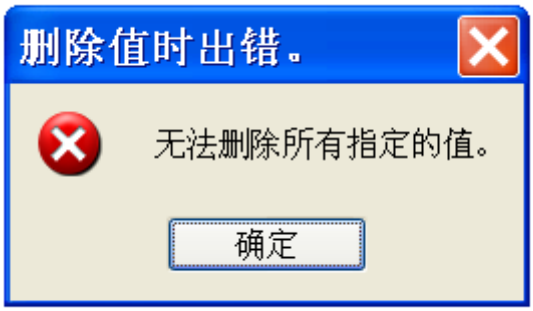


0x01 尝试修改注册表

删除注册表360相关项



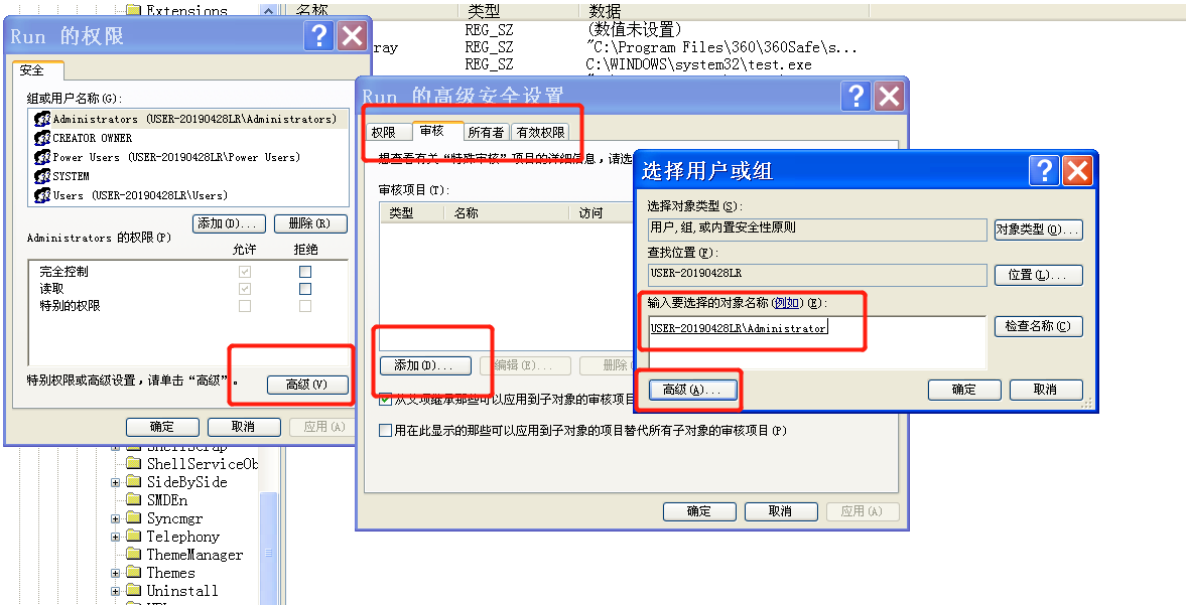
直接删除，权限不足：



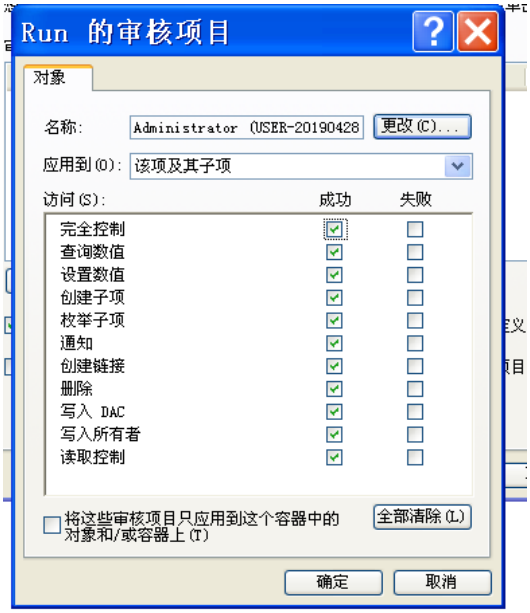
修改`Run`注册表的控制权限，依然权限不足：

0x02 提升审核权限

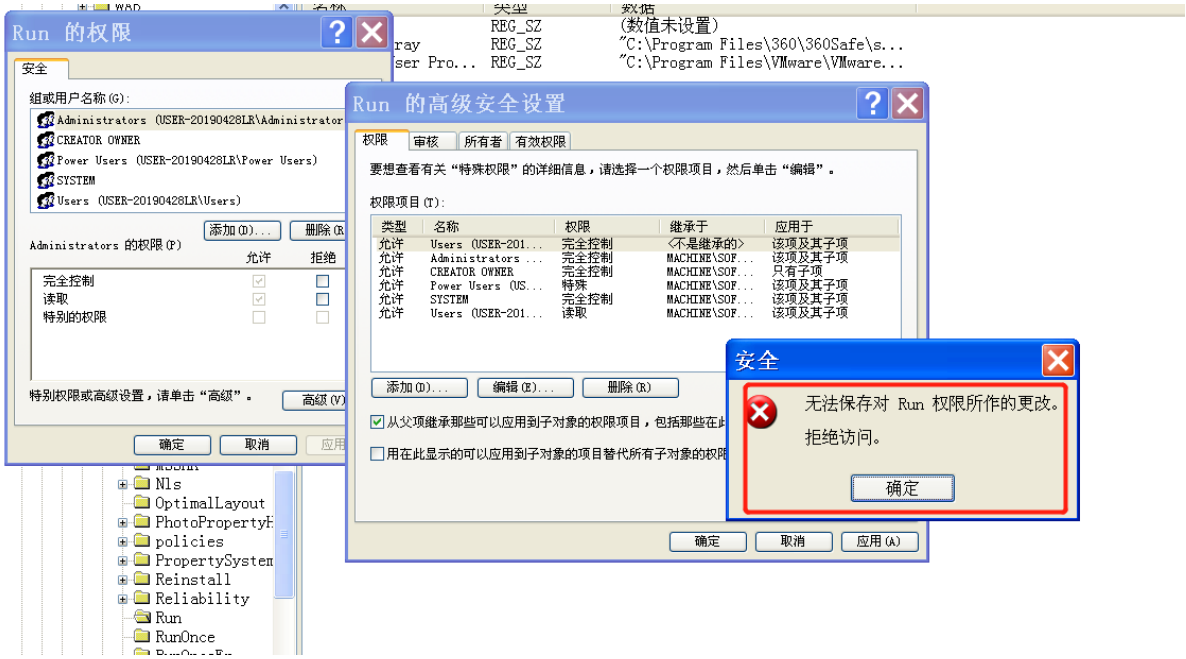
`权限-->高级-->审核-->添加-->高级`，自动检测对象名



设置控制权限：

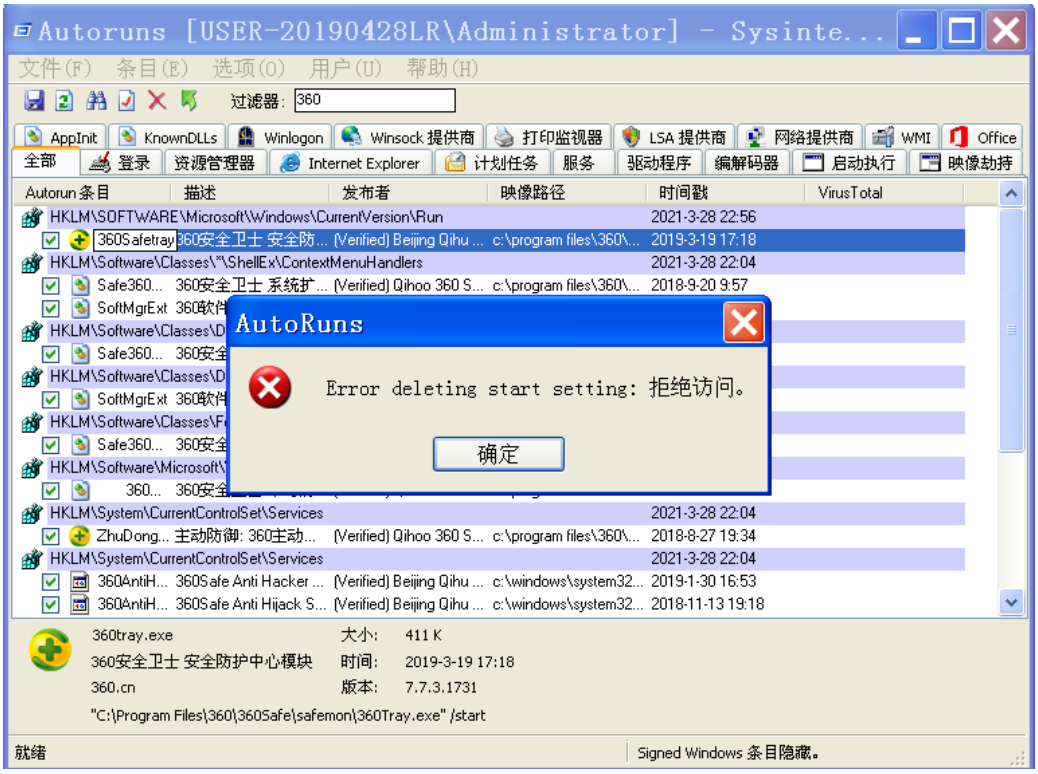


然而依然无法修改……权限被`360Kernel`锁死



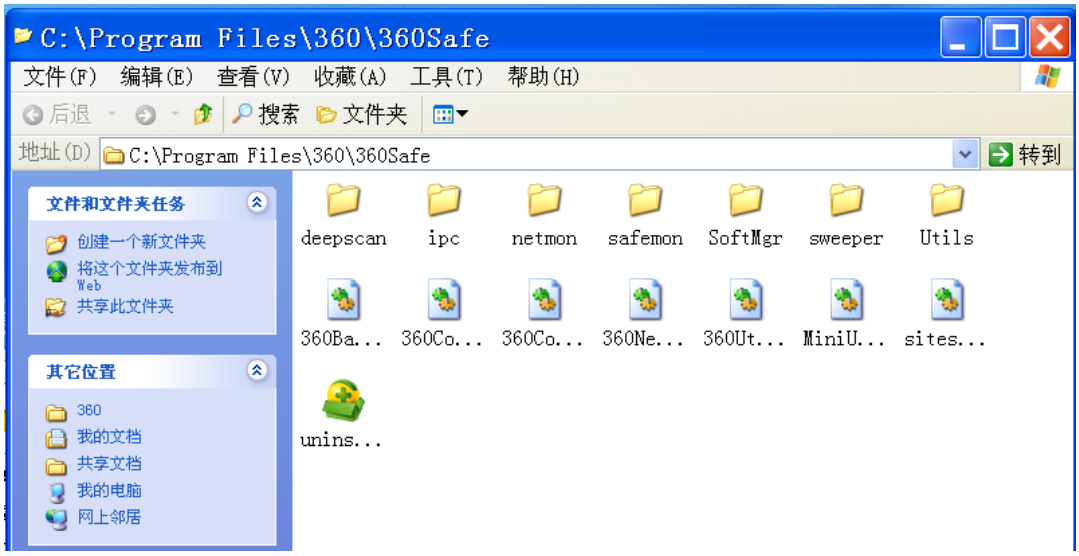
0x03 使用autoruns

搜索360，直接删除注册表相关，依然权限不足：

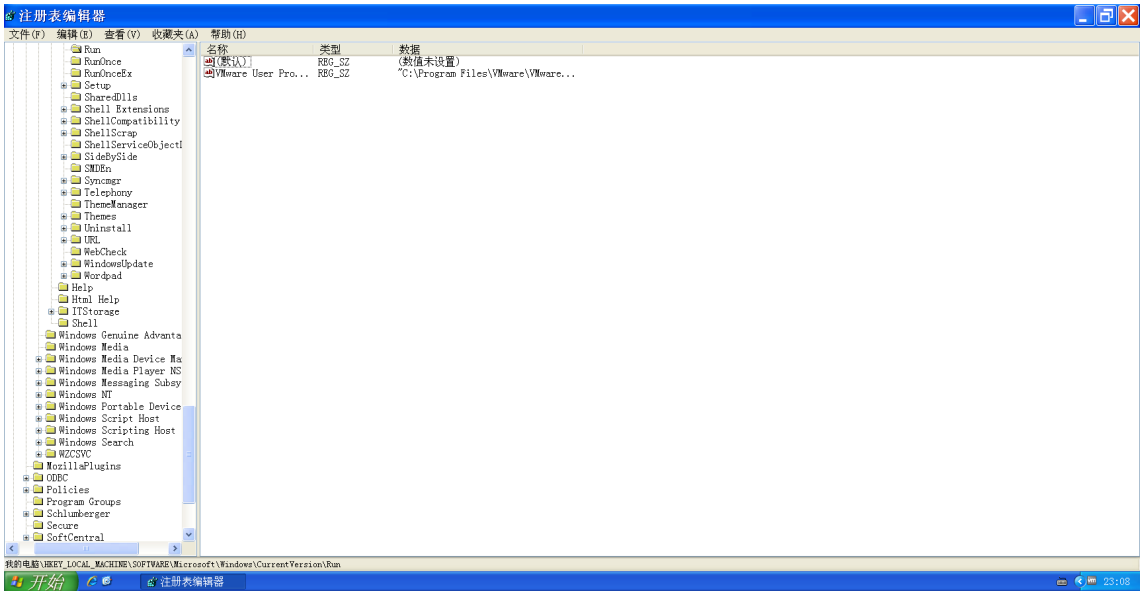


0x04 卸载后再修改

卸载之后的文件夹剩余内容：有文件残余



卸载后注册表内容：启动项已删除



实验心得

- 木马的工作原理与操作流程比较简单，但是做免杀、脱数据以及防溯源比较困难；
  - 本次实验使用的现有木马程序没有添加任何程序壳，被杀毒软件静态特征识别，没能免杀；
  - 木马手动加壳后躲过某杀软的静态识别，但在启动时，行为特征被识别，没能免杀；
  - 此木马脱数据、防溯源的可能性几乎为零；
- 修改注册表以使木马自启动，但隐蔽性差，容易被杀软发现；
- `360`的启动项被`360Kernel`锁死，在卸载之前几乎无法获取到目录控制权限，无法直接通过修改注册表的的方式禁止360的启动；在直接卸载`360`之后会有残留，需要手动清理文件和注册表
- 别装流氓软件，别装流氓软件，别装流氓软件，重要的事情说三遍