“手动查杀”：不使用代码或只使用少量dos, 手动查杀往往并不能彻底将病毒清除。

手动查杀流程：1排查可疑进程。（这要求我们熟悉正常进程）2检查启动项3删除病毒。在排查可疑进程和检查启动项的过程中往往可以确定病毒主体的位置，这样就可以顺藤摸瓜地删除病毒的主体文件4修复被病毒破坏的文件（这往往无法直接纯手工完成，往往需要利用相应的软件）

学会手动杀毒的重要性：杀毒软件具有严重的滞后性；编写专杀工具的基本思路流程和手动查杀是一致的。

运行熊猫烧香。1先排查可疑进程，打开任务管理器发现熊猫烧香已经使得任务管理器一闪而过，无法观察。破解方法：cmd tasklist（话说exe不能全局禁用cmd?），找到病毒进程及其pid后使用taskkill /f /im [taskpidd]命令强制终止进程。

2检查启动项。运行msconfig,