识别系统的非法进程及杀灭 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/470/2021_2022__E8_AF_86_E5_88_AB_E7_B3_BB_E7_c67_470802.htm 进程的重要性体现在可以通过观察它，来判断系统中到底运行了哪些程序，以及判断系统中是否入驻了非法程序。正确地分析进程能够帮助我们在杀毒软件不起作用时，手动除掉病毒或木马。 望进程 如何知道系统中目前有哪些进程？ 在Windows98/Me/2000/XP/2003中，按下“ Ctrl Alt Delete ”组合键就可以直接查看进程，或打开“ Windows 任务管理器 ”的“ 进程 ”选项来查看进程。通常来说，系统常见的进程有winlogon.exe，services.exe，explorer.exe，svchost.exe等。要熟悉进程，首先就要熟悉最常见的系统进程，这样当发现其它奇怪的进程名（如HELLO，GETPASSWORD，WINDOWSSERVICE等等）时就方便判断了。 常规杀灭进程法 1.有的进程在进程选项中无法删除，这时可以打开注册表编辑器（在“ 开始→运行 ”中键入regedit），找到“ HKEY_LOCAL_MACHINE＼SOFTWARE＼Microsoft＼Windows＼CurrentVersion＼Run ”下面的键，将可疑的选项删除。 2.另外，还可以通过系统的“ 管理工具 ”里面的“ 服务 ”查看目前的全部进程。这里重点要看服务中启动选项为“ 自动 ”的那部分进程，检查它们的名字、路径以及登录账户、服务属性的“ 恢复“ 里面有没有重启计算机的选项（有些机器不断的重新启动的秘密就在这里）。一旦发现可疑的名字需要马上禁止此进程的运行。 而要彻底删除这些程序进程可以用下面的办法： 打开注册表编辑器,展开分支

“ HKEY_LOCAL_MACHINE＼SYSTEM＼Current＼Control SetServices ”,在右侧窗格中显示的就是本机安装的服务项，如果要删除某项服务，只要删除注册表中相关键值即可。 3.除了上面两种方法，我们还可以先查看这个进程文件所在的路径和名称。重启系统，按F8键进入安全模式，然后在安全模式下删除这个程序。 这里，笔者编写了容易被大家认出来的非法进程服务（系统进程）举例说明：HELLO-WORLD SERVICE 1。我们可以轻松地在进程列表和“ 服务 ”中找到它。根据上面的方法，我们可以把这个进程杀掉或禁用。 不少病毒和木马是以用户进程的形式出现的，所以大部分人认为“ 病毒是不可能获得‘ SYSTEM ’权限的 ”。其实，这是个错误的想法，很多病毒或木马也能获得SYSTEM权限，并伪装成系统进程出现在你面前。所以这类病毒就相当容易迷惑人，遇到这种情况，只有不断提高并关注系统安全方面的知识，才能准确判断该进程是否安全。 