如何巧妙从进程信息中判断病毒和木马思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/624/2021_2022__E5_A6_82_E4_BD_95_E5_B7_A7_E5_c101_624870.htm 任何病毒和木马存在于系统中，都无法彻底和进程脱离关系，即使采用了隐藏技术，也还是能够从进程中找到蛛丝马迹，因此，查看系统中活动的进程成为我们检测病毒木马最直接的方法。但是系统中同时运行的进程那么多，哪些是正常的系统进程，哪些是木马的进程，而经常被病毒木马假冒的系统进程在系统中又扮演着什么角色呢？请看本文。 病毒进程隐藏三法 当我们确认系统中存在病毒，但是通过“ 任务管理器 ”查看系统中的进程时又找不出异样的进程，这说明病毒采用了一些隐藏措施，总结出来有三法： 1.以假乱真 系统中的正常进程有：svchost.exe、explorer.exe、iexplore.exe、winlogon.exe等，可能你发现过系统中存在这样的进程：svch0st.exe、explore.exe、iexplorer.exe、winlogin.exe。对比一下，发现区别了么？这是病毒经常使用的伎俩，目的就是迷惑用户的眼睛。通常它们会将系统中正常进程名的o改为0，l改为i，i改为j，然后成为自己的进程名，仅仅一字之差，意义却完全不同。又或者多一个字母或少一个字母，例如explorer.exe和iexplore.exe本来就容易搞混，再出现个iexplorer.exe就更加混乱了。如果用户不仔细，一般就忽略了，病毒的进程就逃过了一劫。 2.偷梁换柱 如果用户比较心细，那么上面这招就没用了，病毒会被就地正法。于是乎，病毒也学聪明了，懂得了偷梁换柱这一招。如果一个进程的名字为svchost.exe，和正常的系统进程名分毫不差。那么这个进程是不是就安全了呢？非也，其实它

只是利用了“ 任务管理器 ”无法查看进程对应可执行文件这一缺陷。我们知道svchost.exe进程对应的可执行文件位于“ C:\WINDOWS\system32 ”目录下（Windows2000则是C:\WINNT\system32目录），如果病毒将自身复制到“ C:\WINDOWS\ ”中，并改名为svchost.exe，运行后，我们在“ 任务管理器 ”中看到的也是svchost.exe，和正常的系统进程无异。你能辨别出其中哪一个是病毒的进程吗？ 3.借尸还魂 除了上文中的两种方法外，病毒还有一招终极大法借尸还魂。所谓的借尸还魂就是病毒采用了进程插入技术，将病毒运行所需的dll文件插入正常的系统进程中，表面上看无任何可疑情况，实质上系统进程已经被病毒控制了，除非我们借助专业的进程检测工具，否则要想发现隐藏在其中的病毒是很困难的。 系统进程解惑 上文中提到了很多系统进程，这些系统进程到底有何作用，其运行原理又是什么？下面我们将对这些系统进程进行逐一讲解，相信在熟知这些系统进程后，就能成功破解病毒的“ 以假乱真 ”和“ 偷梁换柱 ”了。