巧妙从进程中判断出病毒和木马 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/272/2021_2022__E5_B7_A7_E5_A6_99_E4_BB_8E_E8_c100_272214.htm explorer.exe 常被病毒冒充的进程名有：iexplorer.exe、expiorer.exe、explore.exe 。explorer.exe就是我们经常会用到的“ 资源管理器 ”。如果在“ 任务管理器 ”中将explorer.exe进程结束，那么包括任务栏、桌面、以及打开的文件都会统统消失，单击“ 任务管理器 ”→“ 文件 ”→“ 新建任务 ”，输入“ explorer.exe ”后，消失的东西又重新回来了。explorer.exe进程的作用就是让我们管理计算机中的资源。 explorer.exe进程默认是和系统一起启动的，其对应可执行文件的路径为“ C:\Windows ”目录，除此之外则为病毒。 iexplore.exe 常被病毒冒充的进程名有：iexplorer.exe、iexploer.exeiexplorer.exe进程和上文中的explorer.exe进程名很相像，因此比较容易搞混，其实iexplorer.exe是Microsoft Internet Explorer所产生的进程，也就是我们平时使用的IE浏览器。知道作用后辨认起来应该就比较容易了，iexplorer.exe进程名的开头为“ ie ”，就是IE浏览器的意思。 iexplore.exe进程对应的可执行程序位于C:\ProgramFiles\InternetExplorer目录中，存在于其他目录则为病毒，除非你将该文件夹进行了转移。此外，有时我们会发现没有打开IE浏览器的情况下，系统中仍然存在iexplore.exe进程，这要分两种情况：1.病毒假冒iexplore.exe进程名。2.病毒偷偷在后台通过iexplore.exe干坏事。因此出现这种情况还是赶快用杀毒软件进行查杀吧。 rundll32.exe 常被病毒冒充的进程名有：rundl132.exe、rundl32.exe。rundll32.exe在系统中的

作用是执行DLL文件中的内部函数，系统中存在多少个Rundll32.exe进程，就表示Rundll32.exe启动了多少个的DLL文件。其实rundll32.exe我们是会经常用到的，他可以控制系统中的一些dll文件，举个例子，在“ 命令提示符 ”中输入“ rundll32.exe user32.dll,LockWorkStation ”，回车后，系统就会快速切换到登录界面了。rundll32.exe的路径为“ C:\Windows\system32 ”，在别的目录则可以判定是病毒。spoolsv.exe 常被病毒冒充的进程名有：spoo1sv.exe、spolsv.exe。spoolsv.exe是系统服务“ Print Spooler ”所对应的可执行程序，其作用是管理所有本地和网络打印队列及控制所有打印工作。如果此服务被停用，计算机上的打印将不可用，同时spoolsv.exe进程也会从计算机上消失。如果你不存在打印机设备，那么就把这项服务关闭吧，可以节省系统资源。停止并关闭服务后，如果系统中还存在spoolsv.exe进程，这就一定是病毒伪装的了。 限于篇幅，关于常见进程的介绍就到这里，我们平时在检查进程的时候如果发现有可疑，只要根据两点来判断： 1.仔细检查进程的文件名. 2.检查其路径。 通过这两点，一般的病毒进程肯定会露出马脚。 找个管理进程的好帮手 系统内置的“ 任务管理器 ”功能太弱，肯定不适合查杀病毒。因此我们可以使用专业的进程管理工具，例如Procexp。Procexp可以区分系统进程和一般进程，并且以不同的颜色进行区分，让假冒系统进程的病毒进程无处可藏。 运行Procexp后，进程会被分为两大块，“ System Idle Process ”下属的进程属于系统进程， explorer.exe“ 下属的进程属于一般进程。我们介绍过的系统进程svchost.exe、winlogon.exe等都隶属于 ” System Idle Process “ ，如果你在 ” explorer.exe “ 中发

现了svchost.exe，那么不用说，肯定是病毒冒充的。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com