深度解析最令人迷惑的两大进程 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/465/2021_2022__E6_B7_B1_E5_BA_A6_E8_A7_A3_E6_c67_465177.htm 在这将着重介绍一下Windows系统的Svchost.exe和Explorer.exe两种进程，作为Windows系统中两种重要的进程，下面我们就来看看他们的特点以及在各个操作系统中的应用。 Explorer.exe 在Windows系列的操作系统中，运行时都会启动一个名为Explorer.exe的进程。这个进程主要负责显示系统桌面上的图标以及任务栏，它在不同的系统中有不同的妙用。 Explorer在Windows 9x中的应用 在Windows 9x中，这个进程是运行系统时所必需的。如果用“ 结束任务 ”的方法来结束Explorer.exe进程，系统就会刷新桌面，并更新注册表。所以，我们也可以利用此方法来快速更新注册表。方法如下：按下Ctrl Alt Del组合键，出现“ 结束任务 ”对话框。在该对话框中选择“ Explorer ”选项，然后单击“ 结束任务 ”按钮，将出现“ 关闭Windows ”对话框。单击“ 否 ”按钮，系统过一会儿将出现另一个对话框，告诉你该程序没有响应，询问是否结束任务。单击“ 结束任务 ”按钮，则更新注册表并返回Windows 9x系统环境中。这比起烦琐的重新启动过程要方便多了？ Explorer在Windows 2000/XP中的应用 在Windows 2000/XP和其他Windows NT内核的系统中，Explorer.exe进程并不是系统运行时所必需的，所以可以用任务管理器来结束它，并不影响系统的正常工作。打开你需要运行的程序，如记事本。然后右击任务栏，选择“ 任务管理器 ”，选中“ 进程 ”选项卡，在窗口中选择Explorer.exe进程，单击“ 结束进

程”按钮，，接下来桌面上除了壁纸(活动桌面Active Desktop的壁纸除外)，所有图标和任务栏都消失了。此时你仍可以像平常一样操作一切软件。 如果你想运行其他软件，但此时桌面上空无一物，怎么办？别着急，下面有两种可以巧妙地打开其他软件： 第一种方法：按下Ctrl Alt Del组合键，出现“Windows安全”对话框，单击“任务管理器”按钮(或是直接按下Ctrl Shift Esc组合键)，在任务管理器窗口中选中“应用程序”选项卡，单击“新任务”，在弹出的“创建新任务”的对话框中，输入你想要打开的软件的路径和名称即可。 你还可以在正在运行的软件上，选择“文件→打开”，在“打开”对话框中，点击“文件类型”下拉列表，选择“所有文件”，再浏览到你想打开的软件，右击它，在快捷菜单中选择“打开”命令，就可以启动你需要的软件了。注意，此时不能够通过单击“打开”按钮来打开软件，此种方法适用于大多数软件，Office系列除外。 通过结束Explorer.exe进程，还可以减少4520KB左右的系统已使用内存，无疑会加快系统的运行速度，为资源紧张的用户腾出了宝贵的空间。
Svchost.exe是NT核心系统的非常重要的进程，对于2000、XP来说，不可或缺。很多病毒、木马也会调用它。所以，深入了解这个程序，是玩电脑的必修课之一。 大家对Windows操作系统一定不陌生，但你是否注意到系统中“Svchost.exe”这个文件呢？细心的朋友会发现Windows中存在多个“Svchost”进程（通过“ctrl alt del”键打开任务管理器，这里的“进程”标签中就可看到了），为什么会这样呢？下面就来揭开它神秘的面纱。 在基于NT内核的Windows操作系统家族中，不同版本的Windows系统，存在不同数量的“Svchost”进程

，用户使用“ 任务管理器 ”可查看其进程数目。一般来说，Win 2000有两个Svchost进程，Win XP中则有四个或四个以上的Svchost进程（以后看到系统中有多个这种进程，千万别立即判定系统有病毒了哟），而Win 2003 server中则更多。这些Svchost进程提供很多系统服务，如：rpcss服务（remote procedure call）、dmserver服务（logical disk manager）、dhcp服务（dhcp clieNT）等 如果要了解每个Svchost进程到底提供了多少系统服务，可以在Win 2000的命令提示符窗口中输入“ tlist -s ”命令来查看，该命令是Win 2000 support tools提供的。在Win XP则使用“ tasklist /svc ”命令。 Svchost中可以包含多个服务 Windows系统进程分为独立进程和共享进程两种，“ Svchost.exe ”文件存在于“ %systemroot% system32 ”目录下，它属于共享进程。随着Windows系统服务不断增多，为了节省系统资源，微软把很多服务做成共享方式，交由Svchost.exe进程来启动。 但Svchost进程只作为服务宿主，并不能实现任何服务功能，即它只能提供条件让其他服务在这里被启动，而它自己却不能给用户提供任何服务。那这些服务是如何实现的呢？ 原来这些系统服务是以动态链接库（dll）形式实现的，它们把可执行程序指向 Svchost，由Svchost调用相应服务的动态链接库来启动服务。那Svchost又怎么知道某个系统服务该调用哪个动态链接库呢？这是通过系统服务在注册表中设置的参数来实现。 从启动参数中可见服务是靠Svchost来启动的。 因为Svchost进程启动各种服务，所以病毒、木马也想尽办法来利用它，企图利用它的特性来迷惑用户，达到感染、入侵、破坏的目的（如冲击波变种病毒“ w32.welchia.worm ”）。但Windows系统存在多个Svchost进

程是很正常的，在受感染的机器中到底哪个是病毒进程呢？这里仅举一例来说明。 假设Windows XP系统被“ w32.welchia.worm ”感染了。正常的Svchost文件存在于“ c:Windowssystem32 ”目录下，如果发现该文件出现在其他目录下就要小心了。“ w32.welchia.worm ”病毒存在于“ c:Windowssystem32Win s ”目录中，因此使用进程管理器查看Svchost进程的执行文件路径就很容易发现系统是否感染了病毒。 Windows系统自带的任务管理器不能够查看进程的路径，可以使用第三方进程管理软件，如“ Windows优化大师 ”进程管理器，通过这些工具就可很容易地查看到所有的Svchost进程的执行文件路径，一旦发现其执行路径为不平常的位置就应该马上进行检测和处理。 