

三招揪出Windows系统自启动项隐患Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/644/2021_2022__E4_B8_89_E6_8B_9B_E6_8F_AA_E5_c100_644208.htm 目前绝大部分木马、黑客程序、病毒来是随系统启动而运行的。因此，揪出系统启动过程中的隐患，可以有效保证电脑的安全。 一

、Msconfig法 传统的Msconfig是我们找出启动隐患最方便的办法。在Windows 98/XP/2003中，我们可以直接打开。其方法是打开“运行”窗口，输入“msconfig”后回车即可打开该配置工具。根据操作系统版本的不同，打开的窗口会有所不同。不过，其中最主要的就是“启动”选项卡，我们只需要切换到该标签，然后从中将下结来历不明的启动项取消，这样即可达到禁止其运行的目的。如果是Windows 2000系统，虽然默认状态下没有提供msconfig，这也没关系。我们只需要到其它系统中复制msconfig.exe，然后将其保存到Windows 2000系统之中。双击复制过来的文件，这时会提示找不到某些系统文件，对此可以直接跳过，直至进入配置窗口。 二、注册表法 注册表同样是我们揪出启动隐患的一个好地方。打开“运行”窗口，输入“regedit”并回车即可打开注册表器。我们只需要依次打开

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run和

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，其右侧的键值就是随系统启动时运行的程序。对于不必随系统启动或强行添加的程序就可以直接按下“DEL”键将其删除。小提示：系统启动是自动运行的项目

，而在任务栏的快速启动中则可以帮助用户快速打开相应的程序。

三、服务查看法

由于系统的各项服务都是在启动时启用的。因此一些病毒、木马会把自己注册为服务，以达到随系统启动的目的。对此，我们同样可以在注册表中进行查看。打开注册表，找到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services，其下面的每一项都代表启动时自动运行的一项服务。在每一项下的start表示启动类型，如果值为2则表示随系统自动启动，3表示手工启动，4表示禁用，根据自己的实际需要决定这些服务是否继续在启动时被执行。查看服务另外一个更简单的方法是在系统中直接打开服务管理器。进入“控制面板”，双击“管理工具”中的“服务”，这样我们就可以非常清楚的查看每个服务的状态和启动方式，同时还可以根据服务的介绍判断该服务是否为系统服务或正规服务。如果是非法服务，那么赶将将其禁用，并将其“启动类型”设为“已禁用”。

来源：考试大 当然，找出系统启动隐患的方法还有很多，例如在启动时使用杀毒软件进行检查等。只要我们注意到系统的异常情况，及时查看任务管理中正在运行的进程，那么一定能够将这些隐患全部揪出来。

编辑特别推荐: WinXP不能访问Windows7共享文件 诊断:电脑中毒后的一些表现 Windows7的新快速键 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