监控Windows7开机启动项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_ti2020/643/2021_2022__E7_9B_91_E6_8E_A7Wind_c100_643960.htm 我们知道，Windows中有自带的启动文件夹，它是最常见的启动项目，但很多人却很少注意仔细检查它。如果把程序装入到这个文件夹中，系统启动就会自动地加载相应程序，而且因为它是暴露在外的，所以非常容易被外在的因素更改。 一、具体的位置是“ 开始 ”菜单中的“ 启动 ”选项 在硬盘上的位置是：C:\Documents andSettings\Administrator\“ 开始 ”菜单\程序\启动. 在注册表中的位置是： HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 现在你可以打开看看里面有没有什么来历不明的程序存在。 二、Msconfig Msconfig是Windows系统中的“ 系统配置实用程序 ”，它管的方面可够宽，包括:system.ini 、win.ini、启动项目等。同样，里面也是自启动程序非常喜欢呆的地方! 1.System.ini 首先，在“ 运行 ”对话框中输入“ msconfig ”启动系统配置实用程序(下同)，找到system.ini标签，里面的“ shell=…… ”就可以用来加载特殊的程序。如果你的shell=后面不是默认的explorer.exe，或者说后面还有一个程序的名字，那你可要小心了，请仔细检查相应的程序是否安全! 2.Win.ini 如果我们想加载一个程序：hack.exe，那么可以在win。ini中用下面的语句来实现： [windows] load=hack.exe run=hacke.exe 该怎么做，你应该知道了吧! 这一点上，使用魔方（点此下载）中的系统设置 - 启动项设置，一目了然，而且可以轻松去除和添加启动项。 3.“ 启动 ”项

目 系统配置实用程序中的启动标签和我们上面讲的“ 启动 ”文件夹并不是同一个东西，在系统配置实用程序中的这个启动项目，是Windows系统启动项目的集合地。几乎所有的启动项目都能在这里找到当然，经过特殊编程处理的程序可以通过另外的方法不在这里显示。 打开“ 启动 ”标签，“ 启动项目 ”中罗列的是开机启动程序的名称，“ 命令 ”下是具体的程序附加命令，最后的“ 位置 ”就是该程序在注册表中的相应位置。你可以对可疑的程序进行详细的路径、命令检查，一旦发现错误，就可以用下方的“ 禁用 ”来禁止该程序开机时候的加载。来源：考试大 一般来讲，除系统基于硬件部分和内核部分的系统软件的启动项目外，其他的启动项目都是可以适当更改的，包括：杀毒程序、特定防火墙程序、播放软件、内存管理软件等。也就是说，启动项目中包含了所有我们可见程序的列表，你完全可以通过它来管理你的启动程序! 三、注册表中相应的启动加载项目 注册表的启动项目是病毒和木马程序的最爱!非常多病毒木马的顽固性就是通过注册表来实现的，所以平常的时候可以下载一个注册表监视器来监视注册表的改动，魔方（点此下载）的后续版本中也将加入一系列的安全方面的功能用于监视恶意软件对系统的修改等等。特别是在安装了新软件或者是运行了新程序的时候，一定不要被程序漂亮的外表迷惑。一定要看清楚它的实质是不是木马的伪装外壳或者是捆绑程序!必要的时候可以根据备份来恢复注册表，这样的注册表程序网上很多，这里也就不再详谈了。本文来源:百考试题网 我们也可以通过手动的方法来检查注册表中相应的位置，虽然它们很多是和上文讲的位置重复，但是对网络安全来讲，小心永远不嫌多! 注意同

安全、清洁的系统注册表相应键进行比较，如果发现不一致的地方，一定要弄清楚它是什么东西!不要相信写在外面的“ system ”、“ windows ”、“ programfiles ”等名称，谁都知道“ 欲盖弥彰 ”的道理。如果经过详细的比较，可以确定它是不明程序的话，不要手软，马上删除! 四、Wininit.ini 我们知道，Windows的安装程序常常调用这个程序来实现安装程序后的删除工作，所以不要小看它，如果在它上面做手脚的话，可以说是非常隐蔽、非常完美的! 它在系统盘的Windows目录下，用记事本打开它(有时候是wininit.hak文件)可以看到相应的内容。很明显，我们可以在里面添加相应的语句来达到修改系统程序或者是删除程序的目的。如果是文件关联型木马，可以通过winint.ini来删除它感染后的原始文件，从而达到真正隐藏自己! 五、DOS下的战斗 最后，我们说说DOS下的启动项目加载，config.sys、autoexec.bat、*.bat等文件都可以用特定的编程方式来实现加载程序的目的。所以不要以为DOS就是个过时的东西，好的DOS下编程往往能达到非常简单、非常实用的功能! 编辑特别推荐: 右键菜单快速整理Windows7磁盘碎片 Windows安全性饱受质疑 Windows虚拟内存详解 