三点突破巧妙从进程中判断病毒木马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_ti2020/623/2021_2022__E4_B8_89_E7_82_B9_E7_AA_81_E7_c100_623910.htm 2009年上半年计算机技术与软件专业技术资格（水平）考试日期：2009年5月23、24日。另外，部分考试科目从2009年上半年开始将采用新修编的考试大纲，具体见： 2009年全国计算机软考考试大纲汇总 2009年计算机软考冲刺辅导，百考试题祝各位考生今天软考顺利通过！ 编辑推荐：2009年5月全国计算机软考真题及答案解析 答案交流 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。 svchost.exe 常被病毒冒充的进程名有：svch0st.exe、schvost.exe、scvhost.exe。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。而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scvhost，由cvhost调用相应服务的动态链接库来启动服务。我们可以打开“ 控制面板 ”→“ 管理工具 ”→服务，双击其中“ ClipBook ”服务，在其属性面板中可以发现对应的可执行文件路径为“ C:\WINDOWS\system32\clipsrv.exe ”。再双击“ Alerter ”服务，可以发现其可执行文件路径为“ C:\WINDOWS\system32\svchost.exe -k LocalService ”，而“ Server ”服务的可执行文件路径为“ C:\WINDOWS\system32\svchost.exe -k netsvcs ”。正是通过这种调用，可以省下不少系统资源，因此系统中出现多个svchost.exe，其实只是系统的服务而已。 在Windows2000系统中正常存在svchost.exe进程，一个是RPCSS(RemoteProcedureCall) 服务进程，另外一个则是由很多服务共享的一个svchost.exe；而在WindowsXP中，则一般有4个以上的svchost.exe服务进程。如果在xp和之前的系统中svchost.exe进程的数量多于5个，就要小心了，很可能是病毒假冒的。但是到了Vista和Windows7时代，8-12个svchost进程都是正常的！是否为系统正常进程的检测方法也很简单，使用一些进程管理工具，例如Vista优化大师的进程管理功能，查看svchost.exe的可执行文件路径，如果在“ C:\WINDOWS\system32 ”目录外，那么就可以判定是病毒了。 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