教你揪出伪装系统木马并清除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__E6_95_99_E4_BD_A0_E6_8F_AA_E5_c100_644252.htm 面对日新月异的病毒和木马，有时利用手工检查及清除病毒，还是有必要的，本文以伪装成系统的Wmiprvse.exe进程木马为例，来对其木马的清除做以循序渐进的讲解。 首先，按住键盘上的“ Ctrl Alt Del ”键，将“ 任务管理器 ”打开，并且切入至“ 进程 ”标签。不过今日与以往不同的是，从“ 进程 ”标签里，却突然发现多出一个Wmiprvse.exe进程。于是利用百度搜索了一下Wmiprvse.exe进程的相关资料，给出的答案是wmiprvse.exe是微软Windows操作系统的一部分。用于通过WinMgmt.exe程序处理WMI操作，这个程序对你系统的正常运行是非常重要的。 看到这里可能觉得这是一个正常安全的程序进程，于是也就没当回事，又开始了自己的网游“ 生涯 ”，但是好景不长没过多久，电脑开始自动重新启动，而且之后又断断续续的重启了几回。在没有任何可怀疑的对象时，可以选择利用系统的搜索功能。查找一下这个突然出现的Wmiprvse.exe程序文件，结果却出现了两个同样的Wmiprvse.exe 文件并存的现象。 仔细观察一下，发现两个程序文件大小相同，不过有个Wmiprvse.exe文件在Windows2 目录下，接着进一步看了两个文件夹的创建时间，Windows2确实是在自己重装系统时间内，所以两个都是系统目录，只是前一个在最后一次没有删除干净。再打开“ 任务管理器 ”对话框，发现系统里存在两个Wmiprvse.exe进程，分别由不同权限的用户运行。位于\System32\wbem文件下的文件才是正常的文件，换句话说

没有直接删除的Windows\System32\wbem下的Wmiprvse.exe文件是病毒文件。接着在“ 任务管理器 ”对话框内，将其进程停止后，又进入到了该进程文件夹内，将其病毒文件删除。本以为病毒就这样被消灭了，还没等重新启动，也就过了十分钟左右，这个病毒进程又出现在了任务管理器上。来源：www.examda.com 抱着宁可错杀一个，绝不放过一个病毒文件的心理，再次停止该木马进程，将Windows2目录里的文件全部删除后，又在注册表器里，搜索将相关键值进行删除，接着重新启动了一下计算机，然后打开“ 任务管理器 ”对话框，发现Wmiprvse.exe进程已经不见了，并且系统总自动重新启机的现象也以消失了，这样一来真假“ 美猴王 ”就见了分晓。如果你一样碰到了伪装Wmiprvse.exe程序的木马，不如按照本文的思路将病毒清除，何必又采用费时费力的重装方案。