找准病毒“ 落脚点 ”从系统中剔除病毒 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/259/2021_2022__E6_89_BE_E5_87_86_E7_97_85_E6_c100_259009.htm 一、让病毒从目录中消失 我们先得从病毒所在的目录入手，如果病毒像正常的软件一样有自己独立的目录，那么我们可以略微的笑笑了这个病毒比较弱。检查目录的创建时间就可以知道您是什么时候染的毒，并可能发现毒从何来。如果它没有自己单独的目录，而是存在于系统目录，那也比较好办，这种病毒的破坏性一般不是很大，您就直接查看它的属性就可以了解到一切必要的信息。如果它存在于您计算机上的每个目录，那这时候Windows自带的文件搜索功能就派上用场了。尽管它复制的到处都是，但这种病毒都只有一个主程序文件，且都是一个娘胎生的，文件大小必然一致。打开文件搜索的高级功能，填入EXE文件类型并把文件的大小输入，然后按下回车键，接着藏在您硬盘每个角落的病毒就会被暴露无疑。利用创建时建排序，您可以发现第一个攻击您机器的病毒了。 现在所有的病毒数据文件几本都在眼前了，至少是病毒能对你发动攻击的主要成分，那么就请大开杀戒吧，把您找到的与任何与病毒相关的EXE、DLL、数据全部删除。不过别做的太绝，留上至少一个EXE作为标本，将其扩展名改为DAT并用RAR打包，我们以后还用的上。另外还是请您非常的小心谨慎，别把不是病毒的文件给误删了，那可是致命的错误!在处理完硬盘病毒后，千万不要重起计算机，那可能会导致前功尽弃，因为有的病毒的正身我们并不能如此轻易的找到。如果有些病毒不以EXE的身份出现，而是其它的比如COM

、RAR等，我们的文件尺寸搜索法一样适用，换个扩展名就行了。不过我还是要告诉您一件不幸的事，主程序文件尺寸不一样的病毒现在还没有但并不代表以后不会有，到那时我们只能用关键数据匹配搜索了。 二、对病毒最后的阵地发动总攻 硬盘上的病毒虽然已被我们斩草除根，但更麻烦的事还在等着我们，要知道负隅顽抗的敌人才是最可怕的。病毒的最后阵地在哪呢?无疑就是那传说中的注册表。因为系统服务的信息都存储在注册表理，我就把服务的内容归类在这一节了。首先应该做的事是仔细检查你的服务列表，仔细核对每一个没有描述的服务，看是否和你刚结束掉的进程有关。对于中文版Windows的用户来说，查出病毒服务是有一定优势的，原因说来比较可笑，那就是国外写病毒的程序员不懂中文，因此他们不会用中文的描述来将自己伪装成系统服务。因此对于一切英文描述的服务也应该格外注意。我还见过更狠的病毒，它将系统正常的进程干掉，然后将那个进程的描述、名称等信息套用在自己身上，伪装的真是天衣无缝。但最终还是露出了马脚，它所对应的EXE文件是完全不对路的。 当确保进程是安全的，那我们就可以直接进入注册表了，先检查系统起动时自动运行的注册项，看有没有可疑的程序。我的经验是在系统启动时基本不运任何程序，真的要运行就放在开始菜单的启动项里，这样不仅安全，而且可以为你发现病毒带来极大的便利。事实上，长期以来的无数次实践证明，将所有的自动启动项都删除对于机器是没有任何不良影响的。系统本身不会把关键的启动程序放在那里，对于系统运行最关键的其实是服务。不过当你在这里发现病毒时先不要急于删除键值，您应该将它记录下来，看看它对应的程

序是否已被你备案。然后将病毒程序可能的名字都复制下来，逐个在注册表中搜索，把找到的所有的匹配项全部删掉。不过这样做还是有一定的危险性，我强烈建议您在删除前导出键值以做备份。在注册表的查杀和扫描工作结束后，我们终于可以长嘘一口气了，因为病毒及其家人很可能已经被我们残忍的屠杀净了。在您再次检查进程列表确保无误后，就可以重起计算机看看病毒是否会再次发作了。 三、真正可怕的对手 还记得上面的内容中层经提到过的寄生在浏览器进程或系统服务进程中的病毒吗?它们当之无愧是我们最可怕的敌人。然而随着您将他们藏在注册表里的信息清除掉，它们中的大多数在您重起机器后就不会再附加在系统进程上了，这时就可以按照上面的方法将它们清除，这听起来并不很复杂是吗?但更加令人恐怖的病毒还在后面，那就是病毒在运行的时候对注册表实施了监控，一旦发现它在注册表里的注册信息被破坏，将会立即复原，使你对注册表的操作无效。对于这样的病毒，我们只能用干净的DOS启动盘启动机器，然后将它的程序文件删掉，再启动进入Windows，删除它在注册表里的信息。有的朋友会问，为什么不进入安全模式杀毒。当然，在安全模式下绝大多数无用的服务和进程不会被启动，然而这对于那些丧心病狂的特殊病毒这是无效的，甚至于当它们发现您的机器进入了安全模式后会立即发动最后猛攻，使您的机器彻底瘫痪。虽然这么狠的病毒对于一般的朋友来说是百年难遇的。