识别病毒文件四个好方法计算机等级考试 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__E8_AF_86_E5_88_AB_E7_97_85_E6_c98_644161.htm 我们在使用杀毒软件杀毒的时候，常常会检测出很多“ 病毒 ”，许多朋友抱着“ 宁可错杀一堆，绝不放过一个 ”的态度，将检测出的“ 病毒 ”全部删掉。其实全删是不可取的，有的是被感染的系统文件，是不能删的。笔者在这里介绍几个识别病毒文件的方法，希望对大家有所帮助。来源：考试大的美女编辑们 一、文件时间 如果你觉得电脑不对劲，用杀毒软件检查后，没什么反映或清除一部分病毒后还是觉得不对劲，可以根据文件时间检查可疑对象。 文件时间分为创建时间、修改时间(还有一个访问时间，不用管)，可以从文件的属性中看到，点选文件，右击，选择菜单中的属性就可以在“ 常规 ”那页看到这些时间了。 通常病毒、木马文件的创建时间和修改时间都比较新，如果你发现的早，基本就是近几日或当天。c:/windows和c:/windows/system32，有时还有c:/windows/system32/drivers，如果是2000系统，就把上面的windows改成winnt，这些地方都是病毒木马常呆的地方，按时间排下序(查看-详细资料，再点下标题栏上的“ 修改时间 ”)，查看下最新几日的文件，特别注意exe和dll文件，有时还有dat、ini、cfg文件，不过后面这些正常的文件也有比较新的修改时间，不能确认就先放一边，重点找exe和dll，反正后三个也不是执行文件。一般来说系统文件特别是exe和dll)不会有如此新的修改时间。来源：考试大 当然更新或安装的其它应用软件可能会有新的修改时间，可以再对照下创建时间，另外自己什么时间有没装过什

么软件应该知道，实在不知道用搜索功能，在全硬盘上找找相关时间有没建立什么文件夹，看看是不是安装的应用软件，只要时间对得上就是正常的。如果都不符合，就是病毒了，删除。 说明一点，正如不是所有最新的文件都是病毒一样，也不是说所有病毒的时间都是最新的，有的病毒文件的日期时间甚至会显示是几年前。 当然我们还有其他的分辨方法。 二、文件名 文件名是第一眼印象，通过文件名来初步判断是否可疑是最直接的方法，之所以放在时间判断后面，实在是从一大堆文件中分拣可疑分子太难了，还是用时间排下序方便些。 我们常说的随机字母(有时还有数字，较少)组合的文件名，病毒最爱用它(曾经发现某些正常软件也有使用这种奇怪组合的习惯，比如雅虎上网助手，每次文件名都不一样，动机可疑，还有某猫的驱动程序也看似随机组合，不过幸好有厂商信息可以协助分辨，这个下一点再说)。本文来源:百考试题网 还有文件名的长度，有的严重超出8位文件名的标准，有10几位之多，这都应列为可疑对象，尤其是IE插件中有这些的文件名出现。 当然光说文件名古怪、随机组合，似乎没有一个标准，不熟悉电脑的人看所有的英文文件名都可能认为是奇怪的、无意义的排列组合，所以真要依靠文件名判断，还是要对系统文件夹下的文件、常规文件有一定了解后才能比较好的掌握。初步来说，结合上面的时间还有其它手段共同判断，还是可以发现点东西的。 还有一种就是假冒正常文件、系统文件的文件名，这倒比较好识别，比如svchost.exe和svch0st.exe，很明显后者在假冒前者，这种欲盖弥彰倒更容易暴露，前提是你对系统文件名比较熟悉，有事没事打开任务管理器学习一下吧。百考试题－全国最大教育

类网站(www．Examda。com) 对应于文件名，还有服务名、驱动名、注册表启动项名，相对而言，这些项目的名字如果没有表示出一定含义，倒真是病毒了，还没几个厂商会不负责任地给自己的软件要用到的服务、驱动、启动项起个无意义、随便组合的名字，如果服务、驱动、启动项名是有问题的，那么下面使用的文件一定是有问题的。 实在没把握，把文件名(有时要包括完整文件路径，不同路径下的同名文件可不一样，这个以后说)、服务名、驱动名、启动项名放到网上搜索一下，看看别人怎么说的，特别是对查不到的、还有服务、驱动、启动项与文件名对不上的(如同一服务名在网上查出有不同文件与之对应，或相反情况)，都可以列为可疑对象。 三、版本信息 检查文件时间有不确定性，再加一个检查项目文件版本，也是在文件的属性中查看，有文件版本、厂商信息等。首先明确一下，不是所有文件都有版本信息，也不是所有无版本信息的文件都是病毒文件，更不是所有显示微软信息的文件都真是微软的。来源：考试大 文件名、文件时间，再对上文件版本，基本可以得出一个结果，比如一个奇怪的文件名，显示微软的厂商信息，明显可疑.或者本来应该是正常的系统文件(如explorer.exe或userinit.exe)却没有版本信息，可能是被病毒替换或破坏了.还有soundman.exe厂商信息竟然是1，可以考虑删除了，应该不是声卡的程序了。 版本信息中除了厂商以外，还有原文件名，有时你会在这里发现一个与检查文件不同的名字，真是别有天地。 四、位置 病毒木马喜欢呆的地方是系统文件夹，windows、windows/system32、windows/system32/drivers，还有c:/program files/internet explorer/c:/program files/internet

explorer/plugin、c:/program files/common files/miscrosoft shared，还有就是临时文件夹、IE缓存 首先临时文件夹c:/documents and settings/你的用户名/local settings/temp和c:/windows/temp是一定要清的，而且可以大胆地删除，不管好坏，删了没事，IE缓存也要清的，不是直接进文件夹删除，而从IE的菜单工具-internet选项进入，删除文件-删除所有脱机文件，最好在高级那设成关闭浏览器时自动清空临时文件，就省事了。其它文件夹，主要看是否有不该存在的文件存在，比如windows文件夹中多了什么瑞星的文件(卡卡的倒是有在那)、realplayer的文件，绝对可疑，还有比如svchost.exe、ctfmon.exe突然出现在windows或其它文件夹中，而不是在它们应该在的system32中，也可以确定是病毒。当然可以结合上面的几个方法一起判断。有的时候是得靠经验，相对而言文件比较少的文件夹比较好判断，多出什么很容易发觉，比如windows、ie文件夹，多看看，就知道基本就是那些，多一两个exe或dll，马上可以发现(很多流氓软件是会在这里安身)。 还有就是结合注册表启动项，一般启动项引用到windws中的不多，基本是输入法、声卡管理，更多的就可疑了，指到system32下的了多看两眼，实在拿不准，老办法，到网上查文件名。如果发现启动项指向font字体文件夹的，那不用想了，一定有问题。本文来源:百考试题网 服务驱动也是如此，不是在system32或driver中的就要多检查下(自然在它们下面的也要检查，何况不在)。 除了文件夹位置，还有注册表位置，除了几个RUN的启动项，还有映像劫持(IFEO)要检查，值有debugger的都要注意一下，除了最后一个your image file name here without a path有个debugger=ntsd -d，其它的是都没

有的，只要有发现就是被劫持(免疫的除外，免疫是把已知病毒程序名劫持到不存在的文件上，使其不能运行)，然后就找劫持文件，就是debugger后面的文件，找到后连同注册表项一起删除。但注意，现在的劫持有的用的不是病毒文件，是系统文件或命令，比如svchost.exe或ntsd -d，这就不要删除文件了，只要把注册表项删除。 还有要注意的注册表项有appinit_dlls，一般为空值(例外，卡卡的一个文件会放这)，如果多出值就是病毒，按名字找到删除。还有一个就是userinit，一般也是空的，多东西修改就要查查是否正常。推荐用SREng来检查，比较方便，也会自动提示以上修改。 结语：说真的，真要从一堆英文名中找出可疑的文件名挺难的，综合使用各个方法，配合工具软件分类显示才是捷径，比如SREng，把服务驱动列出来，名字、文件、路径一摆，就很明显了，有的名字就是乱写的，对照后面的文件名就很清楚了，有的细心的会冒充系统服务名，不过与正常的一对比，连网也不用上，也可以找出问题(隐藏微软服务后非微软的服务就露出来了，如果还顶个系统服务名或接近系统服务的名字，就一定有问题，不是把正常服务改了，就是额外加进来的李鬼)。 