存在安全风险的进程详细分类 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/272/2021_2022__E5_AD_98_E5_9C_A8_E5_AE_89_E5_c100_272183.htm 存在安全风险的进程包括：木马、病毒、蠕虫、广告软件Adware、间谍软件Spyware 什么是木马？ 木马病毒源自古希腊特洛伊战争中著名的“ 木马计 ”而得名，顾名思义就是一种伪装潜伏的网络病毒，等待时机成熟就出来害人。 传染方式：通过电子邮件附件发出，捆绑在其他的程序中。 病毒特性：会修改注册表、驻留内存、在系统中安装后门程序、开机加载附带的木马。 木马病毒的破坏性：木马病毒的发作要在用户的机器里运行客户端程序，一旦发作，就可设置后门，定时地发送该用户的隐私到木马程序指定的地址，一般同时内置可进入该用户电脑的端口，并可任意控制此计算机，进行文件删除、拷贝、改密码等非法操作。 防范措施：用户提高警惕，不下载和运行来历不明的程序，对于不明来历的邮件附件也不要随意打开。 什么是计算机病毒？ 计算机病毒是一个程序，一段可执行码。就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上。当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。除复制能力外，某些计算机病毒还有其它一些共同特性：一个被污染的程序能够传送病毒载体。当你看到病毒载体似乎仅仅表现在文字和图象上时，它们可能也已毁坏了文件、再格式化了你的硬盘驱动或引发了其它类型的灾害。若是病毒并不寄生于一个污染程序，它仍然能通过占据存贮空间给你

带来麻烦，并降低你的计算机的全部性能。可以从不同角度给出计算机病毒的定义。一种定义是通过磁盘、磁带和网络等作为媒介传播扩散，能“ 传染 ”其他程序的程序。另一种是能够实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。还有的定义是一种人为制造的程序，它通过不同的途径潜伏或寄生在存储媒体（如磁盘、内存）或程序里。当某种条件或时机成熟时，它会自生复制并传播,使计算机的资源受到不同程序的破坏等等。这些说法在某种意义上借用了生物学病毒的概念，计算机病毒同生物病毒所相似之处是能够侵入计算机系统和网络，危害正常工作的“ 病原体 ”。它能够对计算机系统进行各种破坏，同时能够自我复制，具有传染性。 所以，计算机病毒就是能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活的具有对计算机资源进行破坏作用的一组程序或指令集合。 什么是蠕虫病毒？ 蠕虫病毒是计算机病毒的一种。它的传染机理是利用网络进行复制和传播，传染途径是通过网络和电子邮件。 比如近几年危害很大的“ 尼姆达 ”病毒就是蠕虫病毒的一种。这一病毒利用了微软视窗操作系统的漏洞，计算机感染这一病毒后，会不断自动拨号上网，并利用文件中的地址信息或者网络共享进行传播，最终破坏用户的大部分重要数据。 蠕虫病毒的一般防治方法是：使用具有实时监控功能的杀毒软件，并且注意不要轻易打开不熟悉的邮件附件。 什么是广告软件Adware？ 广告软件（Adware）是指未经用户允许，下载并安装或与其他软件捆绑通过弹出式广告或以其他形式进行商业广告宣传的程序。安装广告软件之后，往往造成系统运行缓慢或系统异常。 防治广告软件

，应注意以下方面： 1、不要轻易安装共享软件或“ 免费软件 ”，这些软件里往往含有广告程序、间谍软件等不良软件，可能带来安全风险。 2、有些广告软件通过恶意网站安装，所以，不要浏览不良网站。 3、采用安全性比较好的网络浏览器，并注意弥补系统漏洞。 什么是间谍软件Spyware？ 间谍软件（Spyware）是能够在使用者不知情的情况下，在用户电脑上安装后门程序的软件。 用户的隐私数据和重要信息会被那些后门程序捕获， 甚至这些“ 后门程序 ”还能使黑客远程操纵用户的电脑。 防治间谍软件，应注意以下方面： 1、不要轻易安装共享软件或“ 免费软件 ”，这些软件里往往含有广告程序、间谍软件等不良软件，可能带来安全风险。 2、有些间谍软件通过恶意网站安装，所以，不要浏览不良网站。 3、采用安全性比较好的网络浏览器，并注意弥补系统漏洞。 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