

Windows安全诊所：清除间谍软件上篇 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/139/2021_2022_Windows_E5_AE_89_c100_139841.htm 所有人都面临间谍软件的威胁，特别是普通的网络用户。这些网络用户总是很快地点击弹出式对话框，按提示安装软件，接受垃圾邮件的馈赠或者浏览恶意的网站。最佳的预防措施就是对最终用户进行教育。但是，对于大多数人来说，这个事情已经太晚了，间谍软件已经在Windows工作站中疯狂地蔓延开了。为了帮助你识别和修复各种类型的间谍软件的感染，你可以查看一下如下的情况。在做出诊断和介绍三个Windows安全专家讲的课程之后，我们还将介绍一些用户的投诉。你将发现，每一个专家对一个问题都有一个独特的解决方案。因此，在解决你自己的间谍软件的问题时，你一定要考虑一下所有这些解决方案。用户的问题：我为300多个用户提供技术支持。这些用户拥有家庭或者办公室的电脑，采用Windows XP或者Windows 2000操作系统。一些用户报告了下列问题。当浏览器关闭时(有时候甚至都没有连接到互联网)，会出现弹出广告。当打开浏览器时，一个像HotOffers.com的网站出现了，而不是我们内部网的主页。一个名为“Viewpoint”的搜索工具条出现在浏览器上，无论我们在地址栏内输入什么，这个工具条都一直在搜索。我有最新的杀毒软件，并且没有发现病毒。使用查杀间谍软件的工具“SpyBot Search amp.Destroy”对于保护台式电脑并不是万能的解决方案，尽管这是我使用的最好的软件工具。安全专家Tony Bradley：从给出的情况看，这里可能存在两个不同的问题。当计算机甚至还没有连接到互联网的时候

也出现弹出式广告，这类程序可能是通过Windows Messenger服务进入用户计算机的。修改浏览器主页和搜索工具条最有可能是浏览器辅助对象(BHO)出现的问题造成的。间谍软件是一种随看随下(drive-by downloads)的软件。当用户访问恶意网站时，间谍软件利用浏览器中的漏洞不需要用户同意就安装在用户的计算机中。安全专家Lawrence Abrams：当浏览器中的搜索功能和主页被修改之后，通常会出现劫持浏览器的情况，就像“Viewpoint Manager”软件劫持浏览器一样。浏览器劫持一般分为两大类，主动劫持和被动劫持。主动劫持者是一种在计算机启动时就调入的程序。这种程序持续监视计算机的具体设置，确保这些设置符合劫持者的愿望。被动劫持是在计算机启动时开始运行的程序。这种程序修改某些设置并且上传。一旦你确定这种劫持程序，这些问题是很容易修复的。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