病毒攻入电脑首页被改的通用解决方案Microsoft认证考试
 小编点睛：上网令人郁闷的事情有很多，其中IE主页被窜改就是其中之一。更郁闷的是明明用修复IE工具修复了主页，可重新打开浏览器病毒“ 推荐 ”的网页还在，最郁闷的是杀毒软件扫描没有发现异常…… Hao123.com被百度巨资收购，激励更多的人创办网址导航类网站，不过现在的网址导航类网站内容大同小异，同质化非常严重，竞争非常激烈。一些网站不在内容上想办法出彩，而是想着如何提高流量，甚至不惜采取一些见不得人的手段。 现在有一个www.ku2009.com的导航网站，就非常与众不同。这个不同，指的不是内容，而是它特别受病毒的青睐。多种病毒对它都宠爱有加，放毒挂马时不会忘记把这个网站www.ku2009.com设为中毒者的主页。 为什么这些病毒要帮该网站恶意推广呢？背后有没有什么不可告人的秘密呢？病毒作者从来不作亏本的买卖，没有好处的事情他们是不干的，特别是帮网站进行恶意推广广告费是跑不了的。 青睐该网站的病毒有很多，其中不乏一些知名的病毒，例如上期我们报道的死牛病毒的变种、伪威盛广告病毒等。伪威盛广告病毒通过伪装成VIASCSI驱动，将病毒本体藏身于C:\Windows\inf目录下。 然后它随机命名为一个后缀为.inf(如：ufgjqdju.inf)的假驱动文件，一般用户很容易将病毒误看做是威盛的驱动文件而放松警惕。再加上病毒采用了Rootkit技术来隐藏自身，因此我们使用资源管理器查找病毒的时候根本无法发现它们。 当前，首页被窜改成www.ku2009.com的

用户非常多，他们采用了很多方法，例如利用IE工具等，就是无法恢复IE首页，杀毒软件扫描后可能会一无所获，我们应该如何操作才可以恢复IE首页呢？ 安全百科：IE首页是怎么遭到窜改的？为什么一些安全辅助工具不能修复成功呢？以前窜改IE首页的病毒，一般都只是修改了注册表，所以一些安全辅助工具修复IE首页的功能主要就是针对注册表的。 通用解决方案： 前面已经提到，这类病毒之所以能窜改IE首页，主要是驱动文件在起作用，删除了它就可以恢复IE首页。 第一步：下载安装《金山系统急救箱》（软件下载地址：http://www.shudoo.com/bzsoft），它可以对驱动文件的安全性进行判断。运行《金山系统急救箱》，它会自动对系统信息进行扫描，接着将这些文件的MD5数据和服务器中的数据进行对比判断。如果这些数据和服务器中的数据不相同，就可以快速有效的判断出文件是否存在安全隐患。 第二步：当《金山系统急救箱》分析完成以后，在窗口列表中可以看到被判断为可疑或病毒的选项。而列表中的可疑驱动文件，就是造成IE浏览器被窜改的罪魁祸首，点击“ 立即清除 ”按钮就可以删除该文件。 第三步：重新启动系统，打开IE浏览器查看是否还会连接到ku2009。如果没有再打开该网页，说明系统中的病毒文件已经得到成功清除。最后打开杀毒软件（例如《金山毒霸》，下载地址：http://www.duba.net/download/index.shtml）,升级病毒库到最新版本，再进行全盘查杀，彻底清除病毒的残留物。 而现在的此类病毒，很多都是利用驱动文件来窜改首页。当用户打开IE浏览器时，病毒就会释放出病毒驱动，强制打开恶意推广网站链接；而当用户关闭浏览器时，病毒驱动就会被自动

消失。在浏览器属性里面是看不到任何IE被修改的痕迹。