我的浏览器被谁“强制更改”了？

“浏览器主页劫持”现象调查：引导流量，泄露隐私

明明自己没有设置过，打开网页浏览器却直接到了一个陌生网站，想改回原来的主页设置颇费周折，甚至无能为力。很多网民有过类似经历：在安装了一些软件后，自己的浏览器主页就被修改和锁定。

据用户最近的反映和记者的调查，“浏览器主页劫持”“流量劫持”等现象依然猖獗，损害着广大网民的权益。

我的浏览器主页怎么了

本来打算访问A网站，却被强制打开B网站

“下了个驱动精灵，想升级电脑的驱动程序，没想到遇到金山毒霸劫持浏览器主页，连下载其他安全软件开启主页防护都无效，反正删注册表什么的啥都试了，还是不行……”

在各类计算机论坛、百度知道、知乎等网站上，这种关于浏览器主页被劫持的帖子比比皆是。“浏览器主页被毒霸网址大全篡改无法修改怎么办？”“大家对于搜狗输入法劫持主页有什么好的解决办法？”“浏览器主页被劫持为 Hao123怎么办？”“浏览器主页被2345劫持如何处理？”……

令很多网民无可奈何的“浏览器主页劫持”，长久以来一直是互联网安全的顽疾。记者在百度搜索框内敲入“浏览器主页”，“浏览器主页被强制更改” 的百度搜索相关结果超过2000万个，“浏览器主页修改不过来”的搜索结果也超过2700万个。

专家表示，“浏览器主页劫持”指的是用户设置的主页网址，在用户自己不知情的情况下，被强行篡改为其他网址，当用户打开浏览器后，显示的页面变成劫持者设置的页面。

为啥改不回去

很多是通过恶意软件或者插件完成

“上网查了好多解决方案，比如改浏览器设置、删注册表等，都不行。有些软件即使被卸载，计算机重启后，浏览器主页还是被改掉。”“用任何安全工具都无法修复，杀了毒、清空了DNS缓存，都无济于事。”……

尽管一些计算机专业网站专门开设了浏览器主页修改专题，包括金山毒霸也针对如何解除锁定的毒霸导航作了说明，但对大多数用户来说，浏览器主页被劫持后，要改回去往往费力费时，甚至还无法解决问题。

到底是谁在背后捣鬼？一位软件工程师透露，其实对计算机专业人员来说，“浏览器主页劫持”背后的技术操作门槛并不高。

就修改主页来说，通过软件里混入代码、攫取权限、利用漏洞等都可以实现。专家介绍，很多情况下，按照网上摸索出来的攻略能够将浏览器主页修改回来，但对大多数普通用户来说，光是“任务进程”“注册表”这些概念就已经够难懂，像“卸载驱动精灵需要先在任务管理器里杀掉进程，粉碎文件夹如果失败可以先将子文件强力删除”这种话，更是不知所云。

但许多时候，这些改回主页的办法也不管用，即便是恢复最初设置，又会被改回去。中国科学院信息工程研究所副研究员刘奇旭说，这是治标不治本的办法。很多“浏览器主页劫持”都是通过恶意软件或者插件完成，不将其清除，主页还是会被改回去。一些软件会在后台监视当前浏览器设置，一旦发现设置被重置，会重新劫持主页。还有一种方式是通过攻击用户的家用路由器来劫持主页，不需要修改用户电脑设置即可进行，非常隐蔽和难以消除。

一位软件工程师说，最恐怖的在于那些用户根本察觉不到的互联网技术霸凌。他举例说，“挖矿木马”（在用户电脑里植入并赚取比特币的病毒程序）白天不运行，用户晚上合上电脑后才开始运作。“用户毫无察觉，但其实已经被偷走了流量和资源，一直被‘欺负’。在互联网上，用户在复杂的技术面前往往是弱势的一方。”

带来的危害有哪些

用户上网体验差，会导致隐私泄露危及网络安全

“浏览器主页劫持”带来的危害有哪些？工业和信息化部赛迪研究院电子信息研究所副所长陆峰说，首先会给用户带来使用不便和糟糕的体验，增加不必要的麻烦。“我本来习惯访问的是A页面，但被劫持之后就锁定到B页面。有的网民更喜欢简洁的主页，也不需要在首页上设置密密麻麻的导航网站。一旦被篡改劫持，原有的使用习惯被迫改变。往往这种导航主页上会有许多弹窗广告，导致用户体验变得糟糕。”

其次是由于个人数据被持续收集，容易导致用户隐私泄露。刘奇旭说，浏览器网页所用到的“Cookie”是网站常用的用户跟踪和识别技术。

安全风险则是专家们认为的最大危害。陆峰表示，安全隐患可分为两种。一种是对用户个人来说，浏览器主页被劫持，那么个人电脑中就有极大可能存在恶意软件或病毒，存储在电脑上的资料如银行账号、密码等可能被窃取。另外，如果主页被黑客劫持，诱导进入到一些恶意网站甚至钓鱼网页，可能会导致更大的财产损失。

另一种更严重的后果，则是有可能对整个网络安全造成威胁。360安全专家王丁说：“网页挂马，也就是带有病毒木马的网页已成为目前主要的互联网安全威胁之一。”用户被劫持到挂马网页，就会感染木马病毒，从而被黑客控制浏览器乃至电脑，更有甚者还会使用户电脑成为僵尸主机，被用来攻击其它电脑。

“一般来讲，一些浏览器主页服务商篡改主页，主要是为了引导流量，以商业行为为主，不会对用户的电脑做出窃取用户隐私信息等行为。真正的安全隐患来自于黑客的劫持以及访问诱导，利用替换的钓鱼页面骗取用户信息输入。这种劫持已成为互联网黑色产业链条的重要一环，也是当前很多网络电信诈骗的重要形式，亟待加强治理。”陆峰说。

一位业内人士告诉记者，一款浏览器的自主研发投入巨大、耗时耗力，需要编写的代码超过千万行。如果靠劫持主页就可以占有市场、赢得用户，那还有谁会把精力放在自主研发、提升产品品质上来？长此以往，行业创新将难以为继。

延伸

“浏览器主页劫持”有哪些类型

浙江大学网络空间安全学院研究员周亚金介绍，从最简单的一次性修改主页地址，到通过插件修改，甚至通过修改系统设置来实现，“浏览器主页劫持”根据“来源”可分为多类。

第一类是正规互联网公司的应用软件。安装安全软件或应用软件时，未经任何提示完成安装后，浏览器主页地址也随之被修改为相关网址或导航网页。一些浏览器软件在安装过程中，“默认……为浏览器主页”的提示文字标在不起眼位置，或是默认打钩，如果用户没注意，很容易就被替换主页。

第二类是由于某些第三方工具软件的捆绑安装导致。这类软件通常会捆绑安装浏览器和游戏，并默认设定新的目标主页。

第三类则是明目张胆的恶意软件或电脑木马病毒所为。通过对浏览器发起恶性攻击、潜入恶意插件，或利用木马病毒侵入电脑导致系统混乱，也能轻而易举地篡改主页。

■来源：人民日报、中国经济网