上网被“劫持”，问题出在哪儿

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。

随着互联网治理的深入，网络环境在逐步改善。但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。在复杂的互联网技术面前，用户仍居弱势地位，不时遭遇技术霸凌、个人隐私被侵犯和网络安全风险等问题。

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……”

在网上的各类计算机论坛、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”，马上就跟随显示“浏览器主页被强制更改”和“浏览器主页修改不过来”的搜索提示。“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。

“浏览器主页劫持”有哪几种类型？

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。即便是安装过程中弹出“是否同意用户协议”的窗口，由于协议冗长，用户很少会看全或者根本不看就点击“同意”，从而导致主页设置被更改。专家认为，这些含蓄的诱导行为也可认定为“浏览器主页劫持”。

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。

在技术专家眼中，包括“浏览器主页劫持”的互联网技术霸凌行为不在少数。周亚金举例说，包括通过网页弹窗的方式向用户推广掺杂广告的新闻页面，普通用户不知道如何关闭；通过一些诱导性和欺骗性文字如领取红包等来欺骗用户下载应用或者分享链接，乃至获取用户的地理位置；通过比较隐蔽的设置（用户难以看到的地方）默认捆绑软件的安装。

不仅是个人电脑，智能手机等移动端也有类似现象。网民反映，有的手机装机自带一堆软件，用户不需要也无法卸载。最为人所诟病的就是APP获取权限范围过多过泛。实际上，许多APP声称要开启的权限与其功能根本无关，如导航APP要掌控用户的通讯录或是开启电话权限等。

为啥改不回去？

很多“浏览器主页劫持”都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。

专业人士介绍，从简单到复杂，一般有几种“救回”主页的办法。适用普通用户的，包括重启电脑、卸载软件、浏览器重新设置、杀毒等。但不少用户反映，这些方法无济于事。相对需要专业知识的，例如在安全软件的浏览器保护功能中设置浏览器主页锁定，找到并修改系统的注册表，清除开机时自动启动的恶意程序，修改桌面上的浏览器快捷方式属性等。但对部分网友来说，依然解决不了问题。

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。

“能让用户察觉到的浏览器主页修改，还不是最可怕的。”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）在2017年采用的是低级版本，当用户电脑被感染后，能够感觉到电脑运行速度变慢。但到了2018年，“挖矿木马”升级后，变成白天不运行，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。用户使用浏览器浏览网站内容时，网站可以在用户电脑本地存放Cookie，以识别和记录用户的登录、浏览和购买信息。“而一旦被别有用心的人收集和掌握，你上网的偏好、关注的话题、购买商品情况等相关信息都有可能被收集，然后被‘画像’。最典型的例子，就是你在网上搜索了什么商品，然后满屏都是相关的电商广告。”刘奇旭说。

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。如DDoS（分布式拒绝服务）攻击，也就是在某一个时刻，控制成千上万甚至更多用户电脑的浏览器访问同一网站，该网站可能会瞬间崩溃。

“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。

多位专家表示，从整个行业的健康发展来看，浏览器主页被劫持的行为频发，会极大地扰乱市场竞争秩序，不利于互联网行业的健康发展和创新。一位业内人士告诉记者，浏览器是计算机的重要应用软件，也是互联网应用的基础性软件。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。

劫持浏览器有何目的？

“流量劫持”的背后，隐藏着巨大的商业利益

那么，浏览器主页被劫持的情况为何屡屡发生、屡禁不止？

广告依然是当前互联网经济的核心赢利模式之一，也就是“眼球经济”。流量即眼球，这是造成网络“流量劫持”长期泛滥的主要原因。

中国互联网协会副理事长黄澄清认为，这些问题是互联网发展到一定阶段后出现的。互联网时代讲究流量为王，谁有了流量，谁就掌握了创收的法宝。浏览器是个人电脑通往互联网世界的主要入口，也是智能手机等移动终端上网的重要通道。一定程度上讲，控制了浏览器，也就掌握了用户的流量导向。

显然，“浏览器主页劫持”的背后，隐藏着巨大的商业利益。

专家表示，浏览器主页被劫持，相当于用户流量被劫持，无论是投放广告、推广应用还是收集个人隐私，最后都可能形成利益链条。

浏览器主页通过什么方式来变现流量，实现赢利？记者了解到，当前以“搜索引擎+网址导航”为主的浏览器主页赢利模式主要有三种：

第一种最为清晰明了，那就是网站上无处不在的各种广告。记者随意打开一家导航网站，除了主要位置的网址导航，剩下的几乎都是广告。

广告这么多，运营浏览器主页的服务商能挣多少钱？记者拿到某网站的广告市场报价显示，“导航首页右侧电梯浮层”的价格为17.5万元/天，“浏览器新标签页默认开屏”的价格为70万元/天，“热点新闻弹窗”视位置不同，价格从几千元、几万元到上百万元不等……这家企业的营业收入中，互联网广告及服务贡献了绝大部分。可见锁定用户访问的固定页面有多重要。

第二种赢利模式主要通过搜索引擎来实现。业内人士介绍，这些浏览器主页上的显著位置都设有搜索条框，一些热词、关键词的搜索都会给浏览器主页带来收益。每次点击带来的收益通常在几毛钱到几十元钱不等。搜索引擎用户量越多、排名越靠前，其热词的竞价排名收费越高。

第三种赢利模式则是通过采集用户信息来实现。“为什么会有那么多精准的广告投放？就是有了较为精准的用户画像。”专家表示，PC端用户行为数据的收集主要通过网页浏览，移动端则主要通过APP的各种权限来采集。而这些信息，都已经成为互联网黑色产业链条的商品，被明码标价。

周亚金说，将用户的主页锁定到一些搜索引擎、电商网站，软件和被推广的网站都从中获利，算是一种比较“温和”的做法。如果将主页定向到一些博彩赌博网站、钓鱼页面，进一步获得用户的支付信息，那就是赤裸裸的诈骗和非法牟利。

侵犯了用户什么权利？

侵犯了用户的知情权、自主选择权、计算机信息系统拥有权

法律专家认为，以“浏览器主页劫持”为代表的“流量劫持”行为，不仅破坏互联网运营生态，给用户带来不便甚至安全隐患，而且本身就属于违规违法行为。

这种行为侵犯了用户的知情权、选择权。“早年，篡改主页是少数黑客的‘炫技’行为，而今一些网络公司贪图流量价值，通过不正当竞争的方式来获取流量。”中国互联网协会法治工作委员会副秘书长胡钢说。

中国政法大学传播法中心研究员朱巍认为，互联网领域的不正当竞争类型很多。“浏览器主页劫持”利用技术手段干扰用户选择，实际是对用户的误导，侵犯了用户的知情权和选择权。

安全专家表示，一些相对基础的软件作为计算机底层软件，拥有较大权限，因此更应该慎用这种“特权”，任何对用户电脑的干预行为都应该以“实现功能所必需”为前提，而不是借保护用户安全的名义，擅自变更用户浏览器主页来抢夺流量。

此外，这种行为还侵犯了用户对计算机信息系统拥有的权利。北京师范大学刑事法律科学研究院暨法学院副教授吴沈括说，当浏览器被他人劫持，用户无法按照自主意愿使用时，就是侵犯用户对计算机信息系统拥有的权利。

2015年11月，上海浦东法院判决了全国首例“流量劫持”案，其背景就是，网民想要访问A网站，却被突然劫持到了B网站。法院以破坏计算机信息系统罪判处两名被告人有期徒刑三年，缓刑三年；扣押在案的作案工具以及退缴在案的违法所得予以没收。2018年底，最高人民法院将该案发布为指导性案例。胡钢认为，法院的这一判决表明，劫持流量行为不但违法，而且也会构成犯罪。这对于“流量劫持”的治理具有样本意义。

与此同时，“免费”不能成为网络经营者违法的托词。绿盟科技资深网络安全工程师肖召红表示，软件研发的成本比较高，我国大多数软件免费提供给用户使用，流量套现是主要商业模式。近些年，面向用户端的网络红利逐渐耗尽，不少软件企业面临较大的生存压力。这是部分软件企业冒着损害用户利益的风险，想方设法引流的原因之一。

对此，肖召红认为，一些软件企业要健康发展，应通过技术创新等手段拓宽赢利渠道，不应只聚焦在流量上。安全软件企业在企业端市场也还有很大的挖掘空间，这样既能维护网络环境，也能支撑自身的发展。

“一些软件产品的免费模式不应是网络经营者违反法律、侵害网民合法权益、破坏市场竞争秩序的借口。网络从业者需要自觉遵守秩序，这样才能健康发展。”胡钢表示。

中央网信办网络安全协调局相关负责人就此问题接受记者采访时表示，网络安全法对网络运营者收集、使用个人信息有明确规定，企业必须遵循合法、正当、必要的原则，不应过度收集用户个人隐私。

监管治理难在哪里？

应用场景多样，监管、取证的难度较大

专家认为，以“浏览器主页劫持”为代表的“流量劫持”，是黑客及网络黑色产业组织存活的主要源头。尽管在监管治理上出台了不少措施和规定，但“流量劫持”仍然困扰行业多年，其原因是多方面的。

首先，由于应用场景多样，监管、取证的难度较大。吴沈括说，理论上，只要存在数据的传输，就存在“流量劫持”的可能性。数据流通的多个环节如应用程序端、路由器端、运营商端等，都有可能被实施“流量劫持”。多种多样的场景和技术手段，加大了监管的难度。

黄澄清说，如果用户的浏览器被劫持，通常可以向宽带运营商、广告平台投诉举报，以及向“12321”网络不良与垃圾信息举报受理中心举报。但“12321”主要起社会监督作用，网民举报以后，中国互联网协会按照自律公约或者细则的规定向社会曝光，将相关企业列入黑名单。但目前“12321”受关注度还不够高。

由于用户访问网站是个人行为，遭遇“劫持”后取证困难。很多时候，网民只能主动放弃投诉。

其次，是监管机构协同治理机制还不够完善。业内人士表示，当前我国对互联网企业实行属地管理，网络监管又涉及工信部、网信办、公安部等多个部门，这些部门的分工各有侧重，部门间协同治理还有待完善。

早在2006年，中国互联网协会制定了《抵制恶意软件自律公约》，公约第九条规定，尊重用户上网选择，反对浏览器劫持。这是我国较早涉及“流量劫持”的规范。

但治理“浏览器主页劫持”的行为，光有行业自律还不行。“必须要有底线意识，有法律和政府管理做支撑，与行业自律一起打出组合拳，才能形成长效机制。”黄澄清说。

实际上，我国目前已出台不少规范“浏览器主页劫持”等行为的法律规范。吴沈括介绍说，2017年6月实施的网络安全法第十条、第二十一条、第二十七条等规定，都从原则性的角度否定了“流量劫持”行为，但在实践中还需要更详细、可操作的条文。

“互联网发展引发许多新问题，对它们的认识和理解有一个过程，需要把握规范和发展的平衡，应该在深入调研的基础上出台相对应的法律法规，如此才更有效、更有操作性。”黄澄清说。

到底用什么办法治理？

加大监管力度，进一步健全和完善相关法律法规

源源不断的经济利益刺激，让“流量劫持”成为“野火烧不尽”的网络顽疾。有没有办法能够有效治理甚至根治？

专家认为，首先要进一步加强对“流量劫持”行为的监管与治理。

“加大对网站经营者、搜索引擎的监管力度，要鼓励其与网络黑色产业势力对抗，共同创造一个良好的互联网环境。”肖召红期待，工信部、网信办和公安部三部门应进一步加大协同治理的力度。同时让市场监管总局等相关部门也共同参与，互联网协会等行业协会应推动行业加强自律规范。

其次，亟须进一步健全和完善相关法律法规，让“流量劫持”治理有更详细的细则，从而指导实践，进一步加大处罚力度。

陆峰表示，我国现行法律法规在个人信息保护方面的有关规定原则性较强，缺乏具体的实施细则，企业操作的回旋空间还很大，仍需进一步细化。工业和信息化部有关负责人告诉记者，工信部正在加强政策研究，下一步将配合做好《个人信息保护法》立法工作，从操作性上细化法律法规要求，细化标准，如引导企业分场景获取用户明确授权，不“强制索权”等。

此外，受访专家也认为，要加强对最新网络犯罪问题的研判。吴沈括说，对一些高频次、有特点的网络安全案件，有必要以案例形式进行科普，提升认知。

胡钢认为，网络相关立法，特别需要坚持“速立频修”的原则，就是快速建立，频繁修订。“‘速立’解决‘有无’问题，‘频修’解决‘更好’问题，以及时响应快速变化中的各类问题。”

中央网信办网络安全协调局相关负责人介绍，近年来，各有关部门持续对网络黑产加强监管和打击。公安部组织开展“净网”、黑客攻击破坏和侵犯公民个人信息犯罪打击整治等一系列专项行动。工业和信息化部开展专项行动，清理移动智能终端预置恶意软件等问题。中央网信办会同工信部、公安部、市场监管总局开展了APP违法违规收集使用个人信息专项治理。今后各有关部门会继续按照“打源头、摧平台、断链条”原则，对利益链条的上中下游全链条进行打击和治理，包括针对上游提供恶意程序等工具和技术支持、中游实施恶意劫持行为和下游进行利益变现的渠道等一系列问题。

工业和信息化部相关负责人也表示，工信部高度重视用户个人信息保护工作，近年来不断强化电信和互联网用户个人信息保护监管工作，如定期开展技术检测和监督检查，对违规收集使用用户个人信息的企业或手机应用软件进行查处和曝光。该负责人表示，今后将强化监督检查，督促企业落实现有规章制度和行业标准，特别是在用户个人信息收集使用规则公示告知、征得用户授权同意等环节，充分保障用户的知情权、选择权。

专家也建议，网友在使用个人计算机等智能设备时，也应增强防护意识，从正规渠道下载软件或应用；安装新软件、新应用时充分了解授权要求，保护个人权益。

多位受访专家表示，治理“流量劫持”现象需要多方配合、协同作战，在各个环节进行防御。对“流量劫持”这个网络顽疾，记者将持续关注。

记者在此呼吁：那些有“浏览器主页劫持”等侵权行为的行为主体，是改邪归正的时候了！

（据《人民日报》）