责任编辑:张任青子 组版编辑:余永春 校对:张苑

上网被「劫持」问题出在哪儿

想访问A网站却被强制打开B网站

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"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……"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。

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。浙江大学网络空间安全学院研究员周亚金举例,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,这些都属于"浏览器主页劫持"。

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。

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。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。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。

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。一种是个人电脑被劫持后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。如果主页被黑客劫持,诱导进入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,则是对整个网络安全造成威胁。用户被劫持感染木马病毒,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。

那么,浏览器主页被劫持的情况为何屡屡发生、屡禁不止?"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。一定程度上讲,控制了浏览器,也就掌握了用户的流量导向。

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。第二种赢利模式主要通过搜索引擎来实现。热词、关键词的搜索都会给浏览器主页带来收益。第三种赢利模式则是通过采集用户信息来实现。这些信息是互联网黑色产业链条的商品,被明码标价。

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。

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。

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。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年年底,最高人民法院将该案发布为指导性案例。这对于"流量劫持"的治理具有样本意义。

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。

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。

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。绿盟科技资深网络安全工程师肖召红期待,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,"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。"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。

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。

(冯华 吴月辉 喻思南 刘诗瑶 余建斌)