贻害无穷　屡治无果——蹭网 App 如何根治?

一到周末，放假在家的孩子们又与手机“不离不弃”了，本以为“关掉自家 WiFi 就好”的家长发现，各种破解 WiFi 密码的“神器”让孩子畅玩无阻。另一边，用户密码等数据被偷偷上传，隐私安全难以保障。

此类软件的恶意行为究竟有何后果？为何屡禁不止？对此记者进行了调查。

蹭网“神器”：“免费午餐”危害大

“怎样屏蔽邻居的 WiFi”“怎样防止邻居密码被破解”……很多家长在网上发帖求教。讽刺的是，与家长焦虑无奈的求助相比，更多的网帖在传授如何使用 APP 攻破他人 WiFi 密码。

“这些破解 WiFi 密码的软件和教程多如牛毛，让学校和家长在防治青少年沉迷手机游戏的努力付之一炬。”长期从事青少年教育的社工韩立怡说。

记者在安卓手机应用商店里以“WiFi”为关键词搜索，出现上百个 WiFi 分享类 App，下载量多的过亿次，少的也有几千次。一些 App 直言不讳介绍功能：“采用多种破解技术对 WiFi 密码进行破解”“真真正正能够破解别人的 WiFi 密码，让用户随时随地都能连接到 WiFi 网络”……根据艾媒咨询统计，关于 WiFi 密码分享类 App 在各安卓市场超过 500 个。

隐藏在“免费午餐”背后的是数据信息的捕获。360 天马安全团队负责人柴坤哲说，这类 App 打着免费旗号，能够在短期内扩展足够多的用户，积累 WiFi 与密码的对应数据库，并进行其他维度的数据收集，甚至出售数据给第三方平台。

此外，蹭网 App 还破坏了“使用付费”的市场原则。业内人士认为，这些“流量小偷”影响了无线网络的正常使用，造成网络堵车、下载缓慢或者网页打不开等问题，侵害了付费者的正当权益。

违法成本低：打掉一个长出一堆

这些蹭 WiFi 神器究竟是怎么运作的？

据艾媒分析师介绍，WiFi 分享软件“偷密码”的方式主要有两种：第一，暴力破解密码，采用英文字符、数字、特殊符号的组合对密码逐个进行破解尝试；第二，应用未经用户许可或同意，将用户填写或储存的密码上传到服务器供其他用户调用，“也就是说，用户使用这些软件后一旦登录自己家的无线网，家里的无线网也被默认分享了。”

记者在安卓市场上搜到一款名为“万 X 宝”的 App，介绍显示，“不仅能自动破解周围 WiFi，还能手动指定破解 WiFi、显示密码”。另外一款号称“密码查看神器”的 App 则在打开之后弹窗显示，可进行“云破解”，即用软件本身的密码库暴力破解他人密码。

某技术中心工程师团队对安卓市场搜索下载量比较高的部分产品进行了系统测试，结果显示，这些“神器”基本都疑似存在未经用户允许、私自保留与上传用户密码的行为。“对于被蹭网的用户来说，有数据被泄漏的风险，如果这些数据被不法分子利用会造成更大损失。”艾媒咨询 CEO 张毅说。

今年 4 月，工业和信息化部已经对此类 App 开展调查，对涉嫌入侵他人 WiFi 网络、窃取用户个人信息的两款知名 App 依法依规进行了处理。然而，仅仅半年过去，蹭网类 App 又卷土重来。

爱加密 CEO 郭训平分析导致此类 App 禁而不止的原因：开发成本相对较低、开发周期短，在破解代码程序后，更改一个“皮肤”就可自行发布供人下载；此类应用需求量大，开发者可通过植入广告、窃取信息等方式获利，开发成本远远低于违法违规成本；各大应用商店对于 App 进入的审核标准不统一，部分 App 不经应用市场也能直接在网页上下载使用。

让法律长出“牙齿”　让监管形成“闭环”

“密码小偷”明目张胆地破坏市场环境和公序良俗，对蹭网 App 的“牛皮癣”该如何根治？

“App 上线目前尚未做到前置审核，从应用商店的角度来说，也更愿意多集纳新的 App 聚集流量。”郭训平表示，网络监管部门应加强常态化巡查，对于违法违规的企业及个人，应由多部门予以联合惩处。柴坤哲建议，各大应用市场需把好入口关，如有诱导分享等手段需对其进行整改，从渠道上给予此类软件约束。

广东省社科院现代化战略研究所助理研究员谷雨认为，在个人隐私保护和立法上需要加快推进，以法律的形式规定滥用个人信息行为的法律责任，“要让监管形成闭环、让法律的锤子能够落地。”

用户自身安全意识也有待加强。张毅等人建议，社会各界需多途径、多方式加强用户隐私意识教育，用户应对软件默认勾选使用个人信息的行为保持高度重视，不下载安全性能不高的 App，尽量到正规应用商店下载使用评价等级较高的 App。

（据新华网）

>>>相关链接

工信部“出手”调查“WiFi 万能钥匙”等蹭网 APP

工信部网站今年 4 月 2 日发布网络安全管理局关于“蹭网”类移动应用程序的通报。通报称，近日据有关媒体报道，移动应用程序“WiFi 万能钥匙”和“WiFi 钥匙”具有免费向用户提供使用他人 WiFi 网络的功能，涉嫌入侵他人 WiFi 网络和窃取用户个人信息。

为此，网络安全管理局组织网络安全专业机构对移动应用程序“WiFi 万能钥匙”和“WiFi 钥匙”进行技术分析，发现两款移动应用程序具有共享用户所登录 WiFi 网络密码等信息的功能。

目前，工业和信息化部网络安全管理局已要求上海市、福建省通信管理局开展调查工作，将在核查的基础上，依据《网络安全法》等法律法规进行处理，维护广大网民的合法权益。对于主管部门调查，“WiFi 万能钥匙”开发方连尚网络回应，积极配合主管部门。

3 月 29 日，《经济半小时》栏目报道称，通过在多地测试上述两款应用发现，用户可以连接住家、餐饮、银行，以及政府办公附近的无线网络，并指责其窃取用户隐私。

资料显示，“WiFi 万能钥匙”开发方是上海掌门科技有限公司子公司上海连尚网络科技有限公司，产品于 2012 年 9 月上线，截至 2016 年 6 月，其用户总量超过 9 亿；“WiFi 钥匙”的开发者厦门众联世纪科技成立于 2013 年 1 月，其产品 Logo 设计和功能与“WiFi 万能钥匙”相似。

对于央视报道，连尚网络回应称，“WiFi 万能钥匙”的产品名称容易给公众造成误解，但 WiFi 万能钥匙的运行原理是热点共享，不是破解，是通过 WiFi 热点资源共享的方式，让用户便捷连接，安全上网。并且，“WiFi 万能钥匙”并未明文显示密码。央视报道中的密码查看功能属于 WiFi 钥匙提供。

共享 WiFi 的 APP 因其上网的便利性，受到用户的追捧，在应用商店属于热门应用。但这类产品目前仍存在诸多争议。一位 WiFi 方案提供商告诉记者，共享应该是在双方允许之下，通过协议达成，而不是一方不经允许就擅自使用。

对于安全性，业界也存在不同的看法。有安全专家告诉记者，如果企业对接入设备不进行严格管理，就会存在安全隐患，就会为黑客入侵提供快捷通道。但中国 WiFi 产业联盟秘书长雄歌认为，“连接 WiFi 就会存在安全隐患，是社会普遍存在的问题，而非单一共享 WiFi 暴露的问题。”

雄歌表示，对于想要使用公共 WiFi 的用户而言，最安全的方式是经过专业认证过的应用登录。　（据新京报）