卧室隐私在网上以数十元被公开叫卖，谁在偷窥你的家？

新华社厦门9月12日电 “对着卧室的摄像头IP地址10元一个，拍摄到激情画面的20元一个。”原本用来看护家里老人孩子或用作防盗的摄像头，竟然被不法分子用于“窥私”在网上公开叫卖。

近日，北京、浙江等警方接连破获黑客非法入侵居民家用摄像头案件。“新华视点”记者调查了解到，目前，我国的家用摄像头保有量为4000万至5000万个，其中一些存在被攻击风险。在一些QQ群和百度贴吧，有人公然售卖破解摄像头软件，分享他人家庭私密影像。

多地发生家用摄像头入侵案

7月14日，北京警方破获一起网上传播家庭摄像头破解软件案，抓获涉案人员24名。

据犯罪嫌疑人交代，他们非法获取某品牌摄像头破解软件，利用黑客手段破解网络摄像头IP，然后在QQ群中出售。

有涉案者交代，在发现专门破解网络摄像头IP的QQ群后，他加入并向管理员购买了扫描破解软件，轻松破解了100余个摄像头IP，观看保存了摄像头拍摄的内容。

8月初，浙江丽水警方成功打掉浙江省首个网上传播家庭摄像头破解入侵软件的犯罪团伙。已被破解入侵的家庭摄像头IP近万个，涉及云南、江西、浙江等地。

据犯罪嫌疑人王某交代，他非法获取某摄像头破解软件，采用黑客手段破解网络摄像头IP，破解网络摄像头密码，控制摄像头偷窥他人隐私。随之在相关QQ群中出售控制摄像头的软件和已被破解的摄像头IP。

“普通摄像头信息一个卖5元，对着床的一个卖10元，有激情画面的一个可以卖20元。”犯罪嫌疑人王某称，除了贩卖被破解的摄像头IP外，他将偷窥到的录像保存并上传云盘进行贩卖。

去年5月，360攻防实验室发布《国内智能家庭摄像头安全状况评估报告》，直指家用摄像头9大类安全风险：用户隐私泄露、未加密数据传输、无人机识别机制、多数智能设备可横向控制、未对客户端进行安全加固、代码逻辑设计缺陷、存在硬件调试接口、未对启动程序进行保护和没有远程更新机制等。

据360安全研究员严敏睿介绍，安全风险相对突出的是一些与外网相连的摄像头。

记者调查：控制他人摄像头网上70元“包教会”

记者在互联网和社交软件上进行关键词检索发现，尽管一些运营商屏蔽了相关关键词，但仍能搜索到大量暗示性强烈的破解软件和用户隐私录像的交易贴、交流群。

记者加入多个相关QQ群号和QQ账号。在一个名为“ip摄像交流群”的QQ群中，群主除不定时播发破解软件贩卖信息外，还时常分享一些通过被劫持摄像头录制的私密录影，诱导群里的成员购买破解软件。

在不法分子所分享的录制视频中，绝大部分都是隐私的夫妻生活内容，并夹杂一些看似在酒店客房隐蔽位置拍摄的激情视频。

记者添加了尾号为9496的QQ用户。对方称，只需要70元即可将摄像头查看软件卖给记者，并承诺“包教会”。在支付了70元后，对方指导记者下载了一款软件，同时向记者发送了两个包含数百个IP地址的文件和十余个软件教学截图。

对方指引记者添加了6个居民家中的网络摄像头，并获取实时画面。这些摄像头有一些对着床，一些则对着浴室，可通过软件随意选取拍摄角度。画面中的家庭成员均未察觉。记者随即将相关材料交给警方。

据业内人士介绍，只需要掌握用户的摄像头IP地址和账户密码，就可以登录查看摄像头的实时画面，而这些IP地址都是通过扫描软件得到的。

此外，这些被入侵的家庭摄像头还有可能沦为黑客的攻击工具。腾讯安全反病毒实验室安全专家马劲松告诉记者，被控制的摄像头变成了攻击源，而真正的攻击者的位置被隐藏起来，此种攻击可能造成更大范围的危害。

弱口令容易被破解，正确设置密码安全性可达90%以上

“并不是所有的摄像头都容易被入侵。”严敏睿解释说，一些贴牌生产的山寨摄像头自带拨号上网功能，这部分摄像头在外网环境下可以直接被搜索到，攻击起来也相对容易。

据业内人士介绍，家用摄像头主要来自于三种渠道：互联网企业、原生安防企业和“贴牌”生产厂商。其中前两者都具备修改产品软件代码，对产品进行安全性加固的能力，而贴牌生产厂商则完全不具备这种能力，安全性较差。

浙江景宁公安网警大队副大队长陈勇涛表示，在办案过程中民警发现，一些弱口令的摄像头以及安全系数较低的摄像头，嫌疑人使用破解软件都能很快破解。

上海信息安全行业协会专委会副主任张威说，在选购家用摄像头时，选择正规厂家生产的大品牌摄像头就已经为普通用户过滤掉了70%至80%的安全风险，如果用户根据说明书设置密码，家用摄像头的安全性将达到90%以上。

北京师范大学刑事法律科学研究院孙道翠认为，借助网络技术的犯罪具有身份隐秘、地点隐匿、行为轨迹难以追踪性等特征，执法部门要通过提高科技力量进行应对。