家用摄像头变偷拍器 私密视频网上卖

温州警方破获非法控制家用摄像头案，32名嫌犯归案；记者调查发现，网上可轻易买到摄像头账号

据新京报报道，12月17日的晚上，王明夫妇在卧室聊天。妻子手里拿着毛巾，坐在床边洗脚，位置正对着摄像头。她浑然不知，在摄像头另一端，有人将这些看得一清二楚。

这对夫妻可能没想到，两人的日常生活已成为“试看频道”，被偷拍者作为吸引他人购买的福利。这家人使用的摄像头有回放功能，一个月来何时出门、何时回家、做了什么，都被卧室里的摄像头，同步直播下来。

记者调查发现，大量类似的监控视频在网上传播，其背后是一条非法破解摄像头，买卖、传播偷拍视频的黑产链条，除家用摄像头外，一些人还在酒店安装了针孔摄像头偷窥他人隐私。

一组来自行业调查公司IHS Markit数据显示，2017年中国在公共和私人领域（包括机场、火车站和街道）共装有1.76亿个监控摄像头，据媒体报道，预计到2020年内中国安装摄像头的数量会增加到6.26亿个。

近年来，各地警方不断破获黑客非法控制家用摄像头案件。近日，温州警方控制犯罪嫌疑人32名。警方介绍，犯罪分子非法贩卖某公司品牌APP破解工具，利用APP破解工具对他人的摄像头进行扫描，控制数十万只家用摄像头。

警方召开新闻发布会，现场展示犯罪嫌疑人的作案工具。

A 数十万只家用摄像头被非法控制

记者从温州警方了解到，今年6月，温州市公安局网安支队在网上巡查时发现，有人在一些互联网论坛、贴吧、社交工具中，交易多家公司品牌的家用摄像头破解工具和被控制的家用摄像头账号密码。

经进一步侦查，民警发现，嫌疑人还贩卖家用摄像头拍摄的私密视频，部分内容甚至涉及私生活。

警方在侦查中发现，涉案嫌疑人贩卖的监控视频账号达数万个。从视频的拍摄角度和内容可以判断，当事人系在不知情情况下被拍摄录制，且部分摄像头的安装位置敏感、范围广，涉及家庭卧室、美容院、私人会所等。

据温州警方抓获的黑客供述，他们制作扫破摄像头软件，对账号密码设置强度不高的摄像头进行扫描破译，强行侵入并控制他人的家用摄像头系统。

警方介绍，这些人通过非法侵入摄像头系统，获取私密视频后，会通过贴吧、QQ群买卖，或者与他人互换摄像头账号。根据视频的私密程度，定价5元到60元不等。犯罪嫌疑人涉及全国各地。

温州市永嘉县警方抓获的一名30岁的男子，没有正式工作，因出于好奇心在网络论坛上发现有软件可以破译摄像头软件密码，后因贪念建QQ群，用于贩卖破解的账号和密码，赚取生活费。

永嘉县警方透露，此次行动中，他们共抓获犯罪嫌疑人11名，每名嫌疑人在生活中都互不认识，只是在网络上通过虚拟身份联系。他们贩卖摄像头的账号和密码时，会先让客户试看部分片段。客户试看后，通过支付宝、微信红包直接转账，即可获取监控的账号密码。涉案金额达上万元。

温州警方介绍，此类犯罪严重侵犯了公民的隐私，社会危害性极大，属新型网络黑客犯罪。经两个多月的侦查，温州市公安局网安支队组织永嘉、瓯海、龙湾等八个县市区网安部门、派出所等警力开展跨省收网行动，分别在海南、河北、河南等二十多省市抓获张某某、李某某等犯罪嫌疑人32人。

经审查，犯罪嫌疑人对于非法贩卖摄像头破解工具，以及利用摄像头破解工具对他人的摄像头进行扫描、控制的犯罪事实供认不讳。目前，涉案人员均已被采取刑事强制措施，案件还在进一步侦办中。

B 网上存在大量买卖监控视频现象

记者调查发现，目前，网络上仍有大量买卖类似视频的渠道。

“需要监控资源吗？”12月中旬，记者加入一些名为“摄像头共享”“摄像头ID”的QQ群。一进群，就有卖家与记者私聊，推销其手中的监控视频资源。

为了吸引记者购买视频，同时也为了避免封号，一名卖家通过“闪照”功能，发送了一些露骨的画面给记者，虽然这些视频三秒就自动销毁，但仍可以看到日期均为近期。此外，他还发送了数张家庭日常生活监控截图。画面中，有母亲在哺乳，有一位女士坐在床上玩手机，还有一位美容院的客人赤裸上身。从神情来看，他们都不知道自己正在被偷拍。

为了证明自己的货源真实，对方发来一个监控账号，让记者试看。记者按照指示下载相应软件，输入账号、密码就能看到监控画面。记者注意到，这个密码非常简单，是三位连着的数字。

输入密码后，一经联网，画面即弹出。这个账号属于一对夫妻，姓名、地址不详，但他们的一举一动都暴露在他人的手机上。通过视频，可以看到这对夫妻家中卧室、门口走廊的画面。另外，摄像头有夜视功能，晚上可以清晰地看到床上的人睡觉翻身的动作。

在一些贴吧中，同样存在贩卖摄像头账号的行为，买家一旦获取了账号和密码，也就获得了在app中操作摄像头的全部功能，包括录像、回放、转向，甚至还有对讲功能。一位卖家在帖子中强调“不要随便动摄像头”，他们担心他人频繁转向，会引起被偷拍者的察觉。

温州警方在调查取证中也发现，受害人对偷拍毫不知情，一位市民表示，自己完全不知道自己家摄像头被他人破解了，回去后要提醒身边的人。

C 70元可买300个摄像头ID

记者调查发现，在互联网上，破解监控，买卖、交换私密视频，已经形成了一条完整的利益链条。

不同的卖家抛出的价位不同。一名卖家给记者发来十余张不同家庭的卧室截图，并提到“对床视频70元十个”。也有卖家15个ID卖188元，卖家发来的截图有美容院、按摩店、卧室的，其中一张是卧室实时截图，画面中有女士羽绒服和围巾。

在一个群里，一位卖家抛出了更便宜的价位，“70元300个频道任你挑选，按摩、大床、夫妻、美容院居多”。

除了买卖，更多活跃在贴吧和QQ群的人提出互换摄像头账号。换账号的要求很高，必须有“精品”视频，对方才愿意交换。也有人会收购视频账号，“更衣室的精品ID，30元起”，甚至还有人在贴吧中求浴室监控视频账号。

记者注意到，在这些卖家中，有骗子混迹其中，买家将钱转过去后不发账号，还有卖家在贴吧中曝光骗子。

记者调查发现，除了买卖、互换摄像头账号，也有人售卖破解软件。一位卖家的手机中，装有“天眼通”“蓝精灵”“上帝之眼”等，他售卖的“天眼通”APP价格398元，号称可以搜索附近一千米所有品牌摄像头，每天扫描摄像头数量不限量。他透露，这款软件是以前的“天巡”、“刺客”等软件功能的后台整合。

其演示视频显示，软件打开后可同时显示9个画面，有整理、精品收藏、回放功能，其破解摄像头的账号和密码在下方显示。

另一位卖家则售卖一款388元的破解软件，专门扫描某个品牌的摄像头账号。扫描软件截图显示，该APP可以同时扫描一万个ID账号，并有查询在线ID的功能。

D 卖家兜售酒店私密视频账号

记者发现，摄像头账户价格因场景不同有所区别，其中酒店的最贵，卖得最火，一些卖家为了规避审查，会将QQ群名称写成“9店”。

一位卖家主动加了记者微信，兜售酒店私密视频账号，10个账号480元。卖家发来了一段演示视频，他将自己手机上的软件打开，画面展示一对情侣睡在酒店圆床上，时间是12月20日12点，卖家一边操作一边讲解：“这是高档酒店的，你要的话直接发红包。摄像头可以转动、可以放大，高度清晰，可以直接下载或者回看一个月的记录。”

至于视频来源，对方表示“这你就不用管了”，不过他透露，这都是针孔拍摄，对方发现不了。

还有一位卖家，买卖的视频均是酒店内男女发生性关系的场景，20个ID售价188元。卖家表示，他破解了别人在酒店装的针孔摄像头，“不会被发现，都是很隐蔽的，就算发现了也跟你没关系”。

关于酒店安装针孔摄像头的情况早有存在，今年11月，浙江省公安机关在“净网2019”专项行动中，查获了一起从设计制作专用芯片、搭建远程控制平台，到加工组装伪装配件，并线上线下同步销售针孔摄像头的非法制售利益链条。警方发现，下游使用针孔摄像头的安装位置，包括家庭、宾馆、办公场所，其安装意图有的是为了偷窥他人隐私，也有为了传播淫秽物品，甚至有组织卖淫的。

警方介绍，除了无线路由器和时钟，常被改造伪装的日常用品还有烟雾报警器、电源开关插座等屋内常备装置。此外，便携手持的常用设备，如充电宝、手表、打火机，甚至饮水杯，也常被改造成偷拍工具。

据媒体报道，发现隐蔽摄像头的方法非常简便。只需要准备小时候玩的红色玻璃纸，用红色玻璃纸同时遮住手机镜头和闪光灯，在闪光灯开启的状态下给可疑的地方拍摄视频，如果发现发光发亮的物体，那就是针孔摄像头，原理是它会在相机红光的照射下发生反射。

E 密码简单账户易被入侵

温州警方表示，非法入侵他人摄像头社会危害极大。容易诱发人身、财产类犯罪，基于犯罪嫌疑人利用黑客工具非法控制网络智能摄像头进行偷窥、录制、传播不雅视频的不法行为，易引发敲诈勒索、猥亵、强奸等严重侵犯财产和人身权利的犯罪。

网络安全公司白帽汇创始人赵武长期关注摄像头黑产，他此前接受记者采访时提到，破解个人摄像头以窥私并出售私密视频牟利的情况，近几年才出现，这与个人摄像头的普及有关。现在很多人安装网络摄像头，监护家中的小孩、老人或宠物，或者当成家中安防工具。但大量摄像头存在容易被黑客入侵的安全漏洞。赵武的团队曾向监管部门上传过一份报告，指出多款摄像头存在容易被攻击的安全漏洞。甚至有些厂商在生产摄像头过程中，已经预留了可以远程操控的后门。

记者在调查中，得到一张卖家发来的卧室监控画面实时截图，画面上方有白色字体显示“密码过于简单，请立即到电脑端更换设备密码！”一位黑客在论坛中提到，“摄像头都有IP地址，需要密码才能看到监控录像，很多设备没有改默认密码，所以我们就可以随意监控他们了。”

温州警方表示，侦查时发现，被入侵的摄像头账户密码都比较简单，比如连续的数字或英文字母，有些密码和用户名相同。警方提示，用户在使用摄像头时要加强防范意识，如修改原始密码，使用复杂的密码，尽量不要对床，睡觉时将摄像头挡住等。网络安全公司白帽汇创始人赵武认为，厂商也需要不断改进，提高安全系数。

F 破解、买卖摄像头账号行为涉嫌犯罪

记者发现，除了售卖摄像头账号，也有人将一些私密、淫秽的画面录下来，有些用来宣传，有些直接售卖。在记者调查中，一位卖家见记者迟迟不买，就发了一段12月9日晚上10点多，一对夫妻在卧室发生性关系的视频，并称还可以回放其他片段。

温州警方表示，此举涉嫌传播淫秽物品罪，具体需要根据数量和金额判定。在非法破解家用摄像头行为中，嫌疑人更多的是涉嫌非法获取计算机信息系统数据罪和非法控制计算机系统罪。

记者在裁判文书网中注意到，12月11日，北京市朝阳区法院判决了一起非法控制计算机信息系统案，被告人被指通过搭建“上帝之眼”“蓝眼睛”等APP，非法控制监控摄像头18万余个，并通过在网络上推广上述摄像头实时监控画面非法获利人民币89万余元，最终获刑5年。其同伙被以帮助信息网络犯罪活动罪，判处有期徒刑十个月，罚金人民币一万元。

随着警方不断破获黑客非法入侵居民家用摄像头案件，互联网上相关QQ群、贴吧被封了不少。一些卖家开始隐身于普通摄像头品牌贴吧，甚至有些人将品牌摄像头名称作为买卖隐私视频账号的群名。卖家越来越隐秘，有卖家在贴吧中发帖后，引导他人点击其主页才能看到联系方式，也有人在QQ签名中称某个群已封，要求他人加好友进新群。

（赵朋乐）