【治理偷窥黑产之一】

起底摄像头偷窥黑色产业链

不法分子在公共场所偷装摄像头 有的一年进账数百万元

清理违规有害信息2.2万余条，处置平台账号4000余个，下架违规产品1600余件，14家APP厂商被约谈……据中央网信办消息，今年5月以来，多部门集中治理摄像头偷窥等黑产，对群众反映强烈的非法利用摄像头偷窥个人隐私画面等行为进行集中治理，取得显著成效。非法利用摄像头偷窥的行为，严重侵犯他人隐私，危害网络空间安全。此轮集中治理，正是要深入整治这一问题。

改装
摄像头改装到手机底部 电商平台有售

除了长着“第三只眼”的智能手机之外，实际上很多物品被伪装成隐蔽的偷拍设备，家用的智能摄像头也可能成为不法分子偷窥的窗口。一些不法分子利用黑客技术轻易破解并控制家用及公共场所摄像头，偷窥他人生活。更有甚者，在酒店、试衣间、公共卫生间等场所偷偷安装摄像头，偷拍下一些私密的画面，并搭建APP或利用其他平台向客户收取“会员费”“套餐费”牟利，有的则直接通过社交软件叫卖。拍视频者甚至发展成了一条成熟的黑色产业链，一年可获数百万元的进账，一环扣一环。

据了解，有卖家通过隐蔽的方式售卖被破解的摄像头ID及破解软件。“把手机放在桌上，你压根不会想到它的底部扬声器或者耳机孔就在偷拍你。”有人揭露“智能手机改装成盗摄手机”的风险，就是对市面上主流的手机进行改装，把针孔摄像头改装到手机下方的扬声器出孔的位置。

据介绍，针孔连接着前置摄像头协议接口，当使用前置摄像头进行拍摄时，就会切换到手机底部的针孔摄像头进行拍摄。针孔镜头还可以与一个APP配合使用，以达到静默盗摄的目的。据称，这种被改装过的手机有诸多风险。“把手机放在桌上，甚至拿它上厕所玩，压根不会想到它的底部扬声器或者耳机孔就在偷拍你；在大街上，你得小心身边人群中可能的盗摄者，他们有可能会用这种改装过的手机偷拍你的隐私部位。”

4月20日，根据相关网友提供的线索，记者在国外一款即时通讯软件进行了检索，并找到了大量售卖此类改装手机及改装服务的卖家。记者看到，名为“针孔摄像头、偷拍、针孔相机”的群里有1000多名成员。

群里一名卖家介绍，手机定制改装是将摄像头改装顶部或底部，特点是“黑屏录制、后台录制，隐蔽性好、高清”，可远程控制网盘自动上传。其提供的价格表显示，供出售的手机品牌包括华为、小米、红米等，价格从1000多元到4000多元不等。针对苹果手机，其只提供改装服务，价格是1900元。对于用途，有卖家称，改装手机是用于签约谈判记录使用，还可用于直播。

交易
188元买60个摄像头ID 内容全天可看

被改装有针孔摄像头的智能手机，只是不计其数的偷拍设备中的一种。从电风扇、路由器、插排插座、空调等常用家电，到水杯、充电宝等常用物件，实际上，几乎所有物品都能够伪装成偷拍工具。

4月20日，记者在相关社群中看到，有卖家宣称，除手机之外，水杯、打火机、充电器、车钥匙、运动手环等都可以成为拍摄器材。

隐蔽的偷拍设备之外，家用的智能摄像头也可能成为偷窥的窗口。

据了解，如需查看摄像头拍摄的画面，需要安装对应的APP。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。一些不法分子则盯上了这些APP的账号密码（即ID）。警方破获的多起黑客非法入侵家用摄像头案件中，不法分子非法获取摄像头破解软件，利用黑客手段破解网络摄像头IP，并在社交平台出售。

记者发现，有卖家通过隐蔽的方式在售卖被破解的摄像头ID及破解软件。记者曾经尝试申请添加了几个群，按照提示添加一位用户后，对方即发来了“价目表”。其中，188元的套餐可获得“30酒店30家庭”，288元的套餐可获得“50酒店50家庭”，500元可获得“扫台软件和50酒店60家庭”。其中的数量即为卖家提供的摄像头的ID数，内容全天可看；“扫台软件”即为破解软件，“每天更新新内容”，摄像头数量不限。

为确保真实可信，卖家发来一张时长仅有3秒的“闪照”。画面从顶部正对着床，一对男女在床上，他们很可能并不知道自己正在被拍摄。

流向
有人通过破解摄像头系统 非法获利80万余元

这些被偷拍的影像资料可能会流向哪里？

记者了解到，偷拍背后，是一条非法安装、上传、共享、买卖交易的黑色产业链。

有不法分子在酒店、出租屋、商场等场所非法安装隐蔽摄像头偷拍房客隐私视频，被偷拍的隐私视频被层层转手，录制好的视频被标价出售，还有人直接在网络上发布广告，出售宾馆摄像头观看账号，购买账号就可以实时播放多人观看。

2019年3月，在山东济宁市公安局破获的一起非法偷拍、侵犯公民信息案中，犯罪嫌疑人通过互联网购买智能摄像头后，拆下摄像头外壳改装成隐蔽摄像头，安装在宾馆吊灯、空调等隐蔽处，通过手机下载的智能摄像头APP软件收看隐蔽摄像头回传画面，同时将回传画面中的裸体、不雅等镜头截屏发给下线代理，下线代理通过微信、QQ群发布截屏，吸引网民购买摄像头观看账号。

摄像头观看账号的销售有层层代理，作案人数庞大。据警方通报，涉案团伙将每个观看账号以每月100至300元不等的价格出售给代理，代理再以200至400元不等的价格出售给下级代理或网民。个别代理还将隐蔽摄像头回传的视频下载后，存储在网盘中，通过微信、QQ以20至60元不等的价格出售网盘账号。警方收网时，查获偷拍的酒店客房视频达10万余部，还扣押了300余个用于作案的卫星网络摄像头。

在北京市第三中级人民法院日前审结的一起案件中，被告人通过破解摄像头系统非法获利80万余元。被告人巫某某自2018年起通过搭建“蓝眼睛”“上帝之眼”等APP，非法控制位于北京市朝阳区某养老院等地的监控摄像头系统，并通过在网络推广上述摄像头实时监控画面非法获利人民币70余万元。此外，2019年3月5日至3月26日，巫某某专门用于收取贩卖监控实时画面钱款的第三方支付平台共计收款达人民币17万元。

一审法院审理认为，被告人巫某某行为已构成非法控制计算机信息系统罪，判处有期徒刑五年，罚金人民币10万元，并继续追缴其非法所得80万余元。巫某某不服，提起上诉，被北京三中院驳回，维持原判。

恶果
有人曾因为被偷拍而自杀

除了家用摄像头外，酒店、试衣间甚至一些公共空间的摄像头，也是不法分子经常盯上的地方。河南电视台《都市报道》栏目曾报道摄像头偷窥事件。有一段安装在某民宿内的针孔摄像机录制的视频，时长为8个小时。内容是一家三口的日常生活，看似普通，却最为抢手。

此外，还有美容院的偷拍、商场试衣间的偷拍，甚至连厕所的偷拍都有……

在其中一段视频上，24个针孔摄像机的画面被人放到了一个电脑屏幕上，这些摄像头还能被人远程控制，随时调整角度。

不到一个月的时间里，记者在这个群里发现了8000多段针孔摄像机拍摄的视频，这些私密视频几乎来自全国各地，以广东、湖南、湖北较多。

而因为个人隐私视频偷拍售卖，在网上流传被熟人发现，有的人甚至选择了自杀。

2018年的情人节，网友张某和男友，在北京东五环的一家快捷酒店住下.本来是想共度美好的二人世界，享受欢乐时光，可张某怎么也没想到，几天后，自己和男友的视频，被网上疯传，同事们整天都用讥讽异样的眼光对待张某。

没过几天，网上点击量过万，还出现了各种污言秽语，对张某的身材一顿“评价”。张某的男友，原本要与张某谈婚论嫁的，抵不住舆论的压力，以一句“你太不守妇道”了为由，与张某分手。

接二连三的打击下，张某几近崩溃，10个月时间，她自杀3次，最后一次服了一整瓶安眠药，幸亏每次都被家人及时发现，送医院治疗，才没有酿成悲剧。

而这一切的一切，都起因于这家酒店的隐形摄像头偷拍。

隐患
最便宜摄像头仅十几块钱 易被破解

近些年来，随着技术和网络越来越先进，各种各样的摄像头也层出不穷。在几大常见的电商平台上，皆有形形色色的摄像头在售卖：针孔摄像头、家庭摄像头、AI摄像头、手表摄像头……

这些摄像头的价格从几十到几千不等，最便宜的甚至只有十几块钱，而大多数的摄像头，目前都有联网和连接手机APP远程监控的功能。

摄像头的安装步骤非常简单，手机下载APP一键添加就可以在手机上进行远程实时监控，APP需要手机注册，自己可以设置密码。

除了硬件外，各种各样的监控软件APP也非常多，大部分都具备实时视频、语音对讲、历史录像查询、报警查看、隐私保护等功能。

有熟悉代码和网络技术的人士表示：“一些口碑较好的大品牌产品，会不定期升级，甚至做到了一机一密，安全性还是很高的。但一些几十块钱的便宜产品，可能做不到这种加密程度。”

“不过，即使买的是正规品牌产品，如果不及时更改初始密码或设置成像12345678这种简单的弱口令密码，也还是很容易被破解的。”该技术人士表示。

据了解，目前，摄像头偷窥行业的门槛非常低，一些不法分子甚至不需要拥有较高的计算机水平，只需要买到“傻瓜操作”的黑客软件或付费寻找技术人员帮助，就可获取大量破解的摄像头ID。

据了解，有相当一部分人购买摄像头的目的是为了防窃或者便于照看家里的老人和孩子。很多人并不清楚摄像头可能存在的安全漏洞，也并未重新设置复杂的密码，有些为了省钱，甚至购买一些便宜劣质的摄像头。

而这种对摄像头密码和安全性的不敏感，或许也为一些不法分子留下了可趁之机。