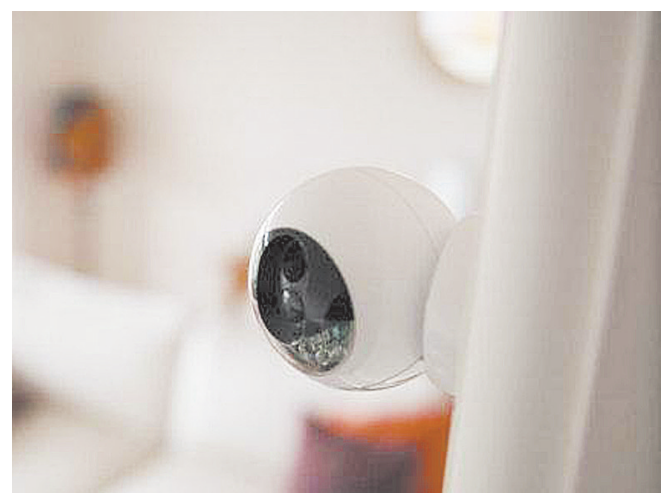
家里装个摄像头 引来千百双眼睛窥探

央视调查显示:大量家用摄像头遭入侵
质检总局:智能摄像头抽检八成存在隐患

据《现代快报》报道,现如今,很多人家里都装有智能摄像头,下载一个相关联的应用程序,可以随时用手机看到家里的情况。比如老人独自在家是否安全,保姆带娃是否尽责,有没有进小偷之类的。

不过,央视及国家质检总局要给装了摄像头的消费者提个醒:除了你,可能此刻还有成百上千双陌生的眼睛,也在看着你家。

网上买软件,记者成功侵入家庭摄像头。



家用摄像头(资料图片)

【调查】

QQ群每天更新破解文件

在QQ搜索栏输入“摄像头破解”关键词后,跳出很多相关聊天群,记者随机加了几个,发现聊天的内容绝大多数有关家庭摄像隐私,时不时会放出一些号称他人家庭摄像头拍下的画面。很快,不少人主动添加记者为好友,询问是否需要扫描软件,并声称这些扫描软件能够攻破摄像头的IP地址。

只要将被破解的IP地址输入播放软件,就可以实现偷窥,且不会被觉察。似乎只有电影中的特工或黑客才能做到的事情,竟然可以这么简单地实现吗?记者决定尝试一下。向其中一个卖家支付188元后,记者收到了两款软件和详细的使用教程。

记者在播放软件中,输入卖家提供的IP地址、登录名和密码后,竟然成功进入了一个摄像头。这户人家的摄像头画面显示的是客厅,一只小狗正在窝里睡觉。卖家称,这家住着一对小夫妻,安摄像头的目的应该就是观看这条宠物狗。

卖家还向记者提供了大量IP账号。为了辨别画面中的影像是不是实时影像,记者再次登录一个账号,进入了另一个摄像头,放大、缩小,居然真的可以实现远程操作。

而在一些QQ群内,IP地址会被群主作为聚拢人气的礼物,免费向群员发放。在这个近2000人的QQ群中,每天都会新增一份最新破解文件,包含200到400个IP地址,每份都被下载几百次。一位叫“大胆吻下去”的卖家告诉记者,靠卖号当天已赚500多元。

记者找到一个可被攻破的IP地址,并联系上这家主人。

记者:请问您家是否有个小书柜,上面有个五星红旗图案的贴纸?

户主:对。这个信息是随便在网上找到的吗?

记者:对,在网上找到的。

户主:如果这样,是谁都能看到是吗?

记者:如果有心搜的话,真的可以看到。

户主:天啊,那不是谁都能看到我家,看到我家什么样子的吗?这也太不安全了吧!

目前,记者已根据获取的材料向警方进行了举报。

【探究】

“弱口令”带来强风险,IP地址和密码泄露

智能摄像头的IP地址是怎么落到别人手中的呢?登录的密码怎么也会一同泄露呢?记者来到国家互联网应急中心寻求答案。

国家互联网应急中心高级工程师高胜称,这种泄露主要是依靠扫描器,用一些弱口令密码,做大范围的扫描。弱口令就是一些user或者admin。

专家介绍,不光是个人购买的摄像头是这样,在用于城市管理、交通监测的公共摄像头中,也大量存在使用弱口令便可以打开的问题。因此,这类摄像头很容易被入侵。不过,监控平台弱口令漏洞频发,是一种世界级的普遍现象。

中国人民大学法学院教授肖中华表示,运用非法的技术侵入他人的家庭生活场景、一般性的隐私权,这也涉嫌刑事责任的问题。肖中华称,个人的行踪轨迹属于个人信息的核心内容,一旦非法获取、出售或者提供50条以上,就触犯了侵犯公民个人信息罪。而截取家庭摄像头中的性行为进行展示,制作、传播到一定数量的,就构成传播淫秽物品罪;如果传播者因此牟利,并达到一定数量,将构成传播淫秽物品牟利罪。

【权威】

智能摄像头抽检八成存在隐患

6月18日,国家质检总局官网发布关于智能摄像头的质量安全的风险警示,称已检测的40批次中,32批次样品存在质量安全隐患,可能导致用户监控视频被泄露,或智能摄像头被恶意控制等危害。

智能摄像头,是指不需要电脑连接,直接使用Wi-Fi联网,配有移动应用,可以远程随时随地查看家里的一切,与家人语音通话,还支持视频分享、远程操作监控视角、报警等功能的一类产品的总称。

据央视新闻6月18日报道,破解智能摄像头的密码,侵入相关系统,偷看或直播智能摄像头监控内容,已经成为一条非法产业链。

质检总局的风险提示称,智能摄像头可能存在终端安全、后端信息系统安全、数据传输安全、移动应用安全等质量安全隐患,若消费者使用不当或超预期使用,容易导致个人隐私信息泄露、财产损失等危害。

质检总局产品质量监督司组织开展了智能摄像头质量安全风险监测:共从市场上采集样品40批次,主要依据GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》等标准要求,对操作系统的更新、恶意代码防护、身份鉴别、弱口令校验、访问控制、信息泄露、数据传输使用安全有效加密、本地存储数据保护等项目进行了检测。

抽检结果表明,32批次样品存在质量安全隐患。其中,28批次样品数据传输未加密;20批次样品初始密码为弱口令,或者用户注册和修改密码时未限制用户密码复杂度;18批次样品在身份鉴别方面,未提供登录失败处理功能;16批次样品对用户密码、敏感信息等数据,在本地存储时未采取加密保护措施;10批次样品后端信息系统存在越权漏洞,同一平台内可以查看任意用户摄像头的视频;8批次样品未对恶意代码和特殊字符进行有效过滤;5批次样品后端信息系统存储的监控视频可被任意下载查看等。这些都可能导致用户监控视频被泄露或被恶意控制。

购买使用家用摄像头请注意这五点:

一是选择正规渠道购买智能摄像头产品,切勿购买“三无”产品,留意权威部门发布的相关产品质量信息。

二是增强隐私信息保护意识,审慎考虑厂商收集、保存和使用用户信息的要求,根据自我实际情况和意愿作出购买和选择决定。

三是使用时,应及时主动修改智能摄像头默认密码,密码设置应有一定的复杂度并定期修改。

四是及时更新智能摄像头操作系统版本和相关的移动应用,发现异常应立即停止使用,并向生产厂商反馈,等待厂商修复,养成定期查杀病毒的好习惯。

五是使用时,摄像头不要正对卧室、浴室等隐私区域,并要经常检查摄像头的角度是否发生变化。 (李丹)

【观点】

设备方有责任维护智能产品的网络安全

现如今,很多人家里都装有智能摄像头。下载一个相关联的应用程序,可以随时用手机看到家里的情况。但是据媒体报道,除了你,可能此刻还有成百上千双陌生的眼睛,也在看着你的家。甚至在你看来一对一的“监控”或许已经变成“直播”。智能摄像头用户信息交易已经是一项“产业”。

如果说个人信息在网上交易还是一堆数字在“裸奔”,那么这种偷窥、交易家庭实时录像的行为就更像是我们本身在“裸奔”。

智能手机、智能摄像头已经进入成千上万普通家庭之中。这些智能产品在实际应用中为人们提供了极大的便利。但与此同时,相关的安全防范技术与安全防范意识却跟不上产品的更新换代。

包括家庭智能摄像头在内,相当一部分高科技产品暴露出的安全漏洞,都与相关平台的安全技术欠缺有关。对此,家庭智能产品的生产厂商有责任提升产品的安全性能,从技术层面升级家庭网络安全防范能力。作为一种网络智能设备,家庭摄像头在制造研发中理应对网络风险有足够的预防意识,并通过相应技术手段来防范其被入侵。

然而,现实中绝大多数家庭智能产品的生产者只对产品本身负责,对其网络安全风险防范往往不予重视。而根据6月1日施行的《网络安全法》,网络产品、服务的提供者应当为其产品、服务持续提供安全维护;在规定或者当事人约定的期限内,不得终止提供安全维护。

另外,用户也应当积极提升家庭网络安全水准,具备主动防范意识。在家庭摄像头的使用中,很多人都没有升级密码或加装安全软件的习惯,疏忽大意给了不法之徒可乘之机。这种情形,与多年前电脑刚刚开始普及时,许多用户不安装安全软件,让自己的电脑“裸奔”于互联网之中,性质是何其相似。

因此,监管部门、设备厂商、使用用户应当共同努力,通过安全技术与安全意识的不断完善提升,使高科技智能产品的安全防范能力跟上其发展应用速度。 (侯坤)