

自家监控成直播现场,专家揭开背后三大问题

智能设备普及,如何守护个人隐私?

原本用来自家监控的摄像头,却有可能成为他人眼中的直播工具。日前,国家质检总局发布智能摄像头质量安全风险警示,在已检测的40批次中32批次样品存在质量安全隐患,引发网友们高度关注。在智能设备越来越普及的今天,如何做才能防止个人隐私被他人围观?

智能摄像头产品杂、用户广、风险多

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。

近年来智能摄像头市场快速发展,360公司的智能摄像头产品累计销量超过500万台,今年预计销量还会增长30%。记者在淘宝上搜索“智能摄像头”,品牌多达20多种,包括乔安、萤石、海尔、海康威视等。按照销量查询,乔安的一款100多元家用监控无线摄像头显示“月销量53680”。据产品介绍,无需复杂布线和设置,简单三步安装:下载APP、联网通电、连接成功。

上海白领陈女士告诉记者,身边妈妈群里很多人用过,自己也在淘宝上买过一款100多元的“小蚁”家用摄像头,起初就是想在上班的时候看看家里宝宝的状况,倒是从没想到如媒体曝光的自家客厅成了人家直播现场。

国家质检总局18日发布智能摄像头质量安全风险警示:共从市场上采集样品40批次进行了检测,结果表明,32批次样品存在质量安全隐患。问题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。

国家互联网应急中心5月份发布的《2016年中国互联网络网络安全报告》显示,2016年国家信息安全漏洞共享平台公开收录的1117个物联网设备漏洞中,网络摄像头、路由器、手机设备漏洞数量位列前三,分别占漏洞总数的10.1%、9.4%、4.7%。

摄像头遭入侵 揭开背后的三大问题

以摄像头为代表的物联网安全并非第一次进入大众的视野,早在2008年就有黑客利用网络监控摄像头攻击了土耳其的石油管道。无论是工业控制系统还是如今日益流行的智能家居,安全问题一直普遍存在。

上海信息安全行业协会会长、众人科技创始人谈剑峰表示,通过攻击用户的物联网设备比如智能摄像头,黑客可以偷取其视频,并利用用户隐私视频进行勒索敲诈或通过QQ群、微信群进行变现。此外,还可以利用撞库、洗库方式对用户的行为数据、位置数据、资产数据等进行提炼筛选,经过层层交易整合后,进行非法牟利活动,比如实施通讯诈骗、盗取游戏装备、盗卡交易等。

其背后的问题主要在于:一是很多物联网设备在设计之初就缺乏安全性的考虑。大多数设备从出厂开始,就存在着弱口令安全漏洞。二是物联网设备多数部署在无人监控的场景中,攻击者可以轻易接触到这些设备,从而对它们造成破坏,甚至在本地操作更换设备的软硬件。三是设备缺乏日常安全评估及维护,不少厂商对于其设备不能及时查出有哪些安全漏洞,并配备打补丁等防护手段。

以智能摄像头为例,北京云视科技有限公司创始人刘一泓告诉记者,因为其运行了操作系统

和网络服务,所以弱密码、网络服务中的执行漏洞都可能造成摄像头被黑客控制。

360高级工程师郑广瑞也表示,安全标准低的智能摄像头,会内置一些弱密码比如123456,有的甚至根本就没有密码,用户还不能更改,黑客很容易就破解拿到用户资料。另外,相较一些大公司依托多年的技术积累以及完备的信息安全检测程序,很多小公司的研发能力相对薄弱,通常是直接购买包含APP、云服务的公模方案。虽然价格很低,但安全方面没有保障。比如很多小厂商共享一个云存储,如果其中一个产品有漏洞被攻陷,其他厂家的用户资料等于同时向黑客敞开大门。

从摄像头到各种智能设备 如何防范个人隐私泄露?

从摄像头、智能恒温器到智能汽车、穿戴设备,一系列物联网产品在人们生活中不断出现和普及。据Gartner统计,平均每天会有550万个新设备连接到互联网中,预计到2020年这类设备总数有可能超过200亿。在激增的设备联网数字下,消费者隐私该如何保护?

郑广瑞建议,作为消费者,在选购设备时,最稳妥的方法是

在正规渠道选购产品,切勿贪图便宜,购买“三无”或者山寨产品。使用前充分了解选购产品和服务的各项功能,使用时需及时修改初始密码,使其具备一定复杂度。

“非必要的情况下,智能摄像头尽量不要联网。此外,在设备厂商更新设备固件的时候,用户也应第一时间更新固件,这与系统更新漏洞补丁是同样的道理。”刘一泓说。

从监管的角度看,谈剑峰建议,监管方应制定相关的物联网安全技术标准和要求,以便于安全评测和认证。出台相应的安全管理办法,对于明显存在安全性问题的设备停止生产和销售直至其达到安全标准。同时,对于国家关键信息基础设施,应当提升安全保护等级,做好各项防护工作,营造良好的物联网安全环境。

据新华社

