来源：半月谈

韩国“N号房”事件发生后,再度唤起公众对摄像设备泄露隐私的担忧。随着物联网发展进程加快,物联网智能摄像头、智能家电设备愈发受到青睐。然而,一些创造便利的物联设备也可能成为不法分子窥探隐私的“千里眼”“顺风耳”,形成网络化、链条化的黑色产业链。

记者通过摸底调查发现,不法分子可以轻易破解部分智能监控设备,并将破解软件、破解ID肆意在网上出售,无数用户的隐私暴露在他人的监视中。

1

一些卧室早已没有秘密

考虑到安全防范等因素,许多用户在家、公司不同位置安装了摄像头,通过手机端App可实时查看。这些摄像头处于长期开机拍摄状态,有的业主说“懒得重启,从不关机”。

用户本以为只能自己观看的监控画面,实际上成了“实时公开播放”。

记者以网友身份加入了以“摄像”“监控”为名的某社交平台群组。10多分钟后,一名群成员询问是否购买摄像头ID,随即发来10余张监控视频截图,其中大部分为家庭摄像头拍摄的场景截图,最近的时间为3月24日,这些图片被设置“阅后即焚”,5秒钟后自动销毁。

在业内看来,安全意识弱是一个较大的漏洞。“很多人没有网络安全意识,或者存在侥幸心理,觉得网络被‘黑’的事情离自己很遥远。”在奇安信集团担任安全专家、

高级架构师的一名工作人员告诉记者,不法分子还会去买同型号产品先做研究分析,找到针对性攻击手段,给安全管控带来更大的挑战。

利用其他物联网设备充当“间谍”的也不在少数:自带摄像头的扫地机器人不断窥探着房间;智能音箱夜间突然发出“神秘笑声”;苹果Siri被曝出会在未经用户允许的情况下,将用户录音上传到服务器……