

字号大、价格便宜、功能简单、操作方便,老人机近年来颇受银发族欢迎。然而,这款为了方便老年人与家人联系而设计的通信产品,如今却被不法分子盯上,不少老人机竟成了他们的牟利工具——

近日,常州两级法院审结了一起老人机被远程控制自动扣费的刑事案件。一部老人机,在机主不知情的情况下被他人操控订购了增值服务并自动扣取话费,而全国竟有98万多部老人机遭遇这种情况。该案一经公布,迅速引发各方关注,也敲响了监管警钟:老人的话费是如何被偷走的?又该如何堵住老人机的安全漏洞?



资料图(新华社)

98万部老人机被远程控制、自动扣费 “欺老”产业链如何斩断?

一次报警

牵出涉及98万部手机的大案

“我当时就觉得这个话费有点儿不对,老人机就是接电话,打电话也都是用无线网视频电话,不可能花到这么多费用。”去年2月,常州市金坛区的姚先生刚给母亲的手机充了100元话费,几天后就显示欠费了。一查才发现,老人手机上开通了多个增值服务。“我翻遍了手机,也没看到订阅提醒,母亲也说自己从来没有操作过,当时就怀疑可能是手机中病毒了。”发现不对劲的姚先生立即向公安机关报案。

顺着这条报警线索查下去,常州市公安局金坛分局大数据侦查中心民警黄泽和同事们有了惊人的发现:被自动扣费的老人机遍布全国,仅在金坛区,就有50多部老人机被非法远程控制,“自动订购”了增值业务。

不同于智能机,老人机可下载的应用程序有限,大多只能通过短信订购增值服务,并以扣话费的方式支付相关费用。经过对涉案手机的数据进行分析和追踪,警方发现,这些老人机均被不法分子通过一款代码远程控制了。这些手机的网络数据都指向一台架设在深圳的服务器。

截至金坛公安成功捣毁相关犯罪团伙时,这台服务器远程控制的手机已多达98万多部,遍布全国各地,共窃取受害人话费近348万元。

该案究竟是以非法控制计算机信息系统罪定性还是以盗窃罪定性,一度让司法机关犯难。在案件承办法官、金坛区人民法院刑事审判庭副庭长王囡囡看来,犯罪团伙虽有非法控制计算机系统的行为,但控制只是手段,其根本目的还是实施盗窃,因此用盗窃罪来定性更为准确。

从量刑上看,以盗窃罪论处的惩治力度更大。王囡囡说,非法控制计算机信息系统的量刑最高不超过7年,而若以盗窃罪量刑,数额特别巨大或者有其他特别严重情节的,可处10年以上有期徒刑或者无期徒刑,并处罚金或没收财产。“考虑到此案侵害对象主要是老年人,以盗窃罪量刑,能够更好发挥刑罚的惩治和震慑功能,真正遏制犯罪势头。”

记者注意到,去年2月,该案犯罪嫌疑人欧阳某生、熊某等人因涉嫌非法控制计算机信息系统罪被刑事拘留。最终,欧阳某生等人被以盗窃罪分别判处有期徒刑5年8个月到12年不等,并处罚金5万元到30万元不等。

“遥控”手机

自动订购增值服务还不留痕迹

39岁的广东人欧阳某生是这起犯罪的“策划者”。

2018年,他还是一名增值服务代理商。一次偶然的机会,他在网上购买了一份手机增值服务代码,发现只要将其植入功能机中,再通过服务器远程发出指令,就能无需用户确认,偷偷扣取用户话费。

于是,欧阳某生开始精心谋划一桩“大买卖”。两年间,他先后找到在功能机主板厂工作的程序员熊某,与SP运营商(即增值服务提供商)相熟的毛某、蒋某,以及善于搭建、维护程序后台系统的张某。约定了分工和利润分成后,一条分工明确的犯罪产业链逐渐成形:

熊某将欧阳某生提供的服务代码植入手机主板,经生产厂商批量加工制成老人机,大量流入市场;毛某、蒋某分头与SP运营商对接,获取增值业务通道号码、控制指令等参数,然后按照事先约定的比例进行分成;张某负责搭建并维护程序后台系统,为犯罪团伙足不出户“偷话费”提供技术支持……

“这条产业链的运行模式,就好比是用遥控器操纵玩具。”王囡囡打了一个形象的比方:一批带有“病毒”的“玩具”被投入市场,在张某所制作的“遥控器”的操控下,“玩具”可以自动订购毛某提供的“商品”即增值服务,而所有的订购痕迹会被同步“毁

尸灭迹”。最终,所得的销售利润由蒋某从SP运营商提回,再按比例分成。

“只要涉案的老人机流到市场,被害人插上手机卡使用,代码程序就会给嫌疑人‘上报’:‘我已经上线了,随时待命’。”黄泽说,犯罪分子掌握了一定数量的手机后,通常会选择在深夜或者凌晨,向某一特定省份的老人机用户发送增值服务订购指令,完成之后,再转向另一省份老人机用户,如此循环往复;所有指令犯罪分子都可以通过遥控后台设置,比如是单月订购还是连续订购。“他们还会控制投诉量,比如江苏的投诉多了,可能这个月就不再向江苏的号码‘伸手’,转向其他地区。”



涉案的老人机

警钟敲响

老人机存在系统安全、市场监管漏洞

盗窃老人机话费,此案并不是首例。去年,四川警方破获一起特大网络案,犯罪团伙通过手机主板植入木马病毒远程操控超千万部老人机,非法获利上亿元。

老人机缘何频频被犯罪分子盯上?黄泽说,在很多人眼里,老人机功能简单,不能上网购物、玩游戏,只能打电话、收短信,使用起来相对安全,本身就会放松警惕意识。加上很多老人对手机熟悉度不高,防范意识相对较弱,这些都让犯罪分子有了更多可乘之机。

更令人担忧的是,犯罪分子在控制老人机后,不仅会“偷”走话费,还可能操控手机去注册各种互联网账号,再用账号去从事电信诈骗、网络赌博、洗钱等“黑灰产”,危害不容小觑。据公开报道,成都一位市民就因一条短信被骗走6400余元,诈骗短信的号主竟是一名使用老人机的75岁退休老人,老人本人根本不会发短信。事后查明,老人机里被植

入了木马程序,犯罪分子通过远程控制老人机,向外发送诈骗短信,3个多月向200多个手机号发送短信380余条。

显然,不法分子通过一款代码就能远程控制老人机,暴露出老人机在系统安全、市场监管等方面存在严重不足。据行业内部人士透露,不少老人机厂商都是“小作坊”,由三五个人改造旧手机,再加入低价买来未经安全检测的主板,批量生产后,再以几十元到几百元不等的价格投入市场。

在南京邮电大学网络与交换技术研究室原主任孟旭东看来,手机的所有核心软件都在主板上,而软件是手机用户访问硬件、使用手机的接口,一旦软件被篡改,无疑是向犯罪分子敞开了“大门”。“堵上老人机的安全漏洞,仅靠打击犯罪团伙还远远不够,还需对上游的生产环节进行综合整治。”他建议,生产厂商在关注老人机基本功能实现的同时,也要

重视安全防护措施的构建,增加代码安全检测机制,防止恶意代码植入。同时,在老人机出厂前,要进行严格的安全测试,确保手机的安全性。相关职能部门也应对老人机生产厂商加大资质审查力度,进行全链条监管,向社会公开专营老人机的合规企业名单。

增值服务代理领域存在的诸多问题,也在案件查办中暴露无遗。黄泽分析已查办的案件发现,运营商往往会将增值业务往下一分拨给下游代理商,尽管同步采取了开通增值服务时需要通过短信二次确认、过量投诉收回代理权等管理措施,但对于品质、防护功能较弱的老人机,这些举措还远远不够有力。

针对行业“内鬼”频出、监管难度较大等问题,孟旭东给出了多条建议:在老人同意的前提下,可以探索建立老人监护人制度,即当老人机办理增值服务时,运营商把服务提交给监护人认可才能付费;大额业务要到柜台办理,避免一些失误操作;设立增值服务代理商“黑名单”制度,进一步倒逼增值服务代理商加大自查力度。(交汇点)