

1400余万部“老年机”被植入木马“短信吸血”上亿元

攀枝花警方破获一起非法控制计算机信息系统案

老人年龄大了,使用智能手机多有不便,操作简便、待机时间长的老年机,成为不少老人的首选。

老年机原本只有接打电话等基础功能,但家住攀枝花的张先生却发现,家中老人的老年机无缘无故产生了不少“手机报”“平安天气”“开机提醒”等小额增值收费业务。怀疑老年机中了病毒,张先生到公安机关报了案。警方调查后,竟查出一起上千万部老年机被植入木马病毒、通过“短信吸血”非法牟利上亿元的涉网络黑灰产特大案件。

9月15日,攀枝花市公安局召开“2023年网络安全宣传周”新闻通气会,公布了这起非法控制计算机信息系统案。目前,该案仍在侦办中。

市民报警

老年机“自动订购”增值业务

张先生为了方便联系家中老人,买了一部功能简单的老年机给老人使用,平时只用来接听电话,从不往外拨打。

在给老人缴纳话费时,张先生发现这部手机每个月的话费都在增加。一开始,张先生以为是老人拨打电话误触产生了费用,没有太在意。然而2022年6月以来,老人使用电话的频率越来越少,而话费却越扣越多。

感觉事有蹊跷的张先生到营业厅查询才知,是用户订购了“手机报”“平安天气”“开机提醒”等小额增值收费业务。但张先生翻遍老人手机,也没



警方调查取证。攀枝花市公安局供图

有看到任何有关开通业务的短信,加上老人也不可能自己进行订购,他怀疑手机中了病毒,赶紧拿着手机到公安机关报案。

手机被远程操控

1400余万部手机被植入木马

接警后,攀枝花市公安局民警开始对手机“自动订购”增值业务开展调查。去年9月29日,民警在开展“网络侦查”工作中突然发现,攀枝花市有89部手机存在2G网络流量消费,以及非机主本人订购额外增值业务消费的异常情况,与报警人张先生的遭遇极其相似,疑似手机被远程操控。

民警通过对“疑似被远程操控”的手机机主进行线下走访调查,线上开展数据回溯来追踪溯源,发现不少老年机

在“自动订购”增值业务,每月被扣除相关增值业务费用多为1元至10元不等。很多老人因为对手机操作不熟悉,常常认为是自己误触导致,因而长期蒙受损失。

网安民警发现,这些手机网络数据都链接到同一个域名的服务器,经远程勘验,确定该服务器即为犯罪嫌疑人实施犯罪行为使用的木马服务器。通过数据追踪,发现全国竟有1400余万部手机被该木马服务器控制,涉及四川省有60余万部,其中攀枝花市有4000余部。

犯罪手法隐蔽

4个犯罪团伙非法牟利上亿元

民警通过多方调查取证,成功锁定租赁该服务器的犯罪嫌疑人孔某身份,并以孔某为突破口循线深挖,一个非法控制

“老年机”的犯罪团伙逐渐浮出水面。

经查明,犯罪团伙在与多家手机主板生产商合作过程中,将木马程序植入手机主板内。装有上述主板的手机出售后,犯罪团伙通过之前植入的木马程序,控制手机回传数据,获取用户手机号码、短信内容等信息,回传至团伙后台数据库。

之后,该团伙“运营专员”利用手机木马程序,向手机用户发送开通增值订购业务确认的短信,同时控制手机终端自动回复“Y”进行开通,一系列操作完成后再将此次收发的短信记录删除,以做到让手机用户无从察觉。

利用这样隐蔽的犯罪手法,该案4个犯罪团伙非法牟利上亿元。

抓获嫌疑人23名

“短信吸血”案实现全链条告破

今年1月,攀枝花警方抽调精干警力,组成两个先遣小组分赴深圳、北京两地展开侦查。

2月1日,专案组抽调80余名警力,组成30余个抓捕小组,分别赶赴广东、北京、海南、湖南等4省市开展集中抓捕行动,成功打掉以陈某、杨某、庞某、林某4人为首的4个犯罪团伙,抓获犯罪嫌疑人23名,冻结、扣押涉案资金6000余万元,扣押涉案车辆4台、房产1套。至此,“短信吸血”案实现全链条告破。

目前,该案已移送起诉12人,取保候审11人,案件仍在进一步侦办中。

华西都市报·封面新闻记者 周翼

1.8万人被骗 这个传销团伙涉案金额超2亿元

资阳警方开展集中收网行动,抓获团伙头目郝某及骨干成员共13人

花2800元买一套“化妆品”入会,再拉拢其他人加入,就能获得不菲的“奖金”?靠着这种欺骗手段,一犯罪团伙先后吸引1.8万人加入,涉案金额超2亿元……

9月15日,记者从资阳市公安局雁江区分局了解到,在资阳市、区两级公安机关“一把手”亲自挂帅、督战下,400余名民警在襄阳、成都、西昌、资阳等4地同步开展收网行动,主要犯罪嫌疑人郝某、蔡某等13人相继落网,一个特大聚集型传销诈骗犯罪团伙被成功打掉。负责侦办此案的民警介绍,这是一起无任何产品销售,以发展人员数量为计酬依据的典型传销案件。

接到多起寻人报警

民警调查发现出租屋藏猫腻

今年3月,资阳雁江警方先后接到多起寻人的报警电话。

“都是外地的,说自己的小孩或者亲戚来资阳工作,但一直联系不上。”雁江区公安分局副局长刘植钢说,警方通过信息研判,分析在当地可能存在一个外省市流窜过来的地下传销组织,“有些报案人也反映,自己小孩曾说买样东西就能挣大钱,让家里人不要管。”

为了尽快破案,辖区派出所进行了人员摸底。“前后梳理出至少11处出租屋疑似传销窝点,民警在现场发现有那种‘打鸡血’鼓劲的标语口号,就更加确信是传销组织。”雁江区公安分局经侦大队副大队长詹伟说,这些出租屋一般位于老旧小区或城区边缘,通常三室一厅的房间住有8-9人,平时基本不外



涉案人员被警方查获。资阳市公安局雁江区分局供图

出。人员之间往往是单线联系,且流动性较大。同时警方还发现,盘踞在资阳的主要为组织底层业务员,高层长期在异地遥控指挥。

3月31日,雁江警方对此事正式立案调查,市、区两级公安立即成立专案组。

花2800元买化妆品 涉案人员骗了同学骗同乡

随着调查的深入,专案组民警发现,该传销组织打着天津某集团旗号,以购买一套2800元的化妆品取得入会资格为由,不断发展下线。

“其实并没有任何产品,相当于拉人交钱就行了。”詹伟解释说,这是典型的聚集型传销组织。组织内部分为ABCDE五个级别,组成“金字塔”式管理,其中E级为最底层,在经过不断拉人交钱后,就能获得提成并不断“晋升”。达到C级时,可以拥有管理职

责,能够自己租一套房拉新。

詹伟介绍,该组织在资阳的参与者全部都是外地人,大多数年龄在25岁以下,平时以介绍工作、做生意、旅游、交友的名义拉拢同乡、同学,到资阳后进行授课洗脑,不断灌输“坐享其成、快速致富”等观念。同时,组织内部还要求成员以绰号代替真名,相互之间不打听身份信息。

“他们平时生活很规律,上午洗脑学习,下午‘老带新’串寝室,晚上又在寝室里面互相探讨如何拉新。”办案民警在调查中还发现,该传销组织仅在资阳就有4个分支,另外这种模式还在湖北、湖南、重庆、贵州、甘肃等省市和四川其他市州不断“繁衍”。

涉案金额超2亿元 团伙头目和骨干共13人落网

今年4月,在得知该案主要犯罪嫌

疑人郝某等人员的重要线索后,专案组民警立即赶赴湖北襄阳进行调查走访,最终成功固定证据链条。

在摸清组织架构后,5月24日,资阳市公安局出动警力400余人、车辆40余辆,在襄阳、成都、西昌、资阳开展统一集中收网行动,抓获团伙头目郝某以及骨干成员共计13人,清查传销窝点、传销课堂及开会场所20余处,一举捣毁这个横跨七省市、发展会员1.8万余人、涉案金额2亿余元的特大传销诈骗犯罪团伙。

目前,13名犯罪嫌疑人已被依法执行逮捕,案件正在进一步办理中。

高层人员挥金如土 底层人员只能啃土豆吃白菜

“我再也不相信天上会掉馅饼的事了。”陈某曾是该传销组织的B级人员,由亲哥哥介绍加入,后深陷其中。

据陈某交代,在传销组织里,新人购买一套2800元的“化妆品”,约有一半的资金被A级别高层瓜分,供他们挥金如土,剩下一半才按照不同级别不同比例进行提成。而像D、E级这种级别不仅工资没有保障,每个月要是拉不到新人交钱,大多数每天只能啃土豆和白菜,连肉都难见到。

詹伟介绍,像达到A级的人员,每月会在襄阳等地聚会,分配所骗钱款后大肆挥霍,“除了吃喝,还会约着一起去越野、旅游,坐直升机玩耍。”

刘云涛 华西都市报·封面新闻记者 陈远扬