伪基站屏蔽运营商 强行发诈骗短信

在抓捕现场,警方收缴嫌疑人使用的主机和笔记本电脑。警方供图

从去年9月起,一种利用高科技仪器进行的新型犯罪引起警方注意。一种被称为伪基站的设备,能强制连接用户手机信号,搜取附近的手机信息,并可以任意冒用手机或公用号码,强行向用户手机发送垃圾广告或诈骗信息。

公安部门昨天指出,这种新型犯罪涉及地域广,严重危害国家通信安全。近日,公安部组织北京、辽宁、湖南、深圳等12省市警方开展集中行动,共铲除伪基站生产窝点4个,打掉各类犯罪团伙72个,抓获217名犯罪嫌疑人,缴获96套伪基站设备。

《京华时报》记者 袁国礼

□案发

市民被当成骗子一天接300个电话

今年3月5日,湖南衡阳的肖先生突然接到一位熟人的电话,质问他为什么发诈骗短信。当天,有近300人给肖先生打电话,都在质问他为何发诈骗短信,甚至还有人对肖先生进行指责、辱骂。被问蒙了的肖先生事后才知道,这些人都接到了以他的手机号发送的一个短信,内容为"工行账户某某,户名某某,办好来信",这是一条常见的诈骗短信。

肖先生意识到问题的严重性,立即向衡阳警方报案。

根据警方的调查,发送诈骗短信的实际上是以谭某为首的5人诈骗团伙。

今年29岁的谭某,来自娄底市双峰县印堂乡。2008年信息技术专业毕业的他,总想着一夜暴富。今年2月28日,他和高中同学、堂弟、姨夫等5人合伙花9.8万元,从深圳明昂科技有限公司黄某手中购买了一台伪基站设备。随后,他们又在网上购买了银行卡,开始实施诈骗。

这伙人将设备放在车上,一般选择人群密集的地方,比如银行门口等发送诈骗短信。5个人进行了分工,有人负责指挥,有人负责发信息,还有人负责取钱。

谭某团伙在长沙发送诈骗短信后,其中一次性诈骗了2.8万元。今年6月18日,正在南昌的谭某等人,被衡阳警方抓获。该团伙的设备在广东被查获。

据悉,湖南警方共查获两个从事生产、销售的团伙。他们在广东、福建、四川、新疆等9地出售伪基站达到60余套,获利近百万元。

□获利

利用4套伪基站3个月骗百万元

与谭某团伙刚伸手就被抓不同,同是双峰人的贺某等人组成的诈骗团伙,利用伪基站,从今年3月到6月,诈骗金额100余万元。

贺某团伙共有13人,这些人之间有错综复杂的关系,有夫妻,有同学,有兄弟等。贺某通过其表兄弟王某,从网上购买了4套伪基站设备,每一台的价格从11万元到12.8万元不等。

与谭某一样,贺某等人也是在人群密集地区发送诈骗短信,包括银行门口、十字路口等。短信内容包括"我是房东,租金请打到我爱人账号上"等。贺某团伙共有70多个账户,这些账户要么是购买的身份证开的户,要么是直接从网上购买的银行卡。该团伙有专人负责取钱,取钱与诈骗会在不同的城市,而且会戴上口罩,甚至是假发。

从3月到6月,贺某团伙的行骗足迹踏遍重庆、长沙、上海、广州、武汉、佛山、惠州、珠海等多个城市。每天发送的诈骗信息有10余万条,每天诈骗的金额从几千元到几万元不等。娄底警方调查发现,该团伙共作案200余起,骗得现金100余万元。目前,该团伙11人已经被刑事拘留,警方还在追捕其他人员。

□影响

移动公司损失一个月达百万

据公安部通报,北京、湖南、广东等12个省市,都发现了利用伪基站进行犯罪的行为。

苏先生是深圳一家手机通信公司的员工,经常到机场接客户,他用的是中国移动手机号。去年10月26日,苏先生到机场接客户。当他把车开到停车场后,发现手机信号时有时无。他跑到候机楼,发现手机此时已经没有信号了。

无奈之下,苏先生开车来到离机场约一公里外的107国道路口,手机才有了信号,这时候客户已经下了飞机在等候。苏先生与客户约好在A楼2号楼门口见面,由于门口不让停车,苏先生因为违章还被罚了款。据苏先生说,当天从11点20分到下午1点多,手机信号基本没有。

据了解,从去年9月下旬开始,中国移动深圳分公司就不断接到用户投诉,反映在机场附近信号不好。根据移动公司的统计,在一个多月的时间内,该地区的资费下降百万元。

深圳市无线电管理局联合移动公司进行联合调查。去年11月22日,在机场的一个停车场内,发现了载有伪基站的汽车,并向深圳警方报警。11月23日,深圳刑警支队成立专案组进行侦查,发现经营票务公司的江某,从上海崔某手中购买了伪基站,在机场附近发送销售机票的广告短信,共发送了62万余条信息。警方调查发现,李某也从崔某手中购买了3套伪基站,在深圳发送民营医院广告。

除了卖往深圳的4套,崔某等人还往山东等地销售了30多套伪基站,共获利600余万元。

去年11月和12月,深圳刑警支队将江某、崔某、李某等9名犯罪嫌疑人抓获,查获4套伪基站设备。目前,9名嫌疑人已经被深圳检方批准逮捕。

□揭秘

每台生产成本约两万元

谭某团伙购买的伪基站是由曹某的公司生产的。今年48岁的曹某是深圳人,他是武汉某大学的一名计算机相关专业的硕士,深圳捷赛通讯有限公司的负责人。从2006年起,曹某开始生产手机信号放大器等通信器材。曹某称,以前的无线电设备都是以硬件为主,软件为辅,成本较高,以软件为主的软件无线电将是一种发展趋势。而伪基站正是以软件为主的设备。曹某在网上找到软件后,组织研发人员进行研发生产。

从去年年底起,曹某共生产了40余台伪基站,并由其一名姓杨的朋友代理销售。据曹某称,伪基站的生产成本每台约为两万元,以5万元左右的价格供给销售人员出售。

三五秒就可屏蔽运营商

曹某称,伪基站主要针对G网手机。手机大约每5秒钟寻找一次基站,当伪基站打开时,由于距离等原因,手机就会自动连上伪基站,三五秒间手机与运营商的联系就断掉。但如果这时候手机在通电话,伪基站就无法切断手机与运营商的联系。由于功率不一样,伪基站所影响的范围从两三百米到3公里不等。

发送短信条数没有上限

伪基站由视频天线、主机和笔记本电脑组成,办案民警向记者演示了使用过程。伪基站打开后,会有一个发送页面,可以选择频点等。根据这台伪基站生产时的设置,发送短信时显示的手机号码一般以"15"或"106"开头,短信内容可以自己随便写,发送短信的条数可以选择,但没有上限。

犯罪分子填好手机号码后,会试打一下,如果能打通,一般不用。据谭某等人称,这是防止有人接到短信后向机主打电话核实。如果这个手机号码无法接通或关机,就会成为犯罪分子发送短信的号码。

由于不通过运营商网络,不法分子使用伪基站发送诈骗短信的成本大大降低。在湖南和深圳查获的案件中,共发现了深圳、上海和长沙等多个生产厂家,这些伪基站被销售到湖南、北京、辽宁、广东等12个省市。

可冒用任意号码发短信

伪基站可以搜取周围数百米到几公里内的手机信息,并冒用他人手机或公用服务号码强行发送诈骗短信或广告信息,导致公众上当受骗。警方指出,如果犯罪分子以公众服务号码发送短信,再在短信内容中写上银行的名字,公众很容易误以为是银行发送的,更容易被骗。

在发送短信时,手机用户无法连接公用电信网络,影响手机用户正常使用,严重危害国家通信安全。在手机用户无法正常通信的同时,也造成运营商的巨大损失。

公安部有关负责人指出,一旦伪基站被别有用心的组织或个人利用,冒用权威部门名义编造、发送虚假信息,造成的社会影响将难以估量。

伪基站构成及工作过程

伪基站由视频天线、主机和笔记本电脑组成,打开伪基站,在发送页面选择频点,在手机号一项可填任意号码,编写短信后点击发送,此时手机用户无法连接公用电信网络。 (据《京华时报》)

相关新闻

短信诈骗42万 套现被捕

收到诈骗短信,主动联系对方被骗42万元!荔湾警方在白云区新市一间邮政储蓄所柜员机前抓获犯罪嫌疑人陈×宁,侦破一宗42万元的特大电信诈骗案。

去年9月12日,事主匡某接到一个诈骗短信,随后拨打电话与对方联系,通过银行转账的方式被骗42万元人民币。办案警察通过调取大量资料研判分析,锁定其中一名犯罪嫌疑人陈×宁,并掌握诈骗分子已转移赃款,分别在番禺区2间金铺购买了大量金器进行套现。1月5日下午,办案警察在广州市白云区新市镇一邮政储蓄柜员机将正在转账的嫌疑人陈×宁抓获。

犯罪嫌疑人陈×宁供认:去年9月中旬,他接到电话要求其帮忙套现42万元,根据"合作伙伴"的要求,到番禺2间金铺购买金器,并将金器和部分现金送至"合作伙伴"处,获得4万元佣金。

目前,犯罪嫌疑人陈×宁已被警方依法刑事拘留,警方正加紧追捕其他在逃嫌疑人。 (据新华网)