涉案金额近千万,嫌疑人多达225人
这起木马网络诈骗大案怎么破的?来看看永康警方——

最紧张的15天

本报记者 陈佳妮 通讯员 叶宁

昨天,永康市公安局主楼内,一场大案发布会正在进行——公安部挂牌督办的系列性木马网络诈骗案成功告破。

发布会现场,瘦高个的刑侦大队副大队长胡海平,淡定地讲述着这起案子中最紧张的15天——

2016年11月2日,正好是一年前的今天,警方收到消息,此案关键嫌疑人黄某,依旧藏匿在福建云霄县。胡海平来不及好好收拾行李,便赶动车前往云霄。

在那个县城里,胡海平遭遇了当地人的质问与跟踪;和疑似犯罪嫌疑人对眼后,体会到了电影中"一眼万年"的漫长;为了摸清对方具体落脚点,还假扮外卖小哥……

这种付出的回报,是这起涉案金额近千万元的案件成功告破——警方共抓获犯罪嫌疑人达225人,为群众挽回经济损失400余万元。

警方查获用于作案的银行卡


警方查获用于作案的电脑

上千家刷单网店纷纷中招

在胡海平出发去云霄县的8天前,永康警方收到一条线报:有一团伙正在利用一款木马软件诈骗网店店主的银行卡资金,其背后可能隐藏着一个更大的团伙,有一条大鱼。专案组对案件进行初步分析后,发现这种木马程序,是一款针对网上银行支付环节的诈骗软件,被害人均为网店卖家。

这些卖家,为提高店铺销量和信誉度,会通过ＩＳ平台、ｙｙ语音、ＱＱ群等网络社交平台,找一些刷单人员帮忙刷单。为了防止刷单时钱被对方骗走,他们也琢磨出了"安全套路"。在进行到付款环节时,商家会远程控制刷单人员的电脑,在对方的账号上,用自己的银行卡支付用于刷单的订单费,这样一来,刷单的钱相当于从自己的卡上出,又回到自己的店铺里,左口袋出右口袋进。

该诈骗团伙便利用这一环节,做出了一个木马程序。在商家远程付款前,开启木马软件拦截资金。也就是说,商家所付的订单,看似是打回到商家自己的口袋,但实际上,是被转到了嫌疑人的账户内。

专案组进一步侦查,发现本案涉及的被害人(商家)多达上千,分布在全国各地,且每笔损失金额都很小,从几十元到几百元,最多几千元,加上怕报案后会被电商平台以刷单为由处罚,因此有些被害人没有报警。

在经过取证阶段后,永康警方正式立案。

第一天被摩托车跟踪

去年11月初,专案组计划对该团伙收网。办案民警兵分5组,前往福建、江苏、吉林、广东、杭州等地展开抓捕行动,5名犯罪嫌疑人陆续归案。民警通过审讯得知,他们的木马软件均从一名黄姓男子处购得。专案组在对缴获的电脑和手机进行分析后发现,黄某的下线多达300多人。

因此,抓获黄某成为了该案的关键。

前往抓捕黄某的,正是胡海平带领的"云霄小分队"。

去年11月2日傍晚6点,火车到站,福建云霄还是夏天一般的温度。他和队员们吃了个路边摊,便直奔目的地——黄某在城区里的落脚点。

那是一个老小区,晚饭过后,不少居民在楼下乘凉闲聊。一行陌生人的出现,很快吸引了当地人的目光。还没来得及四处观察,胡海平便被小茶馆的老板拦下——"你们干嘛的?"

搪塞了几句后,胡海平和队员匆匆离开了这个小区。没想到,走出小区几百米,几辆摩托车就一直不远不近地跟在他们后头。

在前往云霄前,胡海平便得知,其他公安机关曾前往当地进行过抓捕,都空手而归。但他没想到,这伙人的警惕性那么高。

他们作势在附近小店买水果,随后挑了一条小路走,好在那些摩托车没有再跟追上来。于是,"云霄小分队"匆匆赶往当地刑侦部门。

电影慢动作般的一瞥

被惊动的黄某,早已放弃了与外界的一切联系,静静藏匿在这个小县城的某个角落里,伺机而动。


将黄某押解回永康

几天的排摸、走访,进展都不明显,胡海平有些焦躁——抓不到黄某,这案子就算"黄"了。他手上只剩下最后一个线索:黄某与外界隔绝之前,曾跟当地一个朋友走得很近。

这个朋友的住宅区,在云霄县很有名,是一个"富人区"——十几幢五六层高的小楼房,家家户户安装着严密的监控,如果有陌生人多停留些时间,肯定会引起怀疑。

胡海平心里泛起了嘀咕,如何确定黄某是否藏匿于此?"云霄小分队"租了一辆当地车,沿着片区外围侦查时,他突然灵机一动——装扮成外卖小哥去排摸。

接下去的几天,几个新面孔的"外卖小哥"在这个片区里四处穿梭,很快就把可疑范围越缩越小,基本固定在两三幢房子里。

11月15日,胡海平和云霄县当地警方,再次开着一辆本地车,在片区里寻找蛛丝马迹。就在车辆快开到尽头要拐弯时,一名男子出现在胡海平眼前——20多岁,个子不高,穿着短袖、短裤、拖鞋,眼神闪躲,贴着墙边走。

就像电影里的慢镜头一般——汽车缓缓向右拐弯,胡海平向左扭过脑袋,拼命想再看一眼对方的去向,但男子很快消失在拐角……

机会终于来了!

慢动作回放结束,胡海平脑子里只有一个直觉——这就是黄某。但对方一下子没了影,他怕抓不到人反倒打草惊蛇,没有下车去追。下一次,一定还有机会。

这个机会,很快就来了。

11月16日,在重点怀疑的一幢楼房附近,一辆黑色的丰田车停了下来。在此之前,"云霄小分队"侦查到,有一辆丰田车经常停在附近,可能和黄某有关系。从车上下来了一名男子,直接进了这幢可疑楼。

机不可失。胡海平等民警假装到一楼的茶叶铺挑茶叶,趁机也跟了进去,上了2楼。2楼有2间房,敞开着门。一间里头,4个人正热火朝天地打麻将,胡海平瞄了一眼,都不是黄某。

左边的屋子里,非常安静,胡海平走到门口,里面窗帘紧闭,光线昏暗。听到声响,坐在沙发上的男子抬起了头,这正面的一眼,胡海平立刻认出了他——黄某!

胡海平回身冲队员打了一个手势后,便问对方"你叫什么名字?"沙发上的男子没有动,大概他也知道这回躲不过去了,无奈地报出了自己名字:黄某。

2016年11月17日,胡海平等民警顺利将黄某押解回永康。

拔出萝卜带出泥

黄某被抓后,交代了自己的犯罪事实。

前两年,他在网上找了一个"码农"申某,让对方做了一个木马软件,随后以200至600元不等的价格出售,使用期为一个月,到期后需要续费,客户在最多时有400多人。

至此,一个完整的针对刷单的钓鱼软件产业链呈现在永康警方面前。这个产业链包括3个层次:软件开发层、软件销售层、实施诈骗层。根据黄某的供述,警方成功抓获包括申某在内的犯罪嫌疑人101名,扣缴电脑70多台、手机90多部,成功摧毁了以犯罪嫌疑人黄某为首的集编写软件、盗号、销售、诈骗全链条式系列性木马网络诈骗犯罪团伙。

然而,这起案子并没有完全结束。

专案组在审讯过程中,发现了另一条重大线索:黄某团伙中的多名嫌疑人,都曾打款给一名谭姓男子。在随后的调查中,专案组分析,极有可能还存在另一个盗号、贩卖账号的团伙。

今年1月15日,警方在广西柳州抓获谭某,现场查验他所有笔记本电脑,发现电脑内确有大量的盗号木马和一些被盗取的账号、密码。专案组顺藤摸瓜,又陆续抓获了其他犯罪嫌疑人潘某、张某、覃某。

警方分析,谭某等人的团伙,曾向300多人出售过IS平台账号,从中获利100余万元。掌握该线索后,永康警方乘胜追击,3月10日,在浙江省公安厅、金华市公安局的指导下,永康市公安局联合武义、磐安县警方开展系列性木马网络诈骗专案的第二次统一抓捕行动,抓获98名犯罪嫌疑人。

经过两次统一抓捕行动,该案已有225名犯罪嫌疑人被采取刑事强制措施,被移送审查起诉177人,现已进入审判阶段。其中,黄某、申某因涉嫌非法传授犯罪方法罪、诈骗罪被依法起诉,谭某因涉嫌非法获取计算机信息系统数据罪、盗窃罪被依法起诉。