热线:96060 E-mail:xdkb@kuaibao.net 现代快报
责编:张虎 美编:陈恩武 组版:刘峰 2014.6.5 星期四

740多万个QQ号神秘被盗 诈骗团伙背后挖出“钓鱼技术组”

这6个人专门制作钓鱼网站卖给骗子,非法获利300多万 快报记者随江苏警方赴广西,直击团伙二号头目被捕过程

今年3月,江苏油田一职工遭遇QQ盗号诈骗,警方在调查中,无意中发现了电信网络诈骗技术支撑团伙的蛛丝马迹。经过两个多月的侦查,端午节前夕,警方在广西、广东两地同时收网,将这个技术支撑团伙一举摧毁,前后共抓获6名犯罪嫌疑人。现代快报记者了解到,这个团伙分工明确,专门制作木马病毒、钓鱼网站,提供给5000多个直接诈骗团伙,导致740多万个QQ号被盗,从中非法获利300多万元。

据悉,这是江苏警方首次捣毁电信网络诈骗技术支撑团伙,这也标志着江苏警方打击电信网络诈骗向深层次迈进。现代快报记者随警作战,连续蹲守两天,亲历抓捕犯罪团伙二号头目过程。

通讯员 苏宫新 实习生 蔡雪洁
现代快报记者 陶维洲

案发

留学女儿QQ被盗 父亲被骗9万元

张先生51岁,江苏油田职工,22岁的女儿在澳大利亚留学。平时,父女间习惯用QQ联络。今年3月18日,两人QQ聊天,女儿说她有个老师刚刚回国,急需用钱,让爸爸先汇9万块过去。张先生没有怀疑,当即便向“女儿”提供的账号汇去了9万元。

钱汇走了,“女儿”也下线了。张先生感到奇怪,电话联系女儿确认。结果女儿表示,自己在上课没有上QQ。这时,张先生意识到被骗,向扬州市公安局江苏油田分局金洪派出所报案。

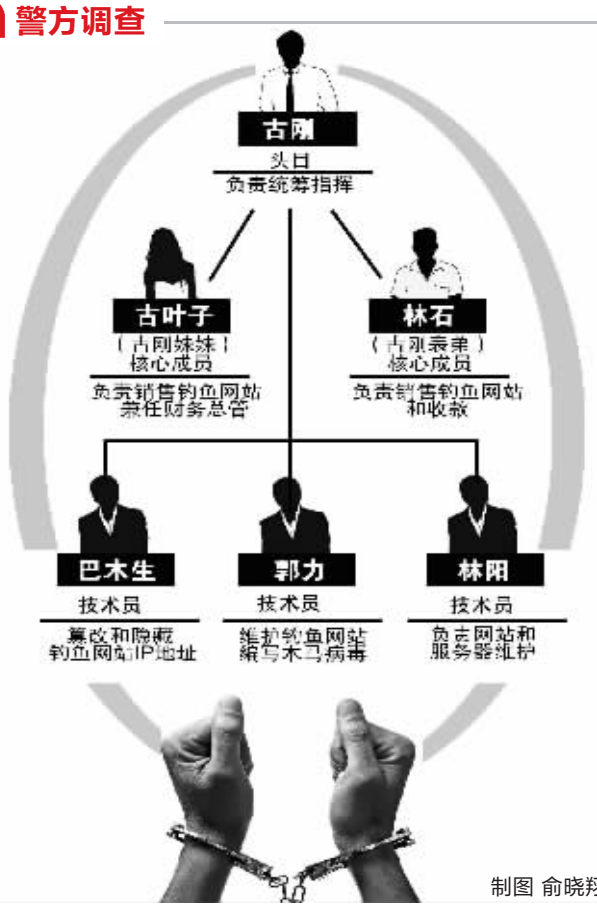
登录“招工网” 泄露了QQ信息

“很显然,张先生遭遇的是典型的QQ盗号诈骗。”金洪派出所所长赵六生作出判断后,立即将案情向上级汇报。扬州市公安局网安支队迅速会同江苏油田分局成立专案组展开调查。

张先生女儿的QQ是怎么被不法分子盗取的?在民警的询问下,小张回忆起来,约半个月前,她用QQ号登录过一个求职网站。民警发现,这个网站声称能为留学生提供兼职机会,不过,必须用真实的QQ号和密码登录。经过侦查,民警发现这是一个钓鱼网站,一旦留学生使用QQ登录,QQ号和密码就被不法分子掌握了。

“显然,这个钓鱼网站就是不法分子开设的,目的就是盗取QQ实施诈骗。”江苏油田分局副局长王日兵说。

警方调查



制图 俞晓翔

技术团伙批量生产几十种钓鱼网站

对钓鱼网站深入调查后,民警发现,有人批量生产这样的钓鱼网站,除了“招工网站”外,还有“商务网站”“会计培训”“合租住房”“网上投票”“模特大赛”等等,共有数十个模板。诈骗分子可以针对特定的人群,定向盗取QQ号码。顺着钓鱼网站这条线展开调查,一个为电信网络诈骗分子提供技术支撑的团伙逐渐浮出水面。他们隐藏在广西、广东两地,以销售、维护木马病毒、钓鱼网站为主业,成为直接诈骗团伙的坚实后盾。

江苏省公安厅相关人士介绍,以前从未发现过专门制作钓鱼网站提供盗号服务的团伙,这在全国来说,也是十分罕见的。案情复杂,专案组南下广东、广西,展开全方位侦查。

有人管销售有人管财务,分工明确

4月23日,专案组在广西凭祥市抓获犯罪嫌疑人古叶子。在技术支撑团伙中,她的角色是销售钓鱼网站兼财务,属于核心成员。根据她的交代,专案组梳理出了整个团伙的框架结构。

扬州市公安局网安支队副支队长孙志惠介绍,技术支撑团伙的头目是古叶子的亲哥哥古刚,宾阳人,31岁的他负责统筹指挥;23岁的古叶子负责销售钓鱼网站,兼任财务总管;古刚表弟、27岁的林石负责销售和取款,每销售一个网站他提成100元,古叶子被抓后,成为团伙二号人物。

在广东,有巴木生、郭力、林阳3名技术人员,他们负责制作木马病毒、钓鱼网站,以及网站维护。巴木生在深圳一家公司工作,古刚一般每个月都会支付其1万多元的报酬,而郭力几乎每三天就能从古刚那得到4000多元的报酬。

卖给5000多个诈骗团伙,获利300多万

专案组初步查明,古刚团伙自2013年7月以来,向广西地区5000多个诈骗团伙销售钓鱼网站,非法获利300余万元。这些诈骗团伙利用钓鱼网站共盗取QQ号码及对应密码740多万条。专案组将该团伙今年盗取的28万余个QQ号码与省内发案的QQ网络诈骗案进行比对,一下子串并出23起假冒QQ好友诈骗案,涉案金额达70多万元,其中扬州一地就有4起。

江苏油田分局刑警大队大队长戴国圣介绍,在广西宾阳,有不少人在销售钓鱼网站。古刚以每个网站800元一个月的价格对外销售,高于当地“市场价”,原因在于他的服务好,随时都能为“客户”提供必要的技术支持,躲过杀毒软件的拦截。

直击抓捕

专案组兵分五路 赴广西、广东抓捕

明确团伙成员的真实身份后,5月28日,专案组分成广西、广东两大抓捕组,又针对每个犯罪嫌疑人分成5个抓捕小组,随时准备收网。5月29日凌晨1点,现代快报记者飞抵南宁随警作战。广西抓捕组的目标人物为古刚和林石,他们分别藏匿在宾阳和来宾。古刚是团伙头目,江苏油田分局刑警大队大队长戴国圣给他的代号是“古老大”。林石是此次抓捕行动的二号人物,代号“小林”。

经过商议,最终定下的抓捕方案是首先抓捕古老大,然后其他4个抓捕组同时收网。根据安排,现代快报记者随江苏油田分局刑警大队副大队长黄俊前往来宾抓捕小林。

抓捕地点 广西宾阳

民警蹲守9个小时,“古老大”落网

5月29日上午,来宾抓捕组抵达目的地,为确认小林的行踪,现代快报记者跟民警来到了小林藏身的小区守候。晚上7点,小林所在房间的灯亮了,到了凌晨1点,灯熄灭了。“他应该就在里面”已经守候了10多个小时的黄俊异常兴奋。确认小林的位置后,民警就等着古老大落网,然后实施抓捕。

虽然现代快报记者身在来宾,但通过微信可以了解整个抓捕行动的进展。宾阳抓捕组在古刚位于宾阳的三处落脚点死守,5月30日早上,民警终于掌握了古刚的位置。戴国圣说,古刚从事的是技术犯罪,警方需要固定大量的技术证据,“所以我们只能等,等他出来!”从早上7点到下午4点,古刚闭门不出。就在焦灼时刻,侦查员发现古刚的情人出门买菜。

抓捕民警决定主动出击,尾随古刚情人进门实施抓捕。就在古刚情人开门的瞬间,戴国圣拉开防盗门,向室内的古刚冲去。古刚见机不妙,躲进里面的房间并将房门反锁。戴国圣一脚将房门踹开,此时古手上已经抓起了手机。戴国圣飞扑上前,将他摁在床上。古老大落网!另外4个抓捕组随即展开行动。

嫌疑人古刚被民警摁在床上 警方供图

抓捕地点 广西来宾

记者随民警冲入房间,抓获二号人物

当古刚落网的消息传来,记者所在的来宾抓捕组立即行动起来,在当地警方的配合下找到房东敲门,门顺利打开。现代快报记者和抓捕民警一起冲入房内,林石还没明白过来怎么回事,冰冷的手铐就戴到了他的手上。此时,距离古老大落网仅仅过去了1个小时。

在林石的住处,民警发现他的电脑开着,正在和诈骗分子谈生意。电脑旁边,放着多张以他人身份证办理的银行卡,还有多张电话卡。在查看林石的电脑后,黄俊倒吸了一口冷气,真悬啊!原来,为了能及时破坏证据,林石的笔记本电脑后盖就没有关,随时可以将硬盘扯出毁掉。

嫌疑人林石被押解回江苏 警方供图

抓捕地点 广东梅州、揭阳、深圳

其他团伙成员相继归案

随着一、二号团伙成员的落网,广东的三个抓捕组也同时行动。梅州的郭力、揭阳的林阳都毫无悬念地被抓,深圳的巴木生最后一个落网。目前,包括古叶子在内的6名犯罪嫌疑人全部被押解到江苏审查。此案还在进一步侦审之中。(文中涉案嫌疑人皆为化名)