5000万条公民信息在“暗网”被倒卖

涉案金额达1.5亿元

江苏响水人顾宏(化名)的个人信息在网上“裸奔”。

他没想到,自己的姓名和联系方式被人包装为“新鲜一手数据”,多次转卖。更没想到,因为被备注“有资金需求”,他已经成为电信诈骗和网络放贷团伙的重点目标。

顾宏并不是唯一的受害者。近日,盐城公安网安支队民警在一个“暗网”平台上截获了一条倒卖公民信息的线索,经过追查,抓获15名长期在网上进行信息数据交易的犯罪嫌疑人。

嫌疑人手上掌握着5000余万条个人信息,涉案金额达1.5亿元。“这说明全国至少有5000余万人的姓名和电话掌握在他们手里。”主办民警倪琛说。


此次行动中,15名犯罪嫌疑人被警方抓获。

倒卖公民信息的群,有些群用“水果群”或暗语伪装。

“暗网”追踪

今年1月底,盐城网安支队的民警在一个“暗网”平台上,发现了一条叫卖我国公民个人信息的帖子。

在网页附带的图片中,盐城市响水县居民顾宏的信息也在其中,并被备注了一串文字:新鲜一手数据,有资金需求。发帖人是“SS52098”。

民警翻查了发帖人此前的信息,发现他并非初犯。从去年开始,他通过该账户在暗网上多次出售公民个人信息,数量惊人。但民警们也只掌握了这串长长的用户名,“暗网”的特殊性和隐蔽性,想要查到发帖人的真实身份并非易事。

民警们决定先从被泄露信息的顾宏身上着手。

顾宏从没想过自己的资料被人当成商品在网上公开叫卖。他告诉办案民警,他从2015年开始就经常会收到一些推销电话,几乎每周都能接到一两个电话或信息,涉及售楼处、网络报考、保险公司、银行办理信用卡、儿童教育等多种机构。给他打电话的人大多知道他的姓氏,有的可以直接喊出他的全名。

“有的电话接了之后就感觉是骗子,有的短信让点击网址链接,明显也是骗局。”顾宏说。

但信息是何时被泄露的,他也说不清。他记得自己曾在朋友圈看到办理信用卡的广告,联系对方的工作人员预留过自己的姓名、手机号码、身份证号等个人信息;也曾经在给孩子报名培训机构时留过电话。

与此同时,办案民警在网络上日夜追踪。响水县公安局网络安全保卫大队教导员韩祝进介绍,嫌疑人反侦查意识特别强,使用境外通联工具来贩卖公民个人信息,其上下线有30多人,且相互不认识。

通过对网络地址追踪等一系列手段,警方逐步锁定了“SS52098”的真实身份——一个名叫王超(化名)的年轻人。2021年1月30日11时许,盐城警方在湖北省荆州市一间工厂宿舍中将王超抓获。

很快,他的两名同伙也在家中落网。警方从王超的电脑中发现了9万多条个人身份信息数据,有姓名加电话号码的,也有带身份证号码和收货地址的。

“上线”与“下线”

27岁的王超是湖北省公安县人。因为没有固定收入,他偶尔会通过“网贷”周转。据他向警方供述,2020年9月,他在QQ平台上搜索“网贷”信息时,无意间加入了交易公民个人身份信息的群。

王超还记得,群里有出售个人身份信息的,也有要买信息的。王超在群里看到一则广告,上面称只要弄到别人的姓名和电话就能卖钱。

在群里简单了解了倒卖信息的流程后,王超试着联系出售公民身份信息的卖家。这些卖家后来都成了他的“上线”。

按照“市场价”,带姓名和手机号的身份信息一般是1.2元至1.5元一条,不带名字的纯手机号只要两三毛一条,这些个人信息在圈子里被称为“料”。

去年11月前后,王超拉来朋友阿龙和阿松入伙。阿龙告诉办案民警,他曾怀疑赚不到钱,但王超说比上班强多了。只过了两三个月,阿龙就从王超手中拿到了1万元的“分红”。

交易一般通过支付宝或银行卡转账,为了逃避追踪,他们还有多款更隐蔽的聊天和收钱软件。

从去年9月到今年1月,王超靠贩卖公民个人信息赚了十几万元,除去购买数据的成本,据王超估计,盈利至少8万块钱。

在这条贩卖个人信息的产业链中,王超只是其中一环,他还有上线和下线。

根据王超的供述,警方顺藤摸瓜找到了他的多名上线和下线,至此,以他们为纽带的非法窃取、层层倒卖、侵犯公民个人信息的黑灰产业链逐渐清晰。

最初和王超合作的上家网名叫“林听风”,王超花了4万多元钱,从“林听风”手中买了十几万条信息。后来“林听风”不干这行了,拉黑王超的联系方式后消失在网络中。

王超称,他还从另外两个卖家手里拿过货,但他们只在网上交易,王超也只有他们的网名。在这次抓捕行动中,其中一名卖家落网,另一人也被警方锁定。

除此之外,王超还有不少下家。这些下家中,张成(化名)做得最“专业”。33岁的江西人张成曾经就读于南昌一所重点大学。毕业后,曾在几家知名企业工作。2019年,他注册了一家网络科技公司,专做网络推广。

张成告诉办案民警,以前在发布网络推广的群里也看到过有人发布买卖个人信息的广告。他主动联系他们,询问了出售流程,也加入了倒卖信息的队伍。

泄露源头无从查起

除了找王超买“料”,张成还有近十个上线。这些上线中,大部分人还有其他上线。公民个人信息在他们手中被层层倒卖,但没人能说清这些信息的泄露源头。

有些个人信息是在无意间泄露的。“平时注册软件都要实名制,如果这个软件出现漏洞,被人用技术手段窃取了资料,就有可能造成信息泄露。”主办民警倪琛说,还有一些黑客专门利用技术手段从软件后台“爬”信息。

“数据库”中的受害者

至于下线为什么要买这些个人信息,个人信息的贩卖者从不多问。

“大多是用来打电话或发信息,或用于发布售楼、网贷等一些广告信息。”王超猜测。他的伙伴阿龙直言,买他们数据的人都是搞电信诈骗的。“他们购买之后用来打电话或发短信以网上发放贷款的名义骗钱。”

抓捕行动结束后,警方从其中一名嫌疑人倒卖的个人信息中,随机抽取了一百多个电话号码放到系统里查询,其中就有十余人曾因为遭遇电信诈骗到公安机关报案。

这些案件跨度从2009年至2020年,诈骗的手段也各不相同。

但更多的信息泄露是被人恶意窃取的。倪琛说,他们7月初刚刚办理一起案件,嫌疑人在某营业厅上班,经常帮来办业务的老年人用手机操作,他用老人的手机偷偷注册某款软件,从中拿回扣。而这些老年人的信息就会被软件方提取到。

还有一些信息来自网络贷款平台,圈子里称作“台子”。据张成所说,他的其中一个上线手里的信息就是从“台子”里提取出来的。

张成解释,申请网络贷款必须先在贷款平台里面注册,注册需要留下姓名、手机号码、身份证号和地址等信息。那个上线有渠道从一些贷款平台后台提取这些信息。

他向警方供述,这些信息数据中通常会标注用户在网贷平台登记注册的日期和时间,还有一些带有银行卡信息,如果有人利用这些资料进行电信诈骗,成功的概率就比较高。

除了“台子”,张成的上线还有刷单平台的管理人员,专门承接各种网上刷单业务,分配给兼职人员完成刷单。“刷单”是网店卖家付款请人假扮顾客购物,提高网店的排名、销量和好评吸引顾客。

据该刷单人员交代,刷单的流程和正常购物流程一样,兼职人员需要把姓名、手机号、地址等个人信息登记在电商平台上。他利用权限潜入后台复制这些信息,再根据下线的需求,把数据筛选、分类后卖出去。此人也在警方的抓捕行动中落网。

损失较少的受害人被骗了不到3000元钱,还有几人被骗上万元。

有人在急需用钱时中了贷款的圈套。警方称,2018年11月,高某接到自称融360网贷的客服工作人员电话,对方称可以帮他办理贷款。之后他用QQ添加了对方好友,按照对方指示,扫描二维码支付了6000元保证金后对方失联了。

有人误信了中奖信息被骗钱。2011年12月28日下午,连云港市新浦区警方接到报案,有人在上网时收到中奖信息,按照对方要求汇款2800元到对方账户,之后发现被诈骗。

(新京报)