来源:经济参考报

从接单、开发，到封装、分发、售后，提供量身定制APP服务，只为让诈骗工具披上正版手机软件的外衣。

有人负责寻找开户人，有人负责为开户人注册公司、办理营业执照并开通对公账户，大量实名开立的银行卡、电话卡被诈骗分子购买或租借后用以实施电信网络诈骗。

高价收币的买家实为电信网络诈骗团伙，循环往复虚拟币交易背后竟是为洗白赃款……

《经济参考报》记者近日多方调研了解到，电信网络诈骗组织化、公司化、产业化日趋明显，量身定制非法
APP、买卖银行卡和电话卡、洗钱等一系列非法交易滋生出黑金产业。

“量身定制”APP成“定制陷阱”

60%以上诈骗通过手机APP实施

北京顺义区，王女士在网友“半杯咖啡”的诱导下扫码下载了一款名为“XX财富管理”的APP。这款APP看起来并无特别之处，王女士当日投款一万元，即刻收益提现1000多元。当王女士再向亲友借款、从银行贷款，甚至还抵押了房产，总共筹集200万全部充入账户后，系统却以“账户存在异常被冻结保护”为由，无法提现。随后，APP竟再也无法登录……

“王女士扫码下载的APP实际上是个‘山寨版’，是由黑灰产技术人员按照电诈分子要求封装的一款冒用知名软件的投资理财APP。”负责办理此案的北京市顺义区人民检察院检察官任巍巍告诉《经济参考报》记者，这款山寨版APP是由某网络服务平台封装完成的，所谓封装，是将网址、应用名、LOGO、启动图打包形成一个APP应用包，使网站以APP形式呈现。

中国信通院安全研究所防范治理电信网络诈骗中心副主任、工信部反诈专班工作负责人常雯介绍，通过APP封装分发平台，开发者只需简单点击操作即可实现APP自动生成与快速分发。与正规应用商店相比，此类封装分发平台缺乏应用风险审核及开发者信息登记制度，成为诈骗分子制作、传播涉诈APP的重要渠道。

“一些技术人员或网络服务平台，明知他人可能利用APP实施信息网络犯罪，但为了获取不法利益，以技术中立为挡箭牌，大肆参与违法APP的制作、封装等活动。

而一次违规封装，就可以让诈骗工具披上正版手机软件的外衣，令受骗家庭倾家荡产。”任巍巍说。

记者了解到，手机APP已经成为实施诈骗的重要作案工具。据公安部统计，2021年以来，60%以上的诈骗都是通过不法分子制作的手机APP实施。而与此相伴相生的是，量身定制APP的产业已经成为电信网络诈骗黑灰产上的重要一环，有的公司从接单、开发，到封装、分发、售后等，提供“一条龙”服务。

某地公安机关打掉一个特大跨境“杀猪盘”犯罪团伙，其中负责APP技术开发和维护的兰某、詹某交代：“封装APP，对我来说很简单，只需要2分钟就能完成，每封装一个我就能挣10元至100元不等”，两人3个月时间已获利10万元。

近期，公安部门陆续查处了数百个涉诈手机APP，内容涵盖社交、贷款、投资、博彩、购物、短视频、手机安全等多个领域。“以社交软件为例，不法分子按照电诈分子要求制作一款具有抓取客户通讯录功能的社交软件后，电诈分子利用该软件与被害人裸聊，抓取通讯录后，以向好友发送裸聊照片为威胁实施敲诈。”任巍巍说。

银行卡、电话卡买卖成帮凶

非法交易滋生黑金产业

21岁的钟某2021年打工时认识了一个名叫“阿风”的男子，对方介绍他到京注册公司、开办银行对公账户，表示这期间不但管吃管住，账户办好后即可卖给他人使用，收益十分可观。钟某对此动了心，于是便由“阿风”安排来京，后在一位绰号“鸟叔”的男子和一位绰号“大姐”的女子带领下注册公司并开办了对公账户，并将账户以1500元的价格卖给二人。此后钟某还在“阿风”的介绍下，被一名叫“老大”的男子发展成为安排开户人员食宿的带队人。

直到北京朝阳警方在梳理相关案件线索时发现钟某在某银行开办的两个对公账户涉嫌帮助电信网络诈骗分子流转犯罪所得资金，这一层次分明、分工严密的大型帮助信息网络犯罪团伙才最终浮出水面：“老大”是总负责人；“阿风”负责寻找开户人，并安排其来京；钟某负责安排开户人的食宿；“鸟叔”和“大姐”负责为开户人注册公司、办理营业执照并开通对公账户，最后由“大姐”将办好的执照、账户等交给“老大”，每个环节的费用均由“老大”支付。

大量实名开立的银行卡、电话卡被诈骗分子购买或租借后用以实施电信网络诈骗等犯罪活动，买卖“两卡”即银行卡、电话卡的非法产业体系也成了为电信网络诈骗“输血送粮”的帮凶。

任巍巍告诉《经济参考报》记者，不法分子大量收购他人的银行卡四件套，即银行卡、U盾、密码、绑定手机卡，或者针对对公账户的八件套，包括公司营业执照、法人身份证等，以实现利用他人银行卡将赃款在多个账户间进行转移、拆分。

据公安部通报，2021年，公安机关共破获电信网络诈骗案件44.1万余起，打掉涉“两卡”违法犯罪团伙4.2万个，涉案银行卡全部为实名开立后非法买卖。

吉林省公安厅刑侦局侦查二处处长杨亮向记者介绍，除了银行卡，手机卡也是诈骗分子接触被害人，进而实施诈骗行为的主要媒介，是社交平台、金融机构进行实名认证的重要载体，诈骗分子为了绕过实名制管理，对手机卡有着巨大需求。

“有些不法分子，在网上发布招聘兼职的信息，声称办理手机卡为营业厅冲业绩，一张卡支付数百元的费用，实际上是将收购来的手机卡加价出售，邮寄到边境或境外。为了防止犯罪行为败露，不法分子本身很少在营业厅附近出现，也很少直接向办卡人付款或以现金形式付款，而是招募带队人具体实施，并且提醒带队人将收购的卡分开存放，以规避处罚。”任巍巍说，在办案中发现，有一些行业内部人员利用制度漏洞，暗中私自开卡、贩卡。

任巍巍透露，有些个体手机店的工作人员在取得电信业务运营商的电话入网业务委托后，以“认证没有通过，重新进行认证、解决网速”等为由对用户进行多次人脸识别，并冒用其电子签名，在客户不知情的情况下多办手机卡并在黑市上出售。他们以每张90元的价格出售，同时还可从渠道商处获得10元的办卡返点，即单张获利100元。此外，有的人自称能实现“不足一小时开卡9张”的“骄人业绩”，这些人明知全国开展“断卡行动”，也知道同行被抓，但仍抱有“卡先留着，不能白费”的侥幸心理，伺机作案。

工信部网络安全管理局相关负责人说，一些不法分子组织农民工、老年人、学生等在电信企业实名登记购买电话卡后，违规私下交易倒卖。由于缺乏法律依据，公安机关对涉诈用户无法实施失信惩戒，致使不法人员、顽固分子屡犯不改。

“炒币”实为“洗钱”

赃款转移方式屡出花招

在北京，丘某通过某社交聊天APP与一个名为“星星”的网友结识，“星星”貌似好心，自称有个“炒币”的项目，收入颇丰，邀请丘某一同参与。二人相约见面，丘某按照“星星”的指示，先是扫码下载“某币”APP和“imToken”APP，并在“某币”APP上完成实名注册，后又通过无须实名注册的“imToken”APP接收来自“星星”转让的虚拟货币即泰达币，并将该虚拟币提现到本人的“某币”APP账

户，之后在“某币”APP上将该虚拟货币向竞价高者出售，同时通过本人银行账户收取人民币并迅速支取现金，扣除本人获利后交给“星星”，完成交易。

只需动动手指，就能轻松挣钱，丘某从此跟随“星星”做起了“炒币”的买卖。由于一天需交易多次，为保证现金及时交到“星星”手中，不受支取额度限制，丘某先后将本人名下多个银行账户绑定“某币”APP，并快速在本人数个账户之间拆分、流转、支取现金。

直到有一天，丘某发现自己用来炒币的银行账户陆续被司法冻结了，原来，高价收币的买家实为电信网络诈骗团伙，而用来收币的钱款则是他们刚刚骗得的赃款。

“卖方在虚拟币交易平台上出售虚拟货币，买方支付人民币用于购买虚拟货币，而实际上买方的账户就是电信诈骗分子控制的账户，卖方用银行账户收取赃款后再进行拆分、取款后，再将现金交给上家，收取虚拟货币，循环往复，洗白赃款。”任巍巍说。

诈骗分子为逃避公安机关止付、冻结措施，往往快速转移涉案资金。犯罪分子不断寻找、试探“资金链”薄弱环节，创新赃款转移方式。

据记者了解，除了通过境内“水房”（洗钱团伙）实施转移以及“跑分平台”拆分交易进行转移之外，诈骗分子也通过购买虚拟货币向境外转移涉诈资金，这种方式查控难度更大。

“虚拟货币一是匿名，二是去中心化，能实现快速、大额的向境外转移资金。而且利用虚拟货币转移赃款的时候，大额资金也会被打散，犯罪团伙内部人员分工负责不同种类的虚拟货币的资金转移。”北京市人民检察院检察官王姝坦言，利用虚拟货币转移赃款的犯罪取证难度更大。

当前，电信网络诈骗有组织、产业化特征愈加凸显。“买卖公民信息、开发技术平台、网络引流推广、转移资金洗钱等实施诈骗各个环节相互衔接，与网络赌博、组织偷渡、绑架勒索、裸聊敲诈等犯罪相互交织，组织化、公司化、产业化日趋明显。”公安部刑侦局打击新型网络犯罪指导处副处长胡志伟表示。

（记者：李佳鹏 孙韶华 张莫 梁倩 郭倩 王阳 周立权）