他们购买机票获取票号号段,利用航空公司系统漏洞,黑进系统非法获取旅客信息,并以每条7元至8元的价格出售给诈骗团伙——

航班退改签背后的“大骗局”

警音长传

□本报记者 史隽
通讯员 陈怡心

“某某旅客,您的航班因故障取消,需办理退改签手续……”这是一通诈骗电话。对方为何能如此精准掌握旅客的姓名、航班号,甚至身份证号码?这些个人信息又是如何被明码标价,在“信息贩子—诈骗团伙”多级流转中,逐渐演变为一场场精心策划的精准诈骗?

2025年11月20日,经浙江省海盐县检察院提起公诉,法院开庭审理了一起利用航空公司系统漏洞非法获取、出售367万余条旅客信息的案件。12月3日,法院以侵犯公民个人信息罪分别判处王某、毛某、李某有期徒刑六年、四年、三年十个月,各并处罚金1000万元、15万元、5万元,责令退缴全部违法所得。一审判决后,被告人提出上诉。

假改签真骗局

2024年5月22日,海盐的王女士通过某网络平台订购了两张6月21日从杭州飞往成都的机票。出发前一天,她接到了一个自称“航空公司工作人员”的电话。

对方先以核对信息为由,说出了王女士的名字、航班号和出发时间,王女士一听信息都准确便深信不疑。随后,对方告诉她,因航班取消需要改签,航空公司会补偿她200元,王女士便听从了对方的安排。

对方称为了方便收款,需要王女士提供网络支付平台账户,得知她没有开通透支功能,骗称只有开通了该功能才能收款。于是,在对方的引导下,王女士开通了多个支付平台账户的透支功能,并下载了一款名为“云服务”的App,点击了对方提供的“官网”链接。此时,王女士已经落入圈套。

同年6月21日,王女士按照改签后的时间来到机场,发现之前的航班已正常起飞,但她没多想就上了飞机。直到8月2日,一个催账短信引起了她的注意。“我都没操作过透支,不仅支付平台账户里的余额没了,还欠了钱,太奇怪了。”更令她震惊的是,其多个网络支付平台账号均有透支情况,总计12272元。王女士立即报警。

但王女士始终都很纳闷,自己明明是从正规渠道购买的机票,个人信息却如此迅速地落入骗子之手,这究竟是怎么回事?

在案件侦办过程中,警方顺藤摸瓜,从欠款的去向查到了诈骗分子,再从诈骗分子那里了解到机票个人信息的来源,最终锁定了一个名为“joker”(化名)的境外社交网络账号。该账号曾大量出售航空旅客的个人信息,其中就有王女士的个人信息。

2024年12月13日,检察官在讨论案情。

虚拟身份被揭开

2024年8月底,“joker”的账号控制者王某,以及毛某、李某相继落网。

经查,李某曾因犯帮助信息网络犯罪活动罪入狱。出狱后,同学毛某为他接风洗尘,他由此结识了毛某的朋友王某。懂点计算机技术的王某提出想以“黑客”方式赚钱,李某和毛某觉得挺新鲜,几人一拍即合。2023年10月至2024年8月,王某等3人通过购买低价机票获取票号号段,利用航空公司系统漏洞,黑进系统非法获取旅客信息,并以每条7元至8元的价格出售给诈骗团伙。该案串并全国机票改签类诈骗案350余起,王某非法获利374万余元,毛某非法获利8.6万余元,李某非法获利3万余元。

侦查阶段,检察机关受邀依法介入,引导公安机关开展取证工作,明确法律适用方向。

2024年9月17日,公安机关提请批准逮捕王某等3人。在审查过程中,王某拒不承认其是账号的使用人,称其仅将相关技术手段传授给李某,毛某则说自己没有参与,李某坚称窃取并出售旅客个人信息的行为均是他一人所为。

为打破困局,办案检察官从海量电子数据中抽丝剥茧,通过对涉案账号的聊天记录、王某过往犯罪记录及活动轨迹进行分析,最终查明王某就是“joker”账号的实际使用者。

在确凿证据面前,王某等3人如实供述了犯罪事实。由此,一个以王某为首、长期从事公民个人信息窃取与贩卖的犯罪团伙浮出水面。2024年9月24日,检察机关依法对王某等3人作出批准逮捕决定。

幕后者受惩罚

据王某交代,不同航空公司系统漏洞并不相同,需开发不同软件来窃取旅客个人信息。他们在出售旅客个人信息时并非随机选取,而是采用了过滤机制,专挑40岁至70岁人群“下手”。

2024年11月22日,王某等3人因涉嫌侵犯公民个人信息罪被公安机关移送至海盐县检察院审查起诉。经审查,检察机关认为,王某等3人违反国家规定,非法获取、出售或者提供公民个人信息,均属情节特别严重,犯罪事实清楚,证据确实、充分,应当分别以侵犯公民个人信息罪追究其刑事责任;李某在刑罚执行完毕后五年内再犯应当判处有期徒刑以上刑罚之罪,系累犯,应当从重处罚,于2025年4月30日依法向法院提起公诉。

“该案暴露出航空公司后台数据安全存在短板。”海盐县检察院副检察长季春说,防范和打击电信网络诈骗是久久为功的长期工程,也是需要全社会共同参与的系统工程,“打”“防”“管”“控”“宣”等各方面工作都不可或缺,航空公司的相关制度、管理的完善落实是重要的一环。为此,该院从建立预警机制、升级安全验证模式、加大宣传力度等多维度向航空公司提出检察建议,帮助企业堵漏建制。

游戏外挂穿上了“DMA马甲”

□本报通讯员 徐轩

一名玩家的举报,牵出了一个涉案金额高达300万元的制作、销售DMA外挂网络的团伙。日前,经江苏省盱眙县检察院提起公诉,法院以提供侵入、非法控制计算机信息系统程序、工具罪分别判处关某、赵某有期徒刑三年,缓刑四年,各并处罚金;14名情节轻微的代理被作不起诉处理,全部违法所得已退缴。

“这根本不是普通作弊,可能涉嫌违法!”2024年6月,刚测试完“JR”外挂(需与DMA硬件一起使用)的资深射击游戏玩家李某带着全套设备走进了派出所。

公安机关根据李某提供的线索,从一张标注“电子配件”的快递单入手,锁定了QQ号为“美羊羊”的销售账号。“虽然收件人信息模糊,但这个销售账号频繁在游戏外挂群发布‘JR卡密’销售信息。”办案民警回忆,通过跨区域协作,警方很快查实“美羊羊”是赵某,并找到其背后的核心技术人员——其表弟关某。

经查,关某高中毕业后自学编程,2022年底起专注研究DMA,不仅研发出适配某知名射击类网络游戏的“JR”系列DMA外挂,还搭建了“SProtect”卡密管理平台,实现外挂权限的自动化管控。赵某则负责生成卡密、招揽代理,构建起全国性销售网络。该团伙通过QQ群、游戏公屏、二手平台等渠道推广,资金结算采用支付宝口令红包、微信扫码等隐蔽方式,逐渐形成了覆盖全国的销售网络,累计销售金额超300万元。

“DMA是一种允许外部设备直接与计算机内存进行数据读写、无需中央处理器持续参与的技术,能大幅提升运行效率,一旦被滥用,就成了绕过游戏防护的作弊利器。”办案检察官指出,DMA外挂能未经授权直接读取游戏内存数据,实现“透视”“自动瞄准”等作弊功能。

“这相当于隔空取物,传统软件反作弊系统很难检测到这种跨设备操控。”经专业机构鉴定,“JR”系列DMA外挂被认定为破坏性程序。

2024年10月,案件被移送至盱眙县检察院审查起诉。办案检察官审查后认为,该案并非普通的游戏作弊,而是典型的技术型网络犯罪,应认定为构成提供侵入、非法控制计算机信息系统程序、工具罪。

检察官在办案中发现,涉案的代理不乏在校学生和失业青年,涉案获利从3000元到7万元不等,且均有自首、坦白、全额退赃等情节。“如果‘一刀切’全部起诉,社会效果未必最佳。”盱眙县检察院贯彻宽严相济刑事政策,经综合考量后,对14名代理依法作出不起诉决定,对关某、赵某依法提起公诉。

通过检察官耐心的释法说理,关某、赵某退缴了全部违法所得300余万元。2025年3月,法院经审理采纳检察机关提出的量刑建议,作出上述判决。

案件审结后,检察机关积极履行社会治理检察职责,重点围绕案件暴露出的深层次问题组织开展了专项调研与分析工作,针对发现的问题,于11月向相关部门提出强化网络黑灰产监管的建议。

组建“洗钱车队” 只为日薪千元

□本报记者 刘立新
通讯员 孙珊珊 卢怡

2025年3月6日,河南省通许县某银行内,郑某持银行卡要求取现70万元(经查为诈骗赃款),被布控民警当场抓获。这起洗钱案的突破口就此打开,主导、协助犯罪的彭某、夏某等4人陆续落网,5人“高薪捞金梦”彻底破碎。

“报销来往车票、包吃住,轻松日薪过千元。”2月的一天,彭某、夏某等人收到一加密通信软件某群内通知,面对“日薪千元”的诱惑,他们通过该软件与上游犯罪人员取得联系,在明知资金可能涉及电信网络犯罪的情况下,仍组建“洗钱车队”提供帮助。

3月1日,彭某作为“车队”负责人,与夏某驾驶租赁车辆从天津辗转来到通许,夏某在收到上线发来招募的卡主信息后对接“取手”郑某,安排其办理银行卡并测试账户、提供信息给上线。彭某还通过林某(另行处理)联系吴某、吕某二人担任“安保”,负责监视郑某取现。

3月6日,按照上线的指令,郑某拿着办好的银行卡来到银行取现,吴某、吕某在附近监视,欲完成赃款洗白。取款时,郑某被公安民警当场抓获,其余4人随后也被警方抓获。

案件侦查初期,面对讯问,郑某、吴某仅承认部分行为,彭某、夏某则一口咬定“不知情”,拒不认罪。为确保案件顺利侦破,公安机关商请通许县检察院依法介入。该院结合案件疑点向公安机关明确取证方向,固定银行监控视频、涉案车辆轨迹等客观证据,提取涉案人员在加密软件上的聊天记录、转账流水等电子数据,形成完整证据链。

6月13日,公安机关将该案移送至通许县检察院审查起诉。7月28日,检察机关对该案提起公诉。近日,法院以掩饰、隐瞒犯罪所得罪分别判处被告人彭某等5人有期徒刑一年八个月至一年不等,各并处罚金。

社会万象

猜密码侵入网站后台 盗数据暗挖东家客户

离职员工凭借对前公司系统的熟悉,靠猜密码的方式非法侵入公司网站后台盗取客户数据。2025年10月11日,经广东省深圳市南山区检察院提起公诉,法院以非法控制计算机信息系统罪判处郑某有期徒刑一年,并处罚金5000元。

郑某原是一家电商服装公司的销售客服,主要负责接待客户、整理订单、下单生产等。2023年2月,郑某从公司离职后,不仅拒不归还公司配发的工作手机,更是玩起了“人间蒸发”,公司无法联系上郑某。

在郑某离职后的几个月里,公司陆续接到客户投诉,反映有人自称是该公司员工,添加微信好友后推销产品。这一异常情况引起了公司的警觉。2023年8月,公司经过内部排查,发现郑某在离职后多次登录公司网站后台并下载了数万条客户资料,于是报警。

经查,郑某离职后,其工作账号已被删除,但他留存了几位前同事的电话号码,并尝试用手机号码后六位作为密码进行登录。与此同时,他还发现了系统漏洞:通过“忘记密码”功能,手机会收到一个四位数验证码,且这个验证码没有有效期限制,他便不断尝试输入,直至成功修改密码,从而非法控制他人账号。据郑某供述,他入职新公司后,想通过获取前公司客户订单情况发展客户,同时了解热销商品以获取销售渠道。

2025年3月,潜逃多时的郑某被警方抓获。9月19日,南山区检察院依法以涉嫌非法控制计算机信息系统罪对郑某提起公诉。(孙羽中 陈芳)

被催债无钱偿还 为应付伪造存单

为了应付好友催债,朱某想出的解决之法竟是网购一张假银行存单。2025年11月28日,经湖北省十堰市张湾区检察院依法提起公诉,法院以伪造金融票证罪判处朱某有期徒刑八个月,缓刑一年,并处罚金2万元。

朱某自2018年起涉足网络虚拟货币交易,一度获利颇丰,这段经历让她被好友视为懂得投资的人。2024年9月,朱某声称自己有赚钱的项目可以带好友一起做,鼓动王某将钱交给她操作,承诺两个月后连本带利归还。出于信任和对高回报的期待,王某将丈夫积攒的45万元交给了朱某,后又从银行贷款15万元交给朱某。

然而,约定期满,朱某承诺的利润却未如期支付,本金也无法取出。原来,朱某投资的虚拟货币因市场规则限制无法及时套现。2025年春节前夕,王某的丈夫开始频繁催促其还款。

“我当时只是想着怎么能先应付过去。”朱某情急之下,在网上联系了一个声称能“做单据”的人,以180元的价格让对方伪造一张户名为王某丈夫、面值为10万元的银行个人定期存单。将假存单交给王某时,朱某特意叮嘱:“大额转账很麻烦,我把钱给你做成了银行存单,这个存单给你丈夫看看让他安心,先别去银行取。”

2025年5月,王某拿着存单前往银行取款,被银行工作人员告知存单是伪造的,随即报警。公安机关立案侦查后,迅速锁定了朱某的犯罪事实。10月24日,张湾区检察院以朱某涉嫌伪造金融票证罪向法院提起公诉。法院经审理,采纳了检察机关的指控和量刑建议,作出上述判决。

(蒋长顺 田玮书)

U币盗窃手段新 欲骗他人反被抓

杨某刑满释放后无事可做,听说盗窃USDT币(虚拟货币,下称U币)能获利,便找同伙张某商议合作,二人随即在短视频平台发布“低价出售京东E卡”消息并引流。尹某与赵某等4人看到消息后,添加张某为好友,得知京东E卡可按照面值的八折购买,量大可按七五折购买,心动不已,几人决定先验证卡的真伪再进行交易,并与张某约定对接事宜。

杨某与尹某等人线下见面后,提出用虚拟货币进行交易,并引导尹某先下载某款数字钱包软件,在此软件内创建波场钱包并充值100枚U币。完成充值后,杨某向尹某交付了从实体店购买的1000元京东E卡,尹某核验后决定继续交易。随后,赵某购买2000枚U币并充值到尹某账户。

这时,杨某提出需查看账户是否安全。尹某在操作时,杨某用某软件与张某通话,趁尹某不备对其账户的密钥二维码进行截图并发送给张某。之后,杨某以外出取卡为由逃离现场。

不久,尹某等人发现账户少了40枚U币,面对质问,杨某称与自己无关。次日,尹某账户内的1999枚U币又被张某转走,杨某依旧坚称自己毫不知情。

尹某、赵某心生疑惑,二人商议后决定“将计就计”:谎称2000多枚U币就当交学费了,想向杨某学习偷窃技术,还提出合伙偷盗尹某朋友价值30万元的U币。杨某信以为真,到尹某所在地传授“技艺”。因杨某离开时间较长,张某联系不上他怀疑其被绑架,遂报案。后杨某被抓获归案,张某主动投案。

2025年10月10日,山西省介休市检察院经审查以涉嫌盗窃罪对杨某、张某提起公诉。12月17日,法院以盗窃罪分别判处杨某有期徒刑一年,并处罚金5000元;判处张某有期徒刑八个月,并处罚金4000元。

(郭萍 李小平)