上海检方公诉的一起涉案金额超5亿元的虚开发票案，牵出非法人脸识别案

“人脸识别破解术”成黑产业，护“脸”亟须查缺补漏

本报记者兰天鸣

人脸识别作为一种易用性强的生物特征验证技术，目前在政务、安防、金融、生活消费等行业都有着广泛应用。不过，新华每日电讯记者调查发现，人脸识别技术存在明显的安全漏洞，对社会和财产安全存在重大隐患，亟须进行系统性的安全排查和堵漏。

一起发票案牵出非法人脸识别案

记者从上海检察机关获悉，在近期上海市虹口区人民检察院公诉的一起特大虚开增值税普通发票案中，被告人通过破解人脸识别技术等方式，注册“皮包公司”用于虚开增值税普通发票。据悉，多名被告人为他人开具增值税普通发票价税合计超过5亿元。

案件中，犯罪嫌疑人首先通过相关政务平台完成注册“皮包公司”，过程中通过平台上注册人的人脸识别是注册成功的关键环节。

为达到目的，犯罪嫌疑人中专门从事人脸识别破解的成员表示，其一般先从他处以30元每个的价格购买他人的高清头像和身份证信息，之后利用“活照片”App对高清头像进行处理，让照片“动起来”，形成包括点头、摇头、眨眼、张嘴等动作视频。

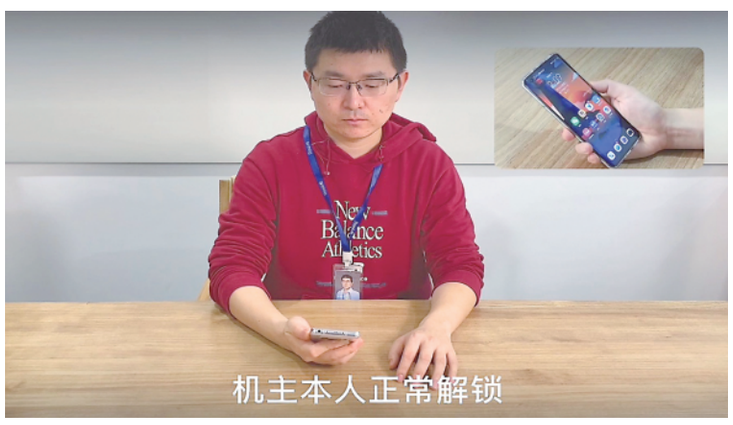
“获取视频后，我们利用特殊处理的手机‘劫持’摄像头，在人脸认证环节时，手机摄像头不会启动，系统获取的是之前做好的视频。系统会认为是本人在摄像头前，最后通过认证。”犯罪嫌疑人说。

同时，该团伙还破解了某广泛用于管理电子营业执照App的人脸识别系统。犯罪嫌疑人下载电子营业执照后，会在App里添加办事员的身份信息。虚开发票团伙就以此通过办事员身份使用电子营业执照。

据犯罪嫌疑人交代，其破解的App类别非常广泛，涉及政务、安防、金融、支付、生活消费等用户量巨大的App。每单的破解价格从25元到300元不等。

15分钟破解19款手机的人脸识别系统

“15分钟破解19款手机的人脸识别系统。”据记者了解，依托清华大学人工智能研究院成立的团队瑞莱智慧近期披露了新的研究成果：研究人员根据一张照片，通过研究算法，制作一副特殊“眼镜”，就可以刷脸解锁他人手机或App身份认证。



图为瑞莱智慧团队研究人员用一副特制眼镜攻破了手机人脸识别系统。 受访者供图

研究人员向记者透露，其团队通过对抗样本攻击，戴上自制眼镜后，15分钟内破解了19款智能手机的人脸识别解锁系统。同样被破解的还包括十余款金融和政务服务类App。

研究人员表示，结合身份证号等个人信息，甚至可冒充机主完成线上银行开户。

“过脸识别技术”群里，黑客成“贵客”

记者发现，网上存在大量提供破解人脸识别技术服务的群组，群名大多采用“过脸”“识别技术”等关键词逃避监管。群人数从100人到300人不等。

在一个名为“过脸识别技术”的群里，有人采取付费的方式邀约群内可以破解支付软件人脸识别审核的人士。黑客，成了人们追捧的“贵客”。

此外，有的群则是对破解技术进行资料、资源分享交流。一个名为“VX三色过脸”的群自称“破解人脸识别技术的扛把子”“适合想入行的新手和小白”，群内多达300人。

名为“蓝叶子”的用户给记者发来一段App人脸识别安防的破解视频，并表示可以出售一台特制的手机。通过导入自行制作的人脸动作视频后，所有在该手机上安装的应用软件，都可以自动跳过人脸认证的环节。每台手机的价格为1650元。

他还告诉记者，虚假的人脸动作视频可以使用“你我当年”“活照片”“轻松换脸”等App完成。

“我们了解到，有的公司上班考勤要进行人脸识别打卡，有员工委托黑客入侵打卡App，利用人脸识别漏洞来完成打卡，每月仅需付给黑客30元。”一位网络安防公司相关负责人向记者透露。

在上述虚开发票案中，犯罪嫌疑人除了利用破解技术从事虚开发票外，还会利用注册新账号从事骗取各类App补贴优惠等违法犯罪。

瑞莱智慧高级产品经理张旭东告诉记者，当前破解人脸识别技术主要是针对活体检测的假体攻击，但针对AI算法自身的对抗样本攻击威胁也逐步凸显。

“由于业界的人脸识别技术主要是固定几个方法，相似度很高。如果黑客提供一个专用于破解人脸识别的开源软件，并在互联网上广泛流传，犯罪分子利用漏洞进行各类App实施违法犯罪将犹如‘入无人之境’。”张旭东说。

在新华三集团安全专家曹亮看来，无论是对抗样本攻击还是针对活体检测的假体攻击，最终目的都是为了骗过“机器眼”。

“当前人脸识别算法大都是人脸上‘三点’‘五点’‘七点’的识别，通过对眼睛、鼻子、嘴、耳朵以及头部活动来实现认证。黑客完全可以通过了解机器内部验证机制和评判规则，再想办法绕过安全防护。”他说。

抓紧查缺补漏，还每一张脸“安全”

专家认为，应尽快排摸国内政务、安防、金融、支付、生活消费等领域的核心App应用存在的相关漏洞，并及时打上补丁，以防发生危害社会安全和财产安全的重大事件。

开展软硬件“对攻升级”。张旭东表示，当务之急应对涉及政务、安防、金融、消费等行业的人脸识别技术漏洞进行完善和升级。

“尤其是对于涉众、涉密、涉及公共利益的相关平台和技术服务提供商，需优先完成技术加固，对手机模拟器要做好防范和拒绝。同时，鼓励和引导更多手机厂商在手机升级时支持3D人脸识别技术。”张旭东说。

“手机厂商在写入手机系统时可内置安全模块，防止黑客绕过手机摄像头启动环节、对摄像头实现劫持，从源头上实现安全守护。”曹亮说。

制定落实人脸识别安全标准。曹亮表示，对核心领域使用人脸识别技术的产品，监管部门可制定并严格实施相关标准，保证产品符合安全技术要求。

“可依据人脸识别在公共或商业应用中对安全的差异化需求，制定分级别、多层次的国家安全标准及行业安全标准。”他说。

加强司法打击，保护每一张“脸”。“违法者可能涉嫌破坏计算机信息系统罪，执法和司法机关应当加强打击力度，形成威慑力。”北京格丰律师事务所合伙人郭玉涛律师说。他建议，当前各大政务、金融、电商等平台都搜集了大量的人脸数据，既存在重复建设的问题，更存在安全隐患和风险。国家和省级层面可建立统一的商用安防大数据中心，以此达到防止人脸信息的滥用、外泄等问题。

“可要求人脸识别算法供应商的模型须在大数据中心内进行训练，实现数据、模型物理上不出专网。算法供应商可租用大数据中心的数据和计算力进行算法模型的升级和更新。”他说。

不给钱就刷差评：起底商业水军“网上碰瓷”索赔套路

本报记者毛鑫

商家：你好，处理纠纷单的。

嫌疑人：你这边想怎么解决呢，我尊重你的选择。

商家：我这边给您补偿50元，商品你也留着用，大家都不容易，你看行吧。

嫌疑人：别人都是588元、488元解决的，以后有事你也可以找我。

商家：优惠点188元吧，大家都不容易。

……

这是发生在2020年11月3日的一段聊天记录，聊天的双方分别是17岁的张某豪与某电商平台商家。15天后，张某豪在当地派出所接受警方调查。

彼时，距离张某豪加入章某强组织的实施网络敲诈的商业水军团伙已有一年。据办案民警介绍，这一团伙以“公益打假”为名，通过组织未成年人及各类闲散人员制造“网上碰瓷”，以恶意评论、灌水等施压手段要挟网店商家索要“保护费”，在电商平台上形成恶劣影响。

不给钱就投诉、刷差评

来自安徽合肥的汪小军怎么也没想到，自己经营一家蛋糕店多年，信誉一直良好，在某电商平台上，竟然被人投诉说“蛋糕中有虫子”。

事情发生在2020年10月24日，一买家从其店中下单一款千层面包蛋糕，到货之后对方即发起纠纷单，并在电商平台聊天界面上说食品有问题，让汪小军私下解决。

买家网名为“您的猪”，称汪小军售卖的蛋糕中有虫子，按照食品安全法规定让其赔偿1000元。该要求遭汪小军拒绝。对方又威胁称，如不答应其要求，会向市场监管部门投诉。因担心平台和监管部门介入后若没处理好，既耽误时间，还影响营业额，汪小军无奈选择妥协，同意了对方“赔偿200元、退款不退货”的要求。

让人意外的是，没几天，汪小军的两个朋友也在该平台遭到买家“您的猪”的恶意投诉勒索。这让他再次确认是遭遇到商业水军敲诈了，于是报警。

面对民警询问，汪小军坚持自己的商品没问题，称只因对方发起了纠纷单，“如果处理不好，平台可能做出降权、扣分，降低店铺的搜索排名等处罚，影响店铺营业。”

警方调查发现，“您的猪”就是章某强。章某强成立了一个涉嫌利用网友实施敲诈勒索的商业水军团伙，该团伙有专门的师傅，收取拜师费之后向团伙成员传授敲诈勒索商家的方法。

广州市公安局南沙分局重案大队副队长邝磊介绍，为确保“碰瓷”顺利进行，章某强团伙在收到商品后，首先通过网购平台聊天软件与商家交涉，简单说明涉假情况后，留下联系方式并要求退款赔偿，对不予配合的商家逐步施压“恶意差评”，如多次提交交易纠纷、恶意举报评论灌水等，向商家逐步威逼。

“对于威逼不成功的商家，该团伙成员会在其同行圈子内群发店铺或商品链接，并组织群内成员对店铺进行恶意下单、退货及差评，甚至从店铺的微博等宣传社交平台入手实施围攻，对商家的客服账号实施恶意举报直至封号，以此作为报复。”邝磊说。

高中生建群收徒敲诈

“碰瓷”蛋糕店不到一个月，章某强被抓。当时他正在江西某职业学院读一年级。他很快向警方交代了自己从事恶意索赔，以及通过社交群组向别人传授恶意索赔经验的过程。

早在上高二时，章某强就接触了恶意索赔。当时，他被一些网友拉进一些关于“网上商城打假退赔”的学习群，他在这些群组里学到了怎样搜索关键字、怎样和商家聊天，有哪些条款作为索赔支撑等。

在他的电脑中，警方发现了大量关于京东、苏宁易购、美团等互联网平台商业场景的恶意索赔方法，其中有关于电动车、水果、牙膏、茶叶、鼻腔喷雾器、植物调和油、篮球鞋，甚至网游兑换码等多种商品的恶意索赔教学内容。

“刚开始，我只是‘吃货’，尝到甜头后，慢慢开始学习向商家索赔现金。”章某强说。

所谓“吃货”，指在网购后以商品三无或其他违规为由投诉，然后逼商家退款，但不退货。

章某强在其制作的一条短视频中，介绍了如何向某社交电商平台水果商家索赔的方法：收货后先手持水果拍照片，画面中要有水果箱、快递单，之后从该平台寻找其他人发的坏水果照片，把坏掉的部分用修图软件“移花接木”到没坏的水果照片上，之后向平台投诉、向商家索赔。

记者了解到，章某强并不知道拉他“入行”好友的真实身份，也没向他们交拜师费，但自己每成功索赔一次，会给“师傅”发一个88元的红包作为“团饭”，这是行规。

2019年6月份，他开始自己收徒，将一些好友拉入自己建的群组，在群内打广告，自诩“白嫖大队”“零撸党”，宣称“不敢说月入过万，好好干月入几千没问题”，让想学敲诈的人向他交拜师费。

按照教授内容深浅程度不同，拜师费分两种套餐：一是388元的“徒弟套餐”，主要教入门级别简单的索赔方法、话术技巧，并偶尔分享瑕疵商品链接等。二是688元的“表弟套餐”，需要提供身份证或户口本进行实名认证，主要教较为全面的索赔思路，包括瑕疵商品链接的寻找思路、与各类互联网平台客服的沟通技巧，以及对商家进行心理控制的顺序步骤等。

随着他生意的火爆，2020年4月1日，章某强18岁生日之后，徒弟套餐涨到688元、表弟套餐涨到888元。到了11月中旬，表弟套餐已涨到1288元。

经查，章某强不断招揽在校学生、社会闲散人员发展下线，组建网络社团“大猪组”，一年来共组建网络群组200余个，发展“学徒”440余名，其中骨干成员36名，仅“拜师费”就非法获利30余万元。

恶意索赔团伙“套路”曝光

负责侦办此案的广州市公安局南沙分局重案大队副队长邝磊介绍，警方查明，该团伙以“招募打假人员-传授犯罪方法-组织围猎店铺-敲诈勒索钱财”的模式实施违法犯罪。

一是研究打假思路，物色瑕疵商品链接。该团伙核心打假人员主要负责研究打假思路，通过各种手段在各大网购平台，寻找使用废止标准的商品、假冒伪劣商品等存在瑕疵的商品，形成“敲诈索赔”思路。邝磊说，一些“山寨”商品因无法提供合法的入货渠道证明而成为打假人员所青睐的瑕疵商品。章某强也坦言，这些卖假冒伪劣产品的商家本身理亏，所以愿意给钱。

二是群发招募广告，线上传授犯罪方法。该团伙核心成员在其圈子内群发“打假收徒”“带赔偿车”等广告，用以往敲诈成功的截图吸引社会闲散人员，以此招收“学徒”。确定师徒关系后，章某强利用网络群组织授课，通过图、文及语音结合的方式讲授索赔技巧，定期汇总各大电商平台的瑕疵商品和服务链接、各种政策规范标准文件及索赔话术，并通过群文件进行分享。

三是恶意差评，逐步施压要挟。为确保“网购碰瓷”顺利进行，该团伙在收到商品后首先通过平台提交交易纠纷，然后与商家进行交涉，留下联系方式并要求退款赔偿。对不予配合的商家，他们会进行恶意举报、差评灌水，并以“封店铺”“上法院”等字眼对商家施压。

特别值得关注的是，该团伙36名骨干成员中，除两人22岁外，其余人员均在15岁至20岁之间。警方表示，该团伙利用未成年人心智未成熟、容易受利诱的特点，不断灌输不正当的牟利方法，新冠肺炎疫情期间，青少年群体的网络线上活跃程度较高，更容易受到这种负面“网赚”氛围的影响。

记者了解到，近年来，全国每年仅市场监管系统收到的恶意投诉举报就多达100多万件。根据对各类平台的调研，商家私下妥协的在500万件以上。

北京消费者权益保护法学研究会副秘书长朱巍建议，市场与网络监管部门应切实履行好监管责任，加强日常巡查，主动受理举报与投诉，将日常执法真正“下沉”到网络空间。社交平台也应承担主体责任、加大治理力度，合力清除这些网络世界中的毒瘤。

警方表示，恶意索赔案件中，有的被害人因敲诈金额小，重视程度不够，愿意息事宁人；有的被害人法律意识淡薄，证据保存意识不够；有的被害人在经营网店过程中确实存在微小过错，担心报警会受到处罚。

公安部在通报中也提醒广大群众，在遭受涉信息网络黑恶势力不法侵害时，一定要沉着冷静，第一时间报警；要保存好聊天记录、交易记录等电子证据；要积极配合公安机关调查取证工作，准确说明情况，并提供涉案账号，方便公安机关深入调查，尽快追赃挽损。