

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

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。”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。

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。

15分钟破解19款手机的人脸识别系统

“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。”一位网络安全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‘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。（据新华每日电讯）

分类天地

服务热线:65917777

家政

■百姓家政:瑞安专业搬家,钟点工服务,专业管道疏通,专业清理化粪池,专业空调维修,电话:66615820。

招聘

■男装定制店诚招店员:2名,形象好,男女不限,有良好的沟通能力和服务意识,有男装销售经验者优先佳,工作地:莘塍,13095779669。

■瑞安董田卫生院诚聘:外科医生、精神科医生、康复医学科医生、妇保医生、药房人员、公共卫生、检验科技师、对外联络部人员各1名,针灸推拿技师5人,护士若干名,报酬面议(有中高级执业资格从优),联系电话:13706642875、13587963221。

定制门窗

■佳思门窗:专业为您定制中空门、断桥窗门、淋浴房、阳光房、金刚网纱窗。电话:18106782333,540588(市府网)。

家电维修

■27年从业经验,精修、安装、清洗:国产、进口制冷设备,疑难故障排除,单位品牌电器整体包修,15867741252。

■瑞丰制冷:空调故障专业维修、鉴定机构,联系电话:18267767246。

求购

■高价购各种旧设备:发电机组、机床折弯机、剪板机、冲床、旧锅炉、制鞋设备、罗拉车、下料机五金化工设备等,13157759176。

搬家

■瑞安百姓搬家公司:居民搬家,长短途搬家、搬运,货运出租,空调拆装等,13967736316。

■专业搬家:公司搬家、居民搬家、事业单位搬家,长短途搬运运输,货运车出租,空调拆装等,13362769032。

转让

■变压器、造粒机转让:(1)800千瓦全套干式变压器1台;(2)双螺杆塑料造粒机,型号:95型1台、65型1台、52型3台、单螺杆2台。联系电话:13705780065陈总。

疏通补漏

■清理化粪池、马桶、下水道、阴沟,空调拆装,钻孔,提供钟点工,18205778338。

注销公告

瑞安市社会治安综合治理协会因不能适应新形势下社会治理的要求,需要注销登记。经本会第一届理事会第二次会议形成注销登记决议,现向社会公告,请债权人在本公告见报之日起15天内向本会申报债权。联系人:林婷婷,电话:65823165。

特此公告

瑞安市社会治安综合治理协会

2021年3月31日

关于对滨江大道四期K0+960~K1+200段实施交通限制的通告

根据瑞安市人民政府专题会议纪要[2020]126号文件,将对滨江大道四期K0+960~K1+200段南半幅进行道路修复,施工期间因工程需要,根据《中华人民共和国道路交通安全法》第三十九条规定,决定于2021年4月6日至2021年5月21日止,对滨江大道K0+960~K1+200段南半幅实施交通限制,北半幅三条机动车道重新组织通行,其中往

陶山及飞云方向设置两条车道,进入市区方向设置一条车道。施工期间,请沿线有关单位与广大市民予以支持配合,并按交通标志指示行驶及服从交通管理人员指挥。

瑞安安阳中心城区开发建设中心

瑞安市公安局交通警察大队

2021年3月31日

遗失

遗失叶涵菲由瑞安市中医院2020年9月8日结算的浙江省医疗机构住院收费收据一张,电脑号:1757857972,住院号:00138525,金额:7818.5元,声明作废。以上费用未在其他地方报销。

遗失宋培林由瑞安瑞生微创外科医院2021年3月29日结算的浙江省医疗服务(住院)发票一张,发票号码:00277676,发票代码:133031931239,住院号:202101608,金额:5976.99元,声明作废。

“讲文明 树新风”公益广告

节约用电

 随手关灯一小步，节约能源一大步。

低碳生活

 倡导低碳生活，呵护生态家园。

瑞安市宣传部

瑞安日报社