保定晚报编辑部主办 E-mail:bdwbzbs@126.com 责编:盖继文

换脸、代过、写代码……

AI很“忙”,别当法“盲”!

□新华社记者 周闻韬 宋立崑

随着AI技术不断发展,一些新型违法犯罪行为开始冒头,给网络空间安全和群众人身财产安全带来威胁,记者采访多地公安机关,揭示犯罪手法,提升防范意识。

图片由AI生成

学AI,竟为“换脸”行骗

“你们公众号怎么开始推荐投资理财App了?靠谱吗?”今年6月10日,某机构工作人员像往常一样打开公司公众号评论区,却被一连串粉丝留言惊出了一身冷汗。

工作人员发现,其运营的公众号不知何时竟发文称即将停更,并号召粉丝关注另一个投资理财类账号。工作人员尝试登录账号后台,发现不仅密码被修改,连公司法人代表信息都被篡改了。

意识到事态严重,工作人员第一时间报案。这也是湖北省首起利用AI换脸技术非法侵入计算机信息系统案。

接警后,武汉网警迅速成立专案组,研判发现被盗公众号的操作痕迹为:犯罪分子通过“AI换脸”技术,更换了公司法人信息,又用新的“脸”识别登录该账号,进而发布涉诈引流信息。

顺着线索追踪,专案组很快锁定了远在山东潍坊的犯罪嫌疑人阿成(化名)。

站在民警眼前的阿成,衣着朴素,从事大棚种植,一度令警察怀疑追错了人。但对其住所搜查时,办案民警通过技术手段从其电脑已删除的电子数据中,找到了大量AI换脸素材及非法所得的虚拟货币。

原来,阿成本是美术技工,嫌寻常做图收入不高,就改行务农,又动了做AI图挣“轻松钱”的歪脑筋。

2022年5月,他在外网接触“人脸代过”灰色产业,加入相关群组后,先在各类小型电商平台接单制作人脸图像,每张收费200元;随着技术提升,他掌握了生成动态人脸视频的方法,“报价”也水涨船高,破解一张AI动态的人脸最高能卖到1000元。案发时,已非法获利40余万元。

“跑马机”作弊成黑产

还有不法分子瞄上培训学时,用AI帮人“打卡”。

今年3月,重庆警方侦查发现,一些驾校学员无需实际练车即可刷满学时,背后是不法分子使用“跑马机”并结合AI技术实施作弊。这一犯罪链条涉及生产、销售、使用等多个环节,已形成黑色产业。

什么是“跑马机”?重庆市南岸区公安分局网安支队民警介绍,这是利用汽车脉冲信号原理制作的设备,其核心功能是通过侵入并篡改驾培计时系统,并运用AI技术模拟学员动态人像,达成伪造培训记录目的。

通过涉案资金追溯显示,利益链条的源头是驾校为了降低运营成本,以提供“快速拿证”为噱头,吸引学员大量报名缴费获利。与此同时,上游负责销售“跑马机”的黑代理商也获利不菲。此外,部分驾校还外接订单“代打卡”获利,其规模化运作模式显示,涉“跑马机”犯罪已演变为机构化犯罪。

截至目前,重庆警方已打掉涉案违法犯罪团伙2个,抓获犯罪嫌疑人70名,查扣“跑马机”设备384台,查处涉案驾校34家。

AI写代码,竟成了黑产源头

今年2月,重庆万州区网安部门发现,辖区犯罪嫌疑人王某针对某社交软件开发群控程序。经调查,一个使用黑产软件从事各类违法犯罪的团伙浮出水面。

据万州区公安局网安支队民警介绍,大专学历的王某自学掌握相关技术后,开始招募多名同伙用AI技术编写程序代码,制作各类黑产应用程序。这类黑产软件无需使用官方客户端,即可直接与后台服务器进行数据交互,具有“多开”“群控”“批量管理”等功能,可实现批量发送消息、红包等操作。

令人惊讶的是,王某还根据下游团伙的犯罪需求,“定制”出各种黑产软件,成为赌博、网络水军、电诈等多个犯罪链条的技术源头。

比如,一到案的犯罪嫌疑人曾是电商从业者,因觉得来钱慢,便与王某技术对接,“转行”专门从事刷单水军活动,其在城中村租下一套房子设立“工作室”,招募多人加入。抓捕时,警方在房间里当场查获多台用于作案的电脑和手机。

目前,专案组已顺藤摸瓜,先后打掉位于重庆、福建、江苏等地从事黑产软件开发及网络水军犯罪团伙4个,抓获犯罪嫌疑人15名,查获各类黑产程序软件25个,查扣资金500余万元,作案电脑、手机100余台。

AI时代已来临,新技术能做的事越来越多,也越来越有想象力。但筑牢安全底线的第一守则就是:AI可以很“忙”,但使用它的人不能法盲。掌握AI技术的专业人员,切勿因贪欲走上违法犯罪道路。同时各方应加强技术监管,进一步完善生物特征检测等AI时代的防伪技术,强化落实对个人隐私和信息的技术保护和法律责任。

据新华社

图为重庆市网安干警正在研判案情。(重庆市公安局供图)

保定新闻传媒中心(集团) 宣