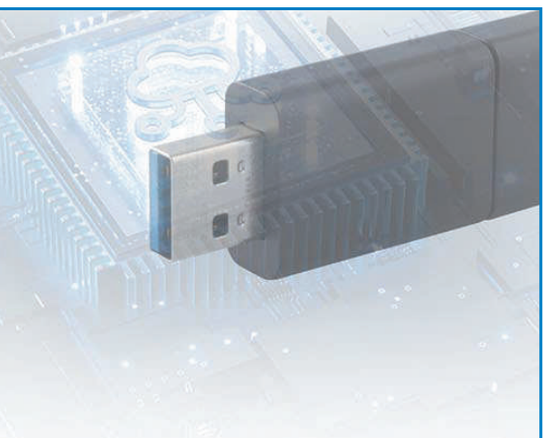
严惩利用技术手段牟利犯罪

售卖盗版加密狗 解锁医疗设备安全系统

检察机关起诉一起规避技术保护措施类侵犯著作权案



新闻眼

□本报通讯员 张熠 朱鹏锦

◆背景知识小贴士

技术保护措施是权利人用于保护和管理作品著作权的技术手段,可分为接触控制措施与版权保护措施。其中,接触控制措施一般表现为身份认证软件、口令验证程序等形式,其作用主要是防止他人未经许可接触作品,就好比权利人为作品安装了“一把锁”。

本是医疗设备的维修人员,却在QQ群中购得50套盗版加密狗(一种破解版密钥,可以通过CT、血管机、超声等医疗设备身份认证系统核验的数字证书),并进行售卖。该盗版加密狗可以在未经医疗机构内部授权的情况下,直接打开医疗设备安全系统的“大门”。经上海市普陀区检察院提起公诉,4月12日,被告人刘某因侵犯著作权罪被法院判处有期徒刑一年二个月,适用缓刑,并处罚金8万元。

2022年2月,公安机关在工作中发现,有人在某二手交易平台上销售破解版医疗设备密钥,涉嫌侵犯知识产权犯罪,遂立即开展调查工作。同年7月,犯罪嫌疑人刘某被抓获归案。不久,该案移送普陀区检察院,该院立即启动疑难复杂案件分配机制,选派精干力量办理此案,依法引导公安机关侦查取证。

刘某是一名科技公司的医疗设备维修人员。他供述称,“这些加密狗主要是为辅助维修使用的,由于近几年医疗设备升级保护措施,进入医疗系统的维修界面需要授权,加密狗主要起到了破解作用。”

2020年9月,刘某在“医疗设备维修”QQ群中以8万元的价格购买了50套盗版加密狗,每套均由一个读卡器和一张芯片组成,使用时只需将USB接入医疗设备主机,在自动弹出的对话框中统一输入预设密码,即可完成身份认证。“这些加密狗插在普通电脑上是没有反应的,也看不出里面是什么东西,只有插在既定的医疗设备主机上,才能被识别。”刘某称他并不清楚盗版加密狗的制作流程,只知道它对维修医疗设备必不可少。

“维修设备需要检测、查看运行日志、确定故障来源,有时还需要重装系统、更换电子模块,这些都必须通过安全系统验证来实现。”刘某将这些加密狗以每个数千元的价格在网上加价出售,一名下游买家表示,其曾用加密狗为客户重装系统20余次,共收费5万余元。

据医疗设备生产企业反映,为了确保设备安全,正版加密狗只向经审批的内部人员授权,或者是向签订协议的客户维修人员发放,从未对外销售。

除了销售加密狗,刘某还在网上获取并销售医疗设备的算码器软件(维修时所用的密码生成软件)和载明了版权声明、标识了著作权属的维修专用说明手册,这些均被他整理后放在网盘里,通过分享网盘链接进行交易。

事实虽已明晰,但刘某的行为是否构罪、构成何罪、如何量刑,需要认真研判。为此,普陀区检察院多次组织召开检察官联席会议进行研讨。经讨论,该院认为,刘某未经著作权人或者与著作权有关的权利人许可,故意避开权利人采取的保护著作权的技术措施,销售加密狗的行为已涉嫌犯罪。

“技术保护措施是权利人用于保护和管理作品著作权的技术手段,可分为接触控制措施与版权保护措施。其中,接触控制措施一般表现为身份认证软件、口令验证程序等形式,其作用主要是防止他人未经许可接触作品,就好比权利人为作品安装了‘一把锁’。公众只有向权利人申请获得了钥匙(密钥工具、用户名、密码等),才能浏览使用作品。”检察官解释道,“本案中,涉案企业为保护自身维修软件、文字作品的著作权及系统安全,专门开发了安全防护系统软件,并部署用于医疗设备终端;使用人必须首先登录安全防护系统,并使用涉案企业授权发放的加密狗工具,通过系统的身份认证,才能解锁使用被隐藏限制的软件功能及加密文件。因此,加密狗的性质就是企业为保护著作权而采取的接触控制措施。”

“刘某通过网络等渠道,向他人销售、提供破解版加密狗是间接规避技术保护措施的行为。一般来讲,直接动手破解技术措施属于直接规避技术保护措施的行为;隐藏于幕后,制造、进口或者向他人提供用于规避技术保护措施的装置、部件或者技术服务的,属于间接规避行为。直接规避往往只有一个侵权人,而间接规避则可能引发下游人群连锁侵权,对著作权人的权利侵害更重。”检察官补充说道。

“针对刘某销售盗版加密狗的行为,我们也排除了认定其为‘销售侵权复制品’。”检察官介绍,“销售侵权复制品罪主要规制的是小摊贩销售盗版图书、光盘等行为,其社会危害性相对较小,但是刘某的行为导致医疗设备上的维修软件处于‘大门敞开’的状态,他人得以自由地接触、使用加密文件,下游买家基本是医疗设备专业维修人员而非普通民众,‘销售侵权复制品’无法充分准确地评价上述行为。相关司法解释也明确指出,实施侵犯著作权犯罪,又销售该侵权复制品,构成犯罪的,应当以侵犯著作权罪定罪处罚。”

法眼观察

别让『霸王式』扫码成为消费自由的『拦路虎』

□何慧敏

近日,有消费者在北京某餐馆用餐后开发票时,被要求必须扫码关注某公众号才能开具发票,“不关注就拿不到公司抬头”(据4月17日《北京青年报》)。

扫码开发票、扫码点餐、扫码交停车费……在如今的“一码通”时代,扫码线上操作看似自主便捷,却在悄然间成为餐饮商家推广引流的新渠道,有的商家为了绑定用户持续推广消费信息,增强用户黏性,要求消费者强制关注相关公众号,上传个人信息,否则谢绝提供服务。此类强制关注、收集信息的行为实则绑架了消费者自主选择的权利,损害了消费者权益。

我国消费者权益保护法明确规定,经营者向消费者提供商品或者服务,不得设定不公平、不合理的交易条件。国家互联网信息办公室新修订的《互联网用户公众账号信息服务管理规定》提出,未经互联网用户知情同意,不得以任何方式强制或者变相强制订阅关注其他用户公众账号。中国消费者协会也发文明确强制扫码点餐、强制关注公众号或授权个人信息的行为违反消费者权益保护法。然而现实中为了实现点单、开发票等目的,消费者被迫历经“关注”“注册”“上传用户名、手机号、生日、性别”等个人信息的重重考验。而且,很多时候历经“磨难”得到的,却是基于用户信息收集后的精准营销、广告轰炸,更有甚者,个人信息被挪作他用,用户陷入信息泄露风险。如此场景下,商家给予的不是数字化服务的“温情脉脉”,而是以强制关注代替征求同意,以索取信息代替自愿分享,是用“不关注不能吃”的霸王逻辑倒逼消费者让渡自主选择的权利。这种“形式上自愿、实质上强制”的交易行为涉嫌侵犯消费者权益,既不合理更不合法。

强制扫码关注行为本质上是限制消费者选择权,在关注之后设置“授权登录”“注册信息”等重重门槛则涉嫌强制收集消费者信息,两者均侵害消费者权益,必须严肃整治。的确,商家重视宣传,提高用户转化率是经营之需,但是注重推广引流的同时也应当严格遵守法律法规、商业伦理,毕竟做生意不是一锤子买卖,需要的是良好的服务体验带来的细水长流,这其中就包括尊重用户自主权,主动保护用户信息安全。商家不应在限制用户点餐、开票等小问题上玩心思,而应该积极主动提供线上、线下服务渠道供消费者自主选择,在扫码小程序上减少不必要的登录、授权环节,别让“强制”挫了好感,别让“绑架”毁了形象。

同时,为商家提供公众账号信息服务的网络平台应当守土有责,进一步规范公众账号推荐订阅关注机制、严格落实二维码使用识别标准,明确用户信息收集边界,加强对公众号的巡查和整治。对于“霸王”式强制扫码、违背用户意愿的信息收集行为及时采取断链、禁用措施,以严厉惩处形成震慑。而且,要进一步畅通互联网投诉机制,不仅要在平台界面上建立一键投诉渠道,更应探索在相关使用界面提示维权方法,引导用户主动举报。相关部门也应加强执法巡查,对于屡教不改的商家予以严惩。

“黑”进公司网站盗转资金

3人因盗窃罪获刑罚

◆背景知识小贴士

有些公司采用某种分布式开发框架搭建网站后台,后台会产生一个默认账号和密码,使用默认账号和密码登录后可以获得框架后台的服务器最高权限,这意味着可以对网站进行任意操作。

本报讯(记者史隽 通讯员沈玲) 数字支付在带来便捷的同时,也隐藏了巨大的风险。有人就挖空心思当起了黑客,铤而走险利用公司网站框架漏洞牟利。日前,经浙江省杭州市富阳区检察院提起公诉,法院以盗窃罪分别判处被告人陈某等3人有期徒刑八年至一年两个月不等,各并处罚金。

陈某大学读的是计算机专业,毕业后一直待业在家。时间一久,陈某便着急起来,想要找个赚“快钱”的工作。2021年7月,陈某在上网时无意间发现了一则帖子,内容是教人如何当黑客赚“快钱”,便立即研究起来。

原来,有些公司采用某种分布式开发框架搭建网站后台,后台会产生一个默认账号和密码,使用默认账号和密码登录后可以获得框架后台的服务器最高权限,这意味着可以对网站进行任意操作。为获得操作权限,陈某加入了一个技术交流群,群里会发布破解软件以及如何操作该软件的文档。此外,该软件的开发公司旗下还有一款搜索引擎,可以搜索出网站的服务器类型、开发框架等,并识别出网站的安全性能级别。

因该搜索引擎需付款使用,陈某便注册了会员,通过搜索引擎筛选出特定框架结构的网站,再用默认的账号和密码去登录这些网站。大部分网站因后台密码被修改过无法登录,但陈某仍不断尝试。没多久,陈某在登录江苏淮安一公司网站后台时,发现默认密码没有修改。陈某惊喜不已,登录网站后台后顺利拿到了服务器权限,并发现了公司的支付宝账号和密钥等支付信息。随后,陈某通过技术手段将该公司2.4万元资金分3次转入自己的账户,用于日常消费和还债。

尝到甜头后,陈某继续寻找公司网站框架漏洞,甚至对很多公司网站进行背后攻击和转账。为了将钱转移得更为隐蔽,陈某找到朋友何某和梁某,让二人提供银行卡账号,将违法所得转至他们名下后,再转回陈某的另一网络钱包。

2022年1月,杭州某公司的会计在对账时发现公司有异常出账情况,经查看后确定公司于2021年12月至2022年1月被转走了30余万元。会计汇报了这一异常情况后,公司老板召开紧急财务会议,最终从账面流水上确定30余万元资金被转至何某和梁某名下的银行账户。老板随即报警。

此后,海南三亚、福建漳州等地陆续接到公司资金被盗转的报警。公安机关立即根据相关线索展开侦查,陈某等3人先后落网。经查,2021年8月至2022年1月,陈某单独或伙同梁某、何某,利用网络技术手段侵入被害公司资金账户,将资金转至自己账户。其中,陈某涉案金额为40余万元,梁某和何某涉案金额为30余万元。2022年10月,公安机关以涉嫌盗窃罪将陈某等3人移送富阳区检察院审查起诉。

“我们只是帮陈某转账,为什么也要定盗窃罪?”针对罪名定性,梁某提出疑问。检察官经审查认定,陈某让梁某、何某二人提供银行卡转账前,已将其盗窃公司资金的行为方式进行告知,二人在事先明知陈某盗窃被害单位资金的情况下,不仅提供自己的账户接收盗窃所得赃款,且参与操作转账,应认定为盗窃罪共犯。

最终,检察机关认为,陈某等3人以非法占有为目的,利用网络技术手段秘密窃取公司财物,犯罪事实清楚,证据确实充分。2022年11月,富阳区检察院以涉嫌盗窃罪对陈某等3人提起公诉。日前,法院作出上述判决。

姚雯/漫画

案讯点击

将面包车改装成“加油车” 被判危险作业罪

本报讯(记者简洁 通讯员佟萌 张照天) 柴油易燃、易爆,属于危险化学品。然而,有人却将面包车改头换面,伪装成市政工程车辆,用于储存销售柴油。近日,经北京市石景山区检察院提起刑事附带民事公益诉讼,被告人刘某因危险作业罪被法院判处有期徒刑六个月,适用缓刑,负担后续无害化处置费用,并在省级以上媒体公开赔礼道歉。

刘某在北京开设了一家机械设备租赁公司,2019年初,他发现一些建筑工地的挖掘机需要加柴油,便开始寻找门路。刘某从可以低价批发到柴油的郝某(另案处理)处购进柴油,再高价转卖给工地,从中赚取差价。为了储存买来的柴油,刘某购买了一辆报废的洒水车和一辆厢式货车,焊上自制油罐,停放在租来的小院里,专门用于储油。他还买来两辆面包车,自行加装了油箱、加油管和加油枪,用于向工地运输和销售柴油。不仅如此,刘某还对运油的两辆面包车进行了“包装”,将车身喷成橙色,绘上“工程车”字样,伪装成市政工程车辆,从而降低上路后被检查的风险。

2021年2月,警方在打击黑加油站和销售不合格成品油专项工作中,发现了刘某非法销售柴油的窝点,起获并扣押了封闭货车2辆、蓝白色储油车1辆、厢式货车1辆等。

案件移送审查起诉后,石景山区检察院审查认为,刘某在未获得相关资质的情况下私购柴油并出售牟利,且储存柴油时没有加装专业的防雷防爆装置等安全设施,其行为存在安全生产风险。为进一步查实危害性,该院检察官多次前往刘某居住地实地走访,发现小院位于浅山区,附近有桥梁、草地和树林,房屋与住户较多,还有一座寺庙,属于不可移动的文物。小院门前是一条行车主干道,来往车辆络绎不绝,路边还有排布密集的高压电线。经安全评估机构评估,小院现场存在8项不符合国家有关安全生产法律法规、标准规范要求的情况,一旦引发火灾,可能造成不特定人员伤亡和财产损失,损害社会公共利益。

2022年12月,石景山区检察院以涉嫌危险作业罪对刘某提起公诉。同时,因刘某的行为可能损害社会公共利益,应承担相应民事责任,该院依法提起刑事附带民事公益诉讼,要求被告人消除存在的安全生产危险,对储存柴油的报废洒水车、改装过的厢式货车进行无害化处置,并在省级以上新闻媒体公开赔礼道歉。鉴于刘某到案后能如实供述自己的罪行,自愿认罪认罚,法院日前作出上述判决。

社址:北京市石景山区香山南路109号 邮编:100144 传真:(010)86423503 86423653 总编室:(010)86423352 出版发行部:(010)86423399 订阅发行:全国各地邮局 定价:每份2.00元 全年398元 印刷:工人日报社(北京市东城区安德路甲61号)