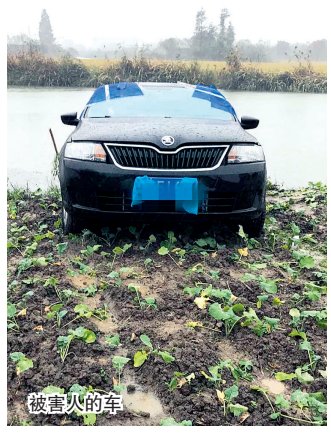
递出一张名片,招来杀身之祸
49岁网约车女司机凌晨接客遇害
嘉兴警方5小时破案

本报记者 陈佳妮 通讯员 钮宇萍

“警察同志,这里有一辆黑色轿车,开着门,没司机……”11月21日上午9点45分,嘉兴南湖警方接到群众报警。

南湖警方赶到位于嘉兴市南湖区七星街道某河道边时,发现停着一辆黑色的斯柯达轿车,后座上有少许血渍。在河道中,警方打捞上了一具女尸……


被害人的车


警方在现场勘查

网约车女司机深夜跑单遇害

“尸身颈部、腰部、上腹部有多处开放性刀伤,我们确认这是一起侵害性案件。”南湖区公安分局刑事犯罪侦查中心重案队队长张春伟,在勘查了现场后,神色有些凝重。

随即,南湖分局启动重大刑事案侦破机制,兵分多路,通过技术手段侦查。

警方很快明确了被害人的身份,杜女士,49岁,河南人,在嘉善摆地摊,是某平台的网约车司机,也是现场发现的黑色斯柯达轿车的车主。

平时,没活的时候,杜女士会给路边的人发名片揽揽活。她有两个孩子,女儿今年刚刚成家,儿子正在读大学,兄弟姐妹都住在嘉善。

在掌握被害人为网约车司机这条线索后,民警通过技术侦查手段,锁定了2名嫌疑人,并立即展开调查。

21日下午3点左右,南湖警方在嘉兴市区某小区内,成功将犯罪嫌疑人孙某、张某一举抓获。目前,2名犯罪嫌疑人因涉嫌故意杀人罪已被南湖警方刑事拘留。

据了解,孙某、张某两人均在嘉兴七星厂里打工,两人是租房内的邻居。其中,犯罪嫌疑人孙某,30岁,江苏人,曾因抢劫罪被判刑7年;而犯罪嫌疑人张某,贵州人,刚满18周岁。

本想“碰瓷”却下了毒手

面对上门来的民警,孙某和张某十分惊讶,很快便坦白,对两人合伙实施的杀人抢劫事实供认不讳。

“11月20日晚上8点左右,我们打车来到嘉善县一酒吧门口,因为没钱花,想找代驾的人‘碰瓷’敲点钱。”孙某说,但直到半夜,都没有等来“碰瓷”的对象。

就在两人等待的时间里,轿车司机杜女士从两人身旁经过。

“需要乘车吗?”杜女士问,孙某和张某拒绝后,杜女士给了他们一张名片,还告知对方,如果需要打车,可以电话联系她。

此时,两位嫌疑人还未打算加害杜女士。

又是2个小时的等待,“碰瓷”对象还是没有出现。孙某和张某失去了耐心,决定约杜女士出来,对她实施抢劫。

谋完财又害命,将女司机扔进河里

为了躲避事后警方的追查,有犯罪前科的孙某向一位陌生人借了电话打给杜女士。当时,杜女士正准备睡觉,但她想着再多赚点钱也好,便在10分钟后到达酒吧门口,接走了孙某和张某。

杜女士一路开车,将他们从嘉善载到嘉兴。到达后,孙某对杜女士说,要去家里拿东西,再去朋友家。实际上,孙某是去拿了作案用的工具——15厘米长的一把剪刀。

随后,当车子开到南湖区320国道杨庙路口往东200米时,孙某和张某凶相毕露,他们拿出凶器,抢劫了杜女士的一条金项链,还有钱包内的700多元现金。这之后,两人还用剪刀威逼杜女士,获取了她的银行卡密码,并且当场将杜女士捅伤令她失去行动能力。

孙某和张某开着杜女士的车子,在附近一处ATM机里,取走了银行卡里的4800元存款。之后,他们把车开回事发地,将被害人和作案工具扔进了河里。原本,他们还想毁了车子,但轿车卡在河岸上,两人只好先离开了案发现场。

21日,两人坐车去湖州,准备把抢劫来的金项链换成现金。由于金银市场监控严格,兑换金银饰品需要对身份证进行备案,两人只好用抢来的27.3克的金项链换了一条27克的金项链,并用“洗白”后的项链换取了6800元现金。

目前,赃款已经全部追回,案件还在进一步调查中。

点开陌生短信链接,银行卡里的钱立马不见
金华警方破获利用木马病毒盗刷银行卡案

新华社 方列

“上次聚会的视频赶快去看哦”“这是我和你老公的开房视频”……这些吸引眼球的手机短信,相关的链接实质上隐藏着木马病毒。如果你缺乏警觉打开查看,手机就可能被植入木马病毒,个人隐私、金融财产等信息将面临被泄露和盗取的巨大风险。

近日,金华市公安机关侦破了一起专门利用木马病毒盗刷银行卡案件,破获系列案件300余起,涉案金额达1000余万元。为了共同的犯罪目的,该犯罪团伙诈骗形成“供、销、产、售”完整的犯罪产业链条。仅浙江省内,就有10多万人收到过此类短信,数万人手机中木马。

一条短信 引出木马诈骗“黑色产业链”

2016年3月23日下午,金华市民林女士的手机收到一条短信,内容为:“我们的聚会录像,发你一份,进入网址查看。”

林女士前段时间确实曾参加过同学聚会,随手在手机上点击了链接。让林女士没有想到的是,点击“聚会录像”后的数小时里,她的银行账户被多次快捷支付,金额一共是2200元,而林女士并没有收到过任何支付提醒。

接到报案后,金华市公安机关并没有因为该案案值小而忽视,而是结合当时全国多地电信诈骗高发的实际,启动合成作战应对机制,对相关案件进行串并,发现仅3月份,浙江省内就有同类案件30多起,涉案价值30余万元。

分析表明,“聚会录像”就是木马病毒,而木马的制作、群发木马短信、盗刷银行卡、公民身份信息获取等环节靠三五个犯罪分子是无法完成的,小案子后面极有可能牵扯着巨大的“黑产业”。

警方对诈骗短信内容中涉及的网址进行分析,发现该网址绑定了一个邮箱,内存大量被害人手机短信和通讯录等内容的邮件。警方由此顺藤摸瓜,掌握了犯罪嫌疑人的活动规律。4月1日,在广西南宁警方的全力支持下,浙江警方在广西宾阳县一家商贸有限公司里一举抓获蒙某等4名广西宾阳籍犯罪嫌疑人。

在抓获蒙某等4名主要犯罪嫌疑人后,警方以此为突破口,针对上下游整个“黑产业链”的每个环节展开全面深入的调查取证。经过近半年的调查,办案民警对发送木马短信、制作木马程序、出售木马程序、贩卖公民信息、贩卖银行信息、盗刷银行卡等6个犯罪环节中数十名犯罪嫌疑人进行了落地查证。警方在全面掌握整个犯罪团伙脉络的情况下,辗转11省16县市,展开抓捕行动,共计抓获犯罪嫌疑人35名。

犯罪团伙分工协作 个别机构工作人员参与其中

随着调查的深入,本案除最早抓获的发送木马短信实施盗窃的团伙外,幕后还有出售手机木马、出售公民信息、出售银行卡信息、盗刷银行卡资金等众多人员参与,虽然他们相互之间并不认识,但在互联网这个虚拟平台上,为了共同的犯罪目的,形成“供、销、产、售”完整的犯罪产业链条。

让办案民警没有想到的是,在这些涉嫌犯罪的人员当中,个别银行和机关单位工作人员,也参与了其中如公民身份信息、银行账户信息等出卖交易,成为整个犯罪链条中不可缺少的重要一环。

据犯罪嫌疑人交代,蒙某等人从单位内部工作人员处获取了部分公民的身份信息、手机号码等,编辑文本后,进行短信群发。被害人一旦点击链接,手机即中木马,手机短信内容和通讯录就会自动转发到绑定的邮箱内,然后蒙某等人又将木马短信继续推送给被害人手机通讯录中的好友,从而木马植入的成功率被成倍扩大。

嫌疑人从被害人处获取到短信内容后,会将其中涉及被害人名字、银行卡、身份证号码、手机号码等信息,发送给出售公民和银行信息的犯罪嫌疑人,购买完整信息,蒙某等人再将信息发给盗刷银行卡资金的犯罪嫌疑人(俗称“洗料员”)。“洗料员”根据所提供的银行卡号、验证码等信息以第三方支付形式进行消费套现,赃款和犯罪嫌疑人分成。

完善法律法规加大打击力度 铲除电信诈骗土壤

浙江省刑侦总队相关负责人说,当前各类电信诈骗案中,钓鱼木马诈骗占了相当的比例,由于其极具隐蔽性,防范难度较大,作案的成功率极高。其中一个很重要的原因是个人信息泄漏,给了诈骗分子精准实施诈骗犯罪的机会。

阿里巴巴资深安全专家虞煜军说,一些互联网技术黑色产业链相关软件、平台的存在,为下游黑色产业链犯罪团伙提供了技术、软件和相关服务,严重破坏互联网正常秩序。

一些办案民警表示,在治理和打击实践中,对诈骗产业链各个环节的人员,比如木马病毒的研发者、贩卖者,往往需要论证其恶意目的“唯一性”,作为执法依据,根据当前的法律法规,很难认定其犯罪,大大增加了打击难度。

我国目前法律、法规以及有关规定,只对部分涉及非法获取、买卖公民个人信息的行为和涉及非法侵入计算机信息系统的行为有明确的法律规定,但对各类恶意软件的制作、销售,以及各类组织地下交易的综合恶意平台,其违法性均没有明确认定,更没有明确的处罚、管理机制出台。

浙江赞程律师事务所程学林律师认为,对于诈骗黑色产业链的各个环节,如果有明知他人利用其环节进行犯罪行为的,比如根据使用者的具体犯罪需求定制钓鱼木马,应根据使用者所实施的具体行为按照共同犯罪处理。