苹果ID被盗背后,藏着三波黑客


作案工具

本报记者 陈佳妮 通讯员 叶婉莹

近一年来,全国多地都发生过苹果手机用户发现自己苹果ID被盗,继而被莫名其妙地扣款,据报道,损失达万元的并不在少数。这背后,其实是黑客的作为,并且他们的手段还在不断“升级”。

日前,金华江南警方便摧毁了这样一条新型的黑色产业链——黑客团伙A,以黑客手段获取苹果ID账号和密码;黑客团伙B,以黑客手段获取境外银行卡信息;最终,团伙C购买这两方的信息,用A的ID绑定B的境外信用卡,从而进行盗刷。

昨日,警方公布了案件详情。

最初的线索,来的有些意外。今年1月22日,金华江南警方接到一起盗取女友支付宝钱款的报警。案件很快就侦破了,嫌疑人朱某落网。但就在警方对朱某的手机进行调查时,却发现了不寻常的线索——朱某极有可能在从事盗刷信用卡的犯罪行为。

在证据面前,朱某开了口:“我都是和‘深哥’联系的,一起买苹果账号和信用卡,然后从信用卡里面刷钱。”

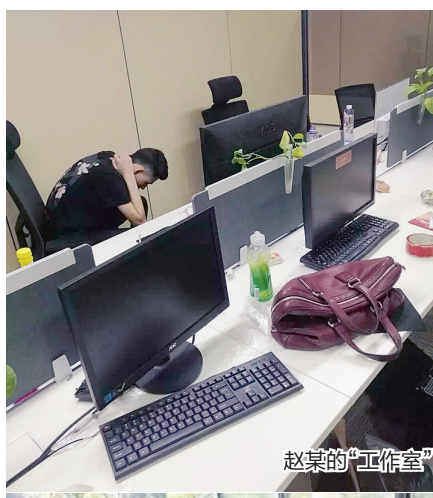
“深哥”是谁,他们又是怎么盗刷信用卡的?警方经过步步深挖,查明了“深哥”的身份。“深哥”是宁波人,姓赵。2016年,他在逛网络论坛时发现了一条“发财路子”,可以神不知鬼不觉地盗刷国外的信用卡。10月,赵某就在奉化开起了工作室,专门研究操作办法。

赵某主要联系2个黑客团伙,一伙是苏某兄妹,他们专门利用黑客技术手段获取大量他人的苹果账号和密码,并以5元至20元不等的价格贩卖;另一伙,是早年就混迹于黑客圈,以张某、骆某为首的一个犯罪团伙,他们到境外网络环境下利用黑客技术手段,获取了大量外籍人员的银行卡信息,并在网上以5元至70元不等的价格贩卖。

拿到“素材”之后,赵某团伙将境外银行卡与苹果ID账号进行绑定后,再通过特殊渠道进入境外网络环境,在苹果APP市场通过购买视频网站会员、充值卡等方式盗刷银行卡,最后再将这些盗刷出来的充值卡和会员账号,在第三方平台进行销售变现。

今年5月26日,赵某将奉化的工作室迁到福建莆田市区,与新的合伙人黄某合作,继续进行盗刷银行卡违法活动。

此刻,赵某并不知道自己已经被金华警方盯上。8月15日,金华警方在全国收网,抓获盗刷团伙嫌疑人共40名。9月30日,因涉嫌侵犯公民个人信息罪,非法获取计算机信息系统数据罪,赵某等23名犯罪嫌疑人被移送至金华市婺城区检察院审查起诉。另外,骆某等17名犯罪嫌疑人也因上述罪名被采取刑事强制措施。目前,警方还在对此案做进一步深挖。


赵某的“工作室”


抓获嫌疑人

离奇!半夜银行卡被盗刷都发生在方圆500米内

四川警方破获该省首例“嗅探”犯罪案

《华西都市报》董兴生 王攀

在睡梦中,自己的手机被远程控制,犯罪嫌疑人不仅可以盗刷银行卡内的资金,还可以控制自己的购物APP,透支消费或贷款。这种令人毛骨悚然的事真实发生在四川什邡市50多位市民身上。近日,四川什邡警方破获了该省首例“嗅探”犯罪案件,抓获了3名犯罪嫌疑人。

一觉醒来 银行卡被盗刷还背上贷款

今年7月27日早上7点,什邡市民陈女士睡醒后打开手机一看,顿时吓得困意全无。“手机里收到上百条短信,大部分都是各种验证码,还有七八笔转账信息,加起来共2万多元。”陈女士说,更为诡异的是,一夜之间,自己的手机上还开通了一种支付功能。每一笔转账,也是通过这一功能完成。

比陈女士还郁闷的是王先生。“4月19日早上8点钟,我发现手机上多了一个购物APP,自己贷了1.2万元,这笔钱到账后又被转走了。”而什邡市民乔大姐,紧赶慢赶都没有跑赢犯罪者。“8月26日早上,我看到银行卡里被刷了200元,觉得不对劲,就赶紧往银行跑,在路上,又被刷了两笔,分别是5000元。”乔大姐说,等他跑到银行时,卡内的资金已被转走1.7万元。

直到先后在派出所报案后才知道,陈女士、王先生和乔大姐都住在东门桥一带,距离不超过500米。而实际上,从今年2月份到9月份,仅在这一片区,就先后有50多人中招,损失的资金总额近60万元。

“嗅探”犯罪 不同于电信诈骗不需要互动

什邡市公安局刑警大队大队长李小虎告诉记者,接到报案后,该大队成立了专案组,对此类案件进行梳理。梳理结果令人震惊,“从2月份到9月份,期间发生了50多起类似案件”。

尽管此前公安机关对此类案件进行了调查,但都是按照普通电信诈骗的方法侦办,所以进展并不理想。“经过研判,我们发现这类案件与以往电信诈骗有很多不一样的地方。”李小虎说,除了案发时间都在凌晨外,案发区域也都集中在什邡市区东门桥一带,方圆500米之内。

李小虎介绍,此类案件还有一个最大的特点,就是嫌疑人不需要与被害人产生任何互动。“被害人没有任何配合操作,都是被动接收短信,不明不白的银行卡里的钱就没了。甚至还会‘帮’你在网上贷款。”

专案组深入研究后确定,这不是普通的电信诈骗,“而是目前国内新型网络犯罪,叫‘嗅探’”。对作案手段有了掌握后,警方发起多警种破案,掌握了3名犯罪嫌疑人的行踪。11月7日凌晨,警方收网,抓获了3名嫌疑人,并起获了一台嗅探设备、7部手机和30多张银行卡。

拦截短信信号 在2G情况下作案

什邡本地人吴某(男)、张某某(女)和李某(男),都是80后,且没有固定工作。其中,吴某和张某某都有吸毒前科。没有收入,又缺少毒资,两个人便动起了歪心思,从网上学会了“嗅探犯罪技术”,并在李某的协助下,疯狂作案。

办案民警介绍,吴某从网上买来嗅探设备,在一家酒店里开了房间,专门用于实施犯罪。而李某明知二人从事犯罪活动,还为他们提供协助。吴某等人利用“GSM劫持+短信嗅探”技术,截获被害人手机号码和短信后实施银行卡资金盗刷。

简单说就是,犯罪分子将一个携带特定程序的启动盘插入电脑,并将电脑与嗅探设备链接。系统运行后,嗅探设备的探头释放出信号,能够拦截方圆500米之内所有的2G短信。“嫌疑人会从拦截的短信中筛选出可以获取被害人手机号码的短信。而且短信都是双份,被害人收到一份,嫌疑人收到一份。”办案民警介绍。

也就是说,只要拿到被害人手机号,犯罪分子就等于控制了被害人的手机。“犯罪分子会对被害人手机绑定的银行卡进行解绑,或对手机上的购物APP进行重置密码。”等银行卡解绑后,犯罪分子将银行卡重新绑定在自己购买的“黑手机卡”上。这也解释了被害人为何会收到上百条带有验证码的短信。

控制了被害人的手机、银行卡、购物APP等后,犯罪分子便可以为所欲为。不仅可以将被害人银行卡内的资金转移到自己的银行卡,还可以在APP上贷款,资金到账后,再转账到自己的银行卡或博彩账户。

因涉嫌盗窃罪,目前,主要犯罪嫌疑人吴某、张某某、李某,均被刑事拘留。

解密“嗅探” 一种新型犯罪技术

网上检索发现,嗅探犯罪已经在河南、福建、广东等多地出现,网上商城和社交网络上,也不乏销售嗅探设备的商家,以及交流群。

那么,究竟何为嗅探?据中国电子技术标准化研究院技术专家何延哲介绍,短信嗅探技术是在不影响用户正常接收短信的情况下,通过植入手机木马或者设立伪基站的方式,获取用户的短信内容,这其中就包括来自银行、第三方支付平台和移动运营商的短信验证码。

“这种犯罪不同于传统电信诈骗,防范难度大。”一名办案民警告诉记者。如何避免这种情况发生?警方建议遇到收到这样的短信要立即关机,避免让对方获取位置信息,或者晚上睡觉前将手机开启飞行模式的状态。

警方在犯罪嫌疑人作案的酒店房间内起获的作案工具