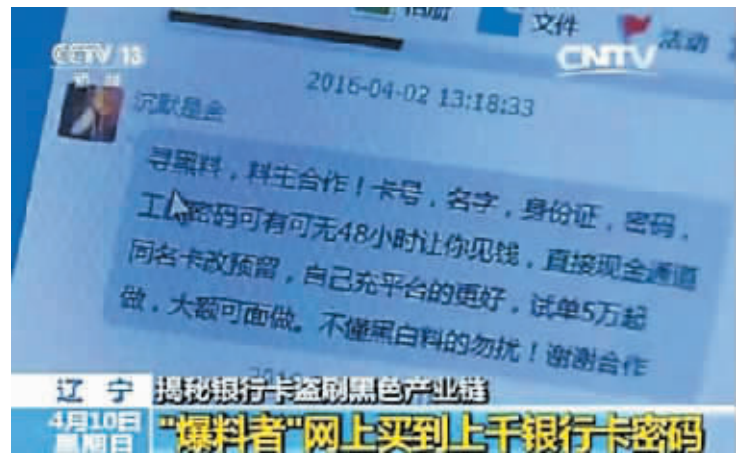
揭秘盗取银行卡信息黑色产业链

5分钟可网上买到上千银行卡信息

“卡在身上,钱莫名其妙地被转走了”,很多人会说这不可能。广州的吴先生原本也认为这不可能,但这匪夷所思的一幕就在他身上发生了。



银行卡在身上
5万存款一周只剩300元

去年12月,吴先生收到了一条陌生号码发来的短信。短信上写着自己的名字,吴先生以为是某个没存号码的朋友发来的,就点击了短信中的图片。

由于手机并未出现什么异常,吴先生便没太在意。可一个星期之后,银行突然发来一条消费短信,原本存有5万多块钱的一张银行卡,余额竟然只剩下300多块钱了。

吴先生查询发现,在这一个星期里他的银行卡陆续在往外转钱,但银行发来的十几条消费短信,他一条也没接到。吴先生把手机拿到客服检查,被告知他的手机中了木马病毒,在一个星期内丧失了接收短信的功能,一个星期后木马病毒失效,短信功能才恢复。

60岁的吴先生平常就不太会用智能手机,所以手机中没有网银、支付宝等客户端,所以即便手机中毒,银行密码也不会泄露。而银行卡也一直在他自己身上,密码也只有他自己知道。吴先生百思不得其解:银行卡里的钱,到底是怎么没的呢?

“爆料者”老徐:
5分钟网上买到上千银行卡密码

就在吴先生的案件发生不久,记者接到了一位自称老徐的爆料人的举报。老徐说,在网络空间存在着一个规模庞大的盗取银行卡的黑色产业链。吴先生匪夷所思的遭遇,在他看来只是小菜一碟。

“像老吴这种信息在黑市里很容易搞到,我用5分钟就能搞到1000个这种信息,包括卡主的姓名、卡号、身份证、电话号码,还有他的银行密码,只要5分钟1000个没有问题。”

为了验证自己所言不虚,老徐打开了几个QQ群,在不到5分钟的时间里,发给了记者一份长达33页的文件。这份文件里记录了1000多条银行卡信息,每条信息都有卡主的姓名、银行卡号、身份证号、银行预留手机号码以及银行密码。记者在文件中随机选取了七十个不同省份的信息进行验证。其中,身份信息和电话号码全部正确,除了5个银行密码错误,其余65个银行卡密码全都正确。

在老徐的帮助下,记者对这个黑市进行了长达3个多月的调查。一步步看到了这个黑色产业链中隐藏的秘密。

揭秘盗取银行卡信息三大方法

要想把银行卡里的钱转走,通常不是一两个犯罪分子能够完成的。他们需要建立一个完整的产业链条。在这个链条上分工不同的犯罪分子,通常是用只加熟人的QQ群进行交流、交易。在“老徐”的帮助下记者进入了这类QQ群,在群里犯罪分子将银行卡信息称为“料”,搜集银行卡信息的人叫做“下料人”,而把银行卡的钱往外转的人叫做“洗料人”。从“下料人”手里买“料”是整个犯罪的第一步。那么,这些“下料人”的“料”是怎么来的呢?

方法一:伪基站发送钓鱼短信

记者采访了数十位被盗取银行卡的受害者,发现其中很多人都有过相同的遭遇,就是收到了类似10086、95533等所谓的电信运营商或银行发来的短信,登录后被要求输入密码。

360首席反诈骗专家裴智勇指出,这些其实都是犯罪分子利用伪基站“包装”后发送给用户的含有钓鱼网站的短信。仅360平台上监控到的钓鱼网站,半天时间就有超过1亿次的点击量。在这些钓鱼网站的虚假网页上,用户登录后就会被要求输入账号、密码、姓名、身份证号、银行预留手机号等信息,而一旦填写了这些信息,骗子就可以把用户的钱骗走了。

裴智勇介绍,钓鱼网站的更新速度非常快,每天都有5000到8000个新的钓鱼网站被监测到。

方法二:免费WIFI窃取个人信息

除了使用钓鱼网站获取个人信息,记者发现犯罪分子还会利用免费WIFI窃取个人信息。

裴智勇介绍,一个WIFI的安全性主要取决于它的架设者是谁,如果是骗子或者是黑客架设了一个免费WIFI,用户一旦接入,所有互联网的数据都可以被黑客监听或窃取。

方法三:改装POS机提取银行卡信息

除了以上两种方式,记者发现黑市中的犯罪分子还有第三种方法——那就是利用改装的POS机提取用户银行卡信息。

在黑市中,POS机提取的信息被称为“轨道料”,数量上要远远少于钓鱼网站上提取的信息。但是卖价却很高,余额较大的信息甚至可以卖到几千块钱一条。而对于这些信息,犯罪分子通常会等半年以上才把信息出售,目的是让消费者积累大量POS机消费记录,这样警方就无法追查是哪台POS机提取了银行卡信息。

完成了“下料”的工作,在这个黑色产业链上,下一步就是将受害者银行卡里的钱转出来,犯罪分子把这个步骤称为“洗料”。这也是很多受害者最疑惑的地方——我的钱究竟是怎么没的?

起底拦截短信验证码两种方法

在QQ群中,每天都会有很多人发“洗拦截料”的广告。这些人被称为“洗料人”,他们可以把受害者银行卡里的钱转出到“料主”指定的卡号里,从而获得30%到50%的提成。而他们主要关注的就是用户短信验证码。

方法一:让手机中毒拦截验证码盗取钱财

验证码是金融机构在用户进行诸如修改密码、转账等操作时,向用户预留手机号码中发送的一次性的密码,没有验证码则无法进行转账等操作。而要想获取验证码,犯罪分子最常用的手段就是向目标手机里发送木马。文章开头的吴先生就是手机木马的受害者。

只要受害者点击木马程序,手机短信内容就会被犯罪分子拦截。犯罪分子通过事先掌握的银行卡主的个人信息将银行卡绑定在第三方支付平台,然后把钱转走。而此时受害者的手机既收不到消费提醒也收不到验证码,卡里的钱就这样被转走了。

方法二:近距离干扰手机信号拦截验证码

让手机中病毒是最为常见的拦截验证码方式,然而却不是唯一的方式。记者发现在黑市中,已经有人不需要木马病毒就可以拦截验证码。他们的方法就是通过特殊的改装设备对手机信号进行干扰,但这种方法有一个限制条件,那就是这个设备就必须处在目标手机一公里范围之内。因此,使用这种拦截方式必须要靠近受害者。

那么,犯罪分子要怎么确定目标的位置呢?“其实这个很简单,一般的手法就是给那个目标打电话,说你自己是送快递的,你这个地址写得不是很清楚,让他把地址再说一遍,只要他把地址说出来,我们就能在一公里范围之内拦截他银行卡的验证码。”老徐说。

>>>相关链接

银行卡被盗刷 你该这么做

冻结卡片,防止损失继续扩大——拨打客服挂失或者通过手机银行自行操作。多数银行有“失卡保障”服务,在挂失前48或72小时发生的盗刷可赔付。

立即报案,立案回执要保存——这样在向银行主张权利时才有据可查。

留取证据——正确的做法是:立刻到附近银行取现,并打印凭证。这样做是为了证明银行卡在你手中,而其他地方发生的交易均为伪卡。

(据央视网)