资深黑客揭秘银行卡盗刷黑色产业链

伪基站发木马短信设局，诱用户填银行卡密码　或与金融从业者存利益“勾兑”

5月9日，最高人民法院通报了《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》。这是两高首次就打击侵犯公民个人信息犯罪出台司法解释。根据此次司法解释，非法获取、出售公民个人信息，情节严重者可获刑。

我们几乎每个人，都曾被推销电话、诈骗短信骚扰过。去年发生的“徐玉玉案”，即是个人信息遭侵犯导致的“恶果”。在此节点，记者通过对航空、征信、银行卡等领域进行调查，以期找到个人信息泄露的源头。记者调查了解到，在银行卡盗刷的黑色产业链中，从伪基站群发木马短信诱导用户点击链接，到钓鱼网站和拦截码“钓出”用户信息，再到“洗料人”通过多种通道将钱“洗白”分赃，银行卡盗刷产业链已经分出了泾渭分明的三块“业务”，每个业务上的黑产从业者各司其职，在几乎为零的成本背后，是“月入十几万”的利润诱惑。

“黑产”从业者

一天发三万条诈骗短信，收费4500元

6月6日，打开手提电脑，看着屏幕里的数字在3秒内从0跳到34，旁边的一部安卓手机发出了“滴滴”的短信提示音，小张知道，伪基站已经开始正常运作了。

屏幕上的数字显示的是他手中设备向外发送出的短信数量，每一个数字的跳动都意味着附近有人接收到了他发出的信息。

“并不是每个人都会看这条短信，”小张说，“但总有人会看，也有人会点击里面的链接。”

当天，小张发出的信息是“工商银行积分兑换活动开始，尊敬的用户，您可用积分4678分，兑换467.8元，点击官网链接兑换。”短信中还附有一个开头为95588的网站链接。

与正常的银行提示不同的是，里面的链接指向的并非工行官网，而是一个钓鱼网站，只要进入这个网站并下载所谓的安全控件，点击人的银行卡信息就会泄露出去。

也许，1000个人中只有100个人会去看这条信息，100个人里只有10个人会点击链接，但对小张来说，只要有10个人点击，就够了。

因为小张一天平均可以发出的信息数量，是三万条。

一位互联网黑产从业者表示，伪基站是银行卡盗刷产业链的上游，“伪基站，顾名思义，是可以伪装成运营商基站的设备。它一般由主机和笔记本电脑、短信群发器、短信发信机等相关设备组成，可以搜取以其为中心、一定半径范围内的手机卡信息，并任意冒用他人手机号码强行向用户手机发送编辑好的信息，伪装成10086、四大行客服都可以。”

“一般的老板都包天，从上午九点半发到晚上八点半，一天收费4500元。”小张介绍。若按此计算，小张一个月可以获得十三万多元的收入。

神秘“伪基站”

藏身在汽车或行人背包里

6月4日，记者曾联系到几家卖伪基站的“科技公司”，公司老板称，基站有车载式，也有背包式，一台基站视功率、大小不同价格也不同，在6000元至1万元间浮动，“价格不算贵，而且只要你找到了好老板，一天就可以回本。”

小张的设备属于“车载式”，他说，只要把设备放在车里，然后去人流密集的地方把设备打开兜圈子就行。“有时会遇到警车，只要机灵点，及时把设备关掉就可以了。”

但现在伪基站越来越容易被检测出来。2016年4月，360公司在首都网络安全日展会上曾展示了伪基站追踪系统，北京地图上显示出了许多黄点和红点，从图中可以看到东城区和朝阳区的“点”最多，据介绍，这些都是伪基站活动的痕迹。

一家贩卖伪基站设备的“科技公司”在广告上赫然显示，目前已经推出了可以过杀毒软件、智能手机甚至包含“安全自毁系统”的新型伪基站。

“我们针对伪基站其实一直在升级防范类的软件，但是有时我们研制了一款软件出来，就发现伪基站已经更新了好几代了。”一家安全防护科技公司的研究人员说。

有毒“钓鱼网”

木马拦截用户短信，盗取卡号密码等信息

当小张通过伪基站将短信轰炸式发送到手机用户手中时，不知情点击短信链接的用户就会掉入小张的“雇主”们精心设计的骗局中。

资深黑客“惊云”（化名）就是小张的雇主之一。6月2日，记者联系到了“惊云”。在黑客圈混了四五年，“惊云”精通源代码编写和网站搭建，但他最主要的业务却是开发钓鱼网站。

在“惊云”演示的一款“工商银行钓鱼搭配拦截码演示”视频中，他制作了一个域名为“95588”的网站，网站界面几乎和工商银行官网一模一样。

谈到做网站的价码，“惊云”说：“搭建钓鱼网站1000元一个月，手机短信拦截码500一个月，手机感染软件周租带链接整套1200一周。”

“域名是可以自己编写的，把95588、95555这种银行客服电话写进去是很容易的，只不过后缀不能是.com，只能用别的。”他说，“我们只要在这个网站里加上‘积分兑换’之类的内容，诱导‘鱼’来填写账户密码就好了。”

在“惊云”的演示中，当他在钓鱼网站点击“积分兑换”选项时，会出现要求填写用户身份证、手机号、银行卡账户和密码的选项，填写完后，这些信息都会发到“惊云”的另一个软件后台。“这样，‘鱼’就上钩了。”

用户填写完这些信息后，钓鱼网站还会以“需要安装安全控件”为名诱导用户安装手机木马。“不管‘鱼’填写安装还是不安装，手机木马都会自动开始安装，这样我们就可以把短信拦截木马植入到用户手机中。”“惊云”说。

在银行卡盗刷黑市里，用户的身份证、手机号、银行卡账户和密码被称为“四大件”，被植入了手机短信拦截木马的用户，黑客可以轻易拦截用户的手机信息，接收手机验证码，被称为“拦截料”。在不少从事地下交易的QQ群里，“拦截料”往往被明码标价出售。

“惊云”本身既向人出售钓鱼网站，自己也通过钓鱼网站获取他人的银行卡信息，并转手出售“拦截料”赚钱。

专业“洗料人”

多通道盗刷银行卡 与金融从业者存利益“勾兑”

在黑市中，银行卡信息被统称为“料”。其中，有验证码的“料”被称为“拦截料”，从博彩网站以黑客技术“拖库”出来的“料”叫做“菠菜料”，而通过POS机或者直接在ATM机上安装盗窃软件取得的料叫做“轨道料”。

不管从哪种途径“出料”，最后都需要借助一些“通道”把银行卡中的钱盗刷出来，这被称作“洗料”。

不管是伪基站也好，钓鱼网站也好，都是窃取用户银行卡信息的手段，但把银行卡中的钱“安全”提取出来，往往需要借助专业“洗料人”所掌握的“通道”。

“惊云”直言，最为“传统”的洗料通道是直接取现，这类“洗料人”被称为“取手团队”，具体手法是通过技术直接复制一张与银行卡原持有人一模一样的银行卡出来，然后找人直接去ATM机取款。“这些人总是最先被抓的，我曾经跟一个取手团队合作过，后来觉得太危险了就叫他们删除了我的联系方式。”

“现在，做通道的人都是金融行业从业者比较多，或者是熟悉金融行业的人士。因为从金融系统或者第三方支付平台上将钱‘划走’比较安全，风险也比较小。”“惊云”说。

6月8日，记者以出料为名联系到一QQ名为“诚信为本”的专业“洗料人”。据他介绍，这一行的“行规”基本是开钓鱼网站的“料主”把出的“料”先提供给洗料人，洗料人通过自己的通道将银行卡里的钱提取出来，所获款项再与“料主”按一定比例分成，一般是隔天回款。

“诚信为本”表示他走的是“银行通道”，和“料主”按6:4分成。“我6你4，如果做得久了，老客户我们可以按照5:5分成。”他向记者出示了一个显示时间为6月7日的招商银行的电子回单，“我们可以出四大行以及招行、浦发的储蓄卡，宗旨是一条料出到底，绝不跑单。”

但实际上，“料主”与“洗料人”之间常常发生“黑吃黑”，“料主”给了“洗料人”钱之后，“洗料人”独吞利润的案例也不鲜见。

6月8日，在一个从事黑料交易的QQ群中，一位“料主”与“洗料人”就发生了争执。“料主”称已把“料”发给了洗料人，但“洗料人”隔了三天都没回款。“洗料人”则喊冤称“钱还在，我根本没有洗这个料”。

“实际上，任何拥有手机短信权限，能通过银行卡卡号和密码进行转账操作的平台，都可以作为‘洗料’的通道，不同的是安全与否。”一位了解互联网黑产的人士告诉记者。 ■据新京报