互联网金融反欺诈解析（黑产）

目录

备注：部分内容来源于网络，如有侵权请私信 Vivian：wmyd80，谢谢

一、黑产常见名词解释

为更好的让大家理解，这里整理收集了下目前市面上常见的欺诈黑产“黑话”以及使用语境，仅供大家参考~

1、黑料

在黑产中，被反复清洗，有金融价值的用户信息。主要指银行卡账户、密码、身份证号码、及绑定手机号码四大类信息

2、内料

境内卡的四要素

3、外料

境外卡的四要素

4、下料

非法途径搜集四要素

5、洗料

洗料在这个行业有很多细分工种，主要指的是资金转账、套现、洗白。

如洗拦截料，通过植入木马病毒拦截用户手机验证码完成套现

6、挂马

制作，出租木马病毒

7、刷货

通过复制银行卡的方式来实施盗刷的过程

8、收菠菜

黑产从业者得到的数据进行整理，除了丰富社工库之外，还利用这些数据对其他网站进行试探性登录，从而获得其他网站上的账户信息

9、拖库

黑产通过社工手段或技术手段盗取目标网站客户资料书数据

10、洗库
黑产将用户账户中的财产或虚拟财产通过各种黑产渠道进行变现

11、撞库
黑产将拿到的数据进行整理，利用这些数据对其网站试探性登录，从而获得其他网站账号信息

12、社工库
社工库是黑客将获取的各种数据库关联起来，对用户进行全方位画像

13、虚假号码
所有用于代替他人接收验证码的手机号码

14、接码平台
即羊毛党和卡商进行验证码短信交易的渠道，类似淘宝平台提供平台服务，赚取分成

15、打码平台
提供批量自动化识别各类验证码的专业服务平台，提供手机号码，获取注册，解封，换绑短信的验证码平台

16、安卓模拟器
具有一键新机的功能，每次启动所有的系统参数都会变化

17、伪基站
搜取一定半径范围内手机卡信息，通过伪装成运营商的基站，冒用他人手机吗发送诈骗信息

18、猫池

猫池厂家负责生产猫池设备，并将设备卖给厂商使用。猫池是一种插上手机卡就可以模拟手机进行收发短信，接打电话，上网等功能的设备，在那个厂行业也有广泛应用，猫池设备可以实现对多张手机卡的管理

19、改机工具
刷新设备指纹，解决单台设备注册上限的问题

20、卡商
卡商指通过各种渠道，如开皮包公司，与代理商打通关系等，从运营商或者代理商那里办理大量手机卡，通过加价专卖下游卡商赚取利润的资源持有者

21、养号
将批量注册的小号，不断发作品关注用户，修改头像，主要目的是为了降低账号被封的概率

22、白号
指接入接码平台直接用手机号码注册的账户，也称直登号

23、活粉
带有作品、个签、个人头像，模拟真实用户操作的一批账户

23、死粉
又称僵尸粉，这类账号，知识带有简单的个签和个人头像，账户活跃度低

24、刷粉
短时间内提高账号的粉丝数量

25
是线上通过技术手段实现，在线上寻找作案目标

26、压门

犯罪分子冒充身份，对受害人进行行骗，一旦有人上当，作为压中了

27、菜商
菜商指的像卖菜一样出售个人信息的人

28、马
或者说病人，骗子的目标

29、抓马
确定目标后，派出人去搭讪，推销

讲完上面的黑话，举个例子：
对话一
A：兄弟，最近手头有料没?
B：刚好搞了一些，都是内料、外料都有，正准备找人刷货。
A：刷货多老土啊，还得买设备，而且现在都是芯片卡，也不好刷。我刚好认识一个挂马的，到时给你洗拦截料，方便快捷还安全。
B：技术真是日新月异啊，你不说我还真不知道。

对话二：
A：有没熟悉的卡商，找他买两千张卡。
B：这么多卡忙得过来吗?
A：你怎么那么笨阿，不是有猫池么。
B：对对对，要是做不过来还可以找打码的帮忙。
A：现在前期资金不够，我们设备有限，你看看找个认识的，整个改机工具，我们也好批量注册。

对话三：
A：上次买的那批卡注册的白号怎么样了?
B：那批现在在养号，咱们之前的号可以出货了。
A：那些活粉好好养着，那些死粉有人需要刷粉的可以卖一卖。

二、黑产常见产业链解析

黑产产业链分为上游、中游和下游。各个环节分工合作，紧密相连。
上游是基础性环节，分为开发研制和资料贩卖。主要是为了提供黑产作恶的基本工具。如打码平台，刷机工具，代理 IP，或者一些盗取的账号密码库。
中游是诈骗实施环节，如点心诈骗、短信群发、在线推广等。
下游则是洗钱销赃环节，实施现金取现、洗钱等。
以下我们根据不同场景为大家介绍~

黑产常见产业链（羊毛党）

1、上游（手机号码贩卖+物料收集）
2、中游（验证服务+网赚平台）
3、下游（实施欺诈+活动套利）

双十一临近，各大电商平台迎来了最强大的敌人羊毛党。无论是优惠、促销、打折、秒杀活动，或是补贴大战，发放红包等，都是羊毛党大显身手的地方。羊毛党特指那些在营销活动中凭技术或人工手段，钻漏洞获取非法利润的欺诈团伙。目前，随时科技的进步，羊毛党逐渐从分散的个体发展为团伙集体，已形成有组织、有规模的职业羊毛党。

以某电商平台举例，平台-邀请账号-被邀请账号和真实顾客。黑产通过批量注册获取大量账号，参与邀请活动（可能是砍价、拼团等），将低价购买的优惠商品发送到指定地址归集，再通过自己的分销平台加价倒卖给真实顾客获利。黑产的收益为倒买倒卖的差价和平台补贴的优惠金。同时平台短期内可能会遇到库存被占用、普通用户无法购得优惠商品引起客诉，长期则可能造成用户流失，平台品牌和信誉度受到影响。

黑产常见产业链（互联网金融）

1、上游（身份贩卖+物料收集）
2、中游（身份包装+情报贩卖）
3、下游（黑产欺诈+欺诈实施）

黑产是互联网金融常见的欺诈风险，一般涉及申请人个人资料信息的四要素，即：姓名+身份证号码+银行卡号+手机号码。常见获取渠道是批量收购，如偏远山区低价收购，或者深圳三和的无业游民批量收购。其身份信息都是真实有效的，并且其成本较低。后续进行身份包装后实施诈骗，也就是骗贷。

黑产常见产业链（盗号盗刷）

1、上游（数据盗取+物料收集）

2、中游（数据加工+目标定位）

3、下游（盗取盗刷+欺诈实施）

盗号盗刷主要发生在银行，常见的借记卡、信用卡及金融账户。一般通过得到银行卡信息后进行盗刷，如发送木马链接获取交易密码，实施欺诈。