1693 阅读 3 回复

同小盾

级别: P5_安全攻城狮

加关注 写私信

【反欺诈专栏】互联网黑产剖析——虚假号码

楼主 发表于: 07-13 只看楼主 更多操作

Author:戒小贤@同盾反欺诈研究院

一、技术原理

“虚假号码”这个词，目前还没有被大多数人所接受。关于虚假号码的来源、危害、各种特性，外界也了解的很少，更不要提如何针对虚假号码进行风险防控了。

“虚假号码”定义：

用于代替他人接受验证码信息的未经实名制手机号码，统称为虚假号码。

国内的大批接码平台，提供了大量的虚假号码。比如之前被查处的爱码平台，累计经手的虚假号码达到了2000万，每天可用的虚假号码在500万以上。

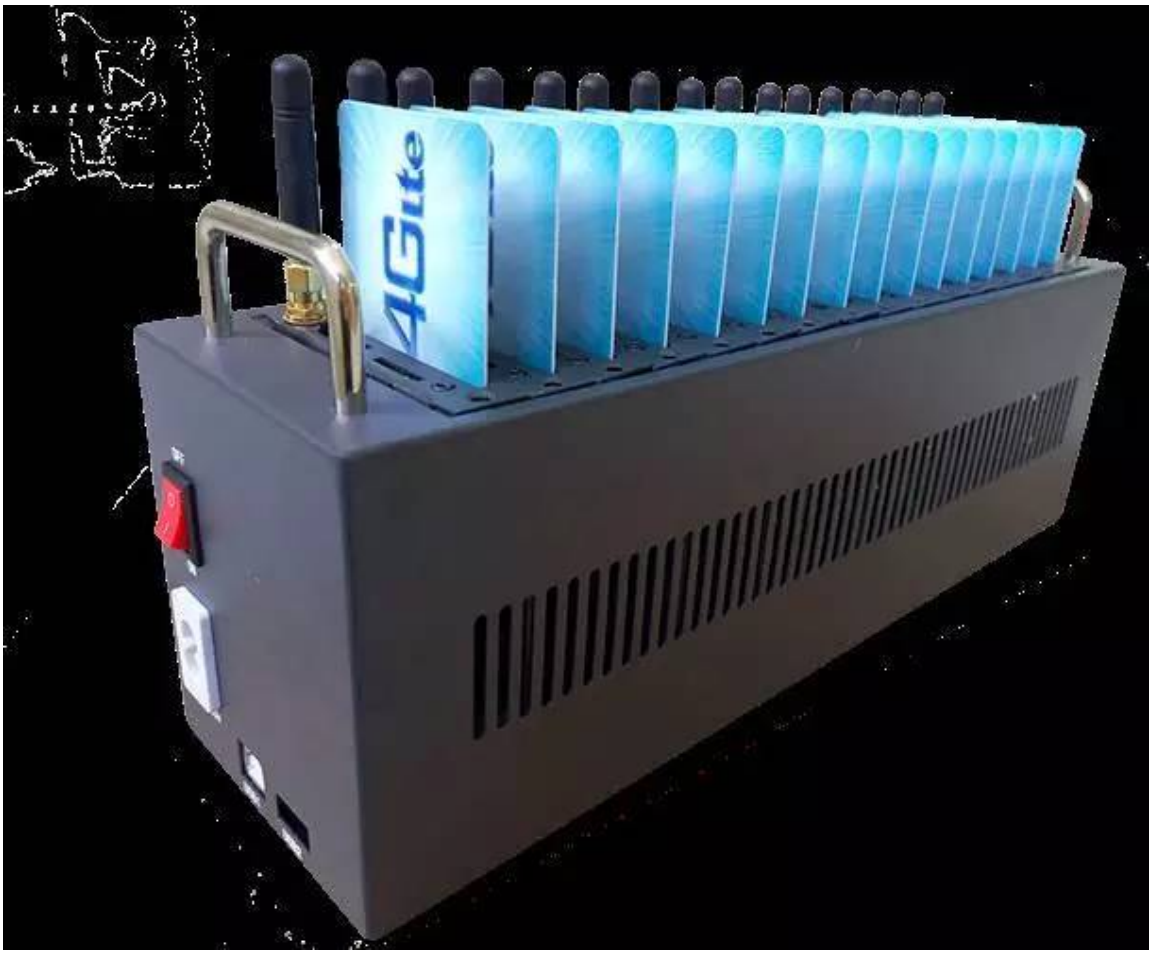
此外，还有大批虚假号码，被黑产团伙直接持有，他们会自己开发自动化工具，来完成验证码接收和使用。目前这批虚假号码的规模无法估计。下面，来一起见识一下虚假号码的原理。

“猫池”定义：

英文名 Modem Pool。 Modem，即调制解调器，普通的家用宽带拨号所使用的"猫"也是一种modem。字面翻译过来，就是猫池。

Modem中一般封装了拨号协议，宽带所使用的Modem，封装的是PPPOE协议。猫池所使用的Modem，封装的是GSM、CDMA或其他的一些通讯协议。两种Modem都可以通过AT指令集来进行控制。

”



这是目前国内比较普遍的一种猫池，16个卡槽，每个卡槽，是一个GSM模块。设备通过USB和PC连接，挂载为一个串口设备。通过软件或驱动程序，向Modem发送AT指令，来完成特定的操作。

比如：电话呼叫13905168888

ATD+13905168888\r\n

挂断

ATH\r\n

读取短信

AT+CMG\r\n

由于AT指令通过串口发送，可以支持全平台、全语言，开发难度、成本都非常低。近年来随着物联网技术的发展，越来越多的地方需要使用到GSM协议。与此相关的技术、硬件、软件相继被开发出来，门槛也越来越低，互联网上存在很多非常成熟的猫池软件。

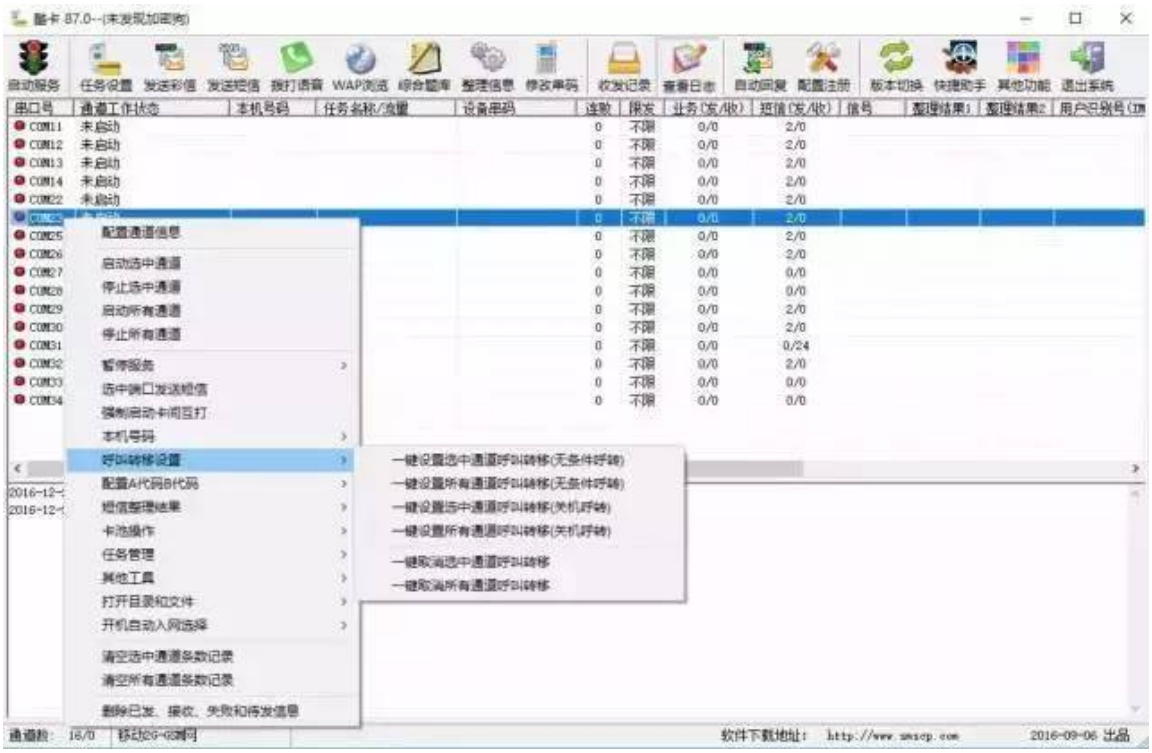
软件通过AT指令，读取到SIM中的短信，然后保存到数据库中，包括发信人、短信主体、收信时间等。并且，通过模板匹配，可以精确提取出短信中哪几个字符是验证码，根据发信人的号码，判断验证码对应哪个平台，从而自动填充到注册表单或订单页面中。在条件允许的情况下，一个注册机，一天可以注册超过10万账号。这些账号再后续的一些黑产活动中会被使用。

二、关于验证码

既然说到虚假号码，就不得不说“验证码“，这里指发送到用户手机上的验证码信息，包括短信验证码或者语音验证码。短信验证码可以轻松被猫池读取，那么语音验证码呢?

语音验证码本质上是一次电话呼叫，用户接听后，自动播放一段语音，其中包含朗读的验证码信息。

某些接码平台提供了听码服务，有专门的听码人员，或由开发者提供语音识别的功能，来完成验证码提取。除此之外，通过在猫池上设置呼叫转移，可以把包含验证码信息的短信呼叫，转移到特定的手机号上去，由用户来听取验证码。



使用语音验证码一定程度上提高了验证码获取和使用的难度，但依然无法阻止羊毛大军的脚步。

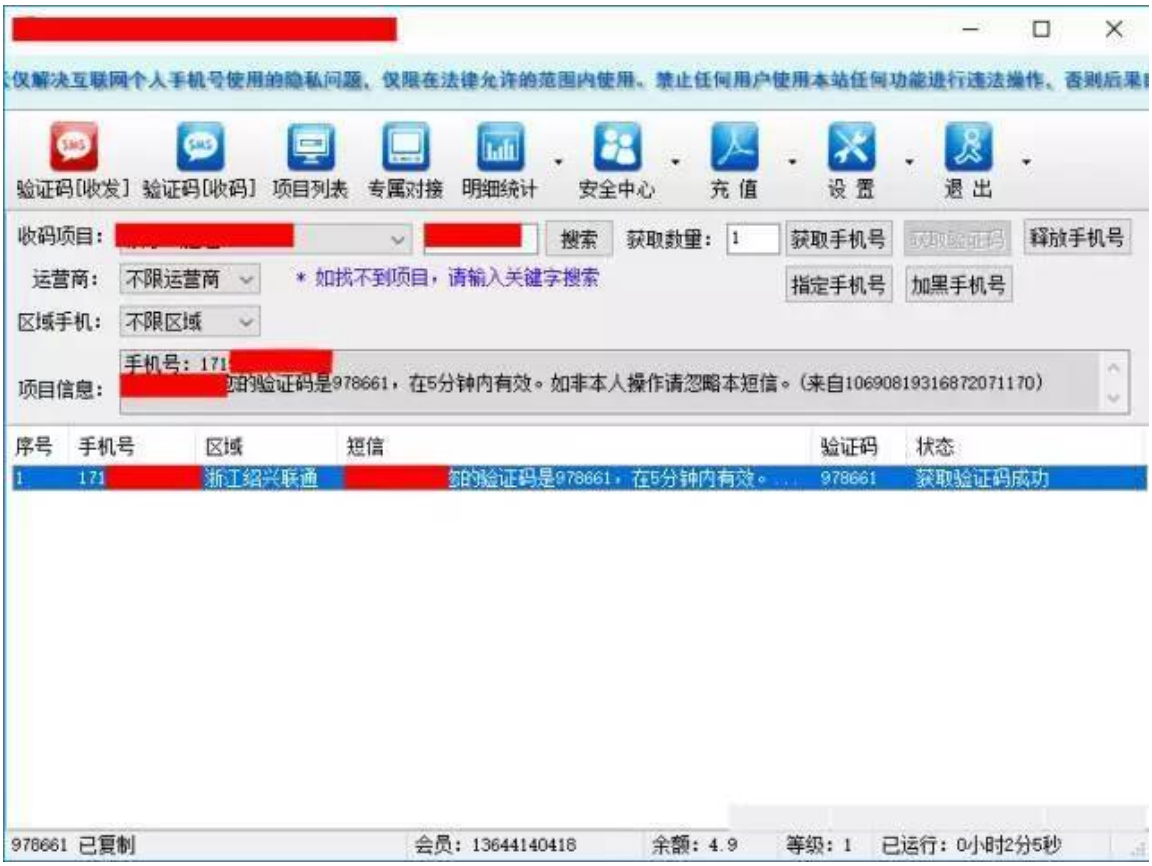
三、虚假号码的使用场景

虚假号码的使用场景非常多，下面逐个进行剖析。

3.1 首单减免

如此巨大的诱惑，很多羊毛党趋之若鹜。即使普通人，也会乐于尝试一些办法来不断地享受这个优惠。

先到接码平台上申请一个手机号，虚假号码一般是独占的，在我申请使用这个号码之后，与我申请的验证码模板相比配的第一条短信，会显示在我的个人界面中。其他人不能使用这个号码。



至此，凭借这条验证码，就可以完成一次注册了。

由于该平台下单，是必须通过移动端进行的，而且该平台已经建立了自己的设备指纹。如果用我自己的手机登陆这个账号，设备指纹会显示我已经拥有过一个账号，然后自动将两个账户合并，优惠券不在发放。

所以，一般还会配合模拟器，或改机工具进行。

3.2 微信抢红包

微信也是虚假号码高度集中的一个区域。

由于很多规模较小的互联网公司，已经不再开发自己独立的App了，转而提供H5页面，通过微信和支付宝的内置浏览器，就可以访问，并且对接了微信或支付宝的一些身份验证机制。

微信本身是不实名的，微信也不会将用户的手机号或其他信息传递给应用产商，仅凭微信账号的唯一标识来区分用户。很多微信上的优惠活动类似于：关注领红包、投票抽奖，就面临了被薅羊毛的风险。

羊毛党会批量的注册微信号，然后通过模拟器、群控手机等方式保持这些账号的活跃。这些账号可以在之后很长一段时间内，参与各种各样的优惠活动，赚取毛利。


脚本配置
微信养号_NZT
飞行换IP（利用开关飞行模式更换IP）
开关VPN换IP（利用开关VPN更换IP）
VPN密码
浏览腾讯新闻
发朋友圈
发朋友圈（文字）
发朋友圈（图片加文字）
发朋友圈（文字）
禁用NZT数据
删除NZT数据
取消
确定

一般的活动中，红包从2~10元不等，一个职业的羊毛党，一天可以稳定收入2000~5000元。每个垃圾账号收到红包之后，全部转移至一个账号上，然后提现。

由于微信不会对账号进行清洗，一个手机号注册过之后，其他人就不能在继续注册，只能申请解绑，或者申诉验证，于是衍生出了很多针对微信解绑的黑产技术，在此不做讨论。

3.3 刷单场景

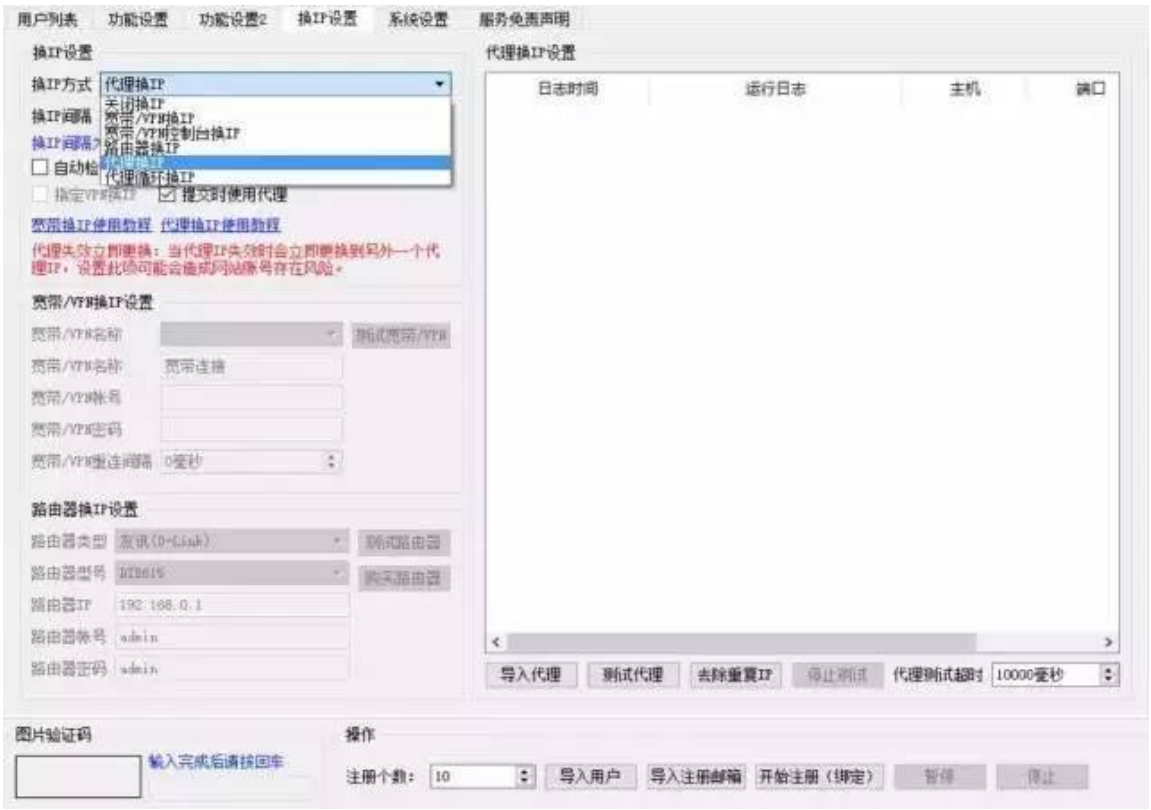
和外卖平台的首单优惠很相似，电商也会有不定期的优惠活动。

这些优惠活动中，一般提供的优惠券，比如：满600减200等等。持有这些优惠券进行购物，实际支付的价格就比真实的价格要低很多。一旦物品到手，他们会以一个比较合理的价格倒手卖出，赚取中间的差价。

整个刷单包含了三个环节：批量注册、扫货和下单，都有自动化的工具。其中，虚假号码就是用在批量注册环节。

这是亚马逊的一个注册机，其中包含了很多功能，包括随机生成账号、自动获取虚假号码和验证码、自动更换IP，自动识别图形验证码等等。

甚至包含了一个生成随机Mac地址的功能。



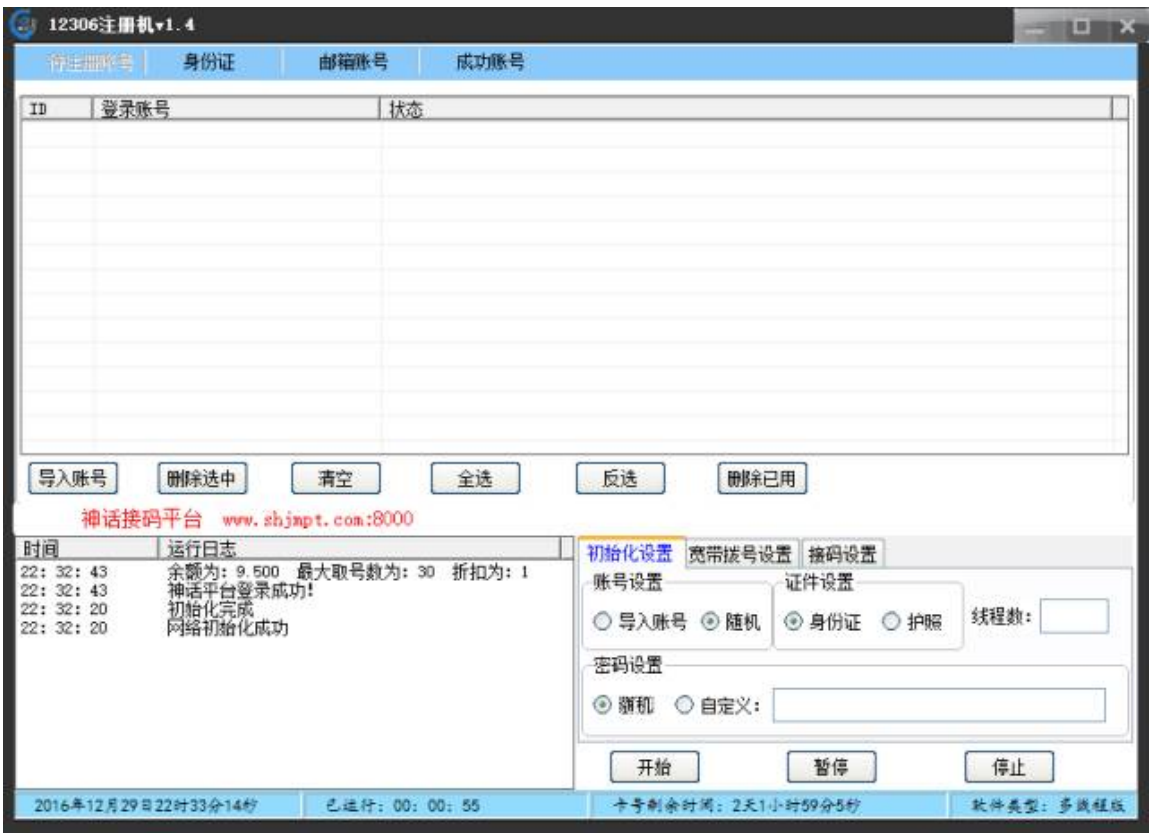
换IP通过宽带或VPN重播，或者设定代理IP来实现。

注册10个账号只用了大约10分钟，单个IP上的频繁注册很容易触发风控规则，而且验证码特别难辨认，注册的速度受到了限制。这些新注册的账号可以享受亚马逊的优惠，比如1元购买电子书。

下图是同一个工作室开发的扫货软件。

除了刷单之外，一些活动也可能使用到这些账号。比如：刷评论，或者每日签到等等，只要能够牟利的地方，都有垃圾账号的用处。

3.4 黄牛抢票



由于12306的注册是需要身份证号的，这里没有尝试效果如何。如大家所知，12306一直是黄牛非常密集的地方。

四、虚假号码的来源

关于虚假号码的来源，目前普遍认为是通过运营商内部流出来的，这和我们目前收集到的情报相吻合。

一些管理不完善的运营商或虚拟运营商，存在内部人员批量拿卡的情况，拿到的卡被批量倒卖，价格一般比较低，而且数量巨大。另外，根据我们的分析，还存在一些其他的途径可以获取到虚假号码。

比如，某些营业厅在给用户办卡的时候，可以获取到用户的身份信息，他们会盗用这些信息，额外多申请几张卡，以满足运营商的一些绩效考核制度。运营商对此是清楚的，所以他们会根据手机号的一些状态，来判断是否存在虚报数量的情况。但是这个判断，仅仅根据"在网状态"来进行，即便卡插在猫池里，也会被认为是开机状态，就不会被认为是虚报。

也有一些，是由于用户的个人信息泄露，而被他人盗用，办理了手机卡。尤其是虚拟运营商，网上申请手机号，仅需要身份证号、姓名、一个在用的手机号以及手持身份证的图片即可。而这些东西，都可以很容易在网上找到，或者在黑市里购买。

以上这些渠道，构成了国内虚假号码最主要的三个来源。具体规模，我们尚不可知，根据这些来源，我们把虚假号码分成两大类：实名的，没有实名的。实名的卡，也叫黑卡或实名黑卡，目前缺乏有效的发现和防控手段，这里先不提及。

我们目前所说的虚假号码，其实是这批没有经过实名的，从运营商内部流出来的号码。

五、虚假号码的用途

前面虽然提到了虚假号码的使用场景，但是并没有全部说明虚假号码的用途，这里汇总如下：

编号	用途	描述
1	垃圾注册	为刷单、刷量、抢票、薅羊毛等行为提供必要的账号
2	验证/绑定/解绑	如果虚假号码已经被注册过一个账号，可能会通过解绑、验证等方式强制收回账号的所有权
3	隐私保护	存在极少数的案例，当事人不愿意暴露自己的真实信息，会使用虚假号码，比如，河南省公安厅网上举报通道

一般的，平台的的优惠政策，诸如：红包、返现、优惠券等等，直接影响虚假号码的数量和占比。

在和虚假号码的对抗中，我们必须关注各个平台的优惠活动，优质的活动必然引来羊毛党的关注。而且，并不是每一个优惠活动都可以被薅，这需要我们投入一定的力量进行分析。

比如，之前客户反馈的一个案例，新用户注册之后，将得到80元的新手礼包，不能提现，但是可以用于购买贵金属。期间，羊毛单通过操作众多账号，批量买入和抛出，80个账号中，有79个都亏了，但是最后一个，可以赚到很多。

如果不是事后的数据分析捕捉到这个异常行为，可能都不会意识到有如此走心的羊毛党。

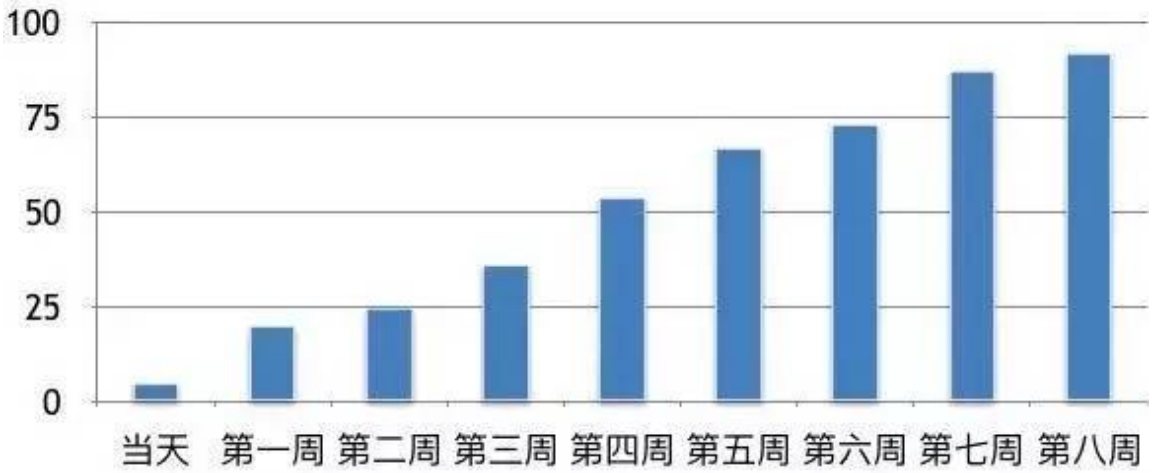
六、虚假号码的防控

目前我们对虚假号码的防护，主要来源于黑名单，黑名单的规模，直接影响了防控的效果。我们对国内所有的接码平台进行监控，7*24小时从这些平台获取虚假号码的数据。接码平台也有一定的技术实力，也会对爬虫进行规避。我们用户爬取的账号平均有效期只有一周，大大增加了我们的工作难度。

我们一直在对各个接码平台进行监控，保证我们数据的持续更新和有效。某些平台迫于一些压力，开始转入地下，我们依然能够通过强大的情报系统找到他们。

6.1 虚拟号码的生存期限

由于虚假号码不会进行实名制登记，存活期一般在60~90天(根据不同的运营商而变化)。我们随机抽取了一份虚假号码样本，在两个月的时间内，对手机号的存活状态进行了一些监测，统计已经失效的手机号占比，结果如下：



手机号状态检测，是我们判断虚假号码最强有力的一种方式。每一个虚假号码，都逃不过被强制停机的命运。但是我们只能在手机号已经停机或变成空号之后才能发现，欺诈分子可能已经利用它参与了很多欺诈活动，在实际的使用中，并不理想。

但手机号状态检测，为我们验证各种猜想提供了可靠的依据。

6.2 基于设备关联关系

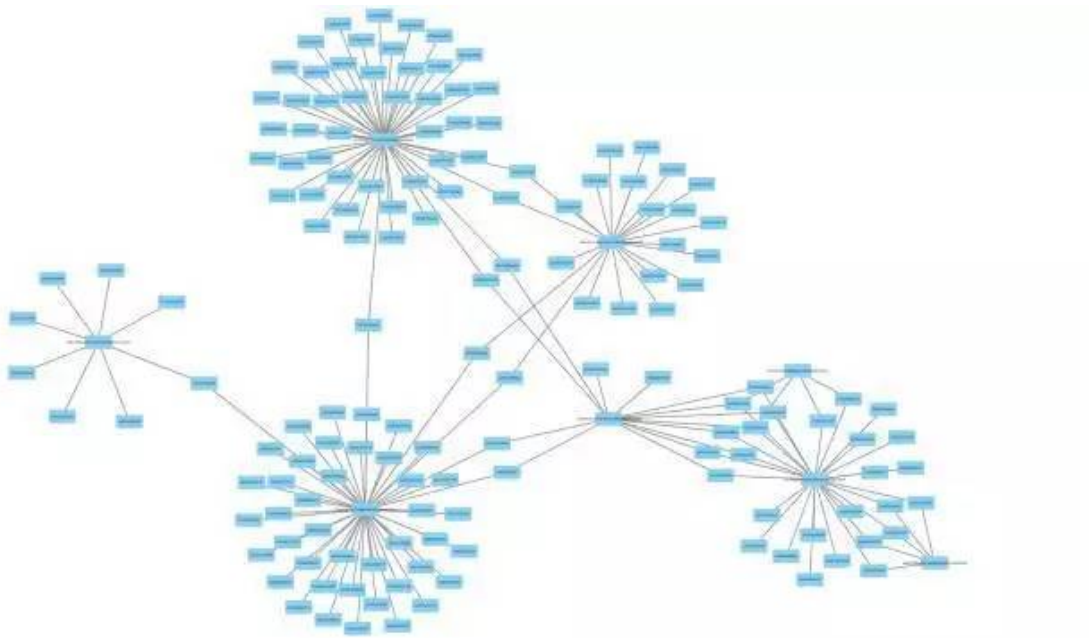
复杂网络，是我们识别虚假号码的方案中最为出色的一种。

基于同盾设备指纹的海量覆盖，我们对设备(安卓、IOS、PC等)进行了唯一标识，通过这个设备进行注册、登陆、交易等活动的手机号，就与这个设备建立了关联关系。

我们通过已知的虚假号码，分析出曾经使用过这些号码的设备；再通过这些设备的唯一标识，去检索与之关联过的其他手机号，顺藤摸瓜，揪出了更多的高风险手机号。一般，散户的羊毛党只会有一到两台手机进行操作；具备一定能力的团伙，会使用数十台甚至数百台设备。

根据我们的目前的数据分析，通过复杂网络分析出来的“可疑手机号”，风险概率高达99%，最终变为空号的概率接近90%。其中有少部分手机号是羊毛党的真实手机号，可以作为定位羊毛党身份的重要依据。

一个电信的虚假号码复杂网络关联效果如下：



6.3 实名制对虚假号码的影响

手机号实名制，从2016年10月开始强制施行。之后的几个月中，我们监测的数十个接码平台，相继下线。但是虚假号码的总体规模，依然保持在原有的水平。随着三个运营商和虚拟运营商的内部监管越来越严格，国内的虚假号码数量会有所下降。

但这并不代表虚假号码会从此消失。

卡商们发现，国内的手机号获取变得困难，就开始转向了国外。尤其是东南亚一些国家，缺乏通信方面的监管，就可以大批量购卡。刚好国内的很多平台，逐步开放了国际注册，比如：微信，熊猫TV，映客等等。

总而言之，和欺诈分子的对抗中，虚假号码占了很重要的角色。在不断的对抗中，我们尝试了各种各样的方法去检测、识别虚假号码；同时，黑产也在持续的裂变中，发明了很多规避检测的手段。

关键词: 互联网黑产 反欺诈 风控 虚假号码 大数据

分享到

回复 引用 举报

c0de

级别: P6_资深安全攻城狮

加关注 写私信

沙发 发表于: 07-13 只看该作者

同小盾就是同盾吗 

回复 引用 举报

hades

级别: Master

加关注 写私信

板凳 发表于: 07-13 只看该作者

回 1楼(c0de) 的帖子

是的 ~ 

回复 引用 举报

c0de

级别: P6_资深安全攻城狮

加关注 写私信

地板 发表于: 07-14 只看该作者

文章什么时候出来，坐等！ 

回复 引用 举报

« 返回列表 上一主题 下一主题 回复主题 发表主题

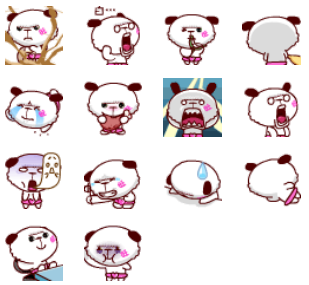
武鸣虾壳

Re:【反欺诈专栏】互联网黑产剖析——虚假号码 限100 字节

如果您提交过一次失败了，可以用”恢复数据”来恢复帖子内容

进入高级模式

默认表情 旺旺



发 布 回复后跳转到最后一页