

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。

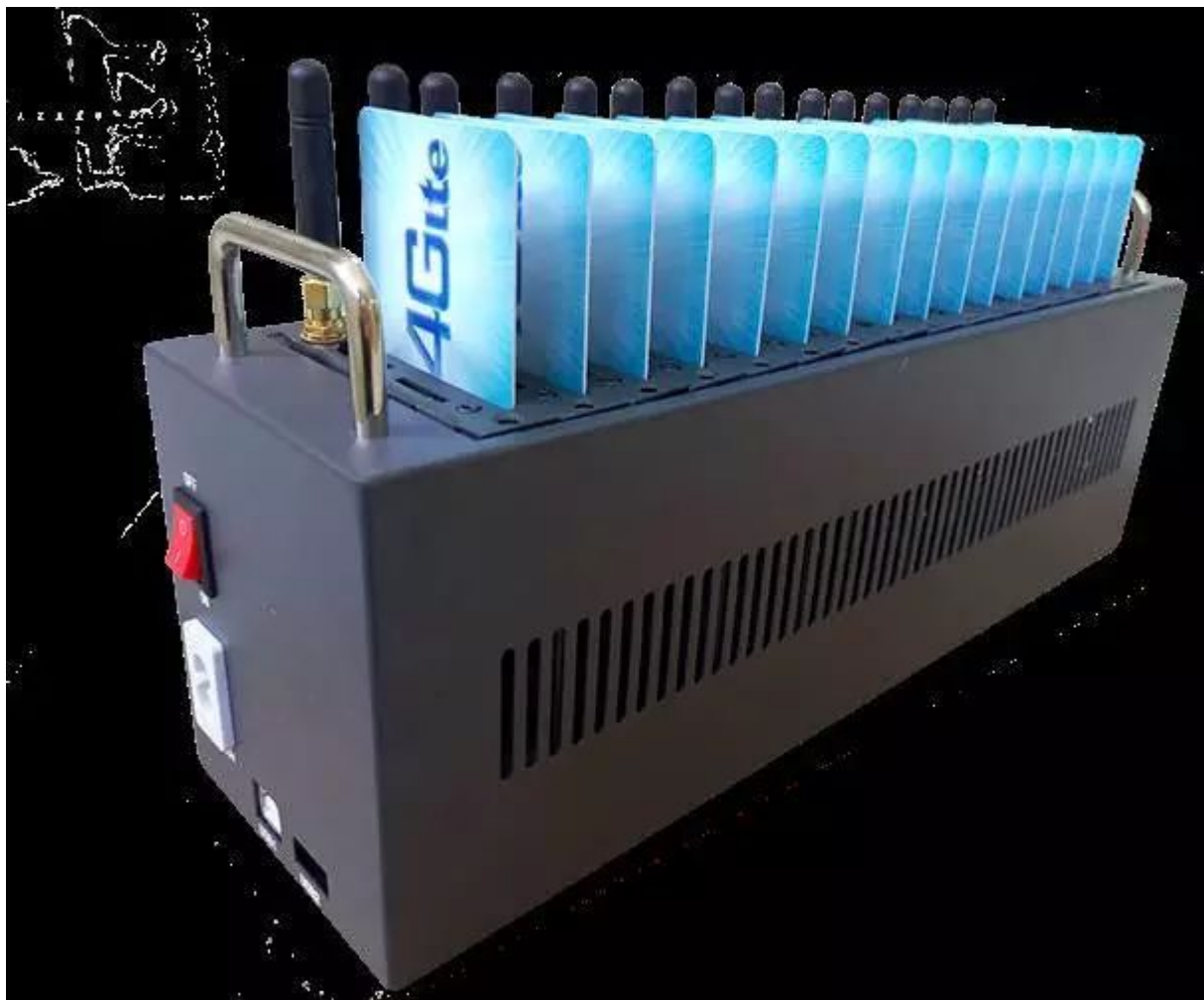
此外，还有大批虚假号码，被黑产团伙直接持有，他们会自己开发自动化工具，来完成验证码接收和使用。目前这批虚假号码的规模无法估计。下面，来一起见识一下虚假号码。

“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

”



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

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、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，

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？

会员登录

会员注册

第一次使用的客户请点击[这里](#)查看使用介绍

会员类型：☒ 用户 ☐ 开发者 ☐ 听码人员

登录账号：

* 4-20个英文、数字或英文数字组合

登陆密码：

* 20字符以内

确认密码：

* 20字符以内

手机号码：

*

Q Q 号码：

*

电子邮箱：

*

收款帐户 (用于提现，请认真填写)

支付宝姓名：

*

支付宝帐号：

*

注册

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

猫卡 87.0-(未发现加密狗)

自动服务

任务设置

发送短信

发送短信

拨打电话

WAP浏览

综合管理

整理信息

修改串码

收发记录

查看日志

自动回复

配置注册

版本切换

快捷助手

其他功能

退出系统

串口号	通道工作状态	本机号码	任务名称/流量	设备串码	连数	闲发	业务(发/收)	短信(发/收)	信号	整理结果1	整理结果2	用户已拨号(通)
COM11	未启动				0	不限	0/0	2/0				
COM12	未启动				0	不限	0/0	2/0				
COM13	未启动				0	不限	0/0	2/0				
COM14	未启动				0	不限	0/0	2/0				
COM22	未启动				0	不限	0/0	2/0				
COM23	未启动				0	不限	0/0	2/0				
COM25	配置语音信息				0	不限	0/0	2/0				
COM26	启动选中通道				0	不限	0/0	2/0				
COM27	停止选中通道				0	不限	0/0	0/0				
COM29	启动所有通道				0	不限	0/0	2/0				
COM30	停止所有通道				0	不限	0/0	2/0				
COM31	暂停服务				0	不限	0/0	0/24				
COM32	选中端口发送短信				0	不限	0/0	2/0				
COM33	强制启动卡间互打				0	不限	0/0	0/0				
COM34	本机号码											
COM35	呼叫转移设置											
COM36	配置AT代码B代码											
COM37	短信整理结果											
COM38	卡池操作											
COM39	任务管理											
COM40	其他工具											
COM41	打开目录和文件											
COM42	开机自动上网选择											
COM43	清空选中通道多数记录											
COM44	清空所有通道多数记录											
COM45	删除已发、接收、失败和待发信息											

一键设置选中通道呼叫转移(无条件呼转)

一键设置所有通道呼叫转移(无条件呼转)

一键设置选中通道呼叫转移(关机呼转)

一键设置所有通道呼叫转移(关机呼转)

一键取消选中通道呼叫转移

一键取消所有通道呼叫转移

通道数: 16/0

移动87-0解密

软件下载地址: <http://www.smscp.com>

2016-09-06 出品

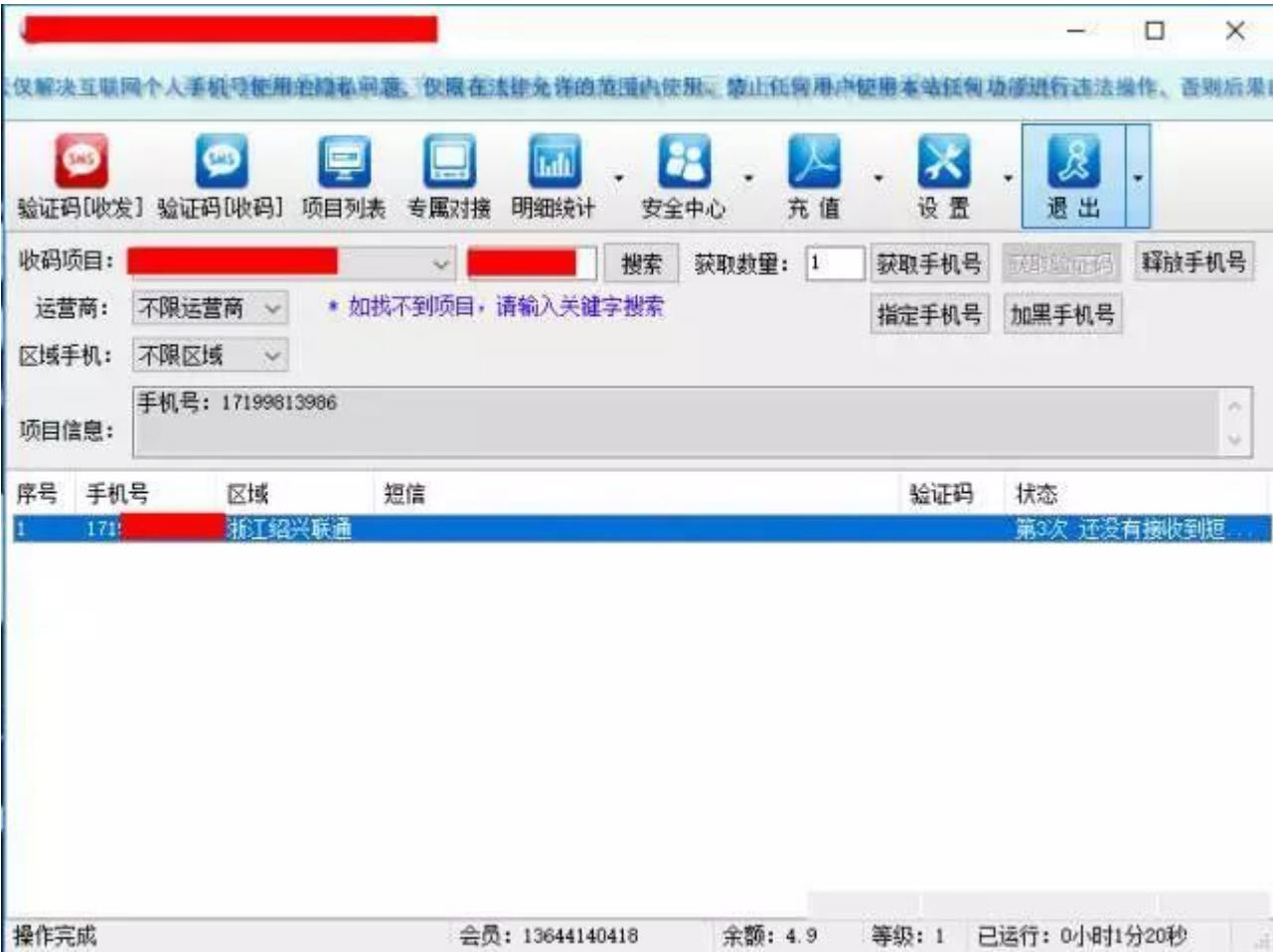
使用语音验证码一定程度上提高了验证码获取和使用的难度，但依然无法阻止羊毛大军脚步。

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匹配的第一条短信，会显示在我的个人界面中。其他人不能

—□×

仅解决互联网个人手机号使用的隐私问题，仅限在法律允许的范围内使用。禁止任何用户使用本站任何功能进行违法操作，否则后果自负。

SMS

SMS

验证码[收发] 验证码[收码] 项目列表 专属对接 明细统计 安全中心 充值 设置 退出

收码项目:

搜索

 获取数量:

1

获取手机号

获取验证码

释放手机号

运营商:

不限运营商

 * 如找不到项目，请输入关键字搜索

指定手机号

加黑手机号

区域手机:

不限区域

项目信息:

手机号: 171 验证码: 978661, 在5分钟内有效。如非本人操作请忽略本短信。(来自10690819316872071170)

序号	手机号	区域	短信	验证码	状态
1	171	浙江绍兴联通	验证码: 978661, 在5分钟内有效。...	978661	获取验证码成功

978661 已复制

会员: 13644140416

余额: 4.9

等级: 1

已运行: 0小时2分5秒

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，然后自动封号。

所以，一般还会配合模拟器，或改机工具进行。

新用户福利

分享

恭喜获得 专享礼包

¥15

新用户专享红包

满15元可用



¥12

免蜂鸟专送配送费

可减免3单，每单最高减4元
限2017.01.28前使用



新用户专享商家
最高优惠30元

立减20



正宗重庆麻辣烫（顺福路...）

★★★★★ 月售1927单

¥22起送 / 配送费¥4

39分钟

新 新用户下单立减20.0元

立减20



蜜菓奶茶&kiss鸡排(和谐...)

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接口。

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、投票抽奖等。

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

	梵蒂冈 梵蒂冈: [红包]恭喜发财，大吉大利！	18:16
	实打实2 实打实2: [红包]恭喜发财，大吉大利！	18:12
	李三 李三: [红包]恭喜发财，大吉大利！	18:10
	阿斯顿 阿斯顿: [红包]恭喜发财，大吉大利！	18:01
	陈凯撒 陈凯撒: [红包]恭喜发财，大吉大利！	17:53
	撒旦 撒旦: [红包]恭喜发财，大吉大利！	17:48
	II啊比 II啊比: [红包]恭喜发财，大吉大利！	17:42
	陈氏 陈氏: [红包]恭喜发财，大吉大利！	17:20
	橙橙 橙橙: [红包]恭喜发财，大吉大利！	17:06
	段呗 段呗: [红包]恭喜发财，大吉大利！	16:46

由于微信不会对账号进行清洗，一个手机号注册过之后，其他人就不能再继续注册，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转手，赚取差价。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。

用户列表							
功能设置							
功能设置2							
换IP设置							
系统设置							
服务免责声明							
日志时间	运行日志	用户名	密码	邮箱账号	邮箱密码	手机号码	
1	2016-11-29 18:...	注册成功!	170714...	96	96	0d	170714...
2	2016-11-29 18:...	注册成功!	171363...	98	98	tee	171363...
3	2016-11-29 18:...	注册成功!	183148...	22	22	nb4	183148...
4	2016-11-29 18:...	注册成功!	171983...	94	94	bp	171983...
5	2016-11-29 18:...	注册成功!	170893...	48	48	0cy	170893...
6	2016-11-29 18:...	注册成功!	159202...	59	59	8y	159202...
7	2016-11-29 18:...	注册成功!	137903...	69	69	uu0	137903...
8	2016-11-29 18:...	注册成功!	153147...	74	74	9a	153147...
9	2016-11-29 18:...	注册成功!	170764...	15	15	any	170764...
10	2016-11-29 18:...	注册成功!	183414...	92	92	vp0	183414...

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，

下图是同一个工作室开发的扫货软件。

全平台下单

价格：¥0.50 | 下载次数：79803 | 有效期内免费维护 | 更新时间：2016-12-22

全平台下单 简介：多端口下单软件。支持APP端、PC端、WAP端、手Q端、京致衣厨、PC端抢购模式等。特色：软件免费使用！ 详细介绍>>

 软件下载

APP下单

价格：¥110.00-¥1000.00 | 下载次数：31731 | 有效期内免费维护 | 更新时间：2016-12-28


手机批量订购 简介：软件从手机客户端(APP端)下单，软件适用于：扫货下单，进货的用户和商家刷单/个人s手/刷单工作室。1、支持下大聚会商品，2、支持礼品卡付款、易付宝代付和银行卡快捷支付，支付宝付款 详细介绍>>

 软件下载

APP端下单

价格：¥120.00-¥1200.00 | 下载次数：30979 | 有效期内免费维护 | 更新时间：2016-12-27

手机订购 **手机APP下单**，扫货、刷单软件。软件支持支付宝在线付款，有货自动购买，激活抵用券使用以及上传赠票资质以及图片。 详细介绍>>

 软件下载

电脑端下单

价格：¥99.00-¥800.00 | 下载次数：15674 | 有效期内免费维护 | 更新时间：2016-12-28

批量订购 简介：软件模拟去电脑端(PC端)网页下单，软件适用于：扫货下单，进货的用户和商家刷单/个人s手/刷单工作室。特色功能：1、支持下大聚会商品 2、礼品卡付款、易付宝代付和银行卡快捷支付以及支付宝付款 3、支持下单成功后更新订单状态。 详细介绍>>

 软件下载

电脑端下单

价格：¥99.00-¥800.00 | 下载次数：15498 | 有效期内免费维护 | 更新时间：2016-12-27

京东批量订购 简介：软件通过网页端(PC端)去下单，支持扫货和刷单。特色功能：1、快钱直接付款。2、关键字搜索下单提高关键字转化率等。 详细介绍>>

 软件下载

电脑端下单

价格：¥1000.00 | 下载次数：7975 | 有效期内免费维护 | 更新时间：2016-12-26

批量下单 软件从电脑端(PC端)下单，软件适用于：扫货下单，进货的用户和商家刷单/个人s手/刷单工作室。1、软件支持使用QQ账号、杉德宝账号登录下单。2、软件支持使用账户积分、优惠券、购物卡等，亦支持导入抵用券下单过程充值并使用。3、软件采用支付宝付款，支持将订单信息导... 详细介绍>>

 软件下载

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。

<div> <div>手机抢红包</div> <div>HOT</div> </div>		价格：¥ 50.00-¥ 280.00 下载次数：661 有效期内免费维护 更新时间：2016-07-11
<div>手机抢红包</div>	详细介绍>>	📄 软件下载
<div> <div>实名认证领红包</div> <div>HOT</div> </div>		价格：¥ 680.00 下载次数：655 有效期内免费维护 更新时间：2016-08-01
<div>实名认证领红包</div>	简介：软件模拟手动通过 电脑端（PC端）网页去易付宝补全资料实名认证领红包。 详细介绍>>	📄 软件下载
<div> <div>APP红包雨</div> <div>HOT</div> </div>		价格：¥ 280.00-¥ 380.00 下载次数：646 有效期内免费维护 更新时间：2016-11-07
<div>APP红包雨</div>	详细介绍>>	📄 软件下载
<div> <div>大牌对战</div> <div>HOT</div> </div>		价格：¥ 60.00-¥ 380.00 下载次数：640 有效期内免费维护 更新时间：2016-06-13
<div>大牌对战</div>	简介：软件模拟手动去 电脑端（PC端）去参加大牌对战活动。 详细介绍>>	📄 软件下载
<div> <div>新人199元大礼包</div> <div>NEW</div> <div>1123</div> <div>HOT</div> </div>		价格：¥ 480.00 下载次数：583 有效期内免费维护 更新时间：2016-12-23
<div>新人199元大礼包</div>	简介：软件模拟手动去手机客户端（APP端）领取199大礼包。 详细介绍>>	📄 软件下载
<div> <div>母婴app领券</div> </div>		价格：¥ 380.00 下载次数：575 有效期内免费维护 更新时间：2016-10-25
<div>母婴app领券</div>	简介：软件模拟手动去 手机客户端（APP端）去领券。 详细介绍>>	📄 软件下载
<div> <div>APP注册</div> <div>NEW</div> </div>		价格：¥ 900.00 下载次数：567 有效期内免费维护 更新时间：2016-11-22
<div>APP注册</div>	详细介绍>>	📄 软件下载

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，还存在一些其他的渠道。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，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照片。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。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、验证等操作
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

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。

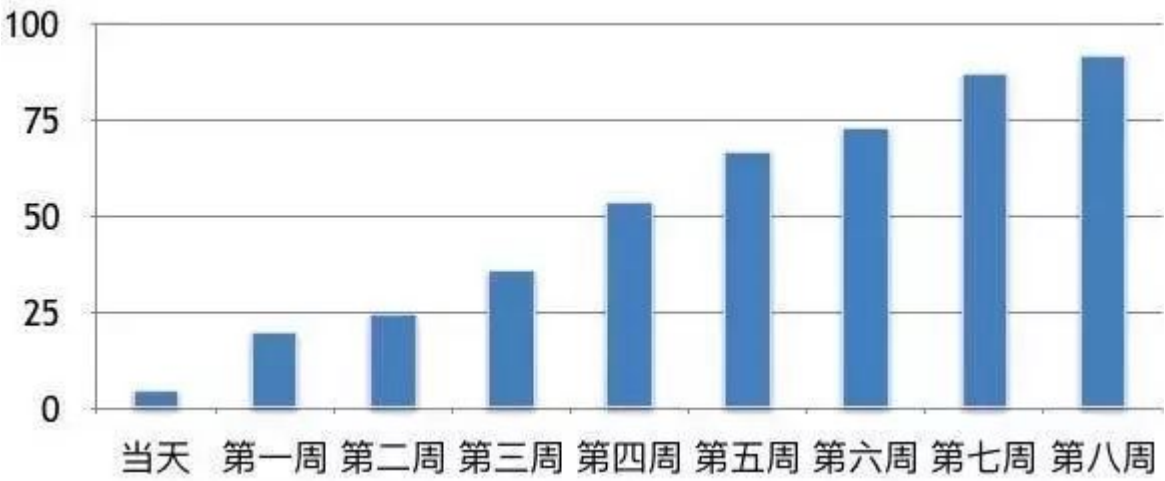
在和虚假号码的对抗中，我们必须关注各个平台的优惠活动，优质的活动必然引来羊毛党的关注。而且，并不是每一个优惠活动都可以被薅，这需要我们投入一定的力量进行监控。比如，之前客户反馈的一个案例，新用户注册之后，将得到80元的新手礼包，不能提现，但是可以用于购买贵金属。期间，羊毛单通过操作众多账号，批量买入和抛出，80元礼包瞬间被抢光。如果不是事后的数据分析捕捉到这个异常行为，可能都不会意识到有如此走心的羊毛党。

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。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



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，欺骗我们。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

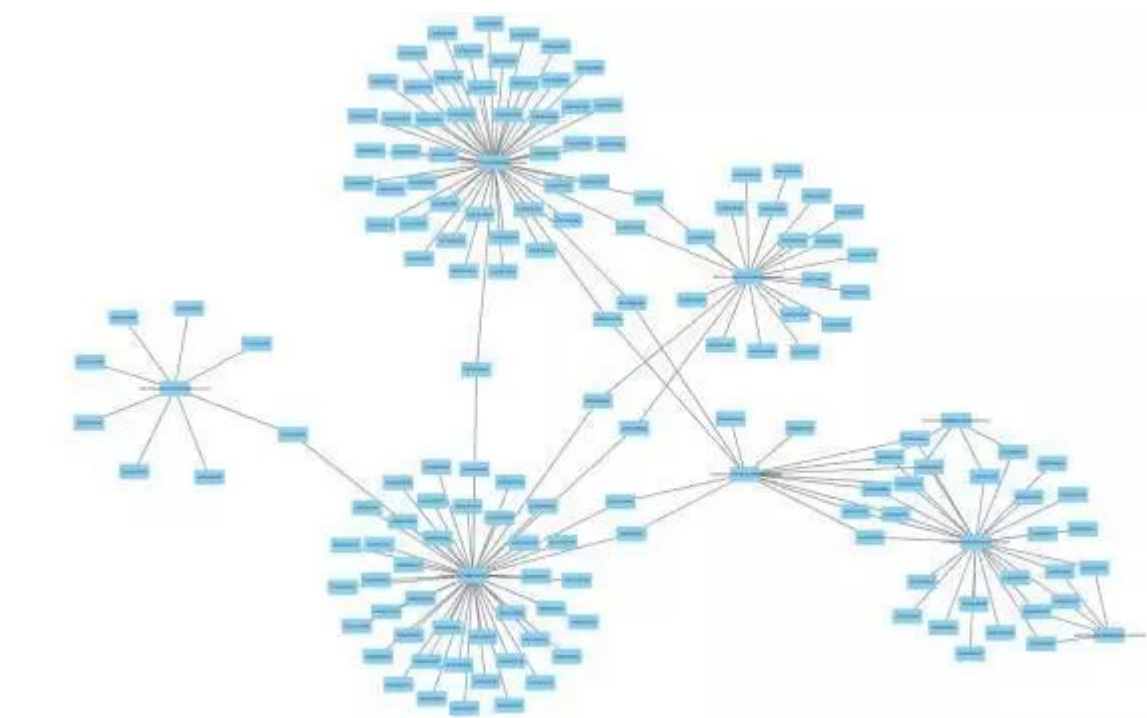
复杂网络，是我们识别虚假号码的方案中最为出色的一种。

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

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

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

但这并不代表虚假号码会从此消失。

国内
可用

缅甸手机卡

· 全新未激活卡 永久0月租



一手批发 大量现货

注册微信号 陌陌等
(可收发信息 信号强卡稳定)

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

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

点击收藏 | 0 关注 | 0

[上一篇：\[福利贴\] 招募大牛完善漏洞信息，...](#) [下一篇：【反欺诈专栏】互联网黑产剖析——代...](#)

1. 3 条回复



同小盾就是同盾吗

0 回复Ta



[hades](#) 2017-07-13 08:45:40

是的 ~

0 回复Ta



[c0de](#) 2017-07-14 08:24:29

文章什么时候出来，坐等！

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)