国舜
www.unisguard.com

互联网渠道营销活动安全防御研究

“羊毛党”威胁分析与研究

国舜股份 副总裁 汤志刚

国舜

目录

CONTENTS

认识羊毛党

分析薅羊毛

防范羊毛党

01

认识羊毛党

苹果36技术薅羊毛过亿

- 苹果公司在向用户收取费用时，设计了40元以下小额充值，可以不经验证购买，先派发商品的安全策略，目的是为了改善用户体验。
- 然而，狡诈的黑产人员却把它发展成一门可以牟利的生意。自2016年初开始，一种名为“苹果36充值”的技术悄然在黑产圈盛行，游戏行业成为了最主要的受害群体。利用这一技术薅羊毛过亿。
- 黑产人员利用苹果的这一策略漏洞，绑定一张没有余额的银行卡或者虚拟银行卡，再通过家庭共享支付（即用一个主帐号绑定最多8个附属帐号，所有附属帐号的消费都可以通过主帐号进行支付）进行盗刷。通过该模式，薅羊毛过亿。

来源：http://www.freebuf.com/articles/others-articles/133311.html

电信翼支付新用户注册送话费

- 2016年10月，电信旗下的翼支付，在部分省份开展“新注册用户送10到15元的抵用券”的活动。
- 职业刷客申宏远，早早就盯上了。他先找到专门提供手机卡的卡商，弄到上万张手机号码。再找到作为黑客集散中心的软件平台，利用这些手机号批量操作，成功注册上万个翼支付新用户。整个流程他轻车熟路，只花了半天时间。注册成本是2000元。
- 拿到代金券后，他找到一家淘宝店家，专门提供话费充值服务，转手将代金券8折卖出。而淘宝店再以9.5折卖给买家，进行手机充值。整个活动薅羊毛10万元。这条产业链环环相扣，所有的人，将翼支付的10万元利益，瓜分殆尽。

来源：http://xiaoywz.com/post-57.html

中国移动被黑卡刷走8.2万G流量

- 中国移动面向消费者推出的流量交易平台爱流量，已经被持有大量黑卡的刷单手攻占。2016年12月10日至2017年1月6日期间，爱流量面向消费者推出有奖答题活动，每天面向消费者推出10万份流量，每份300M。每个手机号每日限领一份。6点活动开始时网页崩溃，6：05网页恢复正常后，奖励流量已抢购一空。“全都是软件刷走的”，一位业内人士向记者出示了截图显示，一份命名为“答题寻宝”的软件，对接了40898个手机号，“这些手机号都是黑卡，不是真实用户。
- 目前，中国移动官网流量1G售价约47.5元，但倒卖爱流量的黑市上，1G售价均低于30元，大多售价在26-28元左右。爱流量一次活动，中国移动被薅400多万元的“羊毛”。

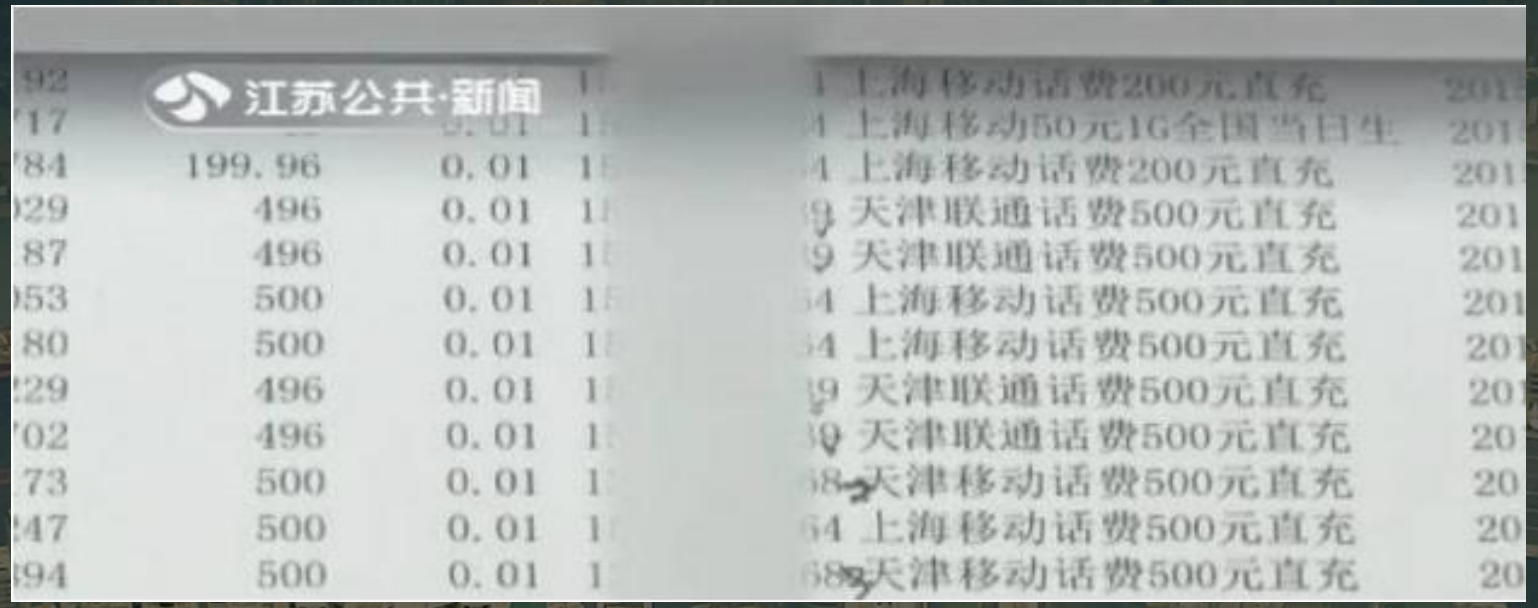
来源：https://www.qcgzxw.cn/?p=742

淘宝新用户注册

- 1月份，淘宝针对新注册用户，出了一系列的激励政策。而活动很快沦为黑产“薅羊毛”的对象，并在一周内形成完整产业链。
- 刷客小欣研究了一轮风控规则后，发现确实有利可图。他从软件平台，购买了代注册和验证码收取业务，“一天薅出来7000元”。

来源：http://www.maijia.com/bbs/thread-69190-1-1.html

1分钱充话费



- 90后的南京小伙小刘正处于无业状态，上网时，QQ聊天群里的爆出了一个攻略，只需花一分钱就能获得上百元的话费。抱着试一试的心态，小刘按照攻略中的步骤操作，在某充值平台篡改了支付金额，果真，只支付了1分钱，200元话费就到账了。
- 小刘开始闷声发大财。他通过QQ、微信、微博等宣称自己可以低价代充话费，不到账不收钱。就这样，小刘先后在这个平台充值了58次，共花费不到一块钱，却到账了26000余元话费。

来源：https://www.anquan.org/news/2731https://www.anquan.org/news/2731

黑客盗刷50万红包

- 2016年底，某公司在进行平台自查时发现手机APP红包业务有异常交易信息，账户内五十万元不翼而飞。据工作人员透露，其APP正在进行一场推广，通过发送积分的方式吸引用户关注并参与，一旦积攒到相应积分便可以换成现金，最终通过微信支付方式送达个人账户。
- 在网上暗藏一批专门盯着这些红包的黑客，他们利用自身技术寻找漏洞，通过作弊软件修改参数，最终以薅羊毛的方式将红包盗刷一空。

来源：http://www.ifuun.com/a20174211836967/

什么是“羊毛”？

随着金融行业互联网化程度越来越深，互联网营销活动的深度和频度都在不断提升。当前互联网营销活动的典型模式是通过开展一些优惠活动吸引活跃用户，例如注册送代金券等。每一份奖励涉及金额都很少，只有几块钱甚至几毛钱，这些金额很小的奖励被称为“**羊毛**”。

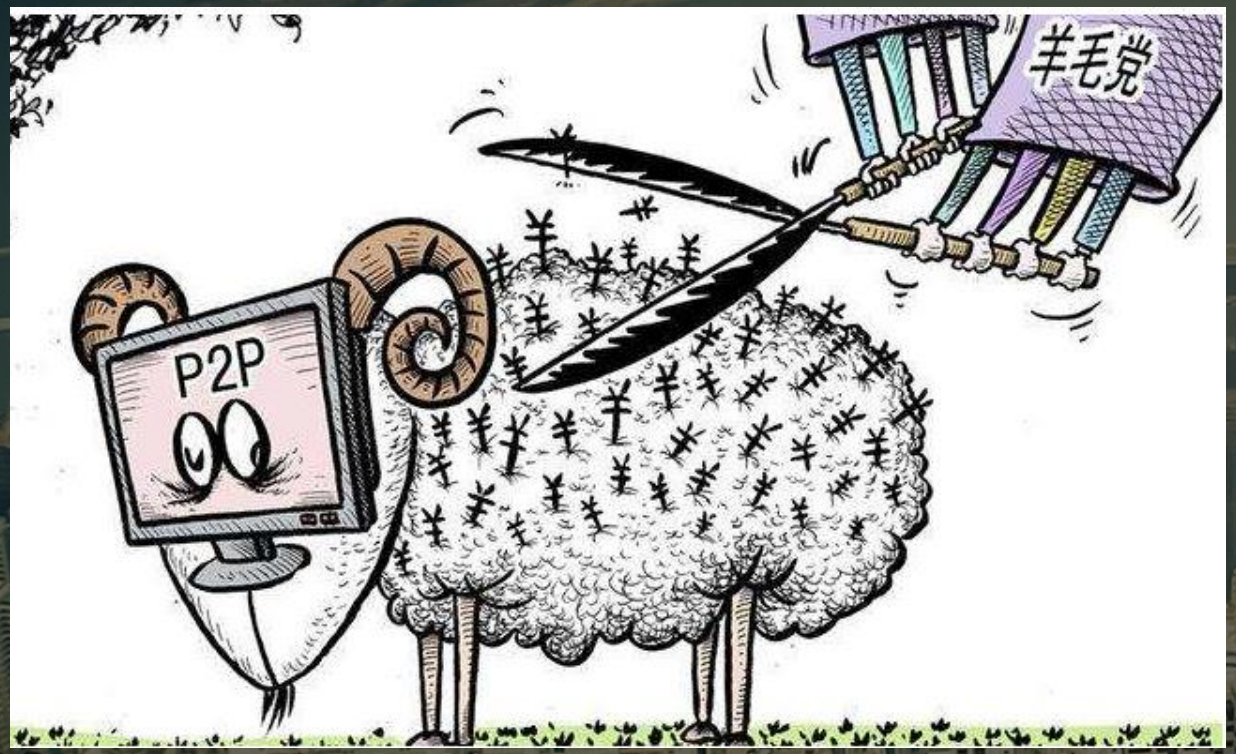
薅羊毛平台

http://www.haoyangmao.cc/

http://www.tuancai88.com/

http://www.woolworker.com/

认识羊毛党



有一些人有选择地参与活动，采取各种非正常手段以相对较低成本甚至零成本换取“羊毛”水平利润，以量变最终达到质变。这一行为被称为**“薅羊毛”**，而关注与热衷于“薅羊毛”的群体就被称作**“羊毛党”**。

恶意“刷羊毛”

一些地下产业研究各种手段，突破互联网营销活动的原始意图，获取远超正常羊毛水平的收益。由于互联网营销活动展开频繁，**周期短，种类多，变化大**，金融业对恶意刷羊毛的攻击难以防范。

分类“羊毛党”

“羊毛党”的攻击手法及作案风格多种多样，针对不同的用户群体有不同的获利方式。

“自撸”党

红包牛

收集了一堆签到网站或者任务站，这种网站每天只需要签到或完成每天的任务就可以领取一定的奖励，然后定期提现。同时他们还关注各类时效性的红包和现金活动，一般多号操作。

实惠牛

以家庭主妇为主，目的为减少生活开销为主。他们关注淘宝京东等各大网购平台活动。撸0元单/优惠券哪里优惠去哪里。

理财牛

此类人专注网贷平台活动（包括虚拟币）有一定资金投入，而且拥有多套资料。当然收入和风险成正比，此类收入5000以上，资料和本金越多收入越多。

技术牛

利用各种专业软件工具，对企业系统进行扫描，发现漏洞，展开攻击。走的是灰色路线。

“倒买倒卖”党

01

黄牛

通过商家活动获得的购物卡,优惠券,加油卡,电影票，等等。统一由黄牛便宜收购，然后再卖给需要的人。也有回收实物卖给超市的。

02

放单牛

通常都是做网贷的（多数有自己的群或者博客,QT,YY），也就是通过特殊渠道拿到的内部单，然后通过返佣形式下放给别人做，自己从中赚差价。

03

推广牛

如今大多数平台都会有推广奖励，一般都是有自己的固定的用户群，比如站长，主播，群主，微信公众号等等。也有花钱投放广告推广的。

“综合”党

项目牛

通过商家活动获得的购物卡，优惠券,加油卡,电影票，等等。统一由黄牛便宜收购，然后再卖给需要的人。也有回收实物卖给超市的。

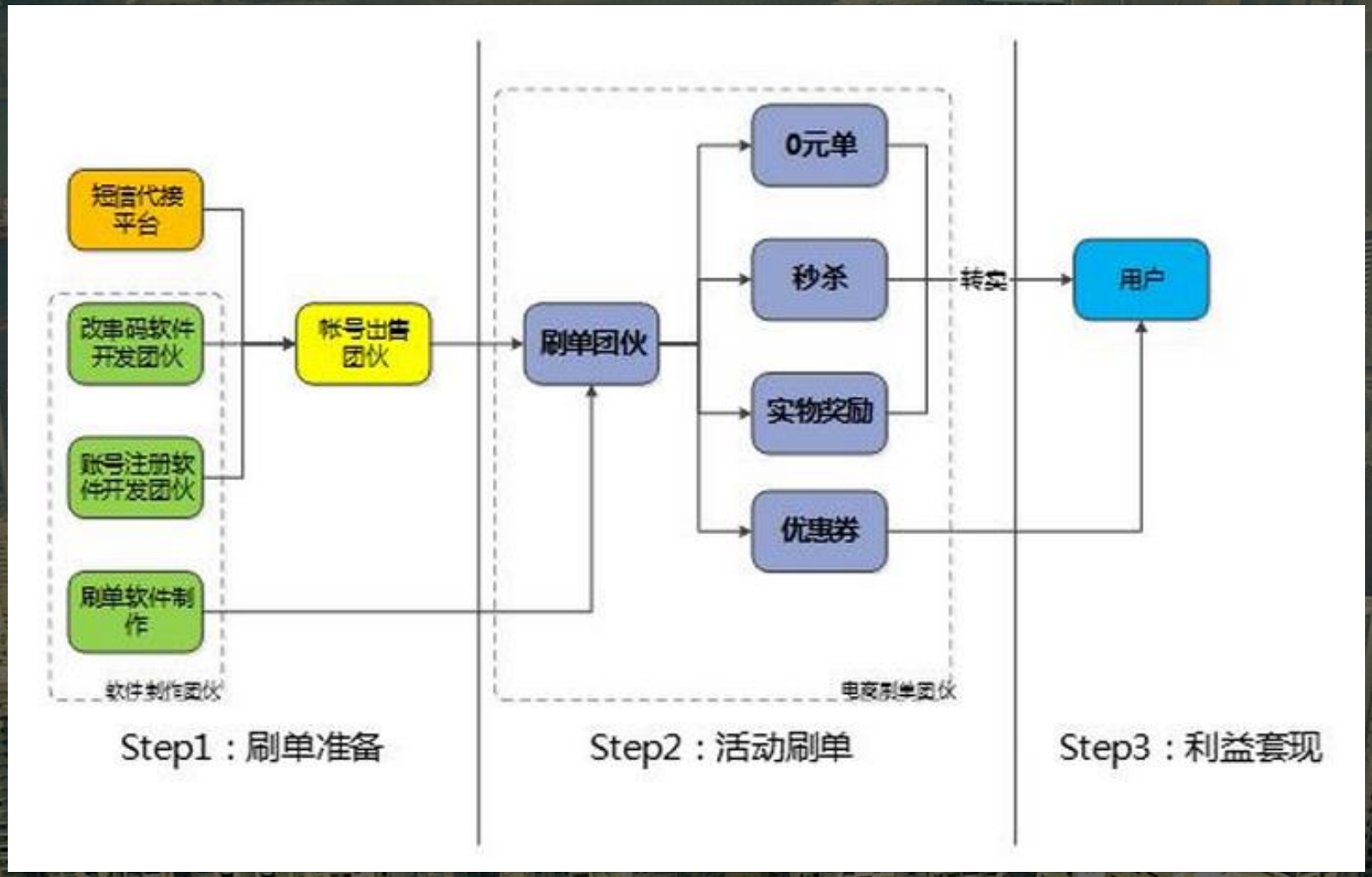
混合撸

通常都是做网贷的（多数有自己的群或者博客,QT,YY），也就是通过特殊渠道拿到的内部单，然后通过返佣形式下放给别人做，自己从中赚差价.


02
分析薅羊毛

黑产‘羊毛党’

在诱人的利益驱动下，黑产“羊毛党”快速形成了庞大而完整的产业链。



黑产“羊毛党”的产业链

最前端是软件制作团伙，专门制作各种专业的自动、半自动的黑产工具，比如自动注册机、刷单自动机等，大大增加了羊毛党的操作效率。

黑产“羊毛党”的产业链

在中端，有账号出售团伙，他们通过黑客的地下社工库找到一些用户数据，或直接从各大平台窃取用户信息，公开售卖;另外，还有短信代接平台，可以自动生成手机号码，并能接受验证码。各大软件平台的背后，是一群卡商，他们负责采集卡、养卡，提供了这条产业链的养料。养卡需要专业设备，行话称为“猫池”和“卡池”，猫池需要放在卡池中，联动操作。

黑产“羊毛党”的产业链

后端是职业刷手进行具体操作。他们常见的操作模式是，三五人组成一个工作室，批量注册。一个毫无安全防备的网贷平台，面对这样的高级刷客，几乎无还手之力，他们每日收入可达到几万，甚至几十万。除了冒一定的风险，这简直就是一个一本万利、坐地收钱的生意。

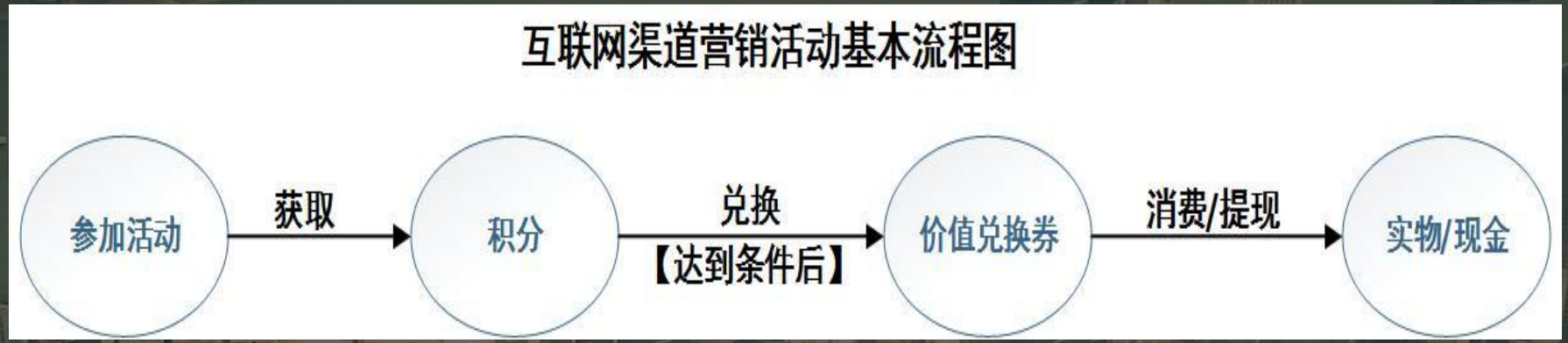
黑产“羊毛党”的产业链

卡商程XX，养了2万张卡。租了一个小平房，将卡池装上后，连接电脑，装上相应的软件，就可以利用手机卡批量注册。在这个20多平米的隐秘小房间中，卡池轰轰运转。每天晚上他将卡一张张取下来，更换新卡——这就是他的日常，小心翼翼养卡，就像浇灌自己的摇钱树，毫不马虎。

2万张卡，前期投入总金额，大概为40多万。而这些卡，每个月都能为他滚动近30万的收入；遇到旺季，每个月能收入近百万。像程XX这样的卡商，在业内只能算小规模，还有一些大卡商，手里养着几十万张卡，“每日滚金几十万”。

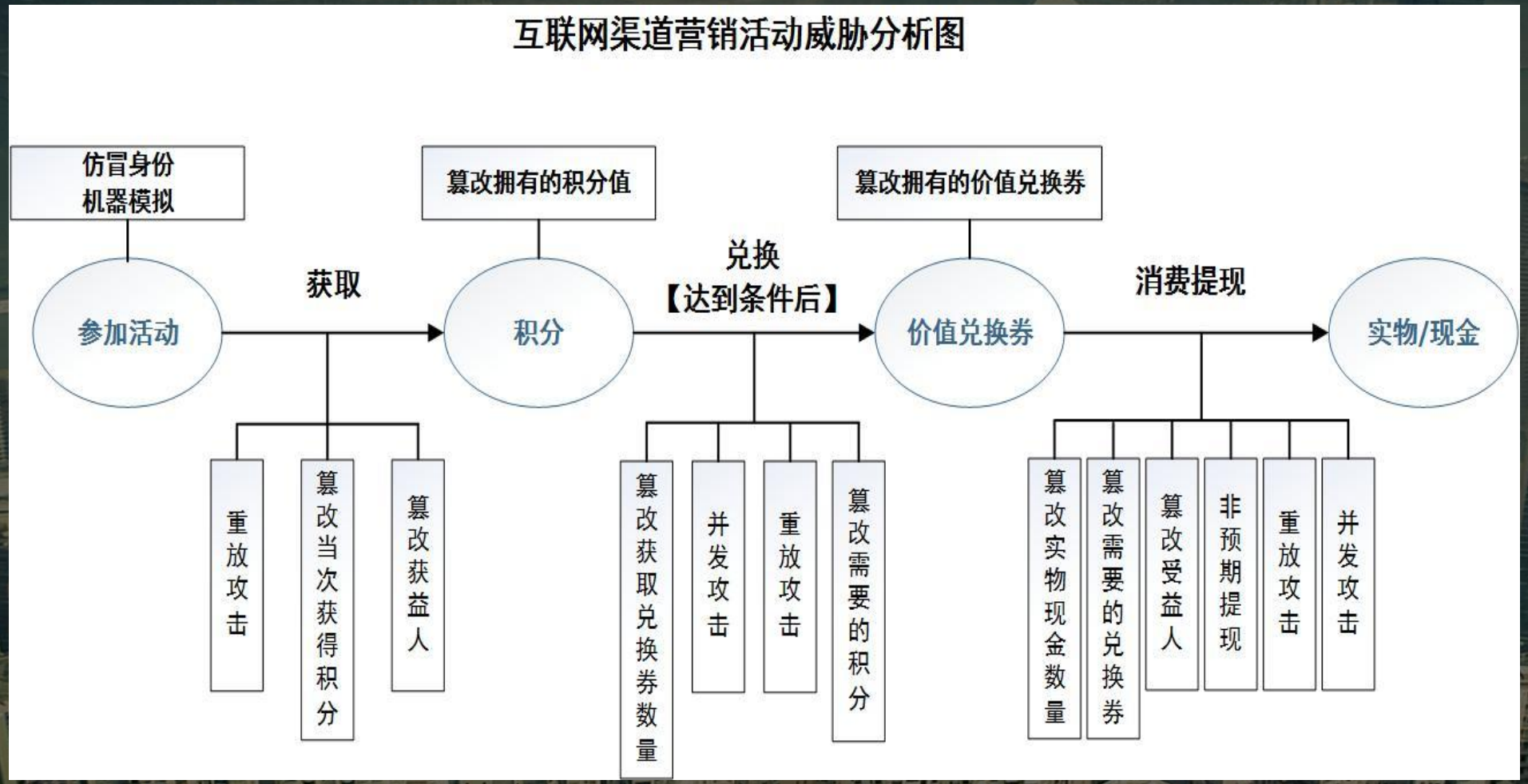
互联网渠道营销活动

互联网营销活动虽然变化万千，但仔细分析，还是能总结其规律。

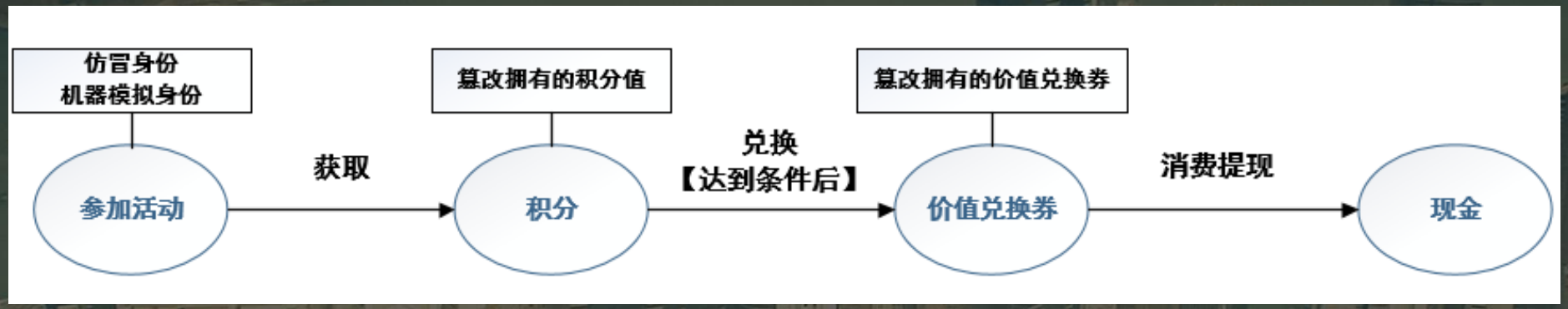


金融机构为了增加会员的参与度推出会员打卡送积分的活动，客户通过“参加活动”——“会员打卡”，获取积分，等积分达到一定条件后，比如1000分以上，就可以用积分兑换“价值兑换券”——“手机充值券”，将手机充值券消费实现手机充值，最终完成整个营销活动。

互联网渠道营销威胁分析

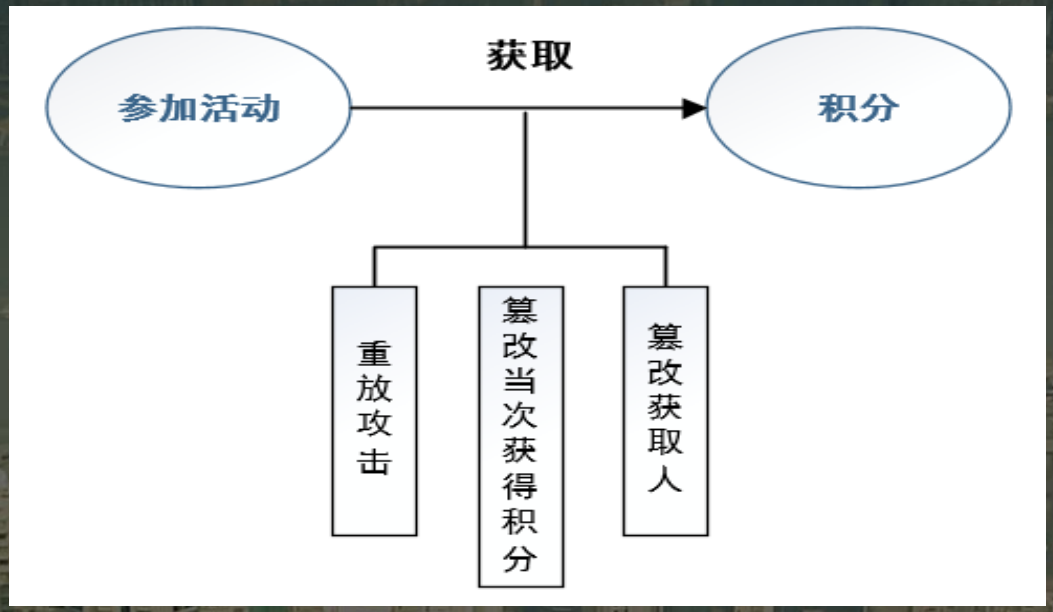


互联网渠道营销威胁分析



- 在用户参加活动环节中，黑色产业链的后端可以编写程序进行机器程序来实现自动化活动，增加羊毛党攻击的效率，如实现程序每天自动打卡换取打卡积分；也存在仿冒他人身份等攻击方式。
- 可用黑客攻击手段直接篡改会员所拥有的积分值来实现获利。
- 可用黑客攻击手段直接篡改会员所拥有的价值券数量来实现获利。

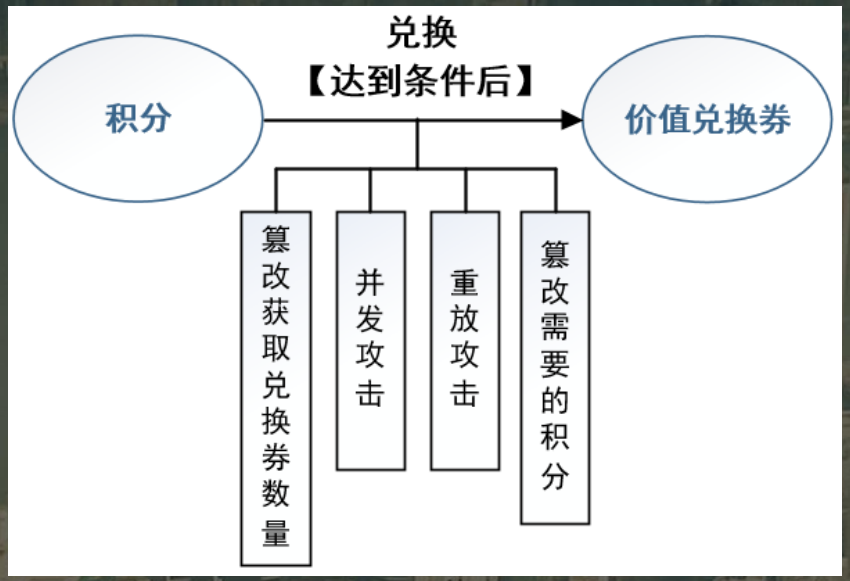
互联网渠道营销威胁分析



在获取积分环节，黑色产业链主要通过对信息系统模块之间的通讯展开攻击，分析通讯协议，对通讯内容进行篡改或重放，实现多样攻击。包括：

- 重放攻击，如将打卡一天的信息包重放100次，获得100倍的奖励积分；
- 篡改当次获取的积分，如本来打开一次获20分，篡改通讯包，实现获益200分；
- 篡改获益人，如将所有人打卡的积分都记在某个用户名下。

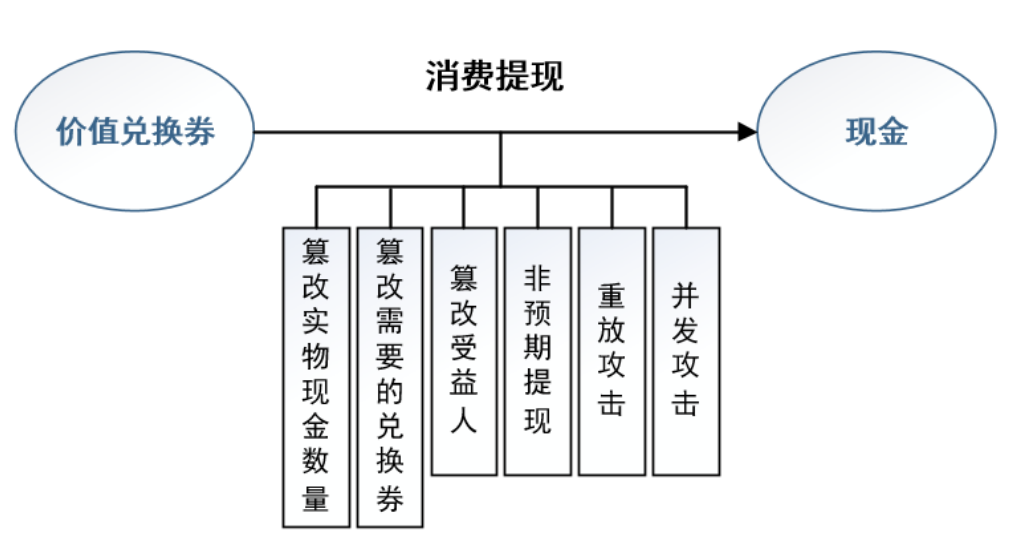
互联网渠道营销威胁分析



在积分兑换环节的攻击也是针对信息系统模块之间的通讯，分析通讯协议，对通讯内容进行篡改或重放，实现多样攻击。

- 篡改获取兑换券的数量，如800积分兑换一张购物券，将兑换的信息包篡改，实现800积分兑换十张购物券。
- 重放攻击，如800积分兑换一张购物券，将兑换的信息包重放100次，获得100张购物券；
- 并发攻击，如同时发送多个兑换请求，实现多个兑换但只扣减一份积分；
- 篡改需要的积分，如800积分兑换一张购物券，将兑换的信息包篡改，实现80积分兑换一张购物券。

互联网渠道营销威胁分析



消费/体现提现环节的攻击也是针对信息系统模块之间的通讯，分析通讯协议，对通讯内容进行篡改或重放，实现多样攻击。

- 篡改实物/现金兑换的数量；
- 篡改需要的兑换券；
- 篡改获益人；如通过修改手机号码等方式，实现手机充值的转移。
- 非预期提现；如突破体现提现限制，把不允许体现提现的钱给提现了。
- 重放攻击；
- 并发攻击。

我们来看一个案例

您肯定关注过微信公众号。

某证券公众号系统推出吸引会员的活动，关注后每日签到可以赚取积分，一定量的积分可兑换手机充值卡。

签到积分获取规则

- 签到可获得10积分
- 当月连续签到累计达10天，可额外获得30积分
- 当月连续签到累计达20天，可额外获得50积分
- 当月全部签到，可额外获得100积分

我们来看一个案例

经过检测发现该系统签到处没有校验用户是否重复签到，可利用此漏洞进行刷积分，通过重放攻击短期内获得大量积分。

我们来看一个案例

接下来利用获得的大量积分去兑换奖品（充值卡），成功兑换后即可使用进行充值,充值的默认号码为绑定的号码，但是通过改包方式发现服务器端未对充值号码进行校验，可修改号码进行充值。

后果分析

01 敌对企业

敌对企业可将信息投放到羊毛党交流圈，利用零散的薅羊毛行为用户对企业进行攻击，将导致企业损失大量资金。

02 网络犯罪人员

从事网络黑产的非法人员如果介入到其中，可能会开发出针对性程序盗取企业资金，企业损失可能将更大。

03 个人攻击

以个人为首的攻击，如普通用户发现有利可图切简便时，可不定时进行盗取小额的企业资金。

小结

在互联网渠道营销活动的各个环节都有可能被攻击，都可能导致损失活动资金，损失活动资金规模在各种攻击手段的重复下可能很大，同时破坏正常的活动秩序，损害正常用户的活动体验，导致活动无法实现预期成果。因此，结合互联网渠道营销活动业务特点，进行针对性的防御非常必要。


03
防范羊毛党

互联网渠道营销分析

导流	企业展开互联网营销活动，无论是促销还是优惠，都是为了导流。
过严	此时，如果制定过严的风控规则，会导致用户体验差，用户感觉企业没有诚意，很难实现导流的目的；
过宽	如果为了保证流畅的体验，规则放宽，必然会导致系统的安全性降低，被黑灰产盯上。
平衡	所以针对互联网营销活动的安全防护是用户体验与资金使用有效性的平衡。
策略	这就意味着防护不是一味地消灭所有的攻击隐患，而是增加攻击者的攻击成本，导致他们得不偿失，保证互联网营销活动的风险受控。

逻辑

奖励变现的便捷程度

增加时间成本

增加资金成本

防护策略

轻管控

保证用户体验

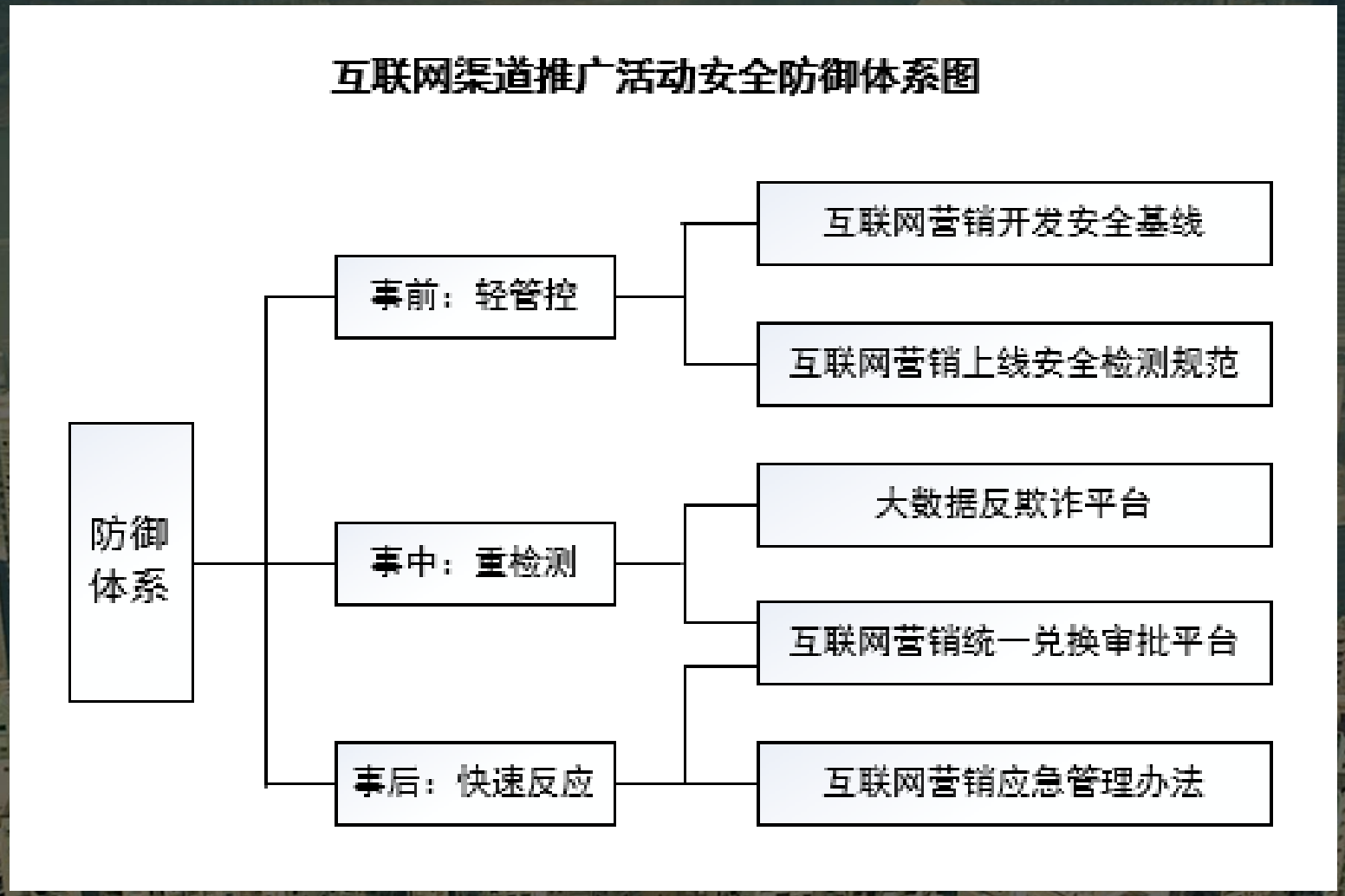
重检测

及时发现恶意行为

快速反应

第一时间快速止损

防护体系


互联网渠道推广活动安全防御体系图
防御体系
事前：轻管控
事中：重检测
事后：快速反应
互联网营销开发安全基线
互联网营销上线安全检测规范
大数据反欺诈平台
互联网营销统一兑换审批平台
互联网营销应急管理办法

开发安全基线

开发安全基线是针对互联网营销活动信息系统威胁分析的结果，制定相应的安全需求，安全设计要求，安全编码要求。并在互联网营销活动信息系统开发过程中实施管理，保证开发安全基线的落地。

开发安全基线

基础安全需求				
技术性安全	应用安全	网络/通信安全	部署安全	特殊安全需求
加密算法	身份认证 会话安全 访问控制 输入校验 数据安全 文件上传下载 图片验证码 短信 APP客户端安全 微信公众平台 安全审计 系统容错	网络边界防护 网络和协议 第三方系统对接 商户证书管理	主机安全 应用部署	互联网金融 积分兑换

安全检测规范

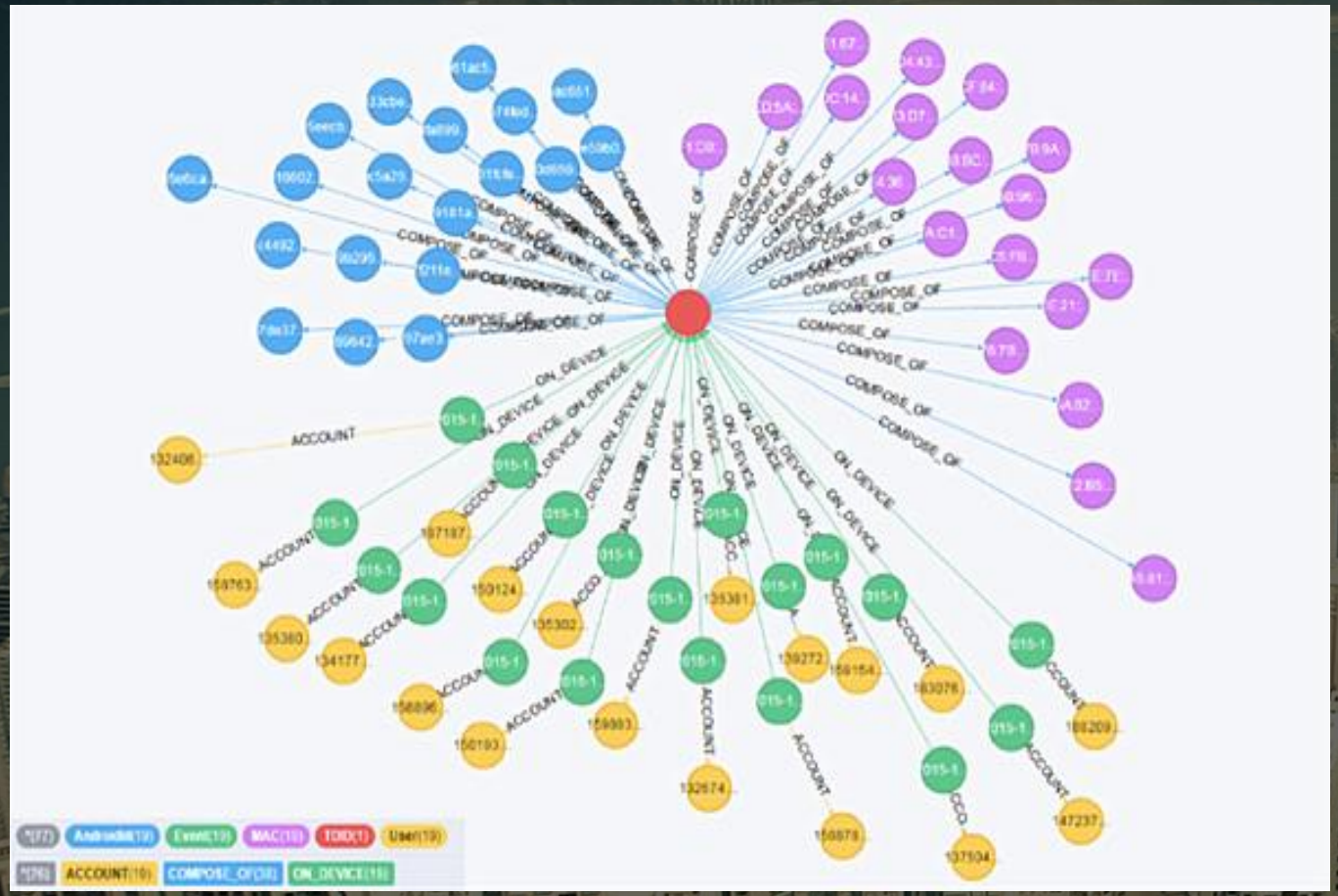
安全检测规范是针对互联网营销活动信息系统威胁分析的结果，制定完备的安全检测内容和要求，保证安全检测的有效性和高效率，实现系统的安全上线。

序号	类别	安全测试用例
1	自动化Web漏洞扫描工具测试	AppScan 应用扫描测试
2		AppScan WebService扫描测试
3		WVS扫描测试
4	服务器信息收集	运行帐号权限测试
5		搜索引擎信息发现和侦察
6		Web服务器端口扫描
7		HTTP方法测试
8		HTTP PUT方法测试
9		HTTP DELETE方法测试
10		HTTP TRACE方法测试
11		HTTP MOVE方法测试
12		HTTP COPY方法测试
13		Web服务器版本信息收集
14	文件、目录测试	工具方式的敏感接口遍历
15		Robots方式的敏感接口查找
16		Web服务器的控制台
17		目录列表测试
18		文件归档测试
19	认证测试	验证码测试
20		认证错误提示
21		锁定策略测试
22		认证绕过测试

序号	类别	安全测试用例
23	认证测试	找回密码测试
24		修改密码测试
25		不安全的数据传输
26		强口令策略测试
27		账户枚举测试
28	会话管理测试	身份信息维护方式测试
29		Cookie存储方式测试
30		用户注销登陆的方式测试
31		注销时会话信息是否清除测试
32		会话超时时间测试
33		会话定置测试
34		会话标识携带
35		会话标识随机性测试
36	权限管理测试	横向测试
37		纵向测试
38		跨站伪造请求测试
39	文件上传下载测试	文件上传测试
40		文件下载测试
41	信息泄漏测试	连接数据库的帐号密码加密测试
42		客户端源代码敏感信息测试
43		客户端源代码注释测试
44		异常处理

序号	类别	安全测试用例
45	信息泄漏测试	HappyAxis
46		Web服务器状态信息测试
47		不安全的存储
48	输入数据测试	SQL注入测试
49		LDAP注入测试
50		MML语法注入
51		命令执行测试
52		回车换行符注入测试
53		XML注入测试
54	跨站脚本测试	GET方式跨站脚本测试
55		POST方式跨站脚本测试
56		URL跨站脚本测试
57	逻辑测试	逻辑测试
58	Web Service测试	Web Service测试
59	HTML5安全测试	跨域资源共享测试
60		Web客户端存储安全测试
61		WebWorker安全测试
62	FLASH安全配置测试	FLASH安全配置测试
63	其他	日志审计
64		class文件反编译测试
65		WEB部署与管理测试
66		Struts2框架测试

大数据技术



- 上图展示了一张汇集了多个数据源的羊毛党数据图谱，从图谱中可以直观的多看到一台安卓设备通过多次刷机形成了19台虚拟设备，这19台设备注册了19个账号完成了19次薅羊毛行动的数据轨迹。
- 依托于大数据技术我们可以建立羊毛人群精细化运营的核心能力：数据共享能力、识别能力和处理能力。

大数据技术

数据

- 客户数据
- 威胁情报数据

识别

- 设备指纹
- 反向探测
- 主动爬虫

分析

- 分析模型

处理

- 积极引导、降低成功率
- 提升参与难度和成本
- 特殊处理（冻结账户等）

大数据反欺诈平台

大数据反欺诈平台依托于大数据技术，将互联网营销活动中的数据也导入大数据平台。利用威胁情报数据，增强黑产识别能力。能够在用户参加活动的时候，每进行一次操作，在背后做几项甚至几十项安全检查，通过多重数据关联叠加后利用特征工程找出羊毛人群的行为规则，快速识别羊毛党，并实现差异化管控：设置黑名单，面向黑名单用户，限制其在平台的行为操作，防止其薅取羊毛；面向灰名单用户，需结合阶段性考核指标，通过对阈值的调整，动态调整其规模；面向疑似潜在的价值用户，对其进行用户维系运营，最终实现整体的风险把控。

统一兑换审批平台

- 建立针对互联网营销活动兑换环节进行统一审批的综合管控平台，能够更容易而有效地发现羊毛党的攻击行为，为大数据反欺诈平台提供有力的支撑。也能在检测成功之后，迅速切断羊毛党的获利途径，最大限度地控制损失，是快速响应的有力手段。
- 某银行信用卡中心就已经针对信用卡的统一审批平台，有效地管控活动繁多带来的不可知风险。

小结

这是一场人性的战争。每一次互联网渠道营销活动中，都如同过一座独木桥——左右权衡，在流量和风控之间，寻求一个平衡点。

国舜

www.unisguard.com

谢谢

北京国舜科技股份有限公司