2017

广告反欺诈白皮书

2017年10月

腾讯灯塔 | 秒针 | AdMaster **联合发布**

Tencent 腾讯

一、广告投放环境现状

根据CNNIC统计，截至 2017 年 6 月，我国手机网民规模达 7.24 亿，网民中使用手机上网的比例提升至 96.3%，手机上网比例持续提升。同时，各类手机应用的用户规模不断上升，场景更加丰富。

在移动互联网蓬勃发展的大背景下，抢夺优质流量、抢占目标用户，成为各广告主不惜重金大力推广的目标。根据emarketer预测，国内数字广告营销费用将从2016年的404亿美元上升到2020年的836亿美元。在如此广大的市场容量下，不少不法份子想通过歪门邪道，在庞大的数字广告市场中分一杯羹。于是，广告黑产就如同幽灵一般，始终围绕着广告主和媒体。

1.1、黑产的组织分工

经过多年的发展，黑产已经形成相当完善的产业链。

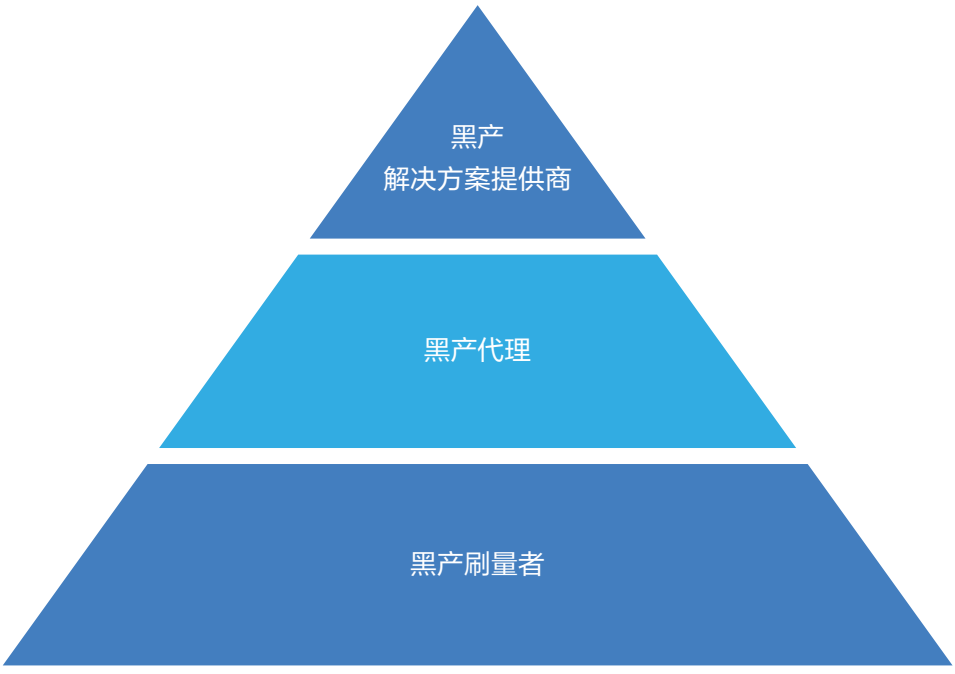

图1 黑产产业链

如图1所示，位于产业链顶端的是黑产解决方案提供商。在这样的公司里，有专门负责研究模型研究破解方式的分析人员，有专职的软件开发人员，有专职的反作弊信息收集的人员，也有负责把刷量软件、脚本分发到市场上的市场的运营人员。

经过一层或多层黑产代理刷量软件、脚本流到了不同的刷量者手中。刷量者通过伪造手段帮助获利者制造假数据，并通过包月或者按分发量分成的模式获利。

如图2，造假者只需要极小的代价，就可以方便地购买到假量。

黑产这个庞大的地下产业链，不断吞噬着广告主的投放资金导致广告主的巨额投入没有收到应有的效果。

图2 黑产产业链

1.2、黑产规模

为了净化肮脏的广告投放环境，腾讯灯塔通过覆盖的10亿月活终端，持续研发反作弊模型。根据腾讯灯塔统计，以2017年6-8月之间为例，腾讯灯塔日均校验40亿次+广告请求，识别的作弊比率稳定在15%左右。在部份行业及campaign中，作弊比例甚至高达60%。如此高比率的作弊流量，给广告主带来了巨额的损失。如下通过2个案例现场的还原，给大家一些感性认知。

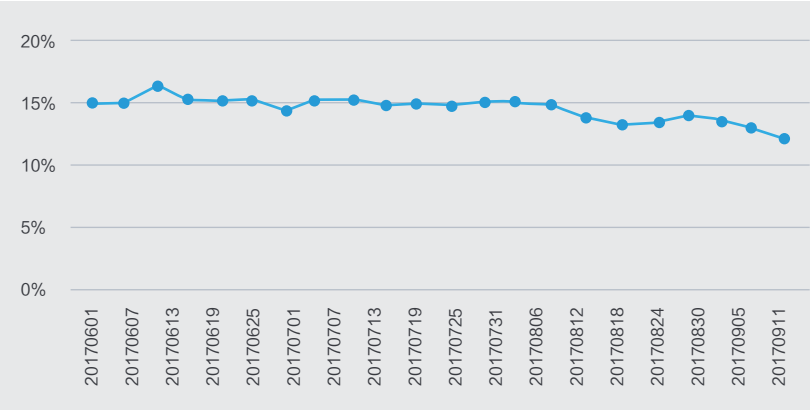

图3 2017年6-8月中国广告市场大盘作弊流量占比

注：数据来源于灯塔稽核服务，含灯塔独自覆盖广告流量、秒针及AdMaster覆盖的安卓侧全量，总校验广告请求3500亿+次

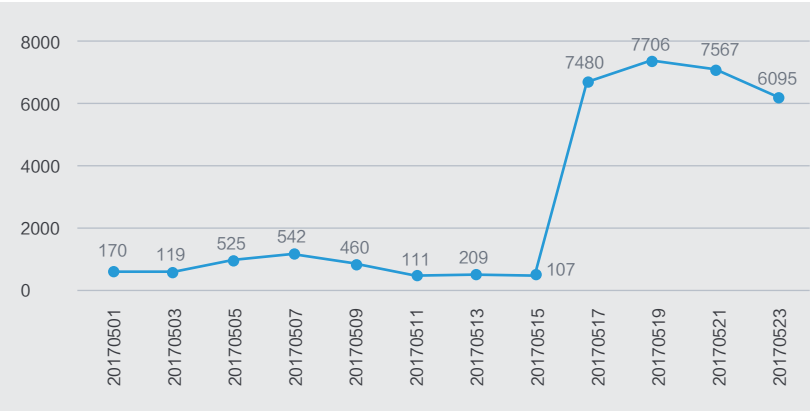

图4 某渠道新增用户趋势

例1：如图4所示，在某大型APP通过某渠道进行地推时，发现新增用户出现暴涨。在暴涨的新增用户中95%以上的用户都具有以下共同特征：

- ROM编译机名称完全一致
- CPU结构为X86，为PC机模拟器
- 指令逃逸差异度与正常用户不一致
- 文件系统类型的差异度与正常用户不一致

从而映证了此渠道高达95%的新增用户均为虚假用户。

例2：某APP某渠道新增用户为86553，其中识别为工作室批量刷新增量有42308，约占新增用户48%，主要特征为安装时间具有明显的批次，手机APP安装数量一致，且有明显的地域集中性。如图5所示，（X轴为时间点，Y轴为安装次数），安装操作集中在20：21~20：22之间，且5月11日~5月22日期间关键身份标识函数劫持现象有所增加。

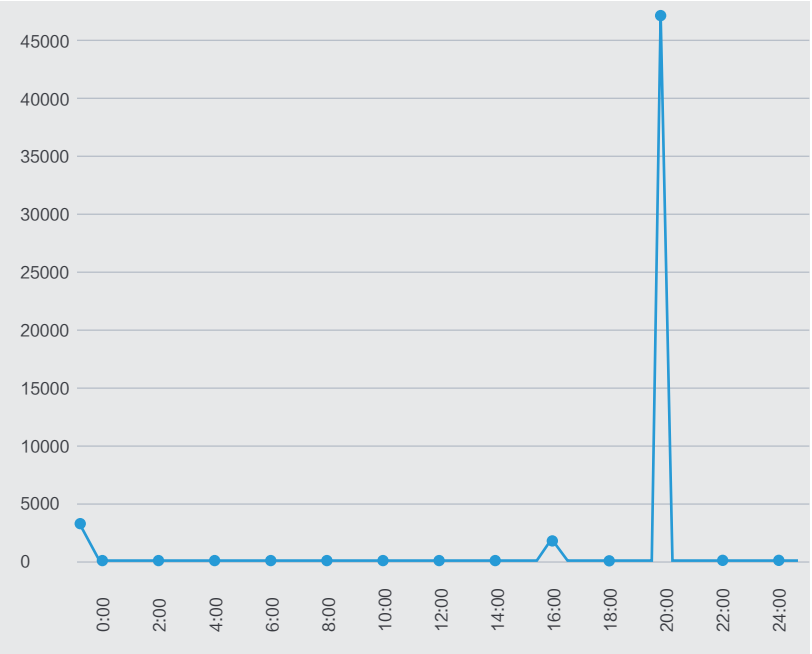

图5 某APP安装时间-安装次数图

1.3、各种不同作弊手段的分布

从图6可看出，黑产已经逐步抛弃较为低级的模拟器作弊、真机假用户作弊，转向更高级、识别门槛更高的虚假激活作弊形式。作弊手段详细介绍请参见本文第二章。

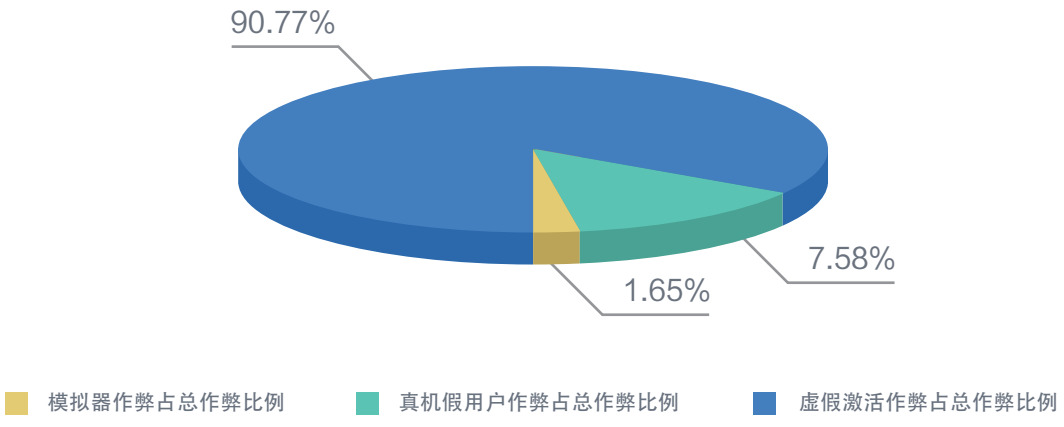

图6 各种作弊手段分布

二、反作弊中的攻防技术

2.1、黑产业务历史发展趋势

从总体上看，移动互联网地下产业的发展大致经历了三个阶段：

（1）原始阶段。主要出现在09、10年移动互联网兴起时，利用内容抄袭、破解、黑卡及手工刷量等原始手段骗取运营商的购机补贴或运营活动Q币奖励等；

（2）批量式智能化阶段。11、12年期间，大量资本在国内移动互联网领域进行了撒网式高密集投放和布局。在高额利润的诱惑下，相关地下产业链也出现迅猛发展的态势：作弊手段随之升级，从上一阶段的单点小作坊式作弊发展到批量式智能化作弊。以智能刷量工具为代表，刷量者开始模拟真实用户的激活行为和后续留存行为；

（3）高度仿真阶段，13年后，一方面由于线上渠道推广、线下厂商渠道的运营成本大幅攀升；另一方面小微初创企业急于曝光引流，大型企业急于垄断长尾流量，同时各大电子市场和企业自身加强对用户质量的监控。受这两方面的共同影响，作弊手段亦随之进化，借力大数据分析技术已经可以做到高度模拟真实用户的行为。

由于iOS系统自身的封闭性，目前移动流量分发渠道主要集中在安卓平台，因此后续讨论的作弊手段分析以安卓平台为主。就目前阶段而言，刷量作弊手段已经渗透到广告产业链的各个环节。如图7所示，以APP推广场景为例，方案提供商、手机制造商、代理商和刷机商均可在手机预装环节进行ROM层或系统应用层作弊，可对用户的终端设备植入恶意应用或木马进行诱导安装或静默安装，也可以使用模拟器、自动化脚本、应用自动分发平台高保真地模拟真实用户的行为。

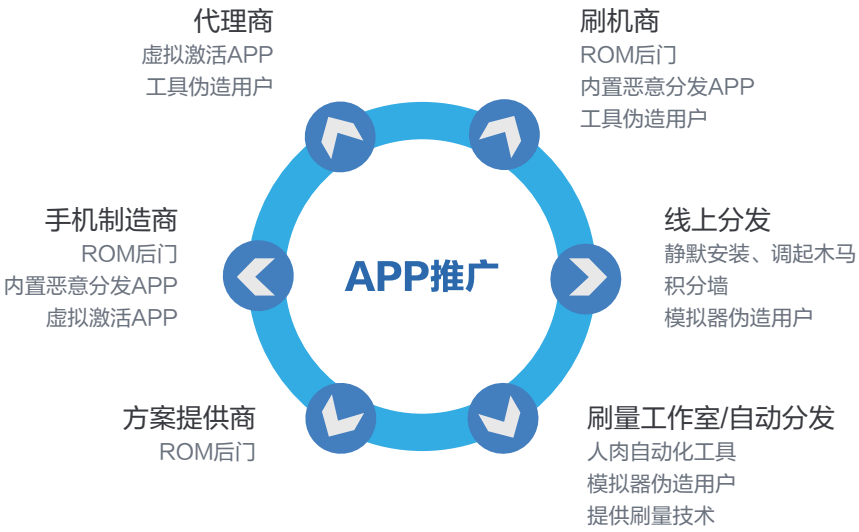

图7 刷量手段在各环节渗透情况

2.2、黑产技术分析

1、广告作弊类型分类

（1）模拟器刷量（假机）

模拟器又分为电脑模拟器刷量、手机软件模拟刷量、脚本刷量。

a、电脑模拟器刷指在一台或多台机器上开很多的虚拟机跑模拟器进行刷量，稍微有实力的作弊者可自己开发模拟器并有专门的服务器挂在全国各地的机房，或者使用VPN不断变化IP，进行24小时不间断的刷量。

b、手机软件模拟刷量指在手机上安装模拟器进行刷量，软件可以从非法渠道买到，也可以根据自己要求定制。经过几年的发展，手机软件模拟刷量一键安装运行已成为标配。部分模拟器甚至能动态修改机型唯一性标识，即使是小白用户也可轻松伪造新增用户。部分刷量玩家结合 PC 时代的技术，编制自动化脚本，单台 PC 单日可伪造数百上千新增用户。更有甚者，可深度定制化模拟器，将伪造新增流水线化，

数十倍提高生产效率。

c、脚本刷量：就是利用一些脚本来模拟用户的行为进行刷量，这类目前占比比较多，常用的一些方法就是使用ACC、IS、IF、IG插件，录制用户的行为生成脚本，并设置循环任务，如果会使用LUA语言并懂点业务，再对用户行为有研究的话，做出一个模拟真实用户使用的脚本应该不是很困难，市面上已经有些脚本跟真实的用户行为几户没太大差别，很难从技术上分辨。

各种模拟器刷量技术门槛、经济门槛已低至任何个体式的作弊者均可随意获取。

（2）真机假用户

真机假用户的方法主要是利用数据线push命令到手机，手机执行命令。刷量者一般会储备大量手机或者sim卡用于刷量，就用这几百台设备刷完一批设备号再换一批设备号刷，这样就等于换了一批新机器。

图8 黑产工作环境示意图

（3）静默安装（真机真用户假行为）

静默安装/激活应用是属于高阶作弊方式之一。所谓静默安装/激活是指刷量者利用人工方式或网络传播方式将木马/具有再分发能力的应用植入到用户手机，形成僵尸网络，刷子在后台利用云控技术对僵尸网络发送统一的命令，在用户无感知的情况下，完成App的下载、激活和删除等一系列操作。

（4）羊毛党（真机真用户真行为假动机）

为了制造更逼真的用户数据、绕过技术封锁，某些刷量者还通过羊毛党的方式进行牟利。这种方式引

入的用户，质量极差，表现为：往往登录一次就删除应用、使用时长极短、留存率极低。在大部份的情况下，这种用户对业务的健康发展并无太大价值。

（5）广告素材、篇幅偷换（不可见）

为了获取高额利润，不良媒体作弊手段无所不用其极。近年来在品牌类广告中出现类似于“1 像素广告”的刷量方式。“1 像素广告”指在用户的手机屏幕上只展示1个像素大小的广告。这种广告，用户看不见，但统计工具可以统计到，仍然会作为曝光广告与广告主结算，给广告主带来经济损失。其它类似于“1像素广告”的刷量方式还体现为私自替换广告主的广告素材、私自修改广告素材篇幅等等，花样百出。

（6）以次充好（不匹配）

广告行业还有一种比较隐秘的作弊方式：以次充好。如视频类广告一线城市受众较二三线城市往往溢价售卖。一线城市的库存经常紧缺。出于牟利动机，部分媒体会将广告主原本定向的一线城市用户偷偷换成二三线城市用户，达到以次充好的目的。地域是标示用户的刚性标签（多方易于达成共识），而类似高收入群体这样的定向，若发生以次充好，在举证环节的沟通成本将极高。

基于以上分析，我们试着对作弊类型做一个全景梳理。营销活动追求，right people，right time，right channel，right message。而黑产带来的威胁，相应可以总结为3个维度：真实，可见，匹配。

真实，要求受众是一个怀着纯正动机的自然人；

可见，要求广告是物理肉眼可见的；

匹配，要求广告被正确地传递给了广告主预设的人群，未发生平台方有意为之的“偷梁换柱”。

读者可以从如下这张全景图，对广告的作弊类型做个概览。

真实：怀着纯正动机的自然人　　可见：肉眼物理可见

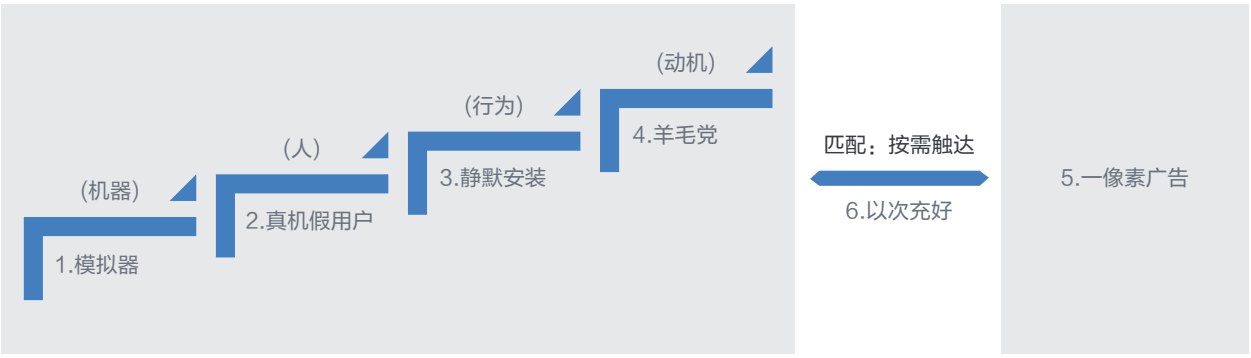

图9 广告作弊类型分类

2、黑产技术手段深究

随着黑产技术手段的不断提高，动态Hook篡改参数、静态编译篡改参数等技术手段已经成为黑产标配。

如图10，Xposed框架可以劫持任意Android API， 在App 无感知情况下篡改 API 接口返回结果，以达到伪造新用户效果。

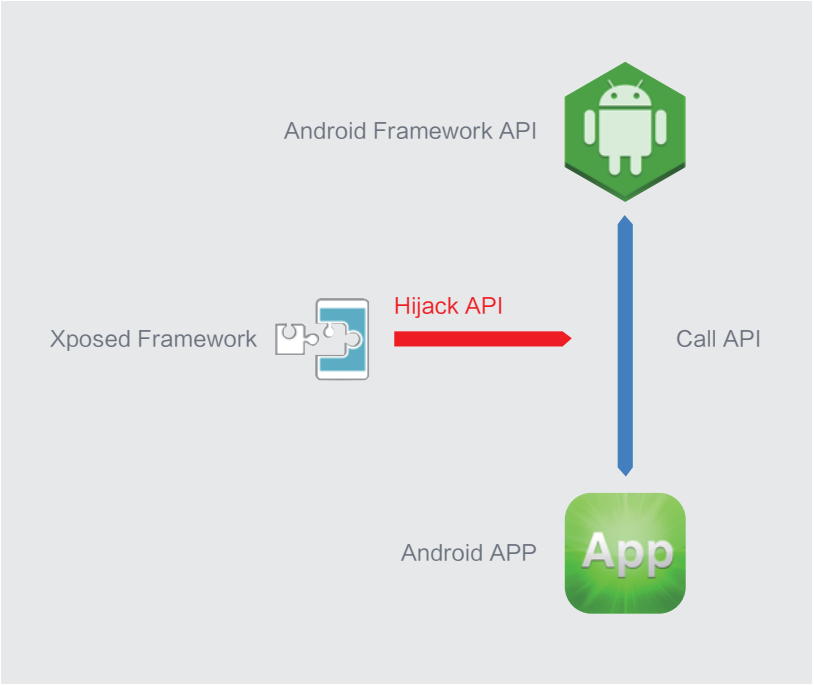

图10 黑产常见技术手段

如图11，直接在 Android Framework 源代码修改 API 具体调用，让 API 返回伪造的结果给 App，这种手段较动态 HOOK 来说更难检测。

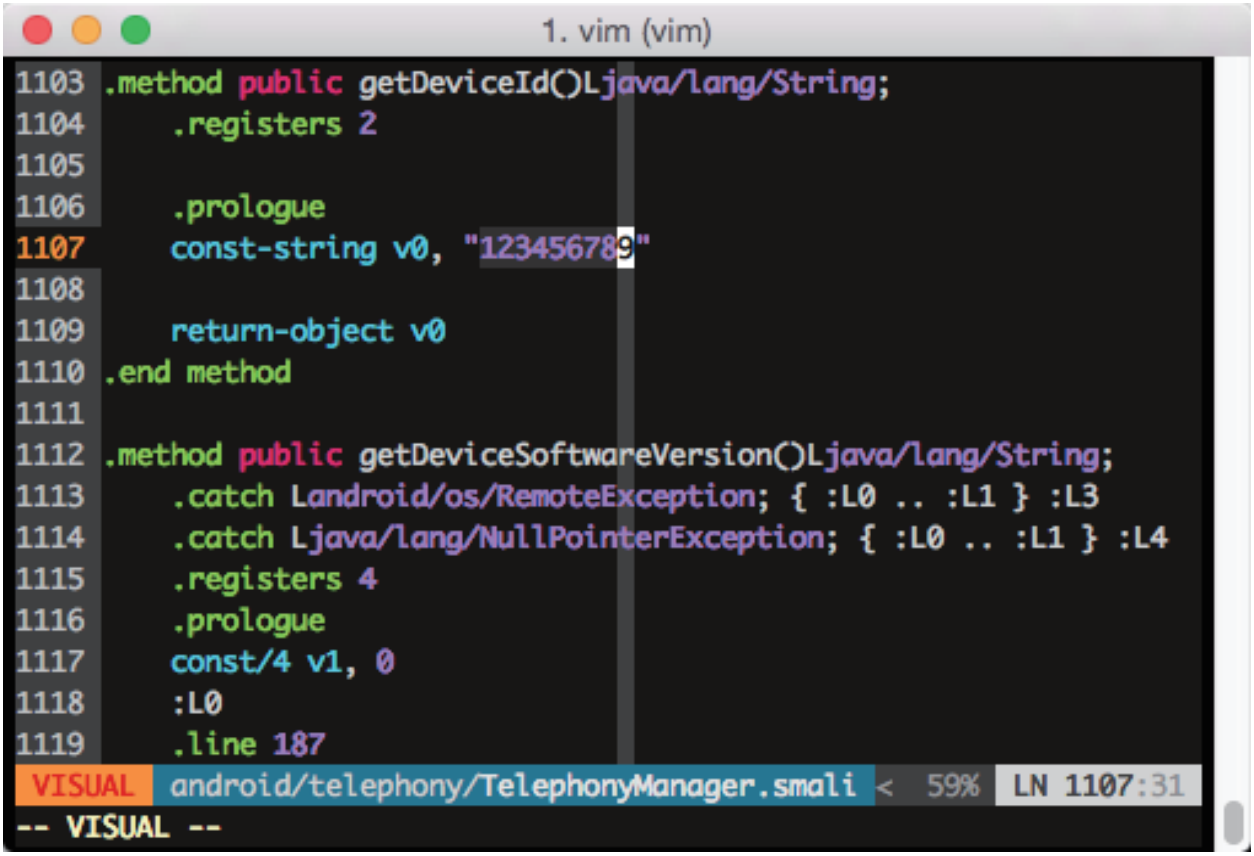

图11 黑产修改Android Framework 源代码示意图

2.3、反作弊技术

1、反作弊技术演进

魔高一尺、道高一丈。在与黑产不断抗争的过程中，反作弊技术也在不断演进。

（1）用户群体数据检测

这是反作弊斗争用到的低阶技术。常见的方式有以下几种：

a、看留存率

刷量者会选择在次日、7日、30日等关键节点导入用户数据。APP在次日、7日、30日这些关键时间点上的数据明显高于其他时间点。而真实的用户的留存曲线是一条平滑的指数衰减曲线，如果发现留存曲线存在陡升陡降的异常波动，则判断刷量者干预了数据。

b、看用户终端、网络信息

如根据经验分析渠道新增用户或者启动用户的设备排名；2G、3G、4G的使用比例分布是否正常等。

c、看用户的注册信息

比如说注册昵称的分布和规律等。

此境界中的运营者严重依赖于个人经验，工具手段不专业化，操作效率低下，耗费人力物力，发现问题时间滞后，而且稍微高级一点的作弊行为不能被发现。

（2）用户行为特征分析

在用户群体数据检测基本失效以后，反作弊斗争进化到用户行为特征分析阶段。这也是当前反作弊斗争中最常见的技术方案。

a、单个指标

与黑IP库进行比对，是否为黑名单IP、是否为代理IP；与IMEI库进行对比，是否为为黑IMEI；

b、群体指标

用户的IP、IMEI、机型、OS、位置信息、运营商、接入方式的分布是否符合先验数据的分布

c、设备一致性的验证，包括：CPU、制造商、MAC地址、IMEI、机型、操作系统的一致性验证。

这个境界的运营者已经摆脱了手工处理、依赖个人经验的阶段，走上了算法和数据的专业化路线。但仍然会有以下问题产生：

a、算法模型过于简单，集中在终端浅层特征分析，容易被刷量者破获。刷量者容易通过简单的指标分析绕过广告主/运营者的反作弊监测；

b、以IP判断用户善恶的方式过于粗暴。往往一个IP下多用户作弊，则视为该IP下所有用户都作弊，造成打击面过大；

c、黑IMEI库没有黑白转换机制，没有多业务交叉判断，误判率较高

因此，要对刷量进行有效精准打击，依靠用户群体数据检测、用户行为特征分析两种方式都是不可能完成的任务。要实现精准打击，必须要溯其本源，在终端特征分析+云端交叉验证的基础上才能达到目的。

（3）反作弊的高阶模式：终端特征分析+云端交叉验证，“查”“杀”“验”三管齐下

在长期与刷量份子的作斗争过程中，腾讯灯塔形成了行之有效的反作弊综合斗争策略：“查”、“杀”、“验”三大模型三管齐下，最大限度提升覆盖率、及时性、准确性。其中，由“查”模型负责找寻黑产界的新型作弊方式，提升整体模型的覆盖率；“杀”模型负责准确识别恶意份子；“验”模型通过多业务交叉验证，负责保证“查”、“杀”模型的准确率。

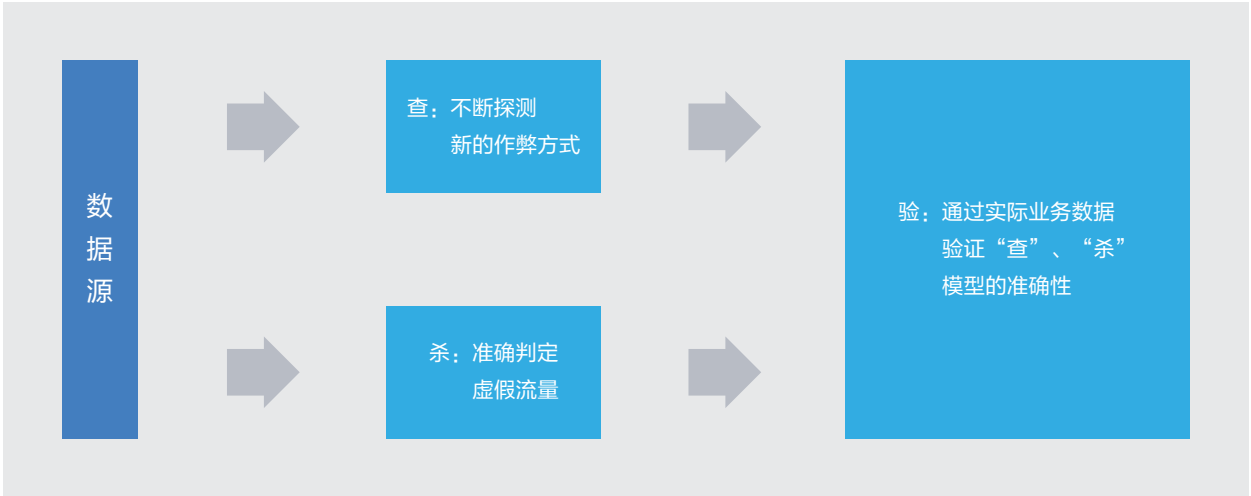

图12 灯塔“查”、“杀”、“验”模型示意图

下面重点讲述灯塔“杀”模型。

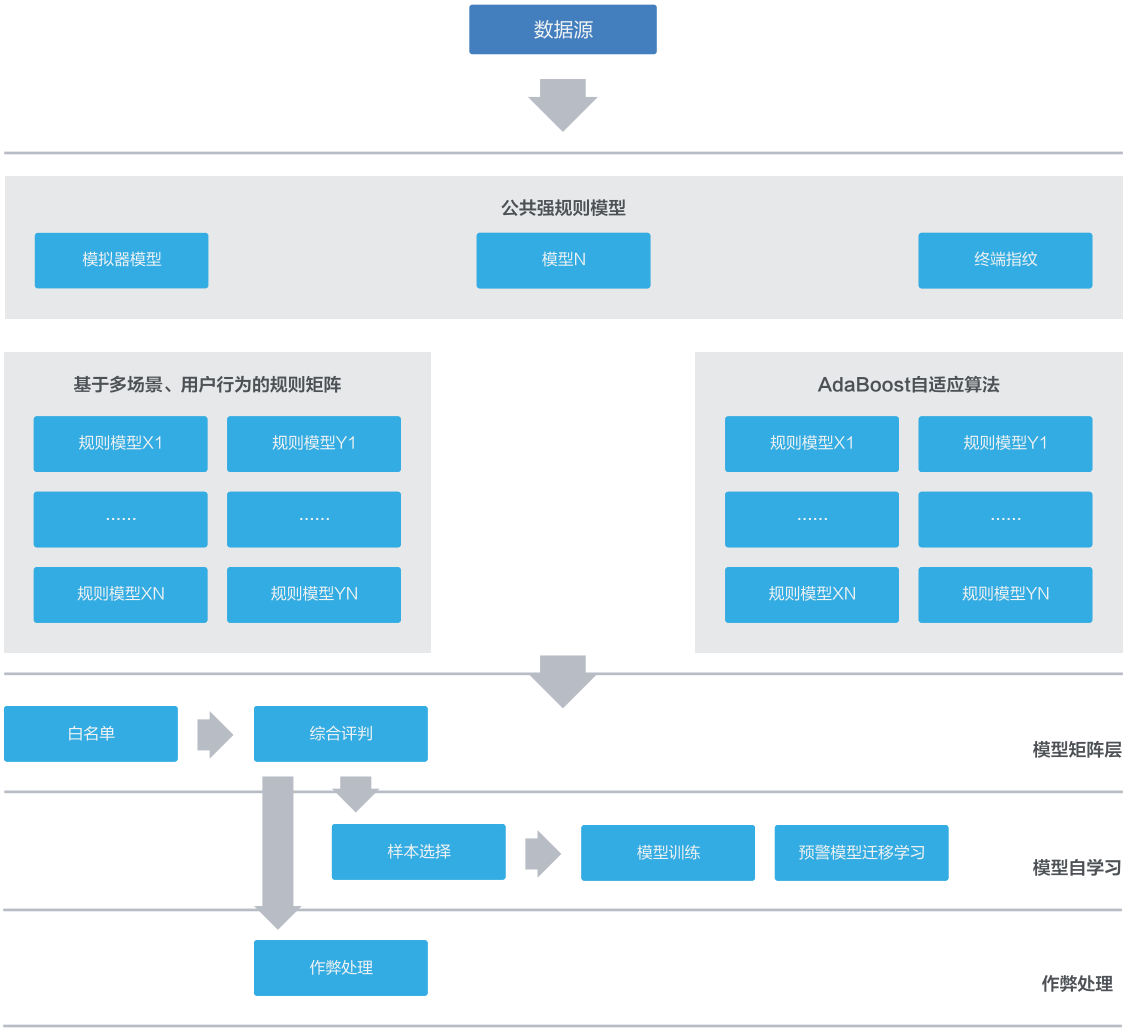

图13 灯塔“杀”模型逻辑结构图

终端识别模块（灯塔SDK稽核模块）：该模块主要是采用机器学习算法选取系统中所有可用的信息作为特征，然后对这些特征进行运算得到该设备的指纹，可以有效识别手机模拟器、修改系统参数等行为。

基于规则的识别模块（业务自有模块）：该模块一般是通过业务经验及对历史可疑渠道的总结形成的反作弊规则，可以理解为多维组合规则，一般需根据业务成本、对渠道的容忍度设置关键变量的阈值。

基于数据挖掘的识别模块（灯塔云端模块）：该模块主要从硬件信息、用户活跃、用户行为进行多维度、多业务交叉验证，分别计算每个维度下面的不同特征值，结合决策树、LR、贝叶斯网络等多种算法进行精准的定位。

同时，为了增强识别的准确性和稳定性，模块之间、模块内部均采用集成学习方法的思想，其核心思想是在模块内对同一个训练集训练不同的分类器，然后把这些分类器结合起来构成一个最终的分类器，而每一个模块可以针对不同的作弊手段进行识别，再把模块与模块结合，才能识别所有的作弊手段。这种设计在实践中有几种好处：

a、解决了边界模糊的问题，每个模块有不同的功能和实现成本，可以针对不同场景使用不同模块的结果，方便快速支持各个业务线。

b、模型训练、模型扩展相对容易，可以针对不同作弊手段分别训练分类器，分类器可以很方便的加入现有的系统中。

以上策略在实践中证明是行之有效的：腾讯灯塔模拟器识别准确率达99%以上；真机假用户、虚假激活的识别准确率达95%以上。

2.4、反作弊误区

1、简单依靠用户行为表象进行判断

依靠用户的留存率、IP分布、机型分布、使用时长等用户行为表象进行流量真假判断，是最直观、最简单的反作弊策略。这种简单粗暴的策略很容易被刷量者所利用。

图14 某刷量工具价格

如图14及图15，在某电商平台上，买主只需要很小的代价，即可刷出完全符合正常用户规律的留存率、IP分布机型分布使用时长等。也就是说，简单依靠用户行为表象进行流量真假判断，是极不可靠的。

正确的做法，必须是透过现象看本质，深入每一个用户的系统层、内核信息，才能判定用户的真假。

专业Android app游戏激活、注册、留存、付费、应用市场好评
我们是团队换运作，技术实时更新，根据客户的不同需求，提供精准化的网络服务，无论量大还是量小，都可以提供真实有效的数据。

1、提供apk安装，激活，注册，留存，数据真实有效，团队化运作，效率高
2、可真实体现不同ip,不同机型，不同用户行为，不重复imei和mac
3、可按要求安排新增，次日留存，7日留存，30日留存，等各种不同天数留存
4、可做使用时长，付费用户数，可模拟用户行为
5、可完善友盟，百度，九游，360，华为一级其他硬件厂商平台统计
6、可按要求刷客户提供的后天统计
7、可定制客户需求，技术实时更新
8、提供高等级账号，评论发帖，收藏关注，独立单机

适用客户范围：
1、完成上司硬件考核需求；　2、渠道补数据；　3、应用补数据；
4、任务需求补数据；

承诺所以项目完全保密，执行过程全部使用代号。

图15 某刷量工具宣传广告

2、知道某一个（某一些）刷量特征就可以识别假流量

为了不断追求更高额的利润，刷量者的技术手段也在不断进步。当刷量者发现某一些作弊特征已经被反作弊者所破获时，就会更换作弊手法，以绕过反作弊者的技术封锁。

如图16，2016年8月腾讯灯塔服务某大型APP之前，该APP刷量者仅凭最低阶的模拟器就获得了大量的利润。随着刷量者发现模拟器作弊被破获后，就将作弊手段转移到了更高阶的真机假用户、虚假激活。

作弊与反作弊，不是突击式冲锋，是需要不断持续投入的攻防对抗，是此消彼长的长期拉锯战。仅仅知道某一个(某一些)刷量特征就试图“一招鲜，吃遍天”，是行不通的。

日期	异常占比(%)	模拟器占比（100%）	真机假用户占比（100%）	虚假激活占比（100%）
2016/08	12.17%	33.18%	27.31%	39.51%
2016/09	12.33%	23.07%	22.58%	54.36%
2016/10	10.46%	17.78%	11.04%	71.18%
2016/11	7.14%	10.26%	14.15%	75.59%
2016/12	7.22%	9.34%	14.56%	76.10%
2017/01	17.36%	3.29%	8.35%	88.36%
2017/02	16.10%	2.58%	6.96%	90.46%
2017/03	14.38%	4.03%	12.47%	83.50%
2017/04	17.29%	3.04%	16.68%	80.29%

图16 某APP作弊比例示意图

3、识别到虚假流量以后，就万事大吉了

识别到虚假流量以后，如何判断识别的准确率？当有新的作弊方式、作弊特征出现时，如何快速发现、快速建模，从而达到快速识别的目的？如果上面的这些问题无法回答，仅仅识别到虚假流量并不能使广告主高忱无忧。

如前文中所描述的那样，通过大规模多业务数据交叉验证，才能准确考量识别准确率。同时在花样百出的作弊手段不断涌现时，能够准确捕获最新作弊动态，并快速建模。

三、精诚合作，净化环境

3.1、全行业的共同斗争

为了净化行业空气、维持广告行业可持续发展，2017年4月，腾讯灯塔携手秒针、AdMaster，分别

成立广告反欺诈大数据实验室。

作为中国领先的互联网增值服务提供商，腾讯公司在互联网广告反欺诈领域有深厚的技术积累、丰富的反作弊经验。腾讯灯塔覆盖10亿月活终端，拥有中国海量准确的IP库以及全面终端机型库。依靠10亿月活用户数据和亿级黑终端库，腾讯灯塔已建立起由终端特征识别、多特征维度、多模型组合、多产品验证的反作弊识别方案，能够实现对移动设备ID和行为路径海量数据的精准分析和识别。

腾讯灯塔、秒针、AdMaster三方通力合作，站在了反黑产斗争的最前线。

广告反欺诈大数据实验室成立至今，共校验终端5000亿+次，累计判断欺诈终端800亿+次，有力地守护了广告主的投放预算。

3.2、面向未来的斗争

广告反欺诈大数据实验室未来还将重点发力以下几个领域：

a、更快速发现新的作弊形态，通过机器自学习更快速建模；

b、更准确判断恶意用户，既不枉杀，也不漏杀；

c、更灵活的验证手段，保证模型的准确性。

面对层出不穷、不断升级的广告作弊方式，反作弊领域的斗争注定是长期的、坚韧的斗争。只有全行业共同行动起来，才能在这项长期的、面向未来的斗争中取得最终的胜利。


腾讯灯塔
Beacon.qq.com