

《中国互联网地下产业链分析白皮书》

灰色黑色产业链商业模式及互联网黑市深度数据分析洞察

版权申明：

本报告是 TOMsInsight 团队研究成果。

本报告内所有数据、观点、结论的版权均属 TOMsInsight 团队拥有。未经书面或邮件许可，任何人不得以全文或部分形式（包含纸制、电子等）引用、复制和传播。不可断章取义或增删、曲解本报告内容。

本报告所涉及的数据来源于行业内公开数据、互联网公司授权、软硬件公司授权、系统集成商授权、渠道授权、客户授权和市场公开数据等，并采用合法的技术手段获取、深度访问、抽样调查等。由于统计方法本身局限、视角不同、数据观察维度不同、报告数据与市场真实也许存在误差。本报告中的数据不能确保百分百精确。

TOMsInsight 团队对其独立研究数据、研究技术方法、研究模型、研究结论及衍生服务产品拥有全部知识产权，任何人不得侵害和擅自使用，违者必究。

本报告及衍生产品最终解释权归 TOMsInsight 团队所有。

内容简介：

中国互联网行业有一定的特殊性：由国情决定了用户需求的多样性，而主流的互联网产品却很难满足所有的用户心理诉求；加上最近几年互联网高速发展带来的红利；以及技术成本的不断降低，都催生了中国互联网的地下产业链。

地下产业链并不是消极的事物，在一定程度上讲，地下产业链更接近用户需求，更能还原互联网的本貌。在中国的传统行业都有一定的所谓黑市门槛，即属于潜规则范畴或者是不为人知的行业秘密，这种信息只流传在最信任的人脉圈子里。读懂了这些，才能算从根本上了解了这个行业。

对于互联网创新者来说，地下产业链代表着最接地气的用户需求和商业模式，可以给我们一定的用户需求理解、商业模式启示和相应的洞察力。另外，从地下产业链角度切入，纵览整个中国互联网产业的各细分领域，可以给我们更好的大局观和启示。这是本报告的意义所在。

本报告分析洞察中国互联网的 22 个细分领域的地下产业链，通过约 7 万字篇幅和 100 幅的数据图表，给每一个读者带来更多的互联网大局观和启示。另外，每一个细分产业链都可能是一部史诗，本报告篇幅有限，并不陷入细分领域，只专注于还原给读者互联网地下产业链全貌。

最后，本报告仅从学术角度研究，并不进行法律探讨。而任何非法的事物必将受到法律严惩。

内容目录：

一、	地下产业链概述与全貌性导读	11
1.	深度研究分析互联网地下产业链的目的	12
2.	中国互联网产业链发展现状概述及分析	13
3.	中国互联网地下产业链发展现状及分析	15
4.	本报告相关概念定义及其整体结构导读	16
5.	本报告数据来源及分析方法定义与说明	16
二、	流量获取分发相关产业链部分	17
0.	流量获取分发相关产业链部分整体分析	18
A.	流量获取分发产业链整体情况	19
B.	细分产业链之间生态关系分析	22
C.	流量获取分发的黑市深度数据	23
1.	搜索引擎流量与分发产业链分析	23
A.	相关地下产业链整体深度分析	27
B.	黑帽 SEO 地下产业链深度分析	28
C.	黑链交易地下产业链深度分析	29
D.	SEM 作弊相关上下游生态分析	31
E.	移动端流量的模式变化与数据	31
2.	腾讯生态流量与分发产业链分析	33
A.	相关地下产业链整体深度分析	34
B.	QQ 引流推广产业链深度分析	34
C.	其他产品引流产业链深度分析	35
D.	信封号产业链与相关生态分析	35
E.	引流推广工具产业链深度分析	40
3.	微信生态流量与分发产业链分析	41

A.	相关地下产业链整体深度分析.....	42
B.	微信号引流推广模式深度分析.....	43
C.	微信朋友圈推广深度数据分析.....	44
D.	微信公众平台地下产业链分析.....	45
E.	微信公众号第三方开发产业链.....	46
4.	广告联盟以及流量再分发产业链.....	47
A.	相关地下产业链整体深度分析.....	48
B.	广告联盟流量产业链深度分析.....	48
C.	流量主流量来源深度数据分析.....	50
D.	广告主盈利模式与利益链分析.....	52
E.	移动广告联盟的深度数据分析.....	52
5.	网络内容与信息推广营销产业链.....	54
A.	相关地下产业链整体深度分析.....	55
B.	新闻媒体类地下引流数据分析.....	56
C.	资讯内容类地下引流数据分析.....	57
D.	垃圾信息类地下引流数据分析.....	58
E.	邮件其他类地下引流数据分析.....	59
6.	安卓应用分发与移动流量产业链.....	60
A.	相关地下产业链整体深度分析.....	61
B.	预装渠道地下产业链深度分析.....	62
C.	诱感渠道地下产业链深度分析.....	62
D.	静默渠道地下产业链深度分析.....	63
E.	其他非法渠道产业链深度分析.....	65
7.	微博等社交应用流量与相关分析.....	67
A.	相关地下产业链整体深度分析.....	68
B.	微博粉丝地下引流的深度分析.....	68
C.	社交私信地下引流的深度分析.....	69

D.	其他社交类产品流量深度分析.....	69
E.	相关黑市交易与推广深度分析.....	70
8.	病毒木马与盗版软件流量产业链.....	71
A.	相关地下产业链整体深度分析.....	72
B.	病毒木马流量产业链深度分析.....	72
C.	盗版软件流量产业链深度分析.....	74
D.	移动端病毒木马数据分析洞察.....	74
E.	移动应用盗版流量产业链分析.....	75
9.	移动流量数据与移动化趋势分析.....	77
A.	相关地下产业链整体深度分析.....	78
B.	移动流量获取分发的发展趋势.....	79
C.	移动流量获取分发的来源分析.....	79
D.	移动流量获取分发的交易分析.....	80
E.	移动流量获取分发的深度数据.....	81
10.	总结与洞察启示.....	83
三、	流量变现盈利相关产业链部分.....	84
0.	流量变现盈利相关产业链部分整体分析	85
A.	流量变现盈利产业链整体情况.....	86
B.	细分产业链之间生态关系分析.....	88
C.	流量变现盈利的黑市深度数据.....	88
1.	淘宝天猫与相关生态变现产业链.....	90
A.	相关地下产业链整体深度分析.....	91
B.	淘宝天猫刷单产业链深度分析.....	91
C.	刷单产业链周边衍生黑产分析.....	92
D.	折扣站淘宝客产业链深度分析.....	92
E.	其他灰色黑色产业链深度分析.....	94
2.	独立网站电商与货到付款类电商.....	95

A.	相关地下产业链整体深度分析.....	96
B.	百度竞价单页产业链深度分析.....	96
C.	货到付款电商产业链深度分析.....	99
D.	网络品牌电商产业链深度分析.....	100
E.	其他独立电商产业链深度分析.....	101
3.	微店类型电商与独立移动端电商.....	102
A.	相关地下产业链整体深度分析.....	103
B.	百度生态移动电商产业链分析.....	105
C.	微信生态移动电商产业链分析.....	105
D.	其他流量移动电商产业链分析.....	106
E.	独立移动电商支付分析与数据.....	107
4.	游戏地下产业链分析与相关生态.....	109
A.	相关地下产业链整体深度分析.....	110
B.	游戏外挂作弊产业链数据分析.....	111
C.	游戏工作室相关的产业链分析.....	111
D.	游戏资产交易与黑市交易分析.....	112
E.	游戏私服与移动游戏盗版分析.....	113
5.	博彩类变现相关地下产业链分析.....	114
A.	相关地下产业链整体深度分析.....	115
B.	网络彩票地下产业链深度分析.....	115
C.	网络赌球地下产业链深度分析.....	120
D.	网络棋牌游戏赌博产业链分析.....	121
E.	其他赌博形式产业链相关分析.....	121
6.	网络色情及诱惑相关产业链分析.....	122
A.	相关地下产业链整体深度分析.....	123
B.	色情网站产业链变现模式分析.....	124
C.	擦边球类型色情网站变现分析.....	125

D.	地下秀场网站产业链深度分析.....	126
E.	移动端色情应用相关深度分析.....	127
7.	网络培训与传销相关产业链分析.....	128
A.	相关地下产业链整体深度分析.....	129
B.	网络培训包装与推广深度分析.....	129
C.	培训内容定位与用户数据分析.....	131
D.	网络传销地下产业链深度分析.....	131
E.	传销结合的网络培训商业模式.....	132
8.	比特币与山寨币相关产业链分析.....	133
A.	相关地下产业链整体深度分析.....	134
B.	比特币交易平台商业模式分析.....	135
C.	国内山寨币商业模式深度分析.....	136
D.	周边相关地下产业链深度分析.....	137
E.	技术与模式变种影响分析洞察.....	138
9.	移动变现数据与移动化趋势分析.....	139
A.	相关地下产业链整体深度分析.....	140
B.	移动流量变现盈利的发展趋势.....	141
C.	移动流量变现盈利的来源分析.....	141
D.	移动流量变现盈利的交易分析.....	142
E.	移动流量变现盈利的深度数据.....	143
10.	总结与洞察启示.....	145
四、	数据信息安全相关产业链部分.....	146
0.	数据信息安全相关产业链部分整体分析	147
A.	数据信息安全产业链整体情况.....	148
B.	细分产业链之间生态关系分析.....	149
C.	数据信息安全的黑市深度数据.....	149
1.	数据窃取与非法交易产业链分析.....	150

A.	相关地下产业链整体深度分析.....	151
B.	数据窃取相关产业链深度分析.....	152
C.	数据交易相关产业链深度分析.....	152
D.	数据购买下游产业链深度分析.....	153
E.	数据黑市交易情况与相关洞察.....	154
2.	网络攻击与敲诈相关产业链分析.....	155
A.	相关地下产业链整体深度分析.....	156
B.	人肉型攻击敲诈勒索深度分析.....	157
C.	信息型攻击敲诈勒索深度分析.....	158
D.	技术型攻击敲诈勒索深度分析.....	159
E.	其他攻击敲诈与周边黑产分析.....	160
3.	病毒木马与挂马相关产业链分析.....	161
A.	相关地下产业链整体深度分析.....	162
B.	病毒木马制作者深度解析分析.....	162
C.	挂马地下产业链深度数据分析.....	163
D.	病毒木马交易与代理模式分析.....	164
E.	手机病毒木马相关产业链分析.....	164
4.	人海战术与打码相关产业链分析.....	166
A.	相关地下产业链整体深度分析.....	167
B.	人海战术商业模式与深度数据.....	167
C.	人海战术模式应用产业链分析.....	168
D.	打码相关产业链深度分析洞察.....	168
E.	周边相关地下产业链深度分析.....	170
5.	账户安全与认证相关产业链分析.....	171
A.	相关地下产业链整体深度分析.....	172
B.	账户黑市交易情况的数据分析.....	172
C.	身份认证识别地下产业链分析.....	173

D.	手机号识别与认证产业链分析.....	174
E.	周边相关地下产业链深度分析.....	174
6.	网络诈骗与相关地下产业链分析.....	175
A.	相关地下产业链整体深度分析.....	176
B.	社交网络诈骗及相关深度数据.....	177
C.	电商购物诈骗及相关深度数据.....	179
D.	商业诈骗和其他种类诈骗分析.....	180
E.	黑市交易与上下游产业链分析.....	180
7.	总结与洞察启示.....	181
五、	总结性分析洞察与结论.....	182
1.	地下产业链相关的风险影响分析	183
2.	地下产业链相关的商业模式分析	183
3.	地下产业链相关的用户需求分析	184
4.	地下产业链相关的行业发展分析	184
5.	地下产业链相关的发展机遇分析	185

一、 地下产业链概述与全貌性导读

中国互联网行业有一定的特殊性：由国情决定了用户需求的多样性，而主流的互联网产品却很难满足所有的用户心理诉求；加上最近几年互联网高速发展带来的红利；以及技术成本的不断降低，都催生了中国互联网的地下产业链。

地下产业链并不是消极的事物，在一定程度上讲，地下产业链更接近用户需求，更能还原互联网的本貌。在中国的传统行业都有一定的所谓黑市门槛，即属于潜规则范畴或者是不为人知的行业秘密，这种信息只流传在最信任的人脉圈子里。读懂了这些，才能算从根本上了解了这个行业。



1. 深度研究分析互联网地下产业链的目的

对于在互联网行业的创新者来说，地下产业链代表着一定的风险和影响，但是我们积极的考虑：灰色黑色产业链甚至是黑市交易，代表着最接地气的用户需求和商业模式，可以给我们一定的用户需求理解、商业模式启示和相应的洞察力。另外，从地下产业链角度切入，纵览整个中国互联网产业的各个细分领域，也可以给我们更多的大局观和启示，这是本报告的意义所在。

我们深度研究分析互联网地下产业链有三个主要目的：

用户需求分析启示：由于自身模式的风险影响，对于存在于互联网生态系统中的地下产业链来说，产品定位和商业模式定位，极其切合用户需求，或者说是用户的心理诉求。当互联网巨头们在构建生态系统的时候，地下产业链表现出来极快速适应能力：一方面在吸取生态系统的养分，另一方面如针尖一样精准的扎向用户的心理诉求痛点。这对我们来说，不管是产品生态系统的运营，还是独立产品的设计，更多的还有对用户的把握，都有很强的启示作用。

风险分析影响启示：众所周知，国外的互联网巨头进入中国，几乎没有成功的案例，大多数有严重的水土不服。这里面有一些政策原因，但是更多的却是对中国互联网环境的不了解，对风险预估的不到位。反观，国内却有很多非常草根的创新却获得大量用户的青睐。对中国互联网用户的理解是一方面，更多的是在商业游戏中，对国内互联网地下产业链的影响没有做到足够的预期的评估。

商业模式分析启示：地下产业链由于存在较大的风险成本，所以在商业模式上都有一定的创新并满足快速变现的需要，在这一点上表现的极具生命力和接地气。特别是由于风险的存在和见不得光的劣势，利用一些社群模式快速的形成规模化和上下游的链条合作，这对于我们在互联网上创业创新来说，有非常大的学习启示作用。

2. 中国互联网产业链发展现状概述及分析

如果我们从地下产业链的视角切入，可以这样来分析目前整个中国的互联网行业：

国内互联网产业，目前有明显的垄断性：和任何行业一样，垄断最基础的资源后，就可以往上挤压增值服务部分的利润；而增值服务的进一步发展，会更加催高基础资源的价值。陷入循环，从而呼叫马太效应。而对于目前互联网产业来说，这个基础的资源就是流量。

高速发展的红利，催高了流量的价格，让这个本应该是互联网人人都可以享受到的红利，集中到少数的利益集团的手中。目前想在国内互联网上获取流量，成本不菲：大的流量入口被巨头企业垄断，而长尾流量却被巨头企业采购，巨头们都看不上眼的流量，也会被广告联盟聚集。

这导致了创新变得有特别明显的定向性：要么需要强变现能力，来支撑起高额的流量费用；要么需要资本力量的介入，可以支撑起初期的发展成本。而前者形成了地下产业链相关的变现模式；而后者资本的接入，反而扰乱了市场：一是由于风投资本的盈利模式和发展现状决定，二是由于热点轮换，导致短时间内在细分领域中汇集大量的创新者，正这些让互联网的创新更多的成为一场博傻的游戏、一场讲故事的比赛、一个编概念的酒局。而真正的创新者，面对的反而是被推高的流量成本，浮躁的行业环境，以及长时间的寂寞和等待。

所以目前的互联网行业的创新者，可以大概分成三类形态：

概念投资型：通常保持在媒体视野之内，被各种科技博客科技媒体争相报道。有着从西方借鉴过来的成熟的商业模式，创始人一般从顶级的公司离职，有着正规军的思维方式和职业化做事风格。被各类风投看好，从天使投资一直拿到 B 轮 C 轮，奔着上市或者被收购为目标，概念创新、市场预期和想象空间要比盈利更重要。这也是中国互联网产业的主流，地面上的部分，但由于仅仅是因为在地面上被人熟知。

草根灰色型：贴着地面生长出来的极接地气的产物，草根特色，一般都在埋头挣钱，鲜有媒体关注，过多的媒体关注对它们而言也不算好事。目标即是盈利，所以在商业模式上和用户需求满足上非常专注。并没有特别多的概念创新，却有长时间的用户反馈的积累和优化。这些类型的互联网产业链占比非常大，而且有着明显的区域性特征，特别是移动互联网的快速发展之后。

非法黑色型：涉及许多见不得光、游离在法律边缘的产业链，但它也不是阳光照射不到之

处滋生繁殖的法外之地，相反，有些大量的用户群。更多时候，无论是为了自保还是业务的安全风险，他们都不会主动的浮出让人发现，他们的商业模式更是非常的机密。然而，在很多时候，非法黑色互联网产业链都无意中直接或者间接的影响着整个互联网的环境，甚至参与制定过一些地上互联网世界也必须遵从的规则。

我们在这篇报告中，主要是从后两者形态产业切入分析，特别是第三种形态。并且分析与第一种形态之间的关联：任何概念投资性的互联网创新，什么包括互联网巨头，都不能离开地面和地下的世界而悬空生长，相反，合理的构建生态系统，从地下吸收养分，制定游戏规则，规范支持，真正帮助最终的用户，是每一个互联网创新者所追求的目标。

3. 中国互联网地下产业链发展现状及分析

外行看热闹，内行看门道。中国互联网行业高速发展，越来越繁华，也越来越浮躁：如同冰山效应，大量“专家”只盯着冰山浮出来的表象做文章，却没人深入水下探索。久而久之，水下的世界越来越不为人知，也越来越复杂。这些复杂的利益关系，商业模式，各种对于漏洞的利用，打擦边球的做法，和一些封闭的信息孤岛，错综复杂，但是也构建了目前中国互联网的部分现状，我们希望称之为地下产业链。

对于地下产业链来说，本质是利用目前国内互联网用户对网络的认知水平不同，精心打造产品，进行的各种获利；而吸附于某互联网细分生态系统中，利用信息差，吸收养分；更有甚者是利用技术水平的优势，进行破坏、侵权及获利。总而言之，地下产业链发展至今，已经不能明确的把它剥离出来，所谓清水池塘不养鱼，这可能也是每一个行业发展都会遇到的规律。

中国互联网地下产业链发展到目前阶段，已经渗透到互联网行业几乎所有的细分行业中。从整体互联网的生态结构上来说，我们可以从三个方面来分析目前地下产业链的发展现状，这也是本报告的整体结构：

流量获取分发：流量的获取和分发是互联网的最基本的入口。获取用户访问的流量，是互联网最基本也是最原生的形态。流量入口造就了互联网巨头，特别是百度更是占据了传统PC互联网的流量入口，通过分发流量发展到了几百亿美元市值的规模。采购和获取用户流量更是互联网企业的最基础的生存保证。而地下产业链更是在围绕流量的获取分发产业链做足了文章，也是最重要一环。

流量变现盈利：流量变现是任何互联网创新服务的基本形态，采购流量->提供增值服务->变现，也是大多数互联网创新的最基础的原理。对于概念投资型互联网项目来说，也许流量变现盈利并不是眼前的问题，但是长期来说，盈利模式也是无法避开的话题。而对于地下产业链来说，由于生存周期一般较短，变现盈利，是最根本的生存法则。

数据信息安全：除了流量获取分发，和流量变现盈利以外，还有一部分地下产业链在围绕数据服务、信息服务、信息与数据安全或是攻击敲诈勒索诈骗上做文章。这一类地下产业链更多的是服务于其他的产业链，但是牵扯更多非法的交易，和对互联网商业环境、互联网终端用户的影响。这部分产业链是影响最大也是最复杂的一部分。

4. 本报告相关概念定义及其整体结构导读

本报告通过三大部分（流量获取分发、流量变现盈利、数据信息安全）来分析中国互联网地下产业链，每一部分都针对整体、移动互联网、总结洞察进行单独分析，共具体分析 22 个细分领域的地下产业链。每一部分都有详细的数据进行论证分析说明。

本报告针对每一个具体的细分地下产业链，都会针对性分析该产业链的风险与影响、数据深度洞察、以及商业模式启示。通过不同的角度尽可能还原客观，理智的看待这些地下产业链存在的意义和对我们的正面作用。

本报告最后一部分通过五方面（风险影响、商业模式、用户需求、行业发展、发展机遇）进行分析洞察，这部分内容是 TOMsInsight 分析师团队的观点，希望给读者带来有见解性的视角洞察、创新思维、以及商业启示。

最后，本报告仅从学术角度研究，并不进行法律探讨。而任何非法的事物必将受到法律严惩。

5. 本报告数据来源及分析方法定义与说明

本报告所有数据均为 TOMsInsight 数据分析团队跟踪监控、抓取整理，分析整合而成。大多数据为技术手段所得，部分数据由抽样采集而成，而由于一些地下产业链的数据，我们会采取一些非常规手段（专家网络、用户访谈、舆情监控、合法购买、调查抽样等）获取，这类数据我们会通过一些算法分析出相应的结论，由于抽样本身的限制或者样本噪点影响，只能部分的代表一定的观点并不能 100% 客观，对于这部分数据我们也会标明。

TOMsInsight 团队保留对所有数据的解释权。

二、 流量获取分发相关产业链部分

流量是互联网行业最基础的资源，也是一切互联网产品和商业模式创新的基础。互联网整体的发展，和移动化的趋势，让流量之争不断的成为新的商业战场。而对于互联网地下产业链来说，更是不可或缺的命脉和核心专注点。

一方面聚集流量，通过正规渠道变现；另一方面聚集流量，再次在黑市中分发，成为地下产业链变现的上游。也是目前互联网地下产业链的基本生存保障。



流量获取分发相关产业链部分整体分析



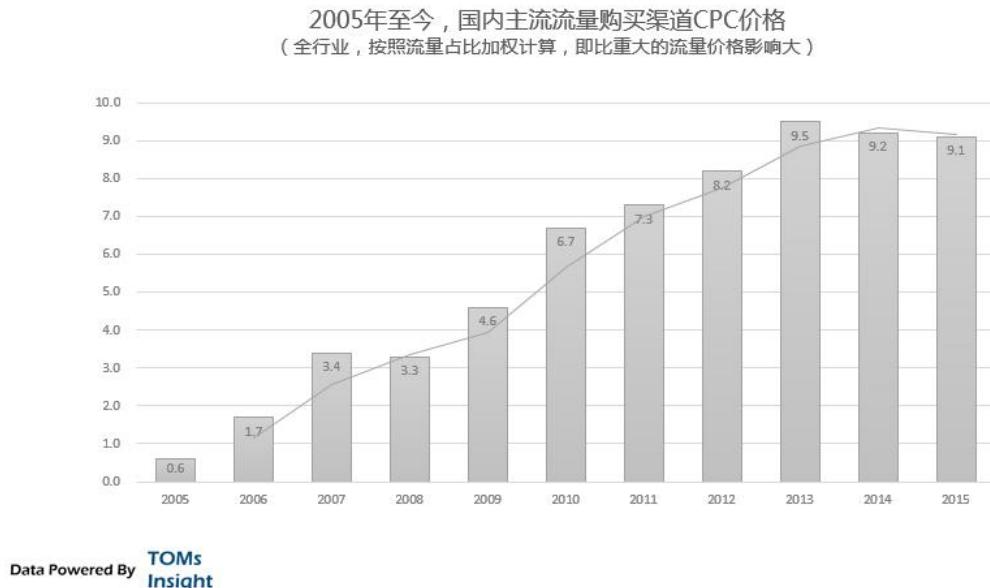
A. 流量获取分发产业链整体情况

很少有人去抽象出来互联网的最简洁的模型，但是假设我们真的去做，我们会发现流量获取分发几乎是一种最精简的抽象方式，特别是在中国互联网行业，在很多意义上，流量的入口和流量的分发权力几乎成了互联网上最重要的资源。

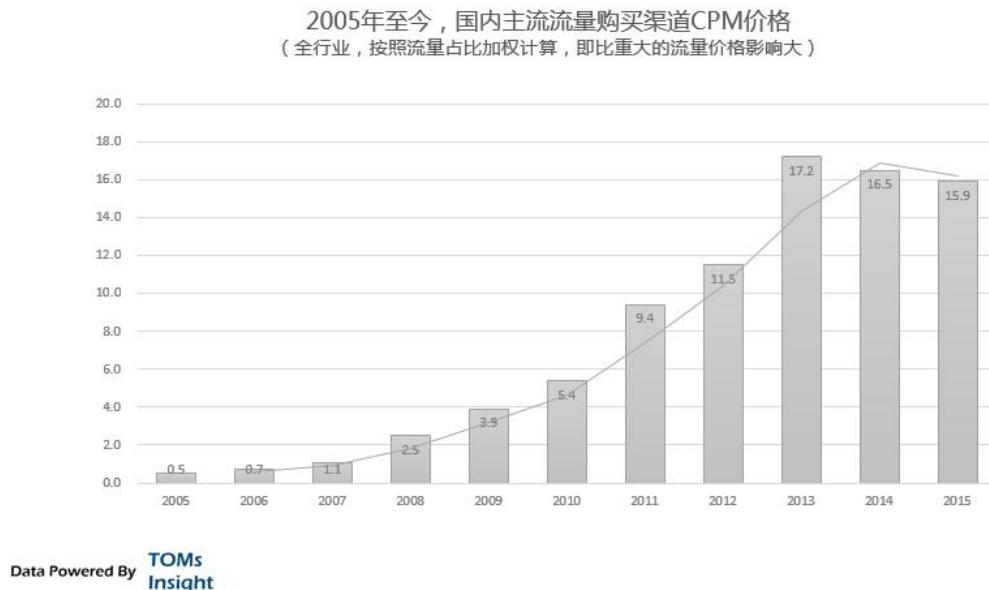
有了流量，就有了在互联网行业生存的能力，而占据了大的流量入口，也就成为了互联网巨头。其实根本的原理就是这么简单。而大量的互联网精英创新者，有先进的理念和方法论，有好的产业设计和完美的商业模式，到最后却没有好的流量获取方式。拿到风投后，大肆的采购流量，却发现几百万在这个行业里面几乎连水花都打不起来。

流量获取分发由于大量的地下产业链的存在，变得极其复杂和水深，有时候懂行的人流量的获取成本非常的低，但有时候却又高的吓人。真实流量和虚假流量很难分清楚，让网络推广也变成了一个热门而又邪乎的行业。

下图是我们跟踪 2005 年至今，国内主流 CPC 和 CPM 价格（CPC 为通过互联网广告采购流量按照点击付费，每一次点击费用；CPM 为通过互联网广告采购流量按照展现付费，每千次展现的费用），全行业：



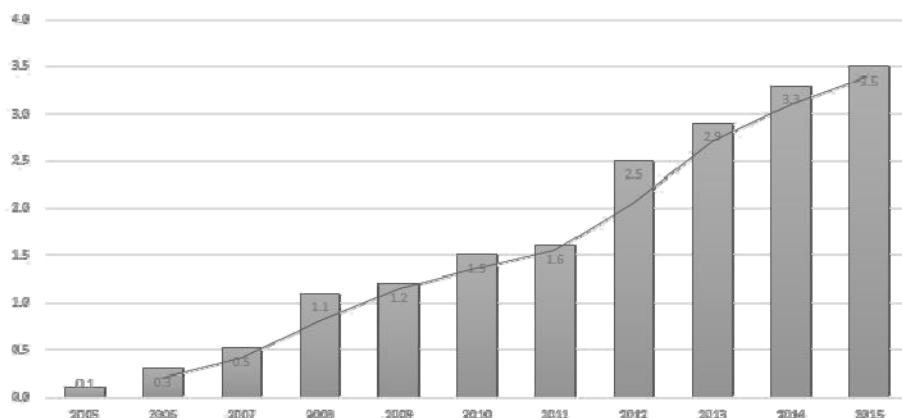
如上图可见从 2005 年到 2013 年，由于互联网发展红利，流量的费用也在逐步上升，最能直观代表互联网流量价格的 CPC 广告，每一次点击（也就是说每一个 IP 流量）从 0.6 元飙升到了 2013 年最高的 9.5 元。但是我们同时也能看出 2014-2015 年稍有回落，也代表互联网流量的价格已经被推升到了一个相对目前互联网发展水平极限的高度。



如上图所见，同样一直升高的也有 CPM 展现广告的费用，值得一提的是，2011 年之后，由于大数据发展，对用户人群更加精准的匹配，让展现广告更多定向。也让 CPM 广告的价格飙升到了平均每千次展现大概 17.2 元的高度。

之前我们分析的是主流渠道流量的购买，而在地下产业链范畴中，流量价格的变化又是什么情况呢。由于地下产业链的形态和产业数据并不是那么公开化，我们通过对弹窗广告、黑链流量、盗版软件流量等可追踪的黑市流量价格进行分析，同样是 CPC 方式的 2005 年后变化分析如下：

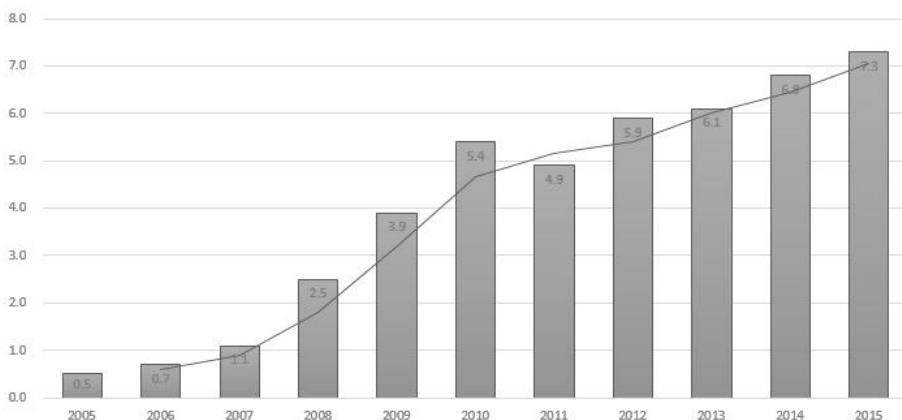
2005年至今，国内地下产业链流量购买渠道CPC价格
(仅通过弹窗广告、黑链流量、盗版软件流量等可追踪的黑市流量价格进行分析)



Data Powered By **TOMs**
Insight

用同样的方法来分析地下产业链中流量生意最主流的 CPM 价格如下，我们可以看出从 2010 年之后，连续几年价格都维持在 5-7 元之间，由于地下黑市上的水分，这也代表着地下产业链 中 CPM 方式采购流量可以接受的最大的价格。

2005年至今，国内地下产业链流量购买渠道CPM价格
(仅通过弹窗广告、黑链流量、盗版软件流量等可追踪的黑市流量价格进行分析)



Data Powered By **TOMs**
Insight

可以从上面两张数据图看出，地下产业链中 CPC 和 CPM 价格明显要比主流渠道低很多，在这里面一方面是由于地下产业链的流量获取分发成本确实要低，另外由于缺乏监管，充斥着虚假流量和相关的骗术。但是由于地下产业链的玩法不断升级，也不断的渗透到主流流量分发渠道的生态圈中，导致了各种的风险和影响，这也是我们报告本部分分析的主要目的所在。

B. 细分产业链之间生态关系分析

我们从 8 个细分产业链来分析地下产业链的流量获取分发部分，分别是：搜索引擎流量与分发、腾讯生态流量与分发、微信生态流量与分发、广告联盟与流量再分发、网络内容与信息推广营销、安卓流量分发、微博等社交应用流量、病毒木马与盗版软件。

从表面上看，好像每个细分领域都相对独立，但是在实际中却由于有再分发而导致错综复杂。也许我们通过实际的例子可以解释的更清楚一些：比如通过百度 SEO 获取的流量，移动流量部分可以在安卓渠道中再分发，最后通过 CPA 变现。而 CPA 投放的广告方 app，通过静默的方式再次分发了病毒的 app；再比如微博的流量，可以引入微信公众账号，而微信公众账号可以用站群互推的方式放大规模效应，最后引入传销式的网络营销培训变现。

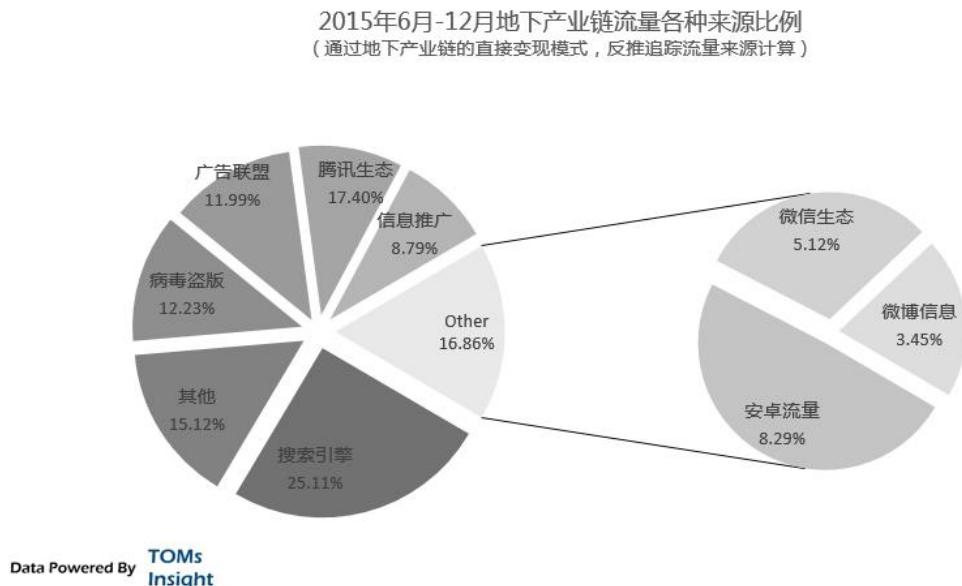


流量再分发的过程，在地下产业链中会有一个放大效应，而这个放大效应也是最近 1-2 年地下产业链所一直追求的创新手段。一般来说，这个放大效应总是在社交网络、移动流量中产生。也许读完我们对这 8 个细分产业链全面分析后，可能会对各个细分产业链中的生态关系，以及这个放大效应有更深刻的理解。

C. 流量获取分发的黑市深度数据

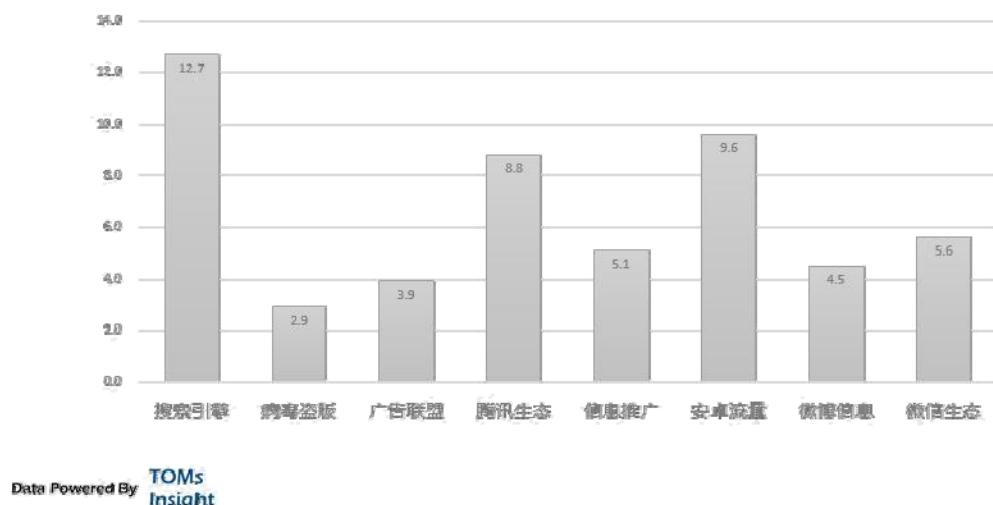
目前来看，地下产业链中流量来源主要还是来自搜索引擎生态。而安卓、微博、微信三大移动生态占据了几乎 17% 的流量来源。

由于在移动端变现远远不如在 PC 端流量变现成熟，所以 17% 的比例已经非常可观了。这也说明地下产业链的流量市场，也消耗掉了一部分资本的推力。



从流量的价格来分析，又完全是另外一种情景了，我们可以从下图看出不同的流量来源的 CPM 价格较大的差异性：

2015年，地下产业链不同类型流量购买CPM价格
(抽样统计及算法预估，统计端点较多并不能100%客观)



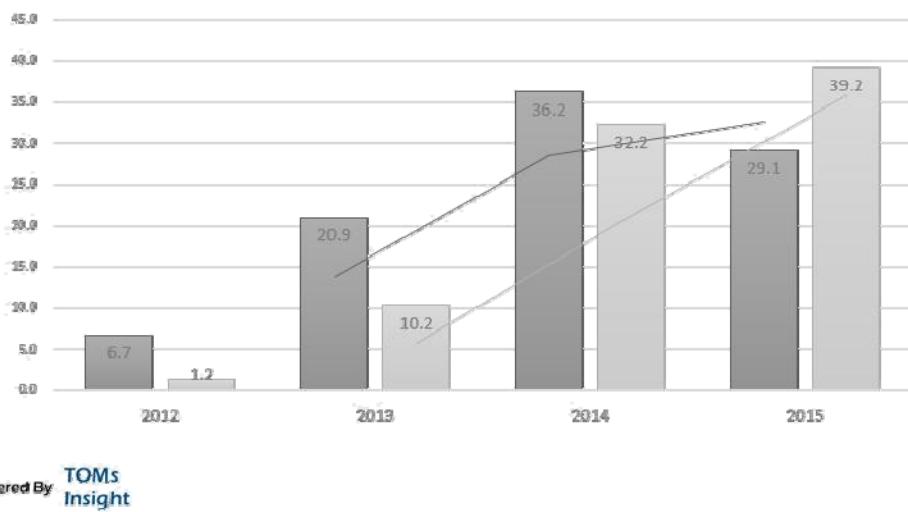
搜索引擎带来的流量，由于其目标客户的准确性，和信任优势，当之无愧的处于最高的价格上。 腾讯生态下的流量，由于信封号和各种引流的存在，加上 QQ 的粘度和附带的社交属性，价格也比平均高出不少。而安卓流量由于各种暗扣和再分发的成熟，以及资本市场对移动概念的追捧，也拉高了 CPM 价格。

而目前火热的微信生态流量，并没有想到的那么火热，由于微信安全性的限制，在 2013 年后 期禁止了微信浏览器对安卓 app 的直接下载，导致了 CPM 的价格在 2014 年降低到了 3.6，但后又由于微商等深度变现的火热，提升到了 2015 年的 5.6。这个价格也是在地下产业链变 现中一个合理的价格。其他的流量来源也在整体环境的影响下，低于平均水平。

我们分析发现，地下产业链中的流量来源分布和价格对比，与主流渠道非常类似。而且几个因为资本原因推升的细分领域流量，在地下产业链中也同样有着高居不下的价格，并消化了一定程度上的资本的推势。例如目前火热的 p2p 金融行业，在地下产业链中的价格，和主渠道的价格对比如下：

(灰色部分为地下渠道，同样都是 CPC 的价格，地下渠道只统计了：弹窗广告联盟、黑链流 量、盗版软件流量、和流量再分发类 app 广告。)

2012年1月至今, P2P金融相关关键词在搜索引擎生态中CPC流量价格
(主流渠道 vs 地下渠道)



从 2012 年的大概 5 倍 , 到 2014 年的几乎一样的价格 , 到 2015 年的超过。 p2p 金融的火热 也同样带动了相关的地下流量。毕竟 , 对于针对于最终用户即是客户的 p2p 金融来说 , 地下 流量和主渠道流量几乎没有什 么区别。如果再加上地下流量的损耗 , 其实意味着地下流量更受 欢迎很多。

这也是我们研究地下产业链流量获取分发的目的 : 深度理解互联网细分行业或创新 , 并不是仅 仅看表面的浮华 , 从最根本的流量来源渠道或对比 , 才能更好的认识这个行业 , 更深度的洞察 这项创新或产品 , 而真正的认识本质 , 也规避了相应的风险。

接下来我们逐一的去分析地下产业链中不同细分行业的流量获取分发。

搜索引擎流量与分发产业链分析

1

A. 相关地下产业链整体深度分析

其实当我们说到搜索引擎的时候，第一个想到的就是百度。百度作为国内几乎垄断性的流量第一入口，也在搜索引擎流量与分发产业链中占据主导地位。所以在本章节，我们都会用百度的例子来说明，360、搜狗、Google 等一是占有市场份额太小，二是由于商业广告产品和流量分发的生态系统的不成熟，我们并不单独分析。而且举一反三，在地下产业链中从百度之外的搜索引擎生态中获取流量并没有特殊的玩法。

不论地上还是地下，通过百度获取流量，主要只有 SEM 和 SEO 两种方式。在这里我们给可能不太了解 SEM 和 SEO 的读者解释一下：

SEM，即英文 Search Engine Marketing 的简称，本意是搜索引擎推广。但是在国内互联网圈，SEM 已经变成了在搜索引擎，或者说是在百度上投放广告的特指。百度广告系统名叫凤巢，2009 年年底上线，代替了之前的竞价排名，从明拍转向了暗拍。而 SEM 即在百度的凤巢的广告系统投放广告，广告会出现在百度搜索的结果页中，或者网站的网盟广告中。

SEO，即英文 Search Engine Optimization 的简称，意思是搜索引擎优化。SEO 是专门利用搜索引擎的搜索规则来提高目前网站在有关搜索引擎内的自然排名的方式。SEO 是搜索引擎构建自己生态结构的一部分，目的是为网站提供生态式的自我营销解决方案，让网站在行业内占据领先地位。SEO 是自然排名的方式，主要针对网站在搜索引擎中做排名优化，长年积累。简单的说，百度 SEO 即是不给百度广告费，通过一些技术手段获取百度分发的流量。

再简单的说，一种是直接花钱买流量，一种是用技术手段获取流量。而由于百度流量价格的越来越高，通过 SEO 获取自然流量的方式也就变得越来越被关注。

通过 SEO 获取流量，就必须遵循百度 SEO 规则，如果按照这个规则，网站如果能得到比较好的收录，获得好的排名，从而得到流量，是一个极其缓慢的过程，少则几个月，多则几年，而且要网站确实收到很好的欢迎程度。因为百度网站收录排名是一个很复杂的算法而且会不断的 变化，但是主要和被收录网站的内容和外链有关系。

但是地下产业链 SEO，就是不遵循百度的 SEO 规则，通过各种黑客手段或者作弊手段，来在短时间内快速提高网站排名，从百度获取流量的办法。

B. 黑帽 SEO 地下产业链深度分析

笼统的说，所有使用作弊手段或可疑手段的，都可以称为黑帽 SEO。比如说垃圾链接，隐藏网页，桥页，关键词堆砌等等。于是对应的正规的手法叫白帽 SEO。

如之前所叙，影响网站的权重主要有两部分构成，一个是内容（文章质量、是不是原创、内容里的关键词等等），一个是外链（别的网站指向此网站链接）；SEO 就是对这两部分不断做优化调整，以提升自己网站的权重，使得自己的网站在检索结果中排名靠前。

白帽和黑帽在操作上有如下区别：内容上白帽会通过优化文章质量，提高原创性、有效性和对应性，来提升网站权重；而黑帽会注重欺骗搜索引擎，比如堆砌关键词、比如站群、让百度的蜘蛛爬虫相信这篇文章说了很多涉及这个词的东西。外链方面白帽添加外链的手法很光明，比如互换友情链接，或者是链接购买，并且只添加与自己网站内容相关站点的链接；黑帽就是越多越好，一般地下产业链中会用黑链来快速增加自己的权重。在真正的操作上，两者之间的界限非常模糊，搜索引擎也在不断调整算法，也许你今天用到办法是白帽的，明天就判做作弊；

地下产业链中常见的黑帽 SEO 手法包括关键字堆砌、地址重定向、域名轰炸、虚假关键字、网页劫持、隐型文本、垃圾链接、斗篷法、桥页或者门页，当然，还有最关键的挂黑链。

百度一旦发展了黑帽 SEO 就会 K 站，而地下产业链的大量的黑帽 SEOer 也会不断的去优化自己的手段，防止被百度 K 站。百度不断的调整自己的网站权重的策略，来防范更多的黑帽 SEO 手段。就如猫鼠游戏，不断的进化但是一直没有输赢。最近一年，比较大型的黑帽 SEO 组织已经可以集结顶级技术高手对百度的策略进行研究并采取新型的解决方案。

下图我们根据舆情来监控百度从 2005 年以来，关于 SEO 策略升级的次数，每一次升级也意味着一些 SEO 手段的作废：



C. 黑链交易地下产业链深度分析

黑链是 SEO 手法中相当普遍的一种手段，笼统地说，它就是指一些人用非正常的手段获取的其它网站的反向链接，最常见的黑链就是通过各种网站程序漏洞获取搜索引擎权重或者 PR 较高的网站的 webshell，进而在被黑网站上链接自己的网站，其性质与明链一致，都是属于为高效率提升排名，而使用的作弊手法。

简单的说，就是如果一个权重很高的网站给你做链接，对你是大有好处的。但是权重很高的网站为什么给你一个不知名的小网站做链接呢？于是用黑客技术，攻破这个高权重网站，偷偷的放入一个链接，还隐藏起来，不被发现，这就叫黑链。

黑链相对于寻找白链要合适的多，但在一定数量上可以说是价格不菲，所以黑链一般用于暴利的地下产业，例如私服，医疗，冷门高利润行业等等。

大多人挂上黑链以后，会选择在市场出售，而不是自己使用，这是由于目前黑帽 SEO 火热程度决定的，也意味着黑帽 SEO 分工已经足够精细化。

黑市上典型的黑链出售套餐价格 (一般来说都有大量的水分)

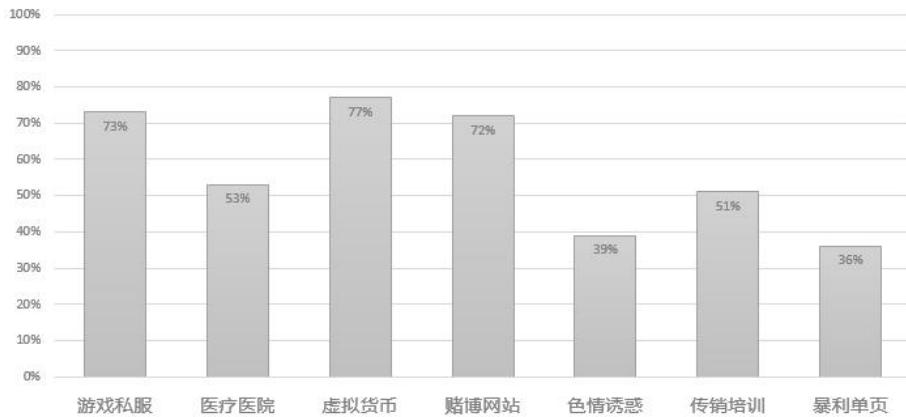
方案组	PR值	网链地址	月租	季租	年度
A套餐	PR1 PR2	PR1=10个PR2=10个共20个端点	10元	30元	稳定性
B套餐	PR2 PR3	PR2=10个PR3=10个共20个端点	20元	60元	稳定性
C套餐	PR2 PR4	PR3=10个PR4=10个共20个端点	30元	90元	稳定性
D套餐	PR3	PR3=10个共10个端点	35元	105元	稳定性
E套餐	PR4	PR4=10个共10个端点	45元	135元	稳定性
F套餐	PR1 PR2 PR3 PR4	PR1=10个PR2=10个PR3=10个PR4=10个共40个端点	80元	240元	稳定性
G套餐	PR1 PR2 PR3 PR4	PR1=20个PR2=20个PR3=20个PR4=20个共80个端点	160元	480元	稳定性
H套餐	PR1 PR2 PR3 PR4	PR2=20个PR3=20个PR4=20个共120个端点	200元	600元	稳定性
I套餐	PR1 PR2 PR3 PR4	PR2=PR4四机 共300个端点	380元	900元	稳定性

方案组	PR1	PR2	PR3	PR4	PR5	PR6	套餐说明	折扣价	质量
包月套餐一	3	3	4	3	-	-	铁块瘤 加密像20日共200个端点	200元	稳定性
包月套餐二	-	-	8	8	-	-	铁块瘤 加密像20日共380个端点	500元	稳定性
包月套餐三	-	-	6	6	2	-	铁块瘤 加密像20日共380个端点	675元	稳定性
包月套餐四	-	-	8	8	2	2	铁块瘤 加密像20日共380个端点	850元	稳定性
包月套餐五	-	-	-	8	8	-	铁块瘤 加密像20日共380个端点	940元	稳定性
包月套餐六	7	7	-	-	-	-	铁块瘤 加密像20日共420个端点	1200元	稳定性
包月套餐七	每台虚拟机需加锁PR2+PR4各需 24条	铁块瘤 加密像20日共1850个端点	630元	稳定性					

Data Powered By **TOMs**
Insight

下图是技术手段抽样扫描不同的地下产业链流量变现行业，使用黑链的网站的比例：

2015年10月，每个行业抽样100个变现，监控使用黑链的比例
(样本库随机抽样，有一定的偶然性，仅作为定性分析)



Data Powered By **TOMs**
Insight

D. SEM 作弊相关上下游生态分析

SEM 在这里特指在百度投放广告获取排名和流量的行为。由于是在百度投放广告，作弊的可能性不大，但是还是会有作弊的情况，并且把获取的流量流入地下产业链。

2009 年之后，百度的竞价排名升级到了凤巢，从原理上来说，从明拍变成了暗拍。暗拍系统大家争相竞价，把利润都交给了百度。后来有些商家做成了联盟，大家并不竞价了，而是轮流坐庄吃利润。还有一种情况是有一些会在百度“一户多开”，做很多网站，开很多凤巢账户，垄断某一个长尾词，也可以降低价格。

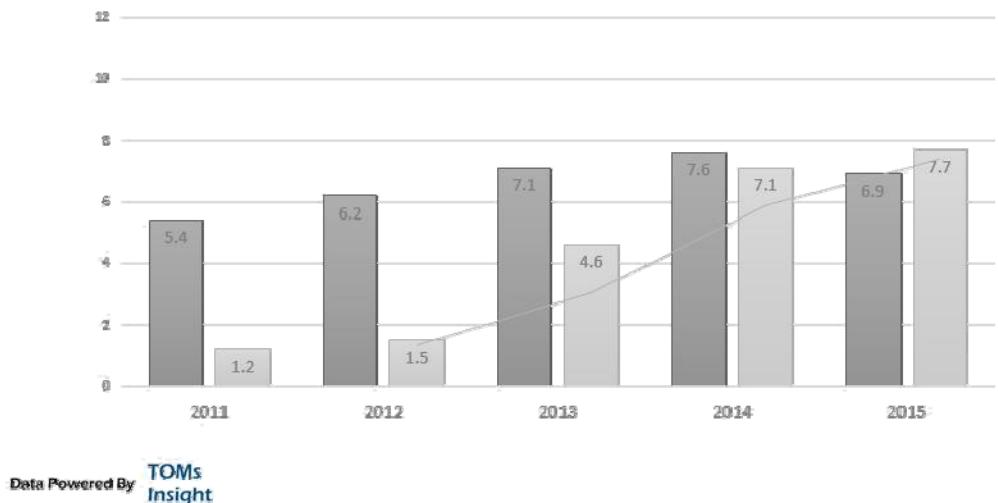
一般来说，结合成联盟之后肯定会有乱入者，而结盟者就会采取类似 DDOS 的攻击手段让乱入者退出，保持联盟的稳定。我们会在本报告的第三部分第 2 章 B 节，介绍 SEM 作弊的下游生态和变现手法。

E. 移动端流量的模式变化与数据

从 2011 年开始，移动端流量占比越来越大，由于变现模式的不同，在地下产业链中，PC 流量和移动流量开始分别出售，并且在不同的行业都有很大的差异性。

不难看出，PC 流量价格一直相对稳中有升，但是移动流量到了 2013 年几乎有了一个爆发性的增长。这一方面是由于 app CPA 推升，但是更多的是移动流量虽然在主流互联网领域中并没有很好的变现方式，但是在地下产业链中却有了先行者。

2011年至今，地下产业链百度生态系统下流量CPC价格（黑帽SEO 和作弊SEM）
(PC流量 vs 移动流量)



从 2014 年开始，移动流量几乎更受欢迎，特别是百度黑帽 SEO 来的移动流量。我们在这一章并不详细的来解释相关的流量变现，在本报告的第三部分我们会对各个细分进行分析。但是此处先从流量上游，来说明这个变化和趋势。

腾讯生态流量与分发产业链分析

2

A. 相关地下产业链整体深度分析

腾讯生态是国内最大的互联网生态系统，仅仅 QQ 就是一个总用户数超过 8 亿，同时在线数超过 2 亿的互联网产品，更不用说腾讯旗下的微信、空间、微博、各款游戏等等。腾讯的产品生态在成就了一个互联网巨头的同时，也同时引出多条地下产业链。

和百度专注流量分发相比，腾讯并没有在流量入口上做足文章，而腾讯的主要盈利方式反而是通过自己产品的流量引入，激活游戏产品线。这在一定程度上，等于是并没有充分的利用自己产品线中的流量资源，反而养活了地下产业链中大量引流产业。

换句简单的说话，百度就好比占据了一个河流口，靠分渠卖水赚钱，所以对别人分了自己的流极其的在意。但是腾讯也占据了一个河流口，但是靠自己开渠养虾赚钱，虽然对别人分流也极度反感，但是还没有上升到势不两立的高度。

所以在通过腾讯引流的地下产业链中，就出现了大量的长期发展的产业模式，并不像百度的黑帽 SEO 一样有着快速的变化，长期发展的产业模式渐渐的出现工具化，集团化的现状。

总体来说，腾讯生态引流的地下产业链可以主要分成：QQ 软件引流，相关产品引流，信封号（微信会在下一章单独分析）三种形态，我们接下来逐一分析。

B. QQ 引流推广产业链深度分析

QQ 软件引流是一种标准的产品入口引流，即在 QQ 产品任何可以曝光的地方，都会有引流的机会。比如说有一些用户会利用在线查找的功能，查找每一个地区在线有摄像头的年轻女性，就会发现有大量的诱惑头像，点击查看签名档会有一个网址和相关介绍，打开这个网址，即获得一个 IP。就是一次很标准的 QQ 引流。

QQ 软件引流在一定程度上来说并不算黑产，只是利用了软件大流量入口的游戏规则。接着之前的例子，我们在晚上 12 点钟的时候搜索并添加一个四线城市的在线有摄像头的年轻女性，发现大多数都是一些特殊行业从业人员，这也是利用了 QQ 软件的规则和入口流量，布局形成自己的推广。

再或者有些少年用户，会理所当然的觉得一些明星的 QQ 号码也是可以搜索的到的，于是也会

在 QQ 上搜索自己偶像的名字，于是有些人会利用这种用户心理，注册大量的以明星名字命名的号码，从而获得流量，这也是一种手法，虽然这种手法也已经过时。

当然还会有一些别的入口，比如说加群，群内聊天，通过技术手段获取对方群成员所有号码，定向打开临时对话窗口，主动加对方好友，等等。

由于超过 8 亿用户的基数，所以这些手段虽然简单却一直可以获得流量。腾讯在一次次打击手法之后，地下产业链从业人员发现所有的技术手段的批量注册，批量挂 QQ，哪怕是批量更改内容消息都会有很大的风险，反而慢慢的转成了人肉模式，即雇佣大量的廉价的键盘手来代替程序的工作。在这种人肉模式发展起来以后，QQ 软件引流就成为了地下产业链流量供养的一个非常稳定的部分：既不像黑帽 SEO 那样来去匆匆，也不像黑链似的不稳定。而是一直在黑市上出售，价格稳定，量也稳定。只是看采购者用何种方式变现。

C. 其他产品引流产业链深度分析

如果仅仅是 QQ 软件引流，还相对有限，腾讯生态还包括了其他的大流量产品：日志、相册、空间、和微博，等等。比如说去比较热门的日志去挂名，做一个比较诱惑的头像；比如说在相册里面上传大量的假自拍图片再打水印然后到处去别人空间留名；再比如加一些人气很高的号然后去 ta 的空间发一些有争议的话题等等。

这些手法的作用都很不明显，也带不来很大的流量，只能算是小打小闹。因为 QQ 的产品设计的核心社交性，如果没有社交性的支持（即大量的好友和关系圈），这些引流的作用都很不明显。所以相关的产品的引流和 QQ 空间引流不同的是，需要本身的好友众多。

但是 QQ 生态流量的地下产业链有一个核心的催化剂：信封号。有了信封号，所有的引流手段，就全部不一样了。而且形成了几何级数的放大效应。

D. 信封号产业链与相关生态分析

信封号，就是被盗的 QQ 号。信封号产业链，就是 QQ 号盗取、销赃、并利用获利的产业链。被盗的 QQ 在黑市上称之为“信封号”。就之前所述，QQ 由于其社交性，引流在没有大

量好友的情况下，效果非常有限，只能利用一些功能入口。但是假设，我们可以掌握一些被盗的 QQ 号，从而掌握了大量的社交关系，和信任，获取的流量，就完全不一样了。而且由于效果号并且非法性（可以黑吃黑，越非法的模式在黑市上骗术越多），在黑市变得极其活跃。我们下面分成销赃和生产两部分来分析观察信封号产业链。

我们先通过黑市术语来分析销赃的过程：

取信：一组 QQ 用户名和密码称为一个“信”，一个信封就是一万个（或者一千个）被盗的 QQ 号和密码。通过各种手段盗取 QQ 号码和密码，以万为单位保存成信息文本。拿到这些信息被称为：“取信”。

洗信：通过一些工具，将信里面有信息（QQ 币、有价值的游戏虚拟装备、QQ 靓号等）筛选出来的过程称为“洗信”。有专门的“洗信人”或者是“洗信工作室”来完成。

洗信过程：盗取后就没有经过任何清洗的信被称为一手信，一手信的洗信主要就是三步：第一步洗 Q 币，把信封里面 Q 币都转移出去，然后在黑市上出售；第二步是游戏虚拟装备，腾讯公司的主要收入就是来自游戏，而被盗取的 QQ 号中蕴藏的游戏虚拟财富必定不菲，所以洗信人接下来会把游戏装备、游戏积分、游戏账号以及游戏币等凡是能兑换成钱的游戏财物转走，存入固定账号。第三步就是 QQ 账号，挑 QQ 靓号（五位数、六位数、或七位数的短号，或者一些含有吉祥数字的号码）来观察是不是有密码保护或者死保（申请了密码保护资料，但是原主人忘记或者丢失了密码保护资料）。

二手信：一手信经过洗信后，称为二手信。二手信一般以更小的单位出售，在二手信的黑市上，一个信封一般只是一千个号。二手信经过洗信人的封装，分成不同的种类，不同的种类有不同的用处，下面是几种比较常见的二手信：

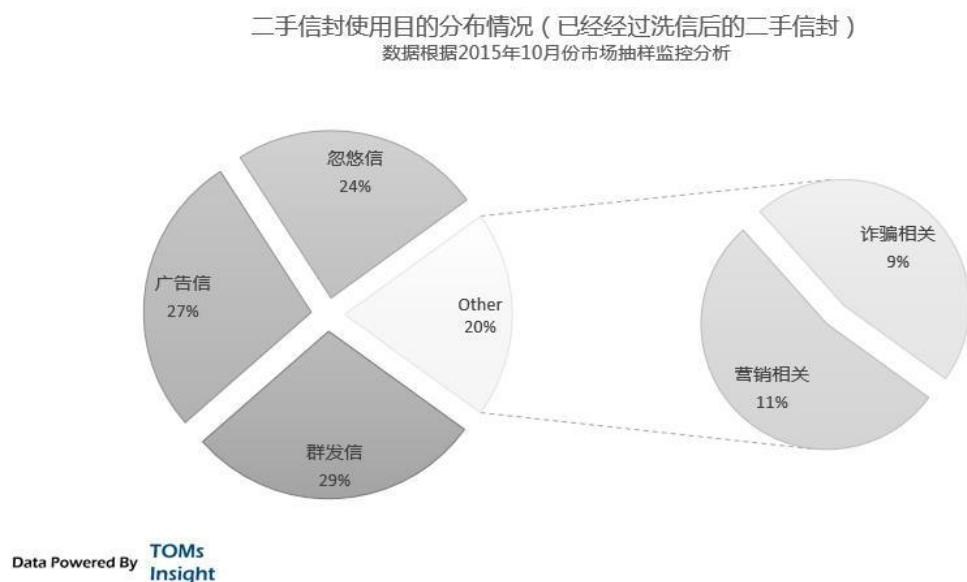
群发信：用来给被盗号的每一个好友发消息，一般发的消息都是特定的广告，例如各种网页游戏，特定的论坛等等，而现在很多 APP 的广告也开始使用群发信。

广告信：在 QQ 空间内植入广告，由于大多数人都开通了 QQ 空间，而一个人的 QQ 空间又会影响被转载到多人，所以效果明显，而且成本低廉，深受一些网络推广者喜爱。在 QQ 空间植入广告的信封由于腾讯安全策略，必须是能提取 cookies 的信封，就是无需验证码直接登录的信封，所以在黑市上也叫 cookies 信。

忽悠信：黑市上的买家登陆被盗的 QQ 号给好友发一些诈骗消息，一般都是急需钱或者出事了

之类的骗局。在忽悠信中还有特定的分类：海外留学忽悠信、女生忽悠信、18-23岁忽悠信等。可以类推这些可耻的骗子的手段。

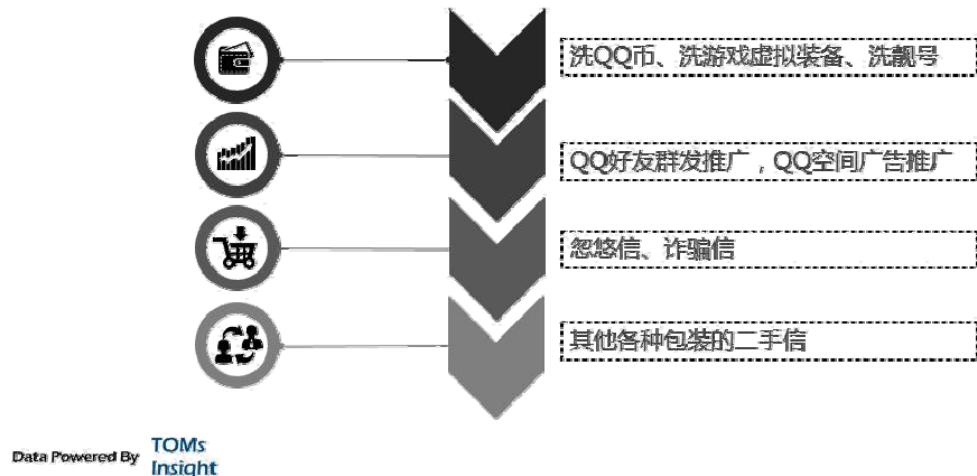
在这个封装过程中，信封的封装者和黑市上的卖家，充分的发挥了创新能力，出品了各种各样的信封：地区信、八位信、过夜信、90后信、蓝钻信、游戏信、等等，几十上百种，分别在黑市上卖给不同目的买家。



老信：最后被榨净的QQ号还会卖给黑客用来编写密码词典，或者邮件群发者群发广告。被盗的QQ号码是黑客用来计算用户密码习惯最好的素材。他们进行编译、分析、比对后，从而对网银或者支付宝之类支付工具进行破解。而邮件群发者不在乎用户是否找回密码，只是根据特定的信息，来发放广告。老信还有其他特定用处。

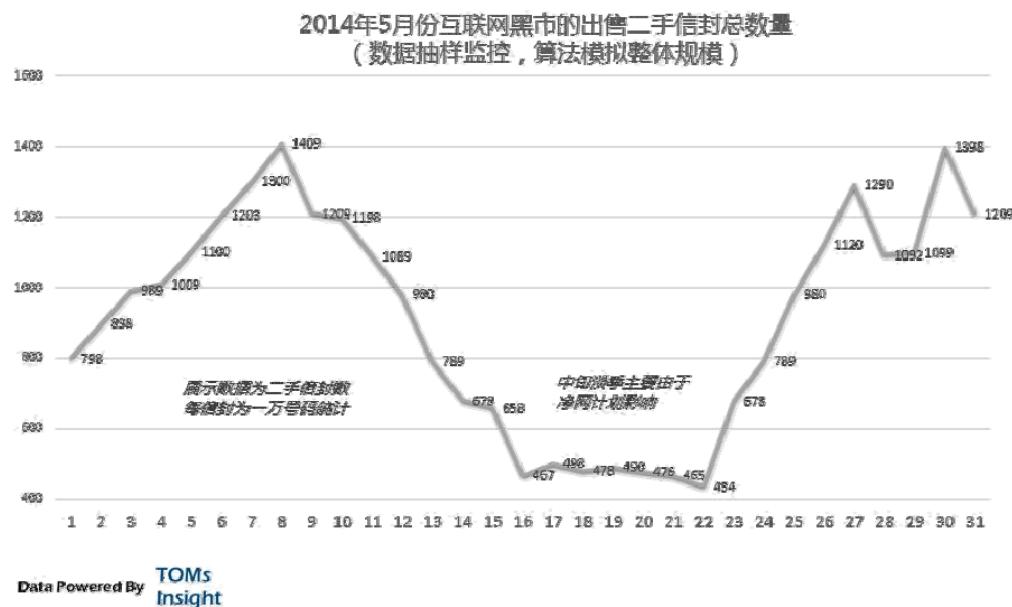
在这个产业链上，每个阶段的工作一般都由不同的“洗信工作室”专攻，而且会非常“守信用”：“洗币”、“洗游戏装备”、“洗靓号”、“做忽悠”、“做广告”等每个部分之间绝不相互侵犯利益。

信封号开箱子以后在黑市上包装与销赃流程



最夸张的是，由于一般都是在晚上 12 点开箱子（开箱子只指新鲜的信封被放到市场上），而 到了第二天天亮，被盗号的用户都会发现自己的 QQ 号被盗，从而修改密码或者采取安全保 护，让信封中大量的号失效，所以整个销赃的过程都集中在晚上 12 点早上 7 点之间。

每天，中国互联网黑市上的信封号出售的数量都大概在 1000 万个左右（有大量反复被盗，和一些死号的存在，所以新鲜用户远不到，几乎差别一个数量级多），我们通过一些非常规手段监控 2014 年 5 月份一个月内黑市的出售二手信封总数量可以见下图，我们能监控到的样本 只占少数所以通过一些算法预估和去重，数据并不非常精确：



而这么多的信封，是如何生产出来的呢？

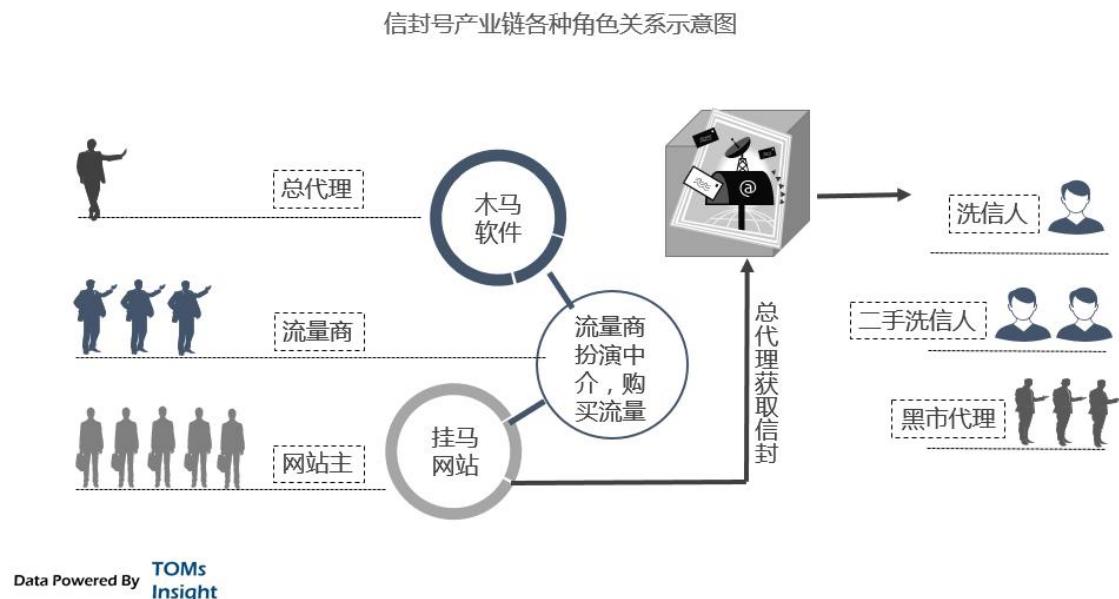
在信封的生产过程中，最核心的也是整个产业的“老大”一般在黑市上称为“总代理”。总代理首先向木马程序编写者购买或者定制专门的盗号木马（做马），然后委托一些流量商，将木马挂在网上。用户只要点击该网页，或者是下载了网页上的资源，其计算机就会被植入木马；木马将截取到的QQ号码和密码发往指定的服务器，总代理每天晚上会在11点左右把收到的号码和密码信息整理（开箱子），分给下面的二级代理（二级带来再分给三级，根据信封的数量），开始在黑市上销赃。

这个产业链中。流量商扮演了极其重要的作用，对于总代理来说，拥有一款效果稳定的木马和下级“二级代理”以及“洗信人”只是第一步，他们更需要将木马植入到用户的电脑中，才能真正获得利益。因此掌握着大量网站资源的人被总代理们格外珍视，这些人在行业内被称为“流量商”，即“挂马”人。流量商或者自己是网站的站长，或者与很多网站站长熟识，他们将病毒木马挂在点击率较高的网页上，当用户点击到那些弹出窗口时，木马病毒就“种”到了用户的计算机上。

在目前行业内，流量商根据IP流量对网站进行付费，1万IP大约需要100元到200元人民币，而流量商向总代理收费则是按信收费，一万个信1000元到1500元不等。而一个质量比较好的站，3万左右的流量就可以拿到一万个信。代理人虽然是整个产业链的核心和“老

大”，却处处被流量商制约。流量商也在黑市上被称为“做箱子的”，行业内，很多总代理为了

讨好流量商，还会对采取分成的合作模式，有的强势的流量商甚至可以拿到比总代理更高的分成。



而与此同时，QQ 流量在地下产业链中所占比重也被信封号放大，变成了仅次于百度的第二大地下流量来源。同样被放大的还有腾讯微博，我们会在本部分第 7 章分析。

E. 引流推广工具产业链深度分析

腾讯引流由于由繁琐的操作过程，和大量的账号的处理，以及之前我们所分析相对比较长期稳定的发展，需要大量的工具来进行引流和再分发操作。

地下产业链引流工具也经过了非常长期的发展，在和腾讯的猫鼠游戏之中，逐步的舍弃了以技术为核心的方式，而转向了人肉模式的发展。

我们会在本报告的第四部分的第四章分析人肉模式和周边产业链。但是此处先给各位读者一个对腾讯生态引流与分发产业链的整体介绍与洞察。

微信生态流量与分发产业链分析

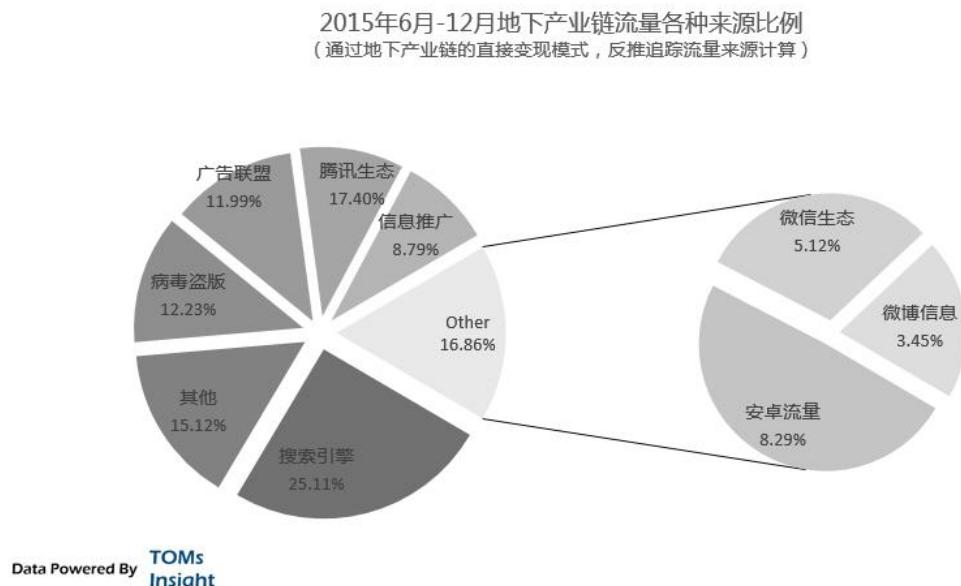
3

A. 相关地下产业链整体深度分析

微信在最近 2 年内非常火爆，一方面飞速的占据了 4 亿以上的月活跃用户，另一方面由于微信的粘性，围绕微信做文章的地下产业链开始活跃。不过在此我们不得不说微信的安全策略相对要成熟稳健的多，一直没有让地下产业链形成规模。

另一方面，由于围绕微信引流的地下产业链由于都是移动端流量，必须在移动端变现。在 2013 年中之前，大多微信引出来的流量是通过安卓 app 的 CPA 激活变现。但是后来微信改变了策略让微信自带浏览器无法直接下载安卓 app，让变现路线堵死，也让流量需求锐减。

2014 年开始，由于地下产业链中移动端流量更多的变现可能，让移动端流量需求增加不少，但是由于微信的特殊性和安全性，也一直没有形成规模。所以目前微信流量只占据地下黑市流量 5.12% 的份额，和比较低的价格，不能不说和微信本身的地位很不相衬。



我们分析微信的地下产业链，是很矛盾的：在 2013 年上半年，几乎如史诗般精彩；但是到了 2013 年下半年特别是 2014 年以后，微信生态的地下产业链逐渐枯萎到几乎可以忽略不计的地步，但是由于微信的地位，我们还是单独拿出来一个章节。

微信生态流量的获取和分发主要通过三个方面：直接添加引流、朋友圈和微信公众号。我们将接下来分别分析这三个不同的方向。

B. 微信号引流推广模式深度分析

和 QQ 一样，所有的添加好友的入口都会成为第一引流的选择，对于微信来说：摇一摇和附近的人，也成为了引流的第一选择。

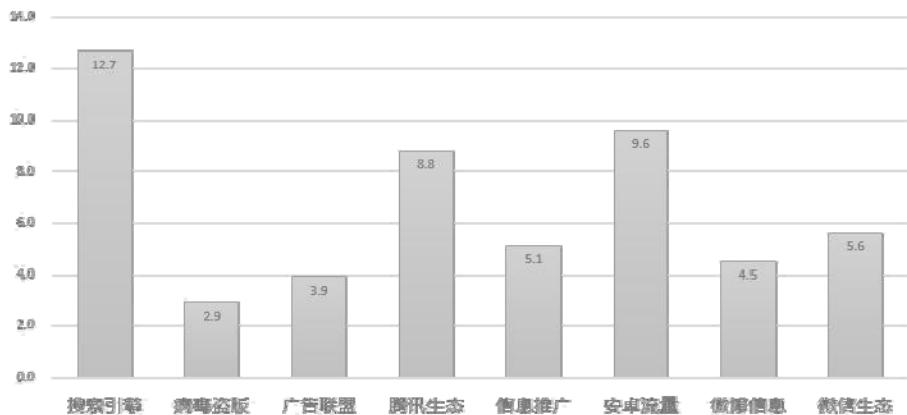
2013 年，地下产业链围绕这两个入口不断的进行软件模拟和软件功能迭代。当时黑市上交易火爆的各种自动摇一摇和站街（把头像和签名起的比较诱惑，打开附近的人功能引流）软件，都几乎是每天更新一次，配以出售的各种微信老号、海外号等等，还是可以获取很大的流量。

在 2013 年初，有些地下产业用自动摇一摇，签名档加上诱惑的网页链接，配以安卓 app CPA 变现，可以做到月收入上千万的水平；也有采取站街软件引流，把网络黄色产业发展到数一数二的规模。而且由于利益的驱动，在黑市上甚至引起多重势力各种攻击手段火并的状况。

但是 2013 年随着微信安全策略的不断升级，这些手法也慢慢的退出历史舞台，相关人员也开始放弃了微信，转而把目光转向了陌陌等其他移动社交软件，或者放弃。而目前市场上各种打着微信自动摇一摇和站街的软件，也都是小骗子来骗小白而已。

这一方面是微信安全策略的升级对这些软件本身的限制，另一方面是由于之前我们所说的微信对安卓 app 下载的禁止，让微信的流量一直没有好的变现方式，也导致了地下产业链的需求变小，价格一直比较低。

2015年，地下产业链不同类型流量购买CPM价格
(抽样统计及算法预估，统计误差较多并不能100%客观)



Data Powered By **TOMs**
Insight

微信大多数流量只能在朋友圈内搞电商变现，由于朋友圈电商的特殊熟人属性，导致了附近的人和摇一摇入口都变成了真正添加朋友的入口，也从软件模拟作业，发展到如今的人肉手动模式。

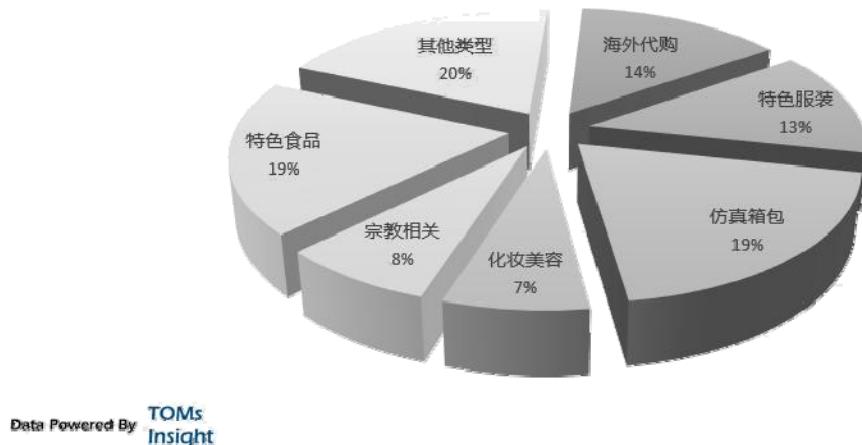
而黑市上出售的，也从站街软件、引流软件、自动摇一摇软件、自动打招呼软件，变成了加满5000每一地区特定好友的微信号。而这些微信号的变现方式，则是通过朋友圈的流量进行变现。

C. 微信朋友圈推广深度数据分析

同样，在2013年之前，有各种互联网地下产业链常用的欺骗性的引诱转发刷屏，配以各种的流量变现。但是微信的策略的不断升级，这些手段也被禁止。

对目前的朋友圈来说，更多的通过采购之前我们所属区域性号码，然后通过朋友圈直接变现盈利。如下图所示，是一些比较常见的变现手段：

监控样本黑市上出售的加满好友的微信号，出售后的进行朋友圈电商活动种类
(2015年10月，基于展现次数和电商数均权处理)



而还有一部分采购这类微信号传播微信公众账号，获取更多的粉丝，但是也不成气候。

D. 微信公众平台地下产业链分析

微信公众平台刚刚推出之际，比现在要热闹的多的多。在 2013 年早期，由于微信公众平台的查询入口还不像现在这么深，而且对于一些特殊关键词的查询并没有禁止，所有产生了很多吃查询流量产生自然增长的大号。

当时由于微信公众平台的注册也没有人工审核，有很多地下产业，直接注册成千上万的公众账号，都是包括一些“美女”、“丝袜”、“明星名字”类似关键词，很快获取大量的流量。这些号码，再配合互推，在 2013 年年初，就聚集了一些超级大号，和搜索长尾带来的大量的垃圾号码。当然这些号码随着微信公众平台的安全策略一次次的升级，和对这些垃圾号码的一次次打击，都慢慢的销声匿迹了。

2014 年后，地下产业链主要采取“养殖场”的玩法。

所谓的养殖场，就是一些非常利于传播的公众号的互推，并且利用大号带或者直接投放微信广告点通的公众号广告，快速的让 10 个或者更多的一组公众号达到总数 100w 的粉丝数，然后在

黑市上出售。由于采取了互推，并且文章比较容易在朋友圈传播，所以 100w 粉丝的成本并不高，一般情况下在几十万的水平。但是卖给一些培训变现、或者等待微信公众号红利的投资者，还是可以卖出百万以上的高价格。

养殖场的玩法其实几乎已经算是正常，并不能是黑产灰产的性质。

E. 微信公众号第三方开发产业链

值得一提的是，由于微信公众号的火爆，也带动了第三方开发机构、和代运营的组织。这些开发和代运营机构有时候也会参与地下黑市交易，主要是把手中掌握的号码指向的第三方网页，加入黑链，再次出售。由于相关的数量巨大，也能形成一定的影响力。

总之，微信生态的地下产业链，已经算是凋零到几乎不值一提的地步了。这可以说是微信产品本身的安全策略的成功，和运营的成熟。在另一方面上讲，也是一个打造产品生态，并不依靠地下产业养分的典型的案例，非常值得我们学习和借鉴。

广告联盟以及流量再分发产业链

4

A. 相关地下产业链整体深度分析

广告联盟就是集合中小网站的流量资源组成联盟，通过联盟平台帮助广告主实现广告投放，广告主则按照网络广告的实际效果向联盟会员支付广告费用。1996 年亚马逊通过这种新方式，为数以万计的网站提供了额外的收入来源。

在国内，百度也有运营的非常不错的广告联盟。广告联盟从本质上说，是互联网巨头向长尾流量中小网站采购流量的一种方式，流量主加入了广告联盟，也就等于把自己的流量交给了联盟代理出售。

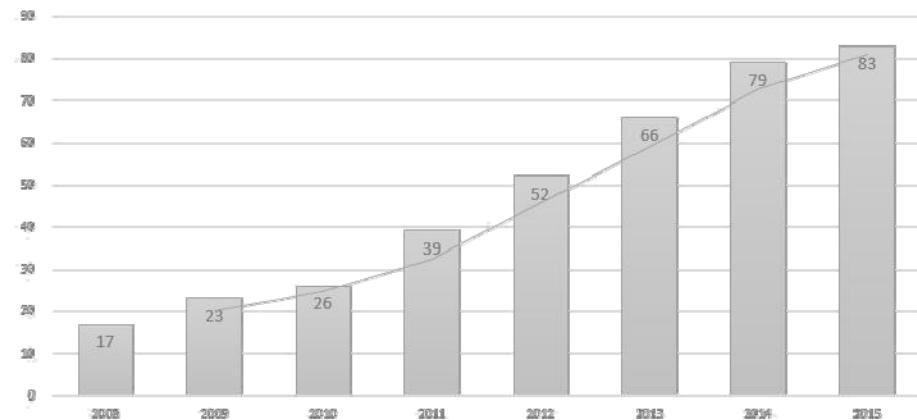
看起来这是很正规的模式，为什么地下产业链中有大量的广告联盟的流量呢？原因是简单，很多广告主的流量来源是非法的，无法加入到正规的广告联盟中来，所以就出现了很多地下广告联盟，收购非法流量，出售给非法变现，成为地下流量的中转点。

B. 广告联盟流量产业链深度分析

无法加入正规的广告联盟，就意味着有一定的来源不合理性。比如典型的就是网站没有备案通过，或者是牵扯到成人内容。而这部分的广告联盟和相关流量又会有多少呢？

下图是从 2008 年至今，国内地下流量广告联盟的个数：

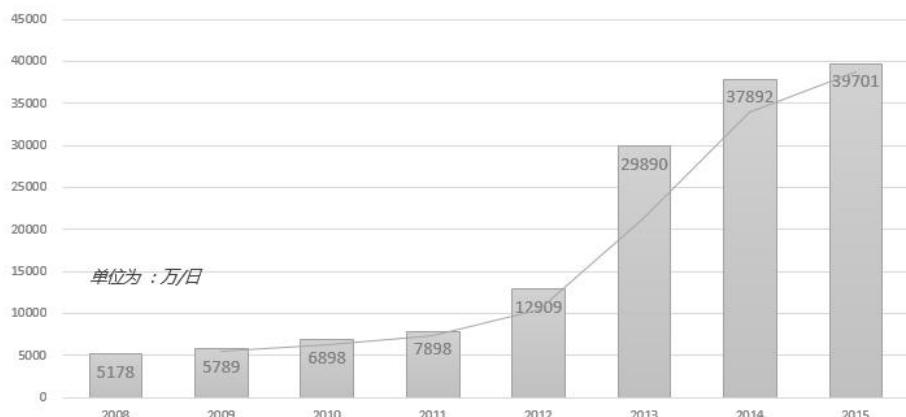
2008年至今，国内地下流量广告联盟个数追踪
(通过各种地下流量再分发链接反向监控分析)



Data Powered By **TOMs**
Insight

而每日的流量，也从 2005 年大概 5000w 的日 PV 展示的级别，发展到了 2014 年大概 3.7 亿 展示的规模，7 年 7 倍以上的发展。由于我们这个统计并没有统计到移动端流量，整体的 盘子 会更大。但是还是让人惊讶，和我们直觉认识到的 PC 端流量枯萎完全不同的是，不仅 仅没有 被移动端流量影响，而且进入到了快速发展通道。

2008年至今，国内地下流量广告联盟展示日PV数追踪
(算法模拟，和真实有一定的误差，只表现大概数量级别和趋势)



Data Powered By **TOMs**
Insight

3.7 亿日均 PV 的展示规模大概是什么级别呢，国内最大的流量分发商百度，也只有大概 10 亿出头的级别，而且有大量的非商业词存在。就算百度的 CPC 模式有着更大的商业价值，那么 3.7 亿的纯商业展现，也是非常惊人的。

那么这么大的流量来源，流量主都是一些什么人，又是怎么获取的这么多流量呢？我们接下来看一下地下广告联盟流量主的分析。

C. 流量主流量来源深度数据分析

地下广告联盟的流量主要是来色情网站和与色情网站类似的诱惑点击。

很多人都低估了色情网站的规模，和大家在寻找色情网站的过程中的路径流量。作为互联网上的第一用户需求，色情网站的流量规模几乎是很难想象的。

从目前全球 Alexa 来看，排名前 500 的网站中有 79 个是色情站点。排名第一的色情站点 Xvideo 目前排名第 43，仅仅在 apple.com 后面一位，而排在 microsoft.com 之前。

网站 Xvideos 在 Alexa 全球网站排名中的位置

42 Apple.com

Official site, with details of products and services.

43 Xvideos.com

44 360.cn

45 Google.ru

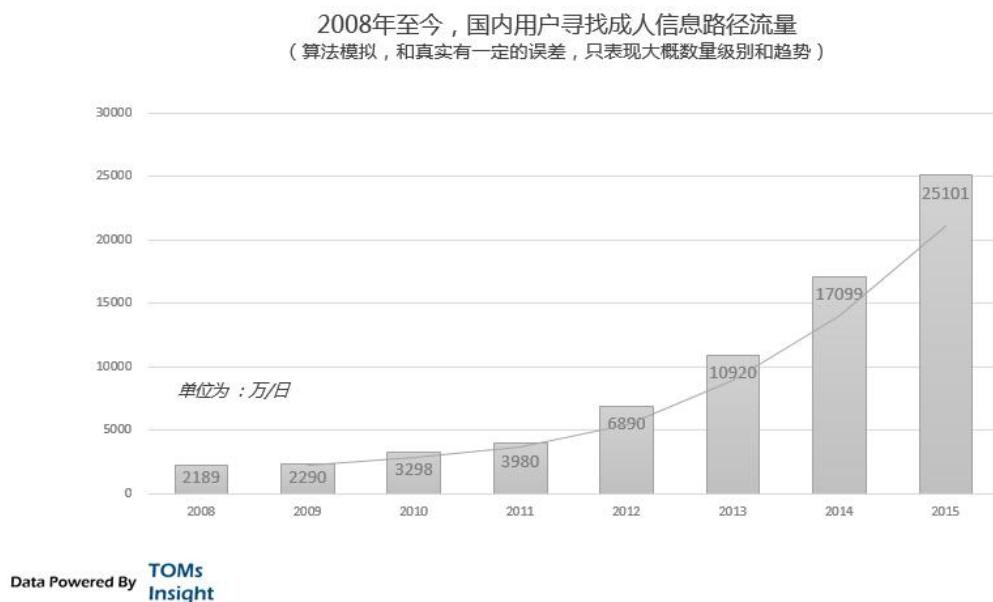
Русскоязычная версия поискового сервера.

46 Microsoft.com

Main site for product information, support, and news.

仅仅是 Xvideo , 每天就有大概 1.5 亿的 PV , 这才仅仅是一个色情网站而已。而在国内 , 由于色情网站的非法性 , 就出现了大量的为了寻找色情网站、或者色情信息而产生的路径流量。

什么意思呢 , 就是假设一个用户产生了看色情网站的需求 , 就会在互联网上用各种方法寻找 , 而他也确实能找到很多近似的、诱惑的、欺骗性的信息。这些信息都属于这个用户的路径流量。这个路径流量的大小有多大呢 ?



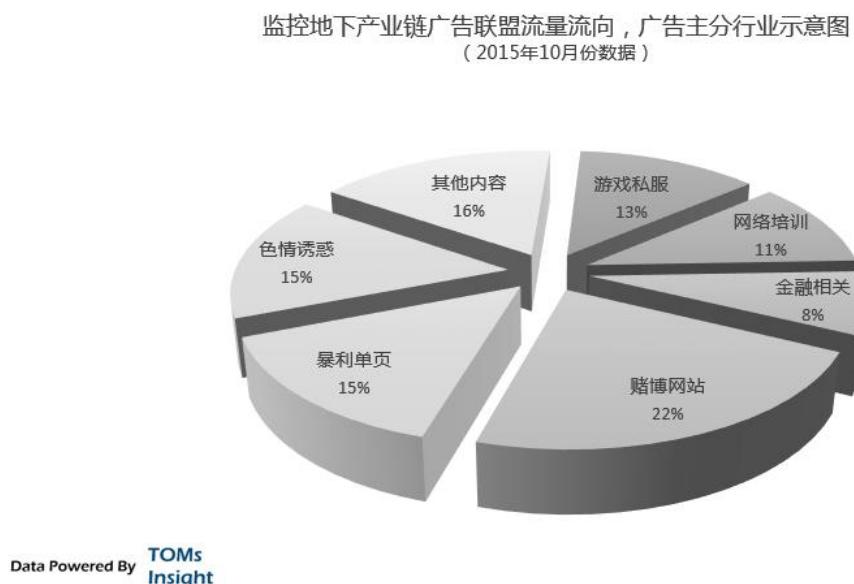
如果我们再拿出来之前的地下广告联盟流量分析就会发现 , 这两个趋势有着惊人的相似。路径流量大概占了 50% 以上部分。

也就是说 , 由于国内成人网站的非法性 , 压抑了国内用户的需求。用户在寻找成人信息的时候 , 被各种欺骗、擦边球似的信息诱惑而去点击 , 产生了路径流量。正常应该占据 30% 互联网流量的内容被压抑后 , 路径流量也到了 2 亿 PV 每天的数量级。

而这部分流量 , 是地下广告联盟的主要流量主供给。

D. 广告主盈利模式与利益链分析

那又是谁来购买这些流量呢，广告主都是些什么行业？我们跟踪所有的 83 家地下广告联盟，发现流量的流向如下表所示：



大多数都是流向了比较传统的地下产业变现大户。由于色情诱惑类流量的匹配效应，也占据了很大的份额。但是由于这个份额仅仅是 2015 年 10 月的数据分析，有一定的时效性，并不代表常态。

我们会在本报告第三部分逐一分析每一个地下变现盈利产业链。

E. 移动广告联盟的深度数据分析

从 2013 以来，移动互联网的火热也催生了移动广告联盟的火热，同样，在地下产业链中，也有大量移动流量分发的存在。

但是由于移动 app 的监管缺乏，很多非法类型的安卓 app 一样可以在主渠道广告联盟充当流量主的角色。比如地下产业中有采用传统的站群玩法，复制几千个安卓 app 投向各大市场，其实内容完全一样都是美女图，但是不断的更改 app 的名字和介绍，获取自然流量红利。但是这部分 app 群，也一样可以在主渠道广告联盟中充当流量主。

这导致了地下产业链中没有专注于移动流量的广告联盟的存在。不得不说这是一种很尴尬的局面：地下产业链少了一环，原因是需求由地上产业链满足了。

最后，关于广告联盟扣量等手法，我们不再分析，因为都属于地下产业链的正常消耗。

网络内容与信息推广营销产业链

5

A. 相关地下产业链整体深度分析

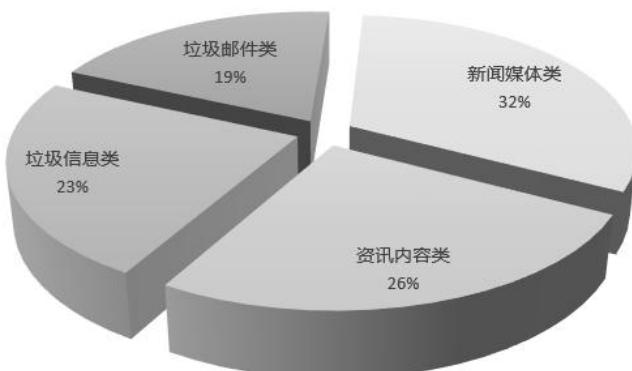
资讯和信息，是互联网的最重要的属性之一。之前利用搜索引擎生态的流量再分发，也只是截住了用户对资讯信息的查询需求，但是用户更多的上网时长是沉淀在资讯信息内容的本身。所以资讯信息内容本身的价值，在某种意义上要远远大于渠道的价值。

内容本身的价值，不仅仅在于流量，还有沉淀性和权威性。而后两者更能提高流量的价值。简单的说，有价值的内容，可以在互联网上沉淀很久，带来源源不断的流量用户，而权威的内容，可以让流量的变现价值大大提高。

所以，网络内容，在地下产业链也构成了重要的一环，占据了大概 9%的地下产业链流量。地下产业链中的内容流量，主要是由新闻媒体类网站、资讯内容类、垃圾信息类和相对独立的垃圾邮件构成的。

同样，如果我们把这 9%的地下产业链流量拆开，数据会如下图所示：

2015年6月-12月，内容与信息推广类地下产业链流量各种来源比例
(通过地下产业链的变现模式，反推追踪流量来源计算)



Data Powered By **TOMs**
Insight

B. 新闻媒体类地下引流数据分析

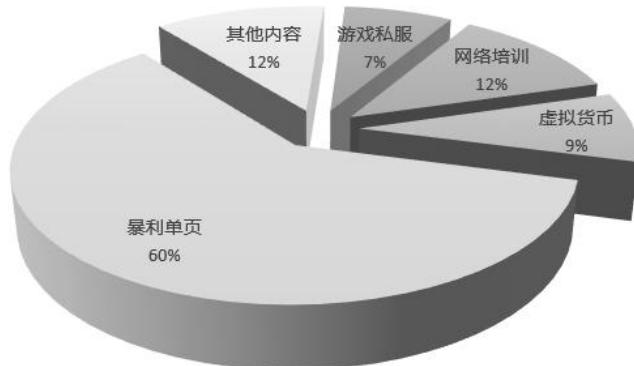
网络新闻媒体由于占据了内容门户，而且由于转发放效应，所以也成为地下产业链内容流量的重要来源。可能很多人都会疑问了，网络媒体不都是一些很正规的新闻么，怎么可能为地下产业链引流呢？其实，目前网络媒体充斥着软文和营销文，而且大多数都明码标价。

除此之外，可能大家也会发现，有很多新闻媒体上，都会有一些很吸引眼球的美女图或者怪诞新闻图片等等，点击去会变成更奇怪的吸引眼球的网站，夹杂一些不太正规的商品广告。这也是一种把流量引入地下产业链的渠道。另外还有很多网络媒体的移动端 app，也都经常会有流量导入地下产业链的情况，和 PC 端一样也是通过一些吸引眼球的图片或者新闻，或者是一些链接，链入地下产业链变现。

由于新闻媒体类的流量导出牵扯的是一些新闻媒体的违规操作和一些擦边球的变现，并没有形成产业，也没有可以对我们有什么启示的地方，所以在此也不详细分析。

如果仅仅从新闻媒体类导出的流量变现来看，主要集中在下面几个类型：

监控新闻媒体类流量流入地下产业链变现行业分类示意图
(2015年10月份数据)



Data Powered By **TOMs**
Insight

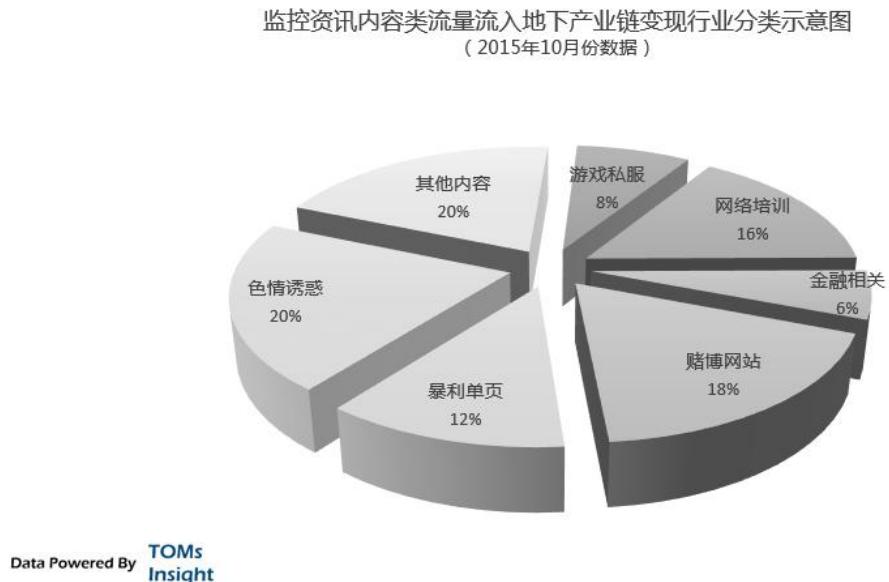
C. 资讯内容类地下引流数据分析

资讯内容类流量几乎是所谓的网络推广最基本也是最常见的手法，一般是通过软件或者人肉的方式，在各大论坛、博客、百科系统、问答系统等等所有的资讯内容类社区或应用中，贴发广告的信息，引入流量到地下产业链中变现。

资讯内容类流量五花八门。特别是一些权重很高占据一定流量入口的网络社区应用，更是充斥着各种广告引流的方式。比如：大家都可能熟悉的天涯论坛的大量水军；百度百科的一些收费创建和更改；百度知道自问自答的推广营销；各种论坛和博客系统的灌水机等等。

由于咨询内容类推广引流已经存在相当长时间，而对于用户来说也渐渐免疫，所以目前效果一般。只是由于此类信息太多所以才在整体流量中占据一定的位置。

如果仅仅从咨询内容类导出的流量变现来看，主要集中在下面几个类型：



D. 垃圾信息类地下引流数据分析

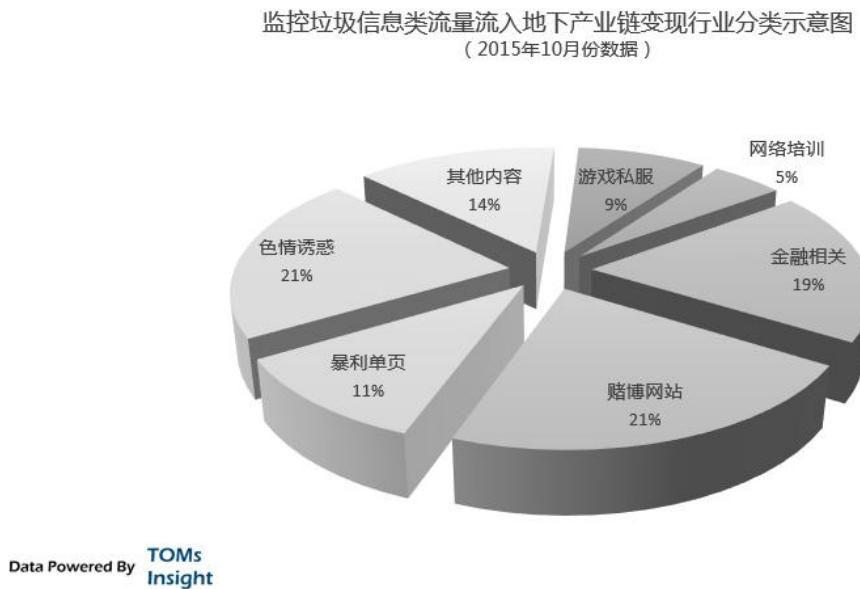
有些并非新闻，也并非资讯，但是在一些组织的炒作下，一定时间内会变得非常火爆的信息。这些信息都是一些垃圾信息，有着极强的时效性和爆炸性，比如大家熟悉的网络红人，或者忽然间就爆发的 xx 门事件。

这些背后都是提前的内容布局，炒作，然后等待信息爆炸后，大量用户流量开始涌入提前布局好的吸流陷阱：即大家可能都会有经验，一旦什么网络红人和 xx 门火起来的时候，搜索相关的信息总是弹出来各种乱七八糟的网站和广告，没错，这就是一次标准的引流过程。

垃圾信息类流量几乎全部都流入地下产业链变现，但是由于爆发性强，时效性短，没有沉淀效应，流量总是被高利润的变现组织吸收。

另外垃圾信息还会用作网络暴利品牌的炒作，我们会在本报告第三部分第 2 章第 4 节分析。

如果仅仅从垃圾信息类导出的流量变现来看，主要集中在下面几个类型：



E. 邮件其他类地下引流数据分析

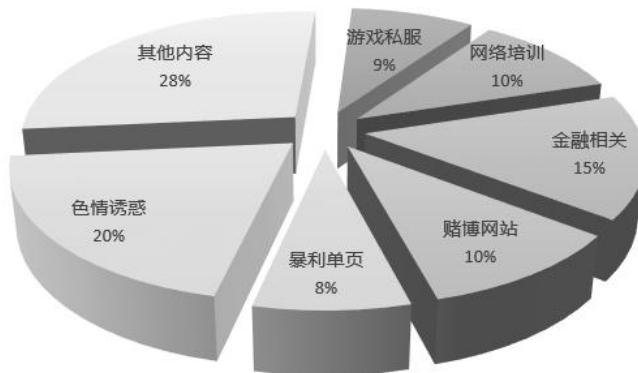
邮件引流即垃圾邮件群发。邮件营销本身是合法的，但是垃圾邮件就是不合法了。这其中区别很多程度上就是邮件广告的内容，是不是正规合理的。

从技术上讲，目前国内主流的邮箱服务商都是提供的企业白名单服务，意思是邮箱营销公司需要去申请白名单，进入白名单后会保证从这个域名来信的接受率。邮箱服务商会对白名单内的发信域名进行质量评估，评估的结果将直接决定以后的接受率，最核心的就是用户对营销邮件反馈，是不是点击、删除、或者点垃圾邮件。

邮箱服务商不断更改白名单策略，对于一些特定的营销（比如说最近的 p2p 金融、交友、app 下载等）进行了抵制，在这样的情况下正规的邮件营销公司如果继续做类似业务，会影响自己的白名单质量，所以选择放弃，而这部分就会变成垃圾邮件的市场。

所以对于垃圾邮件来说，获取的流量几乎都流入一些不合规的产业，或者被邮箱服务商所禁止营销的行业，从垃圾邮件导出的流量变现来看，主要集中在下面几个类型：

监控垃圾邮件类流量流入地下产业链变现行业分类示意图
(2015年10月份数据)



Data Powered By **TOMs**
Insight

安卓应用分发与移动流量产业链

6

A. 相关地下产业链整体深度分析

从 2009 年起，移动互联网开始在国内火热。新人琢磨着如何去打造一个颠覆性的创意无限的应用，而有经验的老手开始复制传统互联网的模式，占据流量入口。由于 IOS 的封闭性，流量分发渠道主要针对安卓系统手机。而这个时候谁也想不到，安卓流量分发渠道市场能发展到如今的规模：八仙过海各显神通，成为中国互联网产业中最有意思水最深的领域之一。

我们从用户需求角度出发，安卓的分发渠道大概可以分成：按需安装、手机预装、诱导安装，静默安装，这四种情况。而下面我们大概概括一下这几种分类方法下的分发手段。

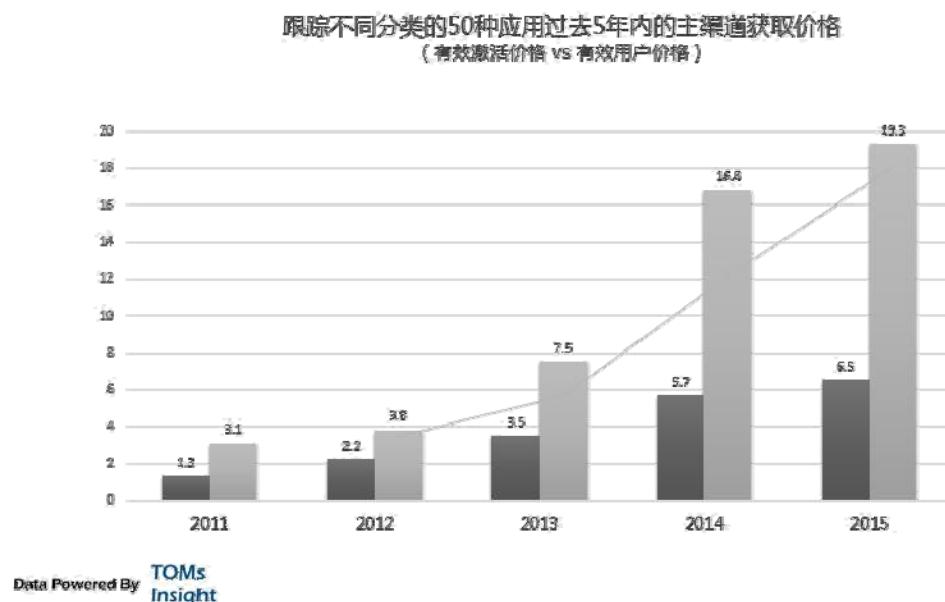
按需安装是安卓分发的最主要的渠道，也是最正常的方式：手机的使用者按照自己的需求选择 app 下载使用。由于安卓系统的开放性，程序的任何存放都可以激活分发，所以按需安装也演变成各种各样的细分。

目前来说，主要的按需安装分发渠道有：国内各大第三方市场、Google 官方市场、搜索引擎、手机管理工具推荐、巨头应用推荐、广告联盟、移动类广告（广告贴、插屏、消息、积分墙等），PC 类广告（广告平台，大流量 CPM、精准 CPC 等）、SNS 平台推广、内容营销推广、各种开发平台应用、新兴的 wifi 渠道、还有传统互联网分发手段等等。另外一个正在快速崛起的渠道是线下渠道，由于主要针对三四线城市或者外来务工人员集中区域，线下渠道针对特定的应用，也在快速的形成小产业链。

按需安装以用户的需求为出发点，也许很多渠道都会有一定的诱导成分（积分墙），但是也都没有到夸张或者离谱的地步。

作为安卓分发的主渠道，应用市场也是各大巨头的战场，而目前也逐渐进入到寡头垄断的局面，以 360、百度系、应用宝、小米几家为代表的寡头甚至占据了 6 成以上的应用市场分发流量。主渠道的特点非常鲜明，流量集中，虽然一些长尾流量也转移到搜索引擎中，但是供给跟不上 app 的需求，也推升了流量价格越来越高。

我们跟踪不同分类的 50 种应用在安卓主渠道的有效激活价格和有效用户获取价格，在过去五年内的变化如下图：



B. 预装渠道地下产业链深度分析

手机预装就是在用户购买手机之前的预装渠道。预装有相对正规的渠道，比如和手机制造厂商合作，或者和定制运营商合作。不过更多是存在刷机利益链中。

不仅仅是水货，由于利益驱使，行货的手机也会被再次安装应用。在销售渠道的各个环节：仓储过程，手机运输过程中，甚至在各个手机卖场都会被安装新的应用。各个节点都会被充分利用，抢占这一入口。这也是一个博弈的过程，之前被安装上的应用会被下一个环节恶意刷掉。

C. 诱惑渠道地下产业链深度分析

诱导安装是利用一些技术或者宣传手段，让用户对应用的质量和内容产生不合理的预期，而诱导下载使用。例如刷榜，是让用户感觉应用质量很好能排名前几；例如美女类诱导，让用户对内容充满幻想。诱导安装是一个非常灰色的地帶，不能说完全不合规，但是也充斥着黑市手段。

最早曝光的是刷榜，刷榜在行业内是常态，但是在 2010 年被媒体曝光后变得出了名：当时著

名的曝光点是一家应用的作弊器忘记关，结果刷的流量超过了雅虎。刷榜就是用自己下载应用商店里自己应用的方式，获得排名，从而获得真正的用户。这个和当年 SP 的自消费业务类似，后来的刷评论也是一样的道理。

接下来是山寨应用，即盗版，由于安卓应用使用 Java 开发，不是原生机器码所以非常容易反编译。流水线一样，批量盗版上千个应用，加入广告，积少成多，赚取流量，出售流量，形成了一股不小的分发渠道。

换壳美女应用也很常见，大家可能会在各大应用市场上看到各种大同小异的美女图片应用，由于人性所致，美女图片类应用被下载次数较多。于是渠道开发一个应用，提交上线后，把自家应用换个皮，改名，再提交一次，不停的换皮，改名，于是，每一次短暂的曝光机会都能带来一些流量，成千上万聚集，也会有收获。

另外还有一些成人论坛，或者是传统网站的一些大流量站群、垃圾站站群、SEO 站群等等所有的细微流量聚集的地方，用极其诱惑的广告语或广告图片，让用户产生预期，从手机流量导入形成分发渠道。甚至是利用信封号进行强制 QQ 空间传播和欺骗好友。

诱导安装在目前的安卓分发渠道中占据了非常大的一环，虽看起来并不如前两种规模，但由于比较低调隐秘，没有聚集，再加上分发的应用数没有相对应的数据宣传，不过总量不可小觑。

D. 静默渠道地下产业链深度分析

静默安装就是指软件在安装时无需用户的干预，直接会按默认设置进行安装。

对已经 root 过的安卓手机来说，应用是可以获得静默安装的权限的。如果你不幸下载了有静默功能的应用后，在你半夜睡觉的时候，你的手机突然下载了很多应用，然后自动打开，自动联网，甚至还可以然后自动卸载，一点痕迹都没有。

或者水平更高一些的，把一些 app 做成木马病毒，不仅仅可以自动静默安装下载 app，还可以有自动去传播，获得更多的被控制的手机。比如之前被曝光的一些手电筒应用。

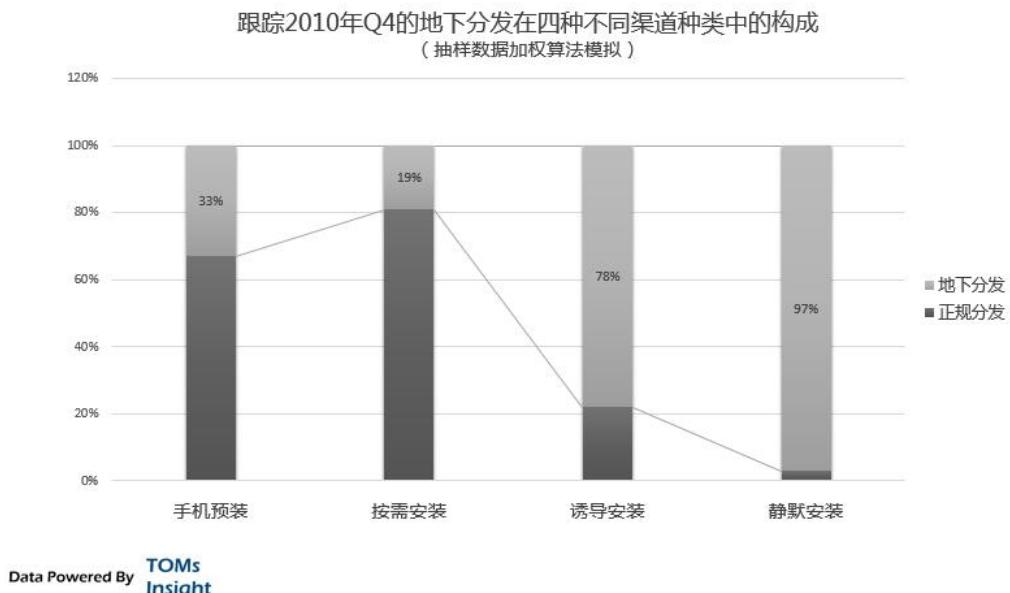
被静默程序控制的手机一般在黑市上称为：野鸡。而被木马程序完全控制的，被称为：肉鸡。

不管是野鸡还是肉鸡，最早，大家都是靠着 SP 暗扣赚钱的（通过控制短信或者流量接口，在用户不知情的情况下发送短信或者访问网站，和 SP 分成），但是慢慢的通过 SP 赚钱的越来越少了。这是怎么回事呢？难道野鸡和肉鸡越来越少？不对。肉鸡越来越多，甚至在国内已经形成了几个非常大的僵尸网络（一群被控制的肉鸡组成的网络），但是都不做暗扣了，因为大家找到了更好的商业模式。

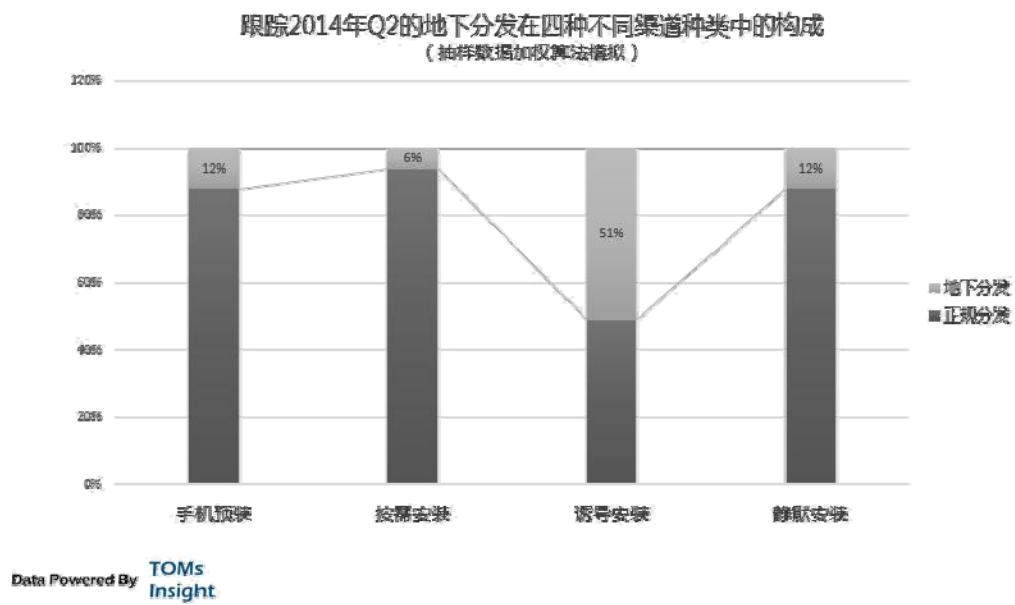
安卓应用的开放性决定 app 有两种类型，一种是直接变现，一种是再分发。第一种大家很容易理解了，比如在手机上装一个游戏，玩游戏买道具直接变现。还有另外一种，比如你安装了一个应用，通过这个应用你还能获取更多的应用（例如应用市场），这就属于再分发。

再分发应用相当于是渠道布局。非法应用也有两类，针对直接变现的“暗扣黄赌”应用，和针对再分发的木马病毒类应用，后者也是静默渠道的形成过程。所以分发“暗扣黄赌”和“木马病毒”类应用的渠道，就是地下产业链中的分发渠道，我们简称地下分发。

我们可以从下面图中看到 2010 年 Q4 的地下分发渠道在刚才说的四种渠道中的构成。



几乎全部的静默安装渠道和一部分诱导安装都可以算是地下分发渠道，由于 2010 年 Q4 时监管问题，手机预装和按需安装也会有一部分。



但是再对比一下 2014 年 Q2 的构成，忽然发现，主力军静默安全渠道，忽然间都不分发非法应用了！那他们都在干什么呢？

E. 其他非法渠道产业链深度分析

从 2012 年开始，由于资本开始追捧移动互联网行业，再加上移动应用分发渠道的集中，供给跟不上 app 的需求，让移动分发成本飞速增加。

到了 2012 年中旬，国内主流的安卓 CPA 激活渠道价格已经到了 2-3 元每个。而这个时候，静默渠道开始放弃了暴利的“暗扣黄赌”进入到分发渠道。由于静默渠道有其独到的优势（可以控制手机下载、打开、甚至使用）所以激活率非常高。

在 2012 年的时候，“暗扣黄赌”类应用里面最赚钱的暗扣，平均每一个“肉鸡”月 aurp 值大概是在 30 元左右，除去下游的 SP 分成和环节成本，他们可以做到 10 元每月每个“肉鸡”。但是如果做静默激活，非常轻松可以一个月超过 50 元每个“肉鸡”。比“暗扣黄赌”还高 5 倍的收入，谁还做非法生意呢？

应用 app 公司慢慢发现大量的用户虽然激活，但是使用率变现率都为零或者很低，从各个渠道过来的用户大多无效，所以导致了有效用户的成本越来越高。

而到了 2013 年，移动互联网竞争愈发火热，再加上 91 被百度的高估值收购，资本市场的再次追捧，有效用户成本的获取价格再次增加。而这个时候，手里面掌握大量“肉鸡”组成的僵尸网络的地下产业，开始进入一个新的领域，给 app 应用做数据。这是什么意思呢？

控制僵尸网络，不仅仅用静默的方式安装一个 app 应用，接下来还控制着这台手机，打开应用、使用、关闭、再使用、甚至消费消费。完全模拟一个真实的用户的行为。这一切都在这个手机的主人完全不知情的情况下（一般都是半夜）发生，而到了早晨，自动卸载掉 app，不留痕迹，晚上继续下载，继续模拟。

对于 app 应用制作商来说，后台数据非常漂亮，用户看上去非常真实，甚至还有一定的消费数据。于是这样的渠道越来越受业内欢迎，当然这样的“真实”用户的成本也越来越高，在一些细分甚至达到几十块每个。

而大多数 app 应用公司的老板，都不知道自己的数据是假的。还都以为自己的产品确实很好，投资他们的风投，还以为自己很有眼光，接手的 B 轮，C 轮，继续炒作，还以为自己捡到了宝贝。其实，风投和海龟创业者的的钱，一大半都被流入了地下产业链。而“野鸡做激活，肉鸡做数据”已经成为这个地下分发渠道的核心秘密。

从最新的趋势看，有一些极其有前瞻性的僵尸网络商，连做数据这些的业务都不做了，他们沉浮下来，专心去分析用户行为，对 app 应用市场进行分析。还有一些僵尸网络商，不做数据，专心去盗取用户的手机支付等工具用户名密码，这是一些小众和完全违法的地下产业链。

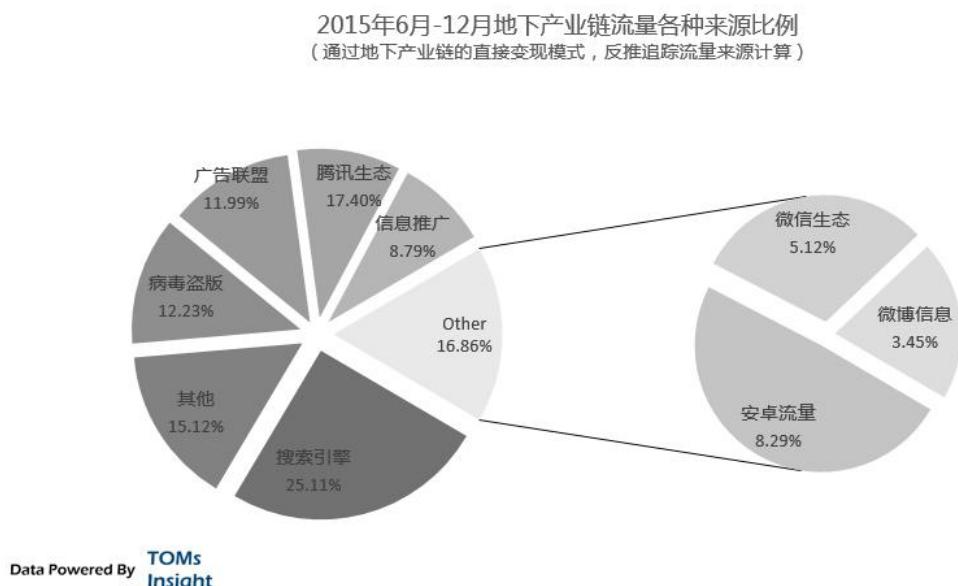
微博等社交应用流量与相关分析

7

A. 相关地下产业链整体深度分析

微博等社交应用从 2010 年开始产生发展，到现在大概有 4 年的时间，接着借助移动互联网的发展红利。同时借力发展起来的还有一系列的移动端应用：陌陌，YY，甚至包括因为移动端红利再次发展的知乎之类的社交应用。

这些应用和之前我们分析微信有几乎类似的趋势，在 2013 年之前几乎能引起地下产业链的火并，但是 2013 年开始，却慢慢的凋零，以至于无人问津到形不成产业链。和微信的安全策略导致的不完全相同，微博等社交应用不仅仅是由于安全策略，更多的是由于本身的产品生态导致的。



虽然在地下产业链中影响甚微，我们还是来分析微博等社交应用

B. 微博粉丝地下引流的深度分析

微博在国内主要是新浪微博和腾讯微博，腾讯微博可以算是腾讯生态系统的一部分，如之前分

析，本身的往黑市引流的并不多，但是由于信封号的放大效应，却产生了不少的流量。

而新浪微博，又是另外一种情况了。在 2013 年之前，新浪微博催生了一个很奇怪的地下产业链：刷粉。这在地下产业链的历史上是非常奇怪的一笔，因为在此之前的地下数据造假产业，比如说刷 IP，刷 PV，刷 alaxa 排名等，都没有那么广阔的用户基础，那么暴利的变现模式。以至于很多刷流量的地下从业人员都开始转行做新浪微博刷粉了。

但是刷粉仅仅是一种地下产业链中的偏门。大家还是希望从新浪微博中引流量变现，但是却让大家失望的是，由于产品生态中的强二八法则，导致流量都集中一些少数的大 V 手里面，而且就算是这些大 V，流量效应也很不明显。

所以新浪微博慢慢转型成了大 V 发软文发广告，而群众只围观的局面。而地下产业链希望得到的流量，却成水中捞月。我们通过对地下流量的监控，发现腾讯微博和新浪微博的比大概是 9:1，而腾讯微博主要是由于信封号的影响，就算是此影响的放大效应，也几乎秒杀掉了新浪微博本身。

C. 社交私信地下引流的深度分析

在 2013 年之前，新浪微博私信营销也火过一阵，在地下产业链中造成了一系列营销。但是随着产品安全策略的升级，和产品定位的发展，私信对流量的效果变得微乎其微了。

因为新浪毕竟不是微信，其社交属性和消息重要程度并没有那么不可取代。而且由于发展策略定位，用户更多的是当成一个媒体而不是一个社交软件。

这些也导致了其账号价值并不大，所以盗号产业也几乎没有染指到新浪微博。我们不知道这算是一个好消息还是坏消息，好是其用户的安全性有了一定的保障，坏是如果一个产品账号如果在地下产业链看起来没有多大的价值，那么其价值体现确实并不直接。

D. 其他社交类产品流量深度分析

当然，还有一系列其他的移动端的社交应用：陌陌、YY、知乎等等，每一个软件都有其特

点，但是也都一样没有在地下形成产业链。其原因一方面和微信、新浪微博一样，另一方面在于其信息孤岛性。

由于 app 和传统网站不同，传统网站的信息可以被搜索引擎的蜘蛛抓取，可以又各种的超链接，有内容的沉淀性和传播的递增性。

而 app 中的内容，很大程度上都在一个信息孤岛中存在，如果这个 app 对用户来言没有那么必须，其价值也有大打折扣。所以这些社交应用看起来很火，不过目前的引流仅仅是小打小闹，并不能形成规模。而通过这些应用获取流量的地下从业人员，也一般都是自采自用，自己找流量自己变现，并不是产业链中的一环。

E. 相关黑市交易与推广深度分析

目前这些社交应用在黑市上，大多数都是一些周边交易，即有一些模式会用到大量的账号，或者大量的粉丝，或者特殊的认证，再或者一些虚假的数据。

而对地下产业流量的影响，大概 86% 的比例都是信封号放大多效下的腾讯微博。

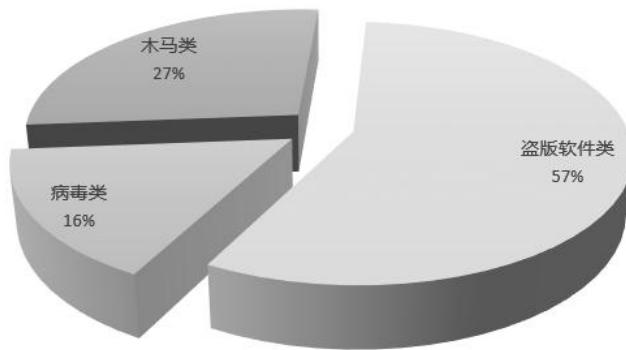
病毒木马与盗版软件流量产业链

8

A. 相关地下产业链整体深度分析

可能很多用户都有这样的经历，就是不管打开什么网站，甚至根本就没有打开浏览器，都会跳出来一堆的弹窗广告。那么，这个用户要么是中的病毒木马，或者是使用了盗版软件。不管是病毒、木马、盗版软件，在流量获取方向上都有一个特点，可以主动的去推送广告，而获取流量。

2015年6月-12月，病毒木马与盗版软件类地下产业链流量各种来源比例
(通过地下产业链的变现模式，反推追踪流量来源计算)



Data Powered By **TOMs**
Insight

由于国内的计算机用户的盗版使用量，和病毒木马的感染率，使得这一类的流量份额在地下产业链中占据了不小的比重。但是由于会导致用户反感，加上在数据统计上的不透明，导致了这些流量的价格却不高。

我们接下来分开来看，并且分析目前移动端的病毒木马和盗版应用的现状。

B. 病毒木马流量产业链深度分析

计算机病毒（Computer Virus）是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能自我复制的一组计算机指令或者程序代码。计算机病毒具有传播

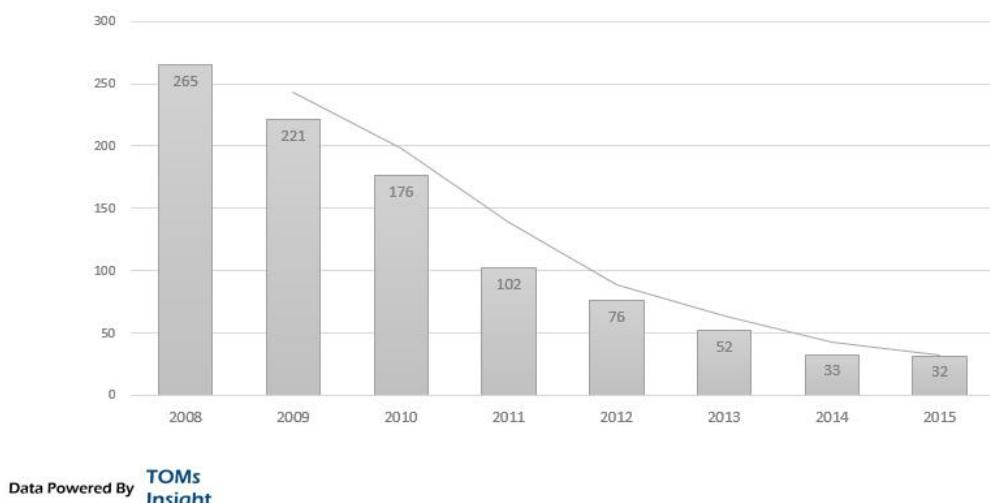
性、隐蔽性、感染性、潜伏性、可激发性、破坏性。

木马 (Trojan) 这个名字来源于古希腊传说，是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种主机的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。

最早的时候，病毒和木马都几乎是黑客在炫耀的手段，后来开始进行一系列的非法使用，比如典型的病毒用来盗取账号，而木马用来自做肉鸡进行 DDOS。

后来黑客们发现不管是盗号还是用做肉鸡，都有时效性太长的特点，换句话说，变现不直接，而且由于杀毒软件的免费化，导致了手中肉鸡存活时间越来越短。我们从下图看出肉鸡平均存活时间的统计：

2008年至今，国内肉鸡的存活时间统计（黑市抽样数据，仅供参考）



从 2008 年的 265 天到 2015 年的 32 天，几乎缩短到了之前 1/8。所以 1 个月的存活期，几乎还接不到 DDOS 的订单呢，那怎么办呢？很简单，直接弹出广告，引流量到其他地下产业链中变现。但是这种变现方式也更暴露了这台肉鸡，让用户更快的发现问题，修补的时间更快。所以这对此地下产业来说是一个恶性循环，而反过来讲也是整体行业的安全性提高的表现。

C. 盗版软件流量产业链深度分析

盗版软件是一个极其古老的地下产业链，几乎和计算机在国内的发展同步进行。最早的盗版叫“脱壳”，而这一门古老的手艺也越来越没人掌握了，相反取而代之的是再包装。

把已经盗版的软件，再次打包，在安装过程中加入自己的部分，让用户在安装完成后可以展现出相应的广告，完成流量的获取和再分发的过程。是目前大多数的盗版软件的模式。

我们从下图可以看出目前盗版软件平均广告平台植入的个数：



不得不说，哪怕是地下产业链，也被浮躁的整体行业气氛影响，0day 组织的“脱壳”记忆和 64k 程序比拼已经不见了，换来的是当年黑客们都很不屑的再打包加广告的商业模式。

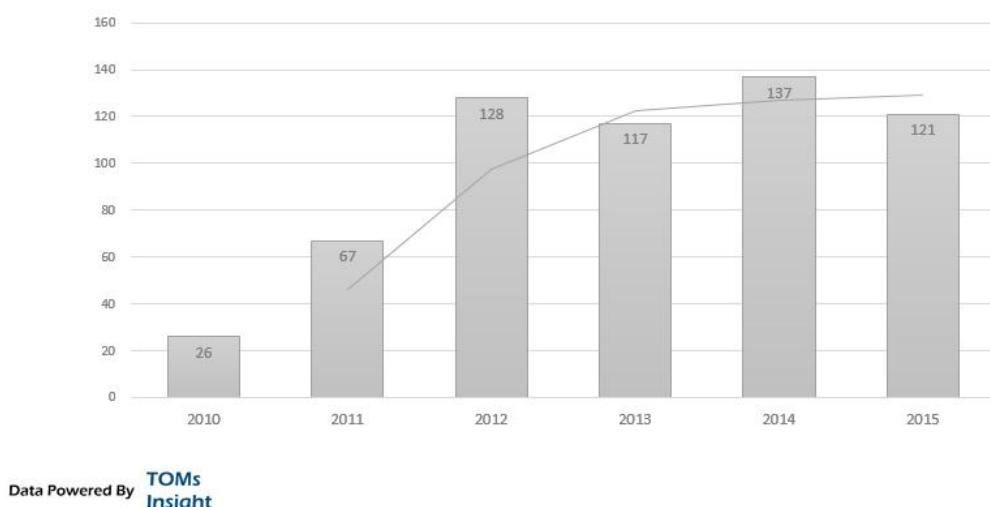
D. 移动端病毒木马数据分析洞察

移动端的病毒木马主要是指带静默功能的安卓 app，此部分我们已经在第 6 章详细分析，在

此不再赘述。但是之所以在此还要再提的原因是，安卓肉鸡的存活时间，和 PC 肉鸡恰恰相反，时间越来越长。

这一方面和地下产业的长期布局有关系，另一方面也和安卓静默安装的再分发感染有关系。

2010年至今，国内安卓肉鸡的存活时间统计（黑市抽样数据，仅供参考）



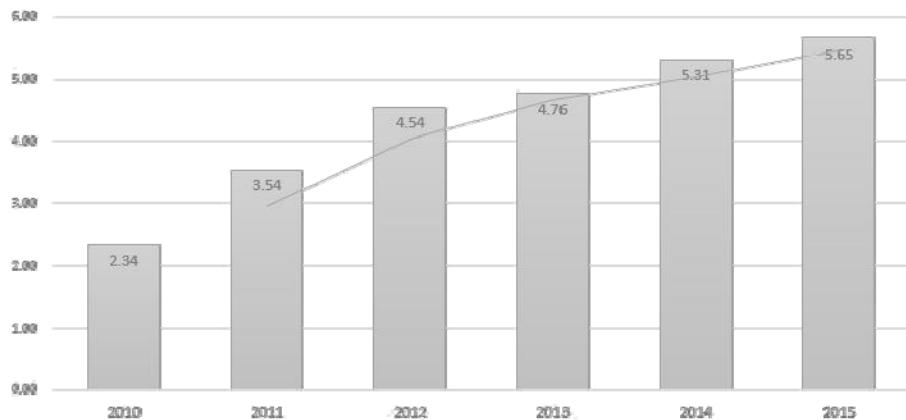
E. 移动应用盗版流量产业链分析

移动端的盗版软件由于安卓使用的 Java 反编译更加容易，所以导致了再打包的技术门槛更低，所以盗版的成本也更低。而且由于和 pc 软件的不同，安卓 app 非常容易程序内再次分发，甚至静默，所以盗版 app 有着更好的传播效应。

特别是盗版 app 本身就可以通过静默作为管道建立渠道，使得盗版 app 传播的渠道成本进一步降低，而流量获取的成本也进一步缩减，就好比是网状连接，虽然没有 pc 流量的搜索引擎作为管道，但是自建管道。

我们同样追踪安卓 app 的盗版软件植入的广告平台，比 PC 端有着更夸张的情况：

2010年至今，安卓盗版app平均植入广告程序个数（抽样7867个盗版app采样）



Data Powered By **TOMs**
Insight

移动流量数据与移动化趋势分析

9

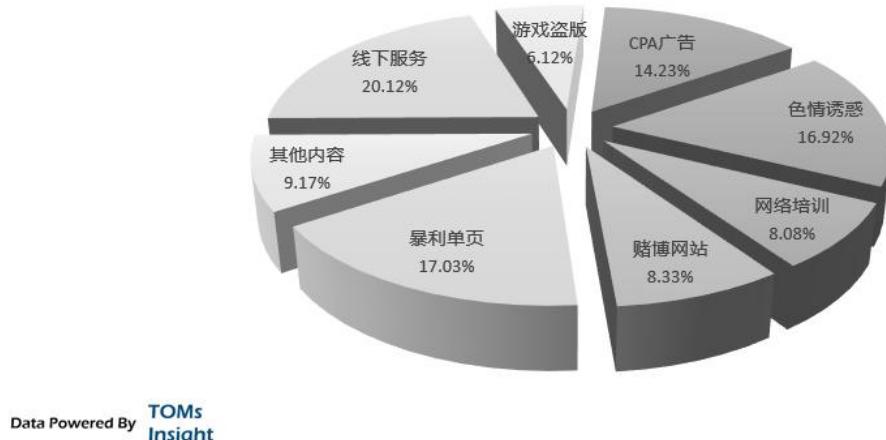
A. 相关地下产业链整体深度分析

之前我们已经分析了不少移动流量的问题，但是由于整体互联网行业移动端发展的趋势，我们还是单独拿出来一章节再分析。在此，我们不再专注在安卓市场，也不仅仅看 app 渠道的地下产业链变化，而是广义的移动流量。

广义上说，任何从手机上上网而贡献给应用的流量，都叫移动流量。移动流量和 PC 流量相比，由于屏幕的限制，明显有内容展现少，但是停留时间长的特点。

对于追逐现金利益的地下产业链来说，在 2014 年之前，除了 CPA 变现之外，几乎没有什么更好的变现手法了。但是从 2014 年之后特别是 2015 年，甚至作为先行者，地下产业链反而开辟了一些移动流量变现的好思路和手法：

监控移动流量流入地下产业链变现行业分类示意图
(2015年10月份数据)



一方面，由于暴利单页产业找到了合适的移动端流量投放，另一方面，由于移动端的 O2O 属性更强，可以获取的用户的地理位置，导致民营医院和本地服务的变现竟然到了 27% 的流量份额。

B. 移动流量获取分发的发展趋势

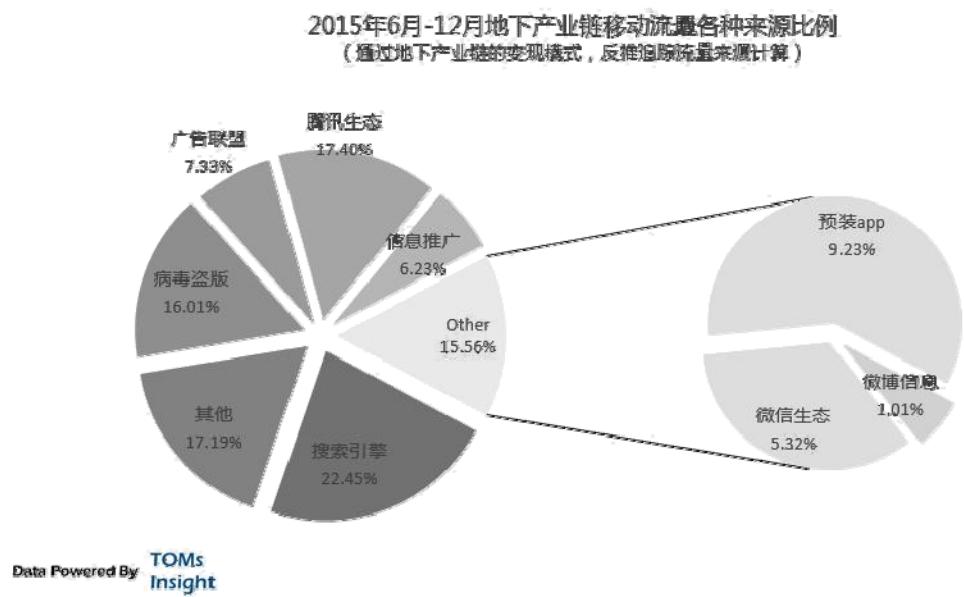
从流量获取分发上来看，移动流量有明显的规模化和聚合化的趋势。之前在很多产业链中被浪费的流量都开始逐步聚合。比如黑帽 SEO 产业中的流量都开始分开出售，更精细的分解和更专业化的变现，也是流量的变现得到更充分。

下图是仅仅百度 CPC 地下产业链中的 pc 流量与移动流量的价格对比：



C. 移动流量获取分发的来源分析

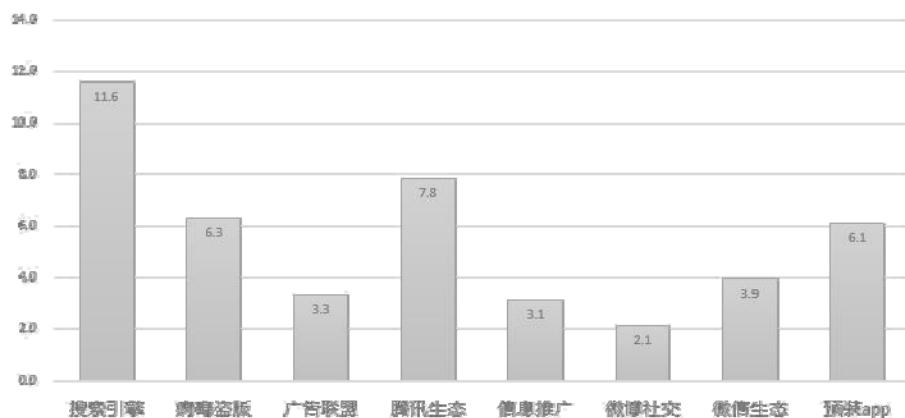
从移动流量获取来源分析，搜索引擎仍然占据了重要入口，特别是在搜索引擎生态中的移动流量更容易分离（根据设备不同分流，用户用 pc 和手机打开的是不同的网站），让来源规模直接得到大幅度提升。而由于病毒盗版的在技术上更容易更猖獗，再加上自带渠道（静默 app 的复制传播性），也让病毒盗版成为重要的移动流量黑市来源。



D. 移动流量获取分发的交易分析

从流量黑市交易来看，搜索引擎生态占据着绝对第一位置。而其他由于手机 QQ 用户量的原因，信封号相关产业链带来的移动流量价格也不低。相对的，传统的信息推广在移动流量获取上，却卖不出去价格。这也和手机端打开文本再跳转的不方便有关。

2015年，地下产业链不同类型移动流量购买CPM价格
(抽样统计及算法预估，一些CPA通过算法估算成CPM)

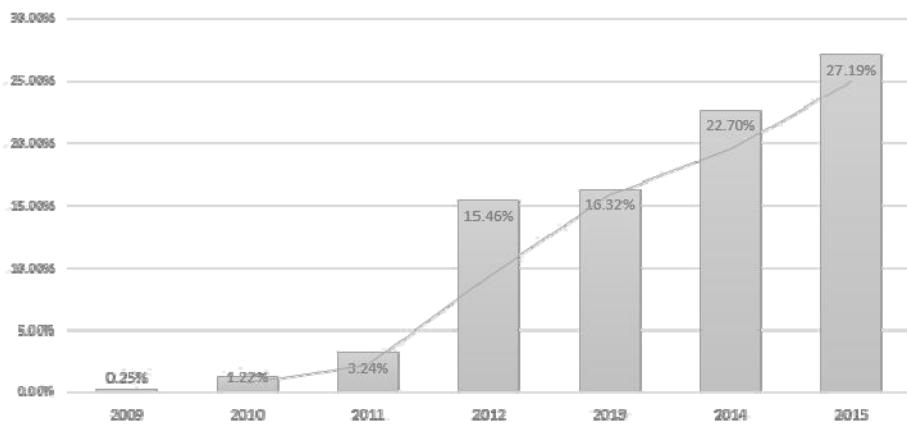


Data Powered By **TOMs**
Insight

E. 移动流量获取分发的深度数据

最后，在地下产业链中的移动流量获取分发的整体比重，也从 2010 年的 0.25%，提高到了目前的 27.2%，虽然和整体应该占据的份额比还相对较小，但是增幅已经大大超出正常水准。

2009年至今，地下产业链流量分发中移动流量占比
(通过地下产业链的变现模式，反推实际流量来源计算)



Data Powered By **TOMs**
Insight

总结与洞察启示

在目前的互联网行业创新，如何获取流量并没有被摆在应有的位置，大多数创新者更多的是专注在产品本身如何打动用户，而打动了用户就会得到访问量和流量也会是很多行业新手觉得理所当然的事情；或者，大家觉得如何推广是很低级的事情；再或者觉得先拿投资，有了投资自然而然的就有了推广能力，从而获取流量也是自然而然的事情。

但是客观却没有那么乐观，互联网创新是很简单的，几乎每个互联网用户都可以有自己的伟大想法和创意，但是门槛却在于如何推广出去并获取流量。这不是一个低级的事情，只能说是由于门槛和复杂程度致使成很多创新者不愿意面对的事情，或者说是不断逃避的事情。逃避是没有任何成功的可能的，所以这也是那么多创新在行业老鸟眼中看起来可笑的原因。

通过地下产业链的流量获取分发分析，能给我们带来很好的借鉴意义。并不是说我们去学习一些非法的手段，而是其对流量获取分发生态系统的理解，通过商业模式达到共赢的手段，和对用户需求准确的把握程度，这些有时候却是主流互联网圈创新者最忽略的。而流量即是第一资源的理念，更是主流互联网圈子创新者应该刻入自己的战术本中的。

另外，大量的流量分支被地下产业链所控制，获得很大的影响力。这不得不说是互联网很有特色的情况，和大多数创新者不得不面对的局面。在很多时候，当脆弱的成长期创新者在和野蛮的地下产业链争抢流量时，几乎会全军覆没。这是所有创新者都需要注意的风险，而这在很大程度上，也是互联网创新圈子都在强调要接地气的原因之一。

三、 流量变现盈利相关产业链部分

对于概念投资型创新来说，盈利模式会停留在概念上很久，甚至一直到上市也没有盈利。而对于地下产业链，高额的流量价格和快速的变化以及风险，都决定了快速变现才是最终的目的和产业链终端。

不管流量如何分发，变现盈利都会是最终的终端出口。而地下产业链中的变现盈利的模式变现、创新、变革，也都会带来上游流量市场的再次洗牌。就如主流互联网创新的资本推动力一样，对于地下产业链来说，变现盈利才是决定整体走向的关键点和聚焦点。



流量变现盈利相关产业链部分整体分析



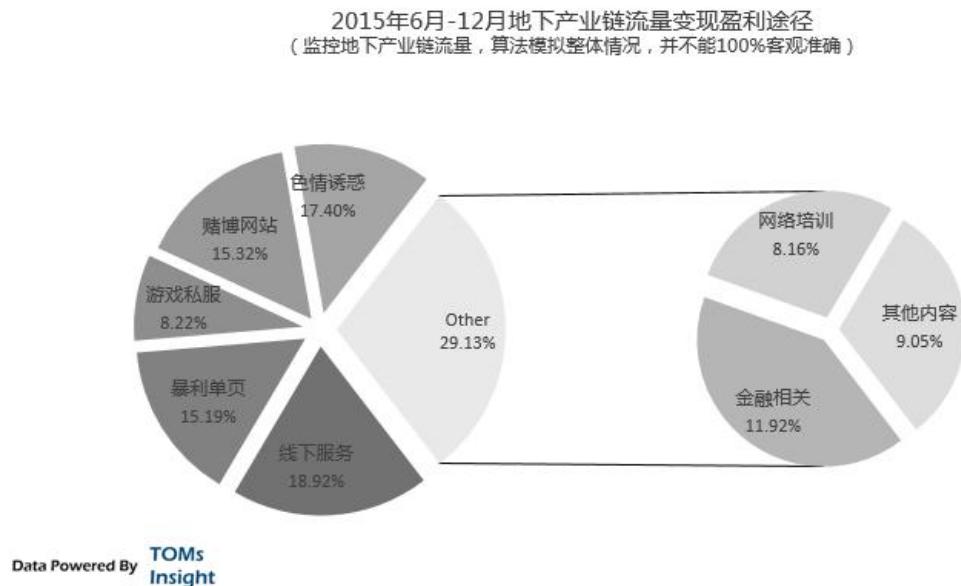
A. 流量变现盈利产业链整体情况

互联网行业最终变现盈利在国内主要是广告、游戏和电商。其实广告只是流量再分发的过程，并不能算是最终的终端出口，所以也就只剩下电商和游戏了。看似热闹非凡，创新不断的互联网行业，最终的盈利模型和传统行业比反而异常的简单。

互联网地下产业链其实也是如此，把流量变现需要很强的盈利能力，而一般主流的变现很难支撑的起流量采购成本，特别是地下产业链的流量时效性强、风险大、而且充满了骗术，如果没有变现能力的支撑，很难在地下生存。

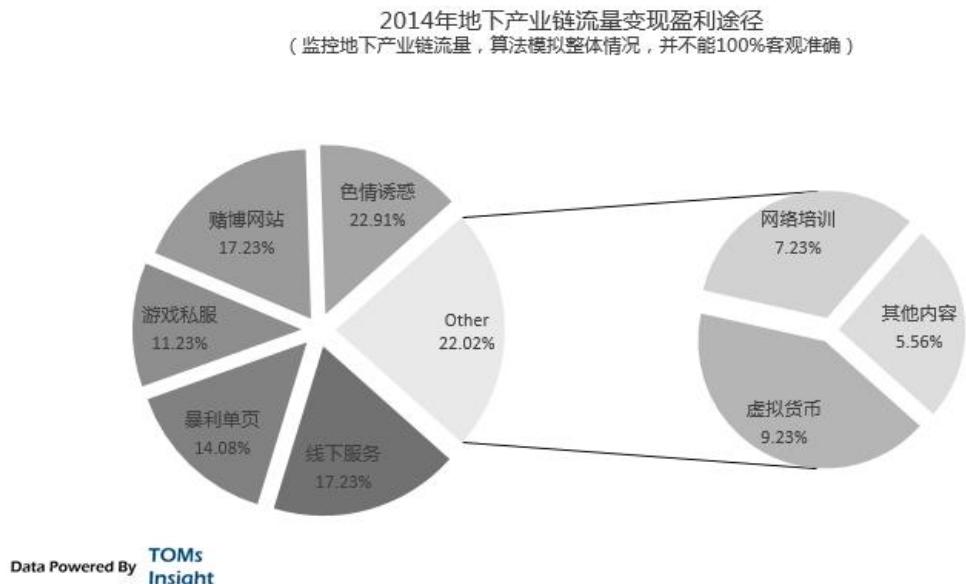
所以地下产业链拥有很特殊的变现环境，但是如果抽象到极简，其实就是：黄、赌、骗。

我们通过监控流量在地下产业链的变现，如下图：



我们可以看出，电商占据了超过 30%的份额（暴利单页+线下服务），线下服务主要是民营医院、美容机构、职业培训等。而黄和赌大概也占据了 30%的份额。和电商一样同属骗模式的还有虚拟货币，网络培训，游戏私服等。

值得一提的是，以上数据是 2015 年 6 月份-12 月份的情况，如果我们把数据回溯到整个 2014 年，发现有另外的数据表现：



虚拟货币产业链从 2013 年的大概只有 1.21% 发展到了 2014 年的 9.23%，又逐步变成 2015 年的牵扯互联网金融的各类变现手段。但如果仅仅看虚拟币相关的变现比重，占总体的比例不到 1%。这是由于 2014 年的比特币和相关山寨币的骗局火热。

由此我们也可以看出，地下变现盈利产业链有非常强的时效性，相关产业观察着最新的热点，不断更新骗术，也嗅探着风险，躲避着相关的打击。

在这种快速的变化中、和竞争下，要求相关变现盈利产业链不断的优化变现率，提高变现水平，而能更加精准的满足用户的需求痛点，同时也在运营的过程中寻找最优的模式。这些虽然都建立在非法的基础上，但是也在一定程度上可以供我们学习参考。这也是在一定程度上此报告本部分的目的所在。

B. 细分产业链之间生态关系分析

我们可以把目前的地下变现盈利产业链分成：淘宝天猫生态、货到付款类电商、移动端微店类型电商、游戏地下产业链、博彩类、网络色情与诱惑、网络培训产业链、虚拟货币产业链。

特别说明的是，这个产业链分类和我们之前的数据并不对应，主要原因是我们把电商类按照生态特定分成三部分分析：淘宝天猫生态下的产业链主要是以刷单为主，但是由于在地下产业链占据非常重要一环，我们还是单独分析；独立电商一般需要从百度、或者其他地下产业链引流，以暴利单页为主；而移动类型的电商最近迅猛发展。

对于线下服务为主的民营医疗、美容机构、职业培训等等变现方式，网络更多的是提供用户的方式，而由于产业链集中在线下部分，我们在本报告中不做更多的分析。

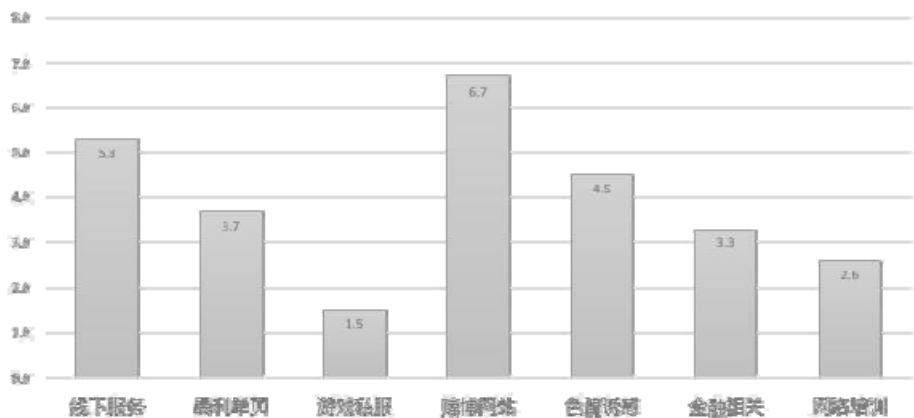
变现盈利产业链之间关联并不大，由于变现盈利产业需要长时间优化和尝试，所以地下从业人员需要一定时间的积累，而整体行业的时效性总是在相近的细分行业内变换，导致了更多是从用户需求入手去促进行业发展，而不是从手段本身。这一点和流量获取分发有很大的不同，也正是因为如此，在变现盈利环节，会更少的依附于某一产品生态，而体现出非常强的独立性。

在这某一定程度上也是整体的地下产业链的特点：流量依托于互联网巨头的产品生态，而变现相对独立。一方面在吸取生态系统的养分，另一方面如针尖一样精准的扎向用户的心理诉求痛点。这对我们来说，不管是产品生态系统的运营，还是独立产品的设计，更多的还有对用户的把握，都有很强的启示作用。

C. 流量变现盈利的黑市深度数据

地下产业链的变现盈利，到底能在一个什么暴利的水平上呢？我们可以看下面的分析。每一个进入 IP 用户即 CPC 的每一次点击，或者 CPM 的每一次点击，进入变现盈利的网站或者应用后的独立 IP，而产生的变现价值可以见下图。赌博类网站（包括黑彩）以超过 6 元的水平独占鳌头，而线下服务排名第二，色情诱惑类超过暴利单页，排在第三。

2015年6月-12月，地下产业链不同类型变现盈利平均到每个进入IP用户
(通过对你网站组件佣金数据，经过算法评估得出)



Data Powered By **TOMs**
Insight

淘宝天猫与相关生态变现产业链

1

A. 相关地下产业链整体深度分析

整个阿里巴巴生态下有超过 800w 的活跃卖家，一次双 11 就几百亿的销售额。而这仅仅是浮出水面的部分，而阿里巴巴的商业模式比百度腾讯都更依赖于生态增值，这也同样也决定了这个生态中有很多地下寄生物。

不过由于淘宝天猫本身的规则（支付宝交易），决定了这些寄生产业都形不成暴利，也很少地下流量在此生态中变现。最多也只是刷刷信用，卖卖假货，这些玩法在地下产业链中属于相对独立的一角，被黑产大佬所不屑，也总是被黑市所唾弃。

但是不可否认，由于整个生态系统的巨大，相关的刷单、刷单周边的骗术和敲诈勒索、淘宝客以及更多的假货的线下生产产业，还是给用户造成了巨大的影响。

由于和地下产业链的核心价值不符，我们并不用过多的篇幅，接下来我们分析下淘宝天猫相关生态下的一些地下产业链。

B. 淘宝天猫刷单产业链深度分析

淘宝卖家呈现强二八法则，由于数据的公开，大家都可以去查阅抓取相关的数据。大多数卖家的级别都很低的，而为了获得更好的淘宝官方流量和信用，大家开始刷单。

刷单经过了几年的发展，已经形成了一个组织网络：分工明确，而纪律严明，有上下线，介绍人，关于刷单的任务，也有详细的细分。而目前刷单组织大多通过 QQ 和 YY 进行联系。

一个新加入者进入刷单组织之后，依次由介绍人、接待、培训聊天；介绍人把你介绍进来，得佣金；接待给你介绍大致的工作模式，培训负责具体的操作教学、考核，经过培训考核后就可以上岗了。主要包括以下几种任务。

浏览单：不需要拍宝贝，好评什么的。只需要浏览别人的网站几分钟或者为网店增加流量、人气，收藏下店铺之类的。这类是人肉适应淘宝的一些展示算法，提高报告度和获取流量。

红包单：由卖家把钱作成红包的形式，给刷信誉者卡号及验证码，刷信誉者领取之后用红包去

购买卖家指定的商品，没有任何的风险，确认收货给好评后获得佣金。

立返单：自己垫付宝贝金额，付款成功以后组织者立返垫付金额，确认收货给好评后佣金马上转到你的支付宝帐号。立返单比其他的更有风险，佣金更高。一般都是 1-10 元根据物品金额。为了提高关键字排名，让刷单者从“碧螺春”之类的关键词搜索，然后直接找他们店。

也可以在组织里面做管理工作：贴广告，拉人入伙；负责接待；负责培训新人；负责给大家分配任务（任务主持人）；拉客户（淘宝商家）；这类地下组织非常高效，接待人员很热情，培训人员很细致，培训材料通俗易懂图文并茂，当然很多高级管理人员都有充分的传销经验。

如之前所说，这些组织都缺乏格局，总是想着赚一些小钱，形不成产业链规模，被真正的地下产业链所唾弃。但是又由于这样的组织众多，经常弄出一些火并的小打小闹的事情。

地下产业链更是江湖，就如黑道上大家也都尊敬一些大哥，瞧不起一些小偷一样，淘宝天猫的刷单产业链逐渐变的热闹非凡但是却又形不成真正的黑产规模。

而对于淘宝卖家来说，就算利用刷单提高信誉，获取流量，甚至有些刷出假货爆品，但是由于利润总归有限，也不能形成很大的利益链条或者利益联盟。

C. 刷单产业链周边衍生黑产分析

同样有刷单组织也有差评组织，同样淘宝天猫的差评组织，也只能算是黑产中敲诈勒索组织的入门级，我们会在本报告的第四部分第 2 节详细分析地下产业链中的敲诈勒索。

D. 折扣站淘宝客产业链深度分析

淘宝客，是淘宝天猫生态中唯一衍生了真正地下产业链的模式。淘宝客的模式简单的说就是流量返点，把流量引入淘宝天猫的店铺或者单品，顾客购买，就会返点给流量提供者。淘宝客给流量主提供了一个很好的变现方式，也可能也是最早的最大的正规渠道的流量直接引入电商领域变现的平台化方式。

最早时期，各个流量主开始尝试淘宝客变现，也给一些地下流量主提供了一个比较见得光的变现方式。在几年之内，淘宝客产生了各种各样的玩法：站群流量引入淘宝客，黑帽 SEO 引入淘宝客，长尾词 SEM 引入淘宝客（SEM 高手），当然还有各类地下流量来源，和比较特殊的淘宝客 Cookie Stuffing。

我们仅仅用淘宝客 Cookie Stuffing 举例：用特定的技术将淘宝客推广链接的 cookie 植入访问者的电脑里。那么，下次访问者直接访问淘宝或天猫的时候，他所发生的任何交易行为，都可以因为 Cookie 的存在，被淘宝联盟跟踪到，从而让此淘宝客获利。

这些方式都给了地下流量主一个变现的终端出口，但是由于淘宝客变现毕竟比起来其他的地下变现盈利要少很多，所以也都是一些小流量主而为。

但是慢慢的淘宝客模式催生了淘宝折扣站这一种很特殊的变现网站，而且于雨后春笋般成长，我们监控最近几年的淘宝折扣站个数发展如下图：



淘宝折扣站不乏有一些做的很成功的著名站点。但是大多数都是通过一些小流量或特殊方法获利的站点，或者可以说是灰色产业。再加上如果更改了网站的商品链接即可更改掉获利人，所以复制折扣站非常容易，而且这之间引发的简单黑客技术的滥用，也让淘宝生态的地下产业链变得混乱且不入流。

E. 其他灰色黑色产业链深度分析

另外，由于刷单产业的存在，一些商品的评价和销量可以和真实不符，在一定程度上失去了公正性。这也让某些商品的制假形成线下产业，这些线下产业链有区域性特点，分工明确，再加上传统的中国制造的基础，逐步发展到了一定的规模。

但是对于这些商品来说，通过淘宝来变现是远远不满足的，于是会和互联网地下产业链的主流电商变现相结合。我们接下来就分析主流的地下电商变现：独立电商网站和货到付款的模式。

独立网站电商与货到付款类电商

2

A. 相关地下产业链整体深度分析

我们在分析独立电商与货到付款模式之前，先来回顾一个相关产业：电视购物。

电视购物在 1992 年进入中国，产品都是市面上少见，配上夸张的广告，加上没有渠道成本，非常暴利。1996 年，以舒亦康、帝威斯等为代表的第一批电视购物机构兴起。此后，各类卫视、地方电视台电视购物风起云涌。1998 年进入发展高潮，电视购物遍及 28 个省市，市场规模达到了 30 亿元人民币左右，销售额占当年社会消费品零售总额的 0.5%，2002 年到 1.2% 左右。（参考数据：目前火热的电商大概在 8%）

由于当时电视购物不受广告法的监控，变得极度的夸张。专注在如何抓住消费者心理：主持人语速极快极有煽动性，不给消费者的大脑留下思考空间，有计时器，加上一些“限量”等词语，很容易勾起购买冲动和不理智心理。而消费人群主要是集中在三四线城市，年龄偏大，接受信息的渠道有限，信息不对等，对电视比较盲目的信任。所以，电视购物的本质是利用消费者对电视频道的信任，利用频道的剩余资源加上特殊的目标人群产生销售的行为。

2006 年 8 月 1 日国家广电总局、国家工商总局颁发了对药品、医疗器械、丰胸、减肥、增高产品等五类商品（简称黑五类，下文中也称之为黑五类）不得在电视购物节目上播放的法规条令，可以说是电视购物在中国落地以来，第一次被重拳出击，电视购物遭遇严重的信誉危机。

也是那一天开始，“黑五类”离开了电视频道，找到了新的广告平台：网络平台。

B. 百度竞价单页产业链深度分析

黑五类最早落地的是百度。2006 年的百度公司，上市没多久，利润还很低，只是占领了一部分中国搜索引擎的份额。采用了“竞价排名”的商业模式。于是，2006 年年底开始，百度上一夜之间，充斥了竞价单页。

竞价单页在之前我们的数据中，都称之为暴利单页，是什么意思呢？就是网站一般只有一个页面（目前都是多个静态页面，但是黑市还是延续称之为暴利单页），但是内容丰富，和电视购物一个套路，专注在如何抓住消费者心理：页面上充斥着大量的图片、视频，销售话术极其有诱惑煽动性，充斥着大量的不合乎广告法的文案，在补充以什么权威机构、专家、医生等来证

明。几乎就是完全把电视购物的效果照搬成一个网站，而一般都采取电话订购或者网上订购，最关键的是采用货到付款的方式，方便不懂网络支付的客户购买。竞价单页再配上专门的网页客服软件（打开网页就弹出客服对话框），就形成了一个比电视购物更优越、更能施展的平台。2006 年到 2007 年度，百度的新开户数量高达 6 万多。

我们在此不举竞价单页的例子了，如果还是没有形象的认识，可以去搜索引擎搜索减肥、丰胸之类的关键词，排名靠前的大多都是竞价单页。

有人说，竞价单页可能是中国互联网水最深的一个行业。看上去非常简单的页面，非常明确的盈利模式，由于暴利和容易复制，导致了大量的隐秘的不为人知的圈子的秘密。这些秘密在黑市上流行，而又不断的进化。由于竞价单页在地下产业链中变现的地位，我们结合上下游，重点分析一下竞价单页模式，按照时间顺序把从 2006 年开始的近 8 年来的竞价单页的生态变化大概分成下面几个阶段：

明拍：最早的百度竞价采取的是明拍，也就是当年被人诟病的“竞价排名”，大家出价多少一目了然，出价高的排名在前。明拍让“黑五类”的暴利程度大大降低，形成恶意竞争。而和所有的明拍系统一样，到了一定程度会产生边际效应：只有大的玩家在玩，小玩家根本玩不起了，总的广告主数量有限。于是百度在 2009 年彻底改变了“竞价排名”策略，推出了“凤巢”系统。

暗拍：凤巢的本质，是一个暗拍系统。让这个生态系统里面的玩家大大增加了，以前看到价格都被吓回去的玩家，都重新进入到这个暗拍系统，大家斗智斗勇，生态也进化到了长尾阶段。

代发平台：由于暗拍的存在，吸引了大量玩家的进入，有些直接主打一些小众的关键词，或者长尾词，有些专门针对一个地点，有些专门针对一个时间，各种竞价单页的玩法层出不穷。但这些小玩家，很少能像那些大玩家一样，有自己的产品设计、包装、制造、客服等配套服务，大家更多的只是复制别人的单页、进货、发货，甚至客服的精力都没有。于是国内出现了一批代发平台。这个平台上所有适合百度竞价单页的产品，主要都是“黑五类”或者各种山寨手表、数码等等，只要你加入这个平台，再去百度开一个账户，你只需要集中精力在广告上，有了订单只需要给代发平台，代发平台帮助你发货，回款。2012 年中旬，国内大概有 7 家左右特别大的百度竞价代发平台。到这个阶段，这个圈子的产业链开始形成。

盗单：产业链形成后，百度单页竞价生态圈里面的玩家越来越多，在 2012 年的左右，仅仅竞价单页类的广告账户就大概有 20 多万，一年大概给百度贡献了 100 多个亿的广告费用。而

流 量资源也在足部的饱和，暗拍下的价格也在足部升高，已经能和之前明拍的时候相持平。
这个

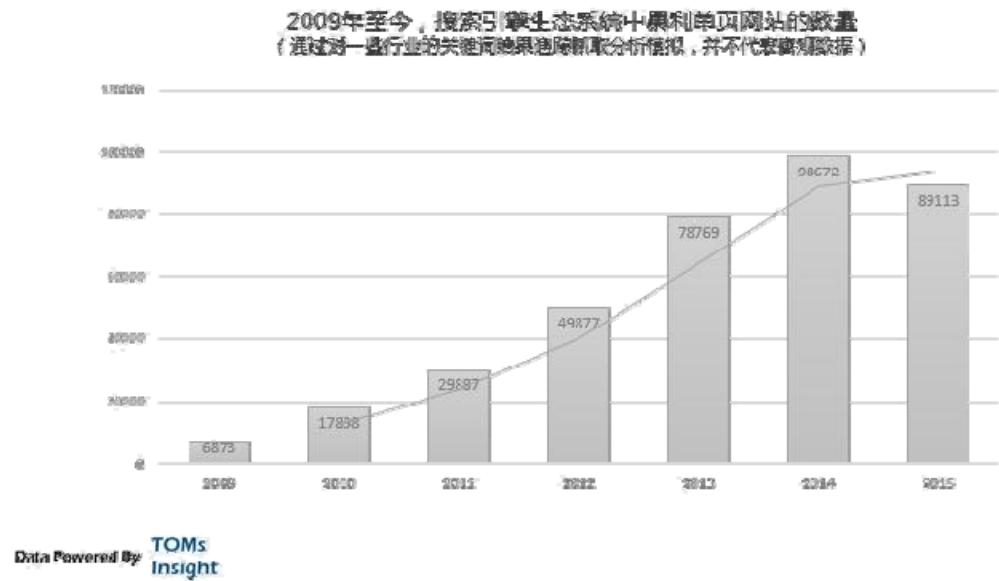
时候产业链里面开始了一股很奇怪的风潮：盗单。由于单页主要重视的是图文广告，对安全性没有重视。甚至都是大量的仿站，订单系统都是由几个简单的网上源程序修改。再加上代发平台控制着大量的订单，非常容易被攻击。黑客攻击后，订单再次转卖，由于百度单页的订单都是后付费。黑客盗用订单后，直接卖给代发平台即可，所以很多黑客都是代发平台雇佣。这个阶段一片混战，但是除了大玩家，还是代发平台统治了小玩家。

DDOS：生态圈又回到了大玩家的时代（包括代发）。但是大玩家之间的争斗地盘的生意更加激烈。为了统治每一类产品的关键词，大玩家之间开始动用了 DDOS。百度凤巢有个策略是如果网站如法访问会自动下线，所以当一个网站被 DDOS 的时候，也会自动从广告系统中下线。一直到现在，很多领域的关键词都是被垄断的，如果你复制一个竞价单页去百度开户，有时候代理都懒得给你开，因为大家都知道你用不了多久就由于被 DDOS 的无法自理要求退款，还不够麻烦。

联盟：到了 2013 年，百度最赚钱的关键词广告，全部都被大玩家所统治，当然还有一些新兴的行业（职业教育、美容手术、留学中介等），由于大玩家就那么一些，大家在几年以后开始坐下来谈一谈，达成一个联盟。不再勇猛的暗拍，激烈的 DDOS。大家私下排名好，都出低价，然后别的小玩家要进入就用黑客手段弄死。2013 年，百度的股价一度到跌破 90 美元，成为一个低点

移动时代：到了 2013 年下半年，移动流量在百度的搜索的比重越来越大。很多媒体都在说百度在移动的新时代落伍了，百度没有拿到门票。但在我们看来，移动时代的到来反而救了百度。因为在 2013 年刚刚形成的联盟，被移动时代的一些新玩法打破了，移动上的单页竞价和 PC 端几乎完全不同，大量的新玩家涌入让这刚刚形成的联盟土崩瓦解。

分析到此，我们大家对于竞价单页（暴利单页）有了一个整体的认识，对相关的地下产业链的发展也有了一定的了解，这样的竞价单页（暴利单页）大概有多少呢？我们通过对一些关键行业词群分析抓取，得到下面的数据：



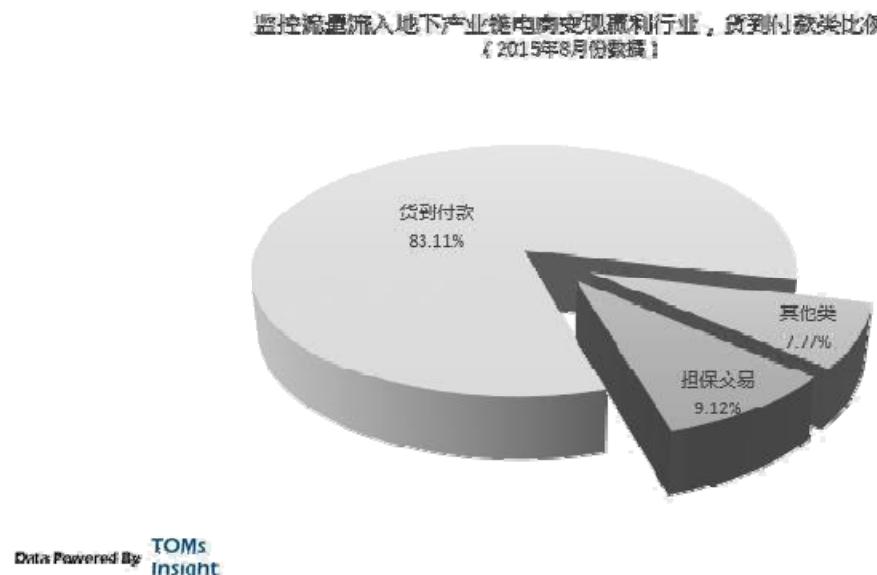
C. 货到付款电商产业链深度分析

竞价单页从模式上几乎无一例外的货到付款。货到付款这种模式看起来好像是低级，但是确是国内互联网电商的主流，我们不能忽略掉四五线城市以及乡镇对互联网没那么了解的用户。

货到付款深受地下变现盈利产业喜爱，几乎成为地下产业链电商中的主流变现方式。一是由于货到付款本身可以逃脱支付接口的监管和投诉，更重要的是用户确认收货的时间较短，没有长时间的试用过程（验货后付款给快递员），而很多物品大家都不会验货（比如成人用品类），导致了这种方式非常适合暴利产品和假冒产品。

而所谓的暴利产品又是什么商品呢？之前我们已经介绍过的黑五类就是典型的暴利产品，比如一款减肥茶，在暴利单页上出售到了300-400元，其实其出厂成本不到5元。

而通过地下产业链引流，通过暴利单页变现，也就变成了一种黄金搭配。



D. 网络品牌电商产业链深度分析

在本报告第一部分第 5 章，我们有提到垃圾信息的网络炒作，这些炒作的地下产业还会有另外一种更直接的变现方式，就是直接炒作暴利品牌。

比如左旋肉碱这个词，在 2010 年忽然火爆，而相关的减肥暴利产品也在网上大卖。其实在这个词火爆之前，地下产业链中的变现盈利组织已经大概提前一年的布局，包装产品，找准定位，生产产品，优化好页面，甚至连搜索引擎的排位都已经定好。才让开始炒作这个词。

这就是地下电商的大玩家，直接包装一个品牌或者一个热门词。如果留心大家就会大发现这样的热门词最近几年也层出不穷，炒热一个概念后，就会有大量的“官网”类的暴利单页，然后推出代发平台，发货给下面的小玩家等等，这些手法大家应该可以想象得知。

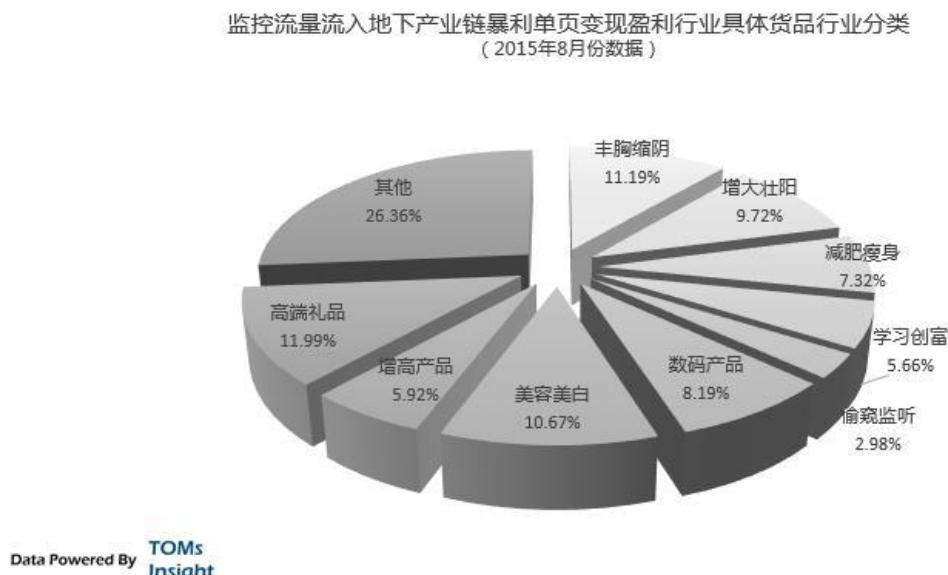
能有能力炒作一个品牌的电商一般都有一定的实力，不仅仅如此更重要的是在地下产业链中的号召力和布局能力，可以在一个热点概念上市之前完成布局，而让大家有秩序的吃掉利润，不引起混乱，不引起恶意竞争。

反观主流互联网产业的热点细分行业的一窝蜂扎堆，还是缺乏一些大局观和秩序。

E. 其他独立电商产业链深度分析

最后还有一些独立电商，伪装成很高大上的网店，但是在支付环节或者货品环节都有欺诈行为，我们会在本报告第四部分第6章详细分析。

但是此类电商也并不成气候，在地下产业链中也只是属于边缘产业。下图我们可以看出货到付款类电商具体的货品行业分类：



另外关于京东、亚马逊之类电商平台下的刷单，或者合作商家的假货的相关产业，玩法相对简单，也并不是地下产业链变现的主流渠道，在此略过。

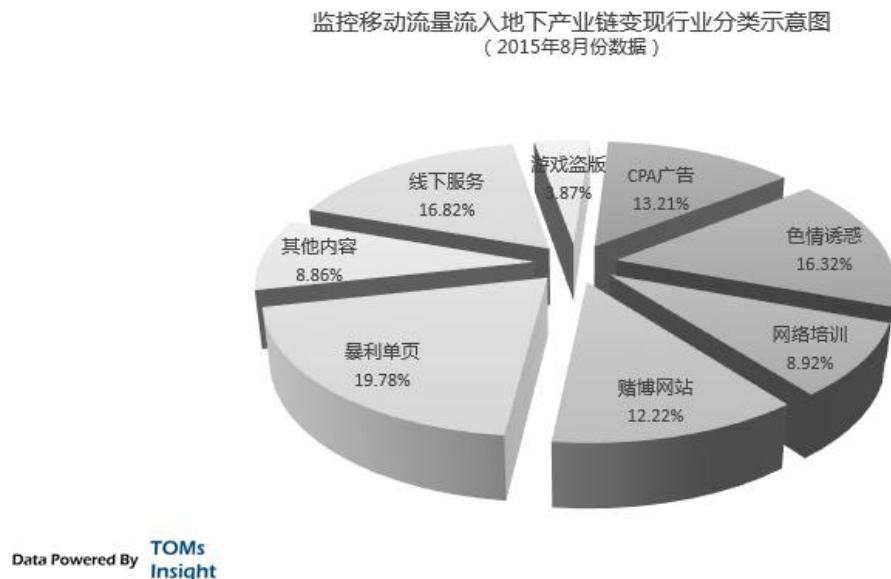
微店类型电商与独立移动端电商

3

A. 相关地下产业链整体深度分析

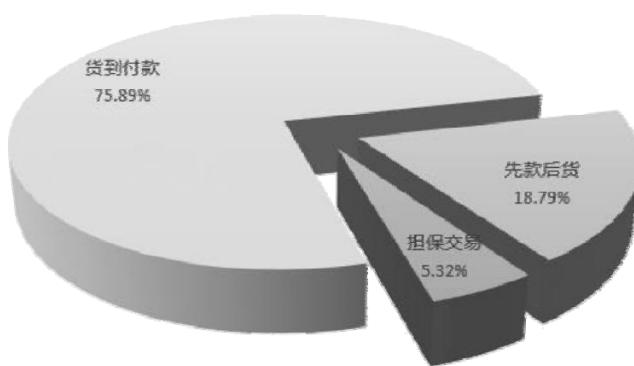
移动互联网的浪潮一样波及到了地下产业链，就如之前讨论，几乎所有的互联网产品生态都不可避免的流量移动化。关于电商类变现盈利产业来说，本章我们并不讨论淘宝天猫、京东亚马逊的手机客户端平台，而是主要专注在独立的移动电商，这些独立电商才是地下产业链移动流量的最终出口。

我们可以从下图看出，地下流量大概有 19% 的变现终端为暴利单页，我们在这个地方的暴利单页定义比较广义。



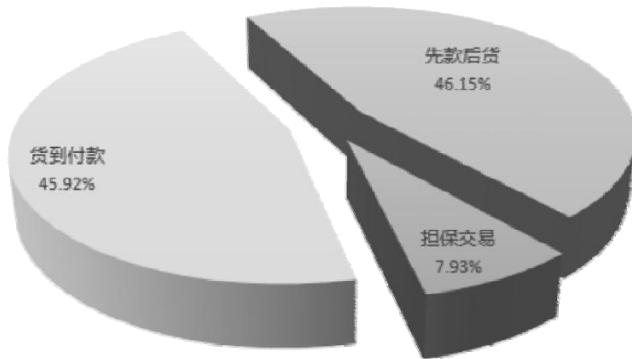
如果把这 19% 的暴利单页再拆开，仔细的研究这部分的电商变现，会发现如下图的数据。

监控移动流量流入地下产业链通过暴利单页变现细分示意图
(2013年1月份数据)



Data Powered By **TOMs**
Insight

监控移动流量流入地下产业链通过暴利单页变现细分示意图
(2015年8月份数据)



Data Powered By **TOMs**
Insight

在 2013 年 1 月份，大概有 75% 的暴利单页是传统的货到付款模式，但是有 18.79% 的是先款后货。我们在此的数据统计是使用主付款方式，即大概 18.79% 的暴利单页使用的首选付款方式竟然是先款后货。这和传统的暴利单页变现完全不同。我们继续追踪这个数字。到了 2015 年 8 月，变到了 46.15%。

这个大概 40% 的现款后货的移动端暴利单页变现模式，在黑市上称之为：微店变现。

B. 百度生态移动电商产业链分析

百度生态下的暴利单页模式已经发展的非常成熟了，如之前的分析，到了 2013 年下半年，移动流量在百度的搜索比重越来越大。很多媒体都在说百度在移动的新时代落伍了，百度没有拿到门票。但在我们看来，移动时代的到来反而救了百度。因为在 2013 年刚刚形成的联盟，被移动时代的一些新玩法打破了，移动上的单页竞价和 PC 端几乎完全不同，大量的新玩家涌入让这刚刚形成的联盟土崩瓦解。而移动端又有什么新的玩法呢？

在 PC 流量时代，长期的暴利单页，或者竞价单页的优化，形成了两个非常关键的要素：货到付款和在线客服，这两个是相辅相成的。在线客户通过长时间优化的话术让用户上当，而货到付款是打消用户疑虑的最佳的方式。

但是到了移动端，由于屏幕的问题导致在线客服这一关键要素并不成立。所以在我 2013 年之前，百度生态下的移动流量几乎没有价值。但是 2013 年之后，地下变现产业摸索出来一条行之有效的方法，就是先款后货的微店变现。

看上去是很矛盾的，本来有客服货到付款，现在变成了没客服而且要先付款，用户岂不是更容易买单么？其实不然，地下变现产业链在长时间的尝试中，对用户心理把握到极致。先款后货的商品一般都是小额付款，不会太贵，而且一般都会通过精美的展示，打动用户，而并不是话术。让用户的购买心理从使用需求转向尝试需求。

这在另一程度上也解决了先款后货的退单问题，所以这条道路开始在移动流量变现领域大肆发展，也让百度生态的移动流量，有了新的价值。而百度生态流量也成为了微店变现的第一主力军。

C. 微信生态移动电商产业链分析

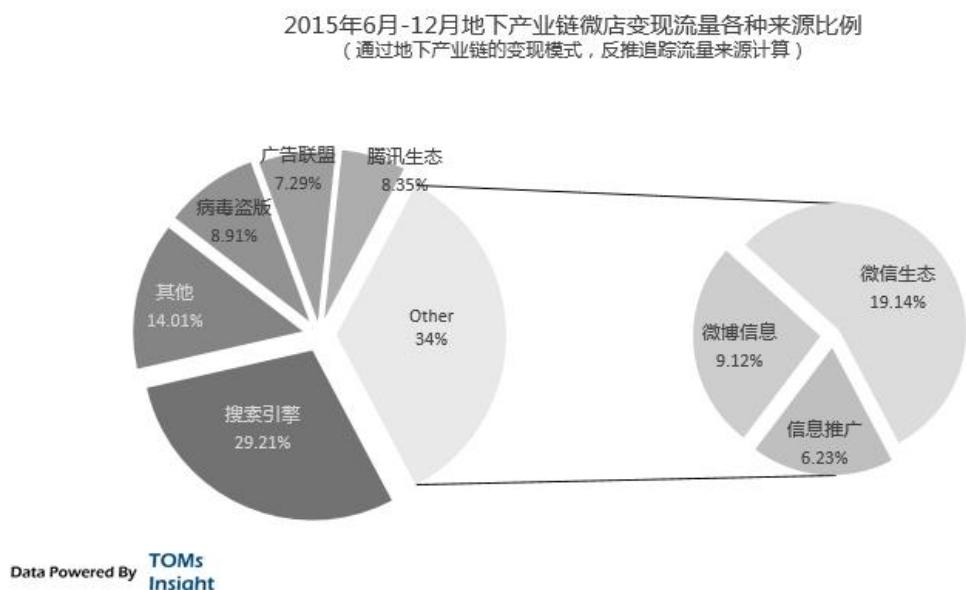
同样，微信生态虽然引入地下产业链中的比例较小，但是却也是现款后货的微店类变现的主力流量来源。特别是 2013 年，大量的微信公众号号群和一些垃圾号的流量，很容易通过阅读原文导入微店，而生产很匹配的消费流量。而一些公共号联盟会不断的相互更改微店变现终端，相互利用各自手中的流量，充分的榨干所有的养分。

但是微信生态虽然很适合此类变现，由于整体安全策略，再加上产品本身的设计（并不是过水流量，粉丝是比较稳定的用户），很难形成地下变现最热爱的“火车站流量”。

所以发展到 2014 年之后，也慢慢凋零了。

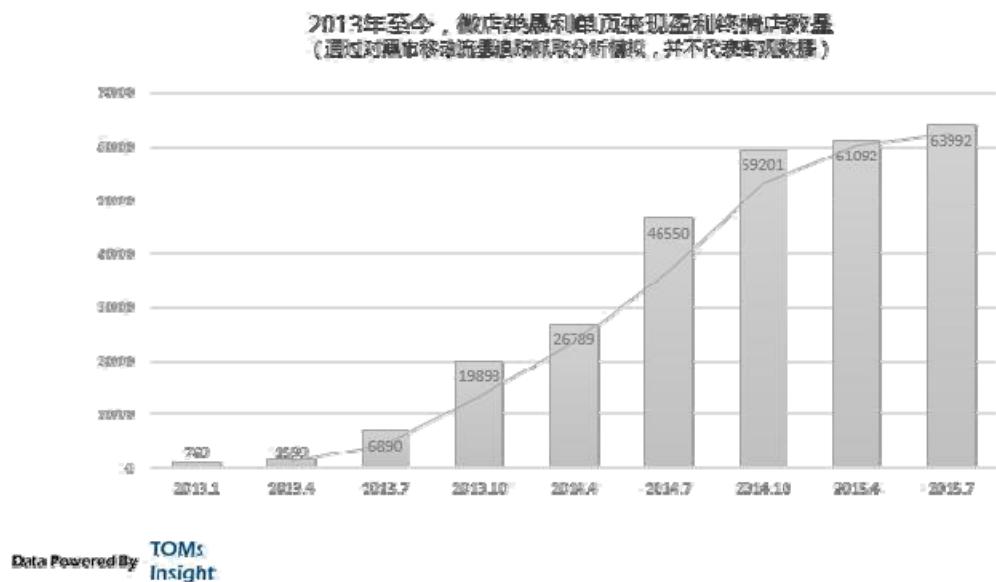
D. 其他流量移动电商产业链分析

除了微信以外，腾讯的其他生态也是微店类重要组成部分。病毒盗版由于流量本身的占比大，也成为微店类变现的导流大户。



微店类变现发展迅猛，还有另一个原因是从移动端用户行为来说，手机端小额的随意性付款已经成为用户行为变现的一个非常重要的部分。而目前来看，微店类变现几乎成为地下产业链中最火爆发展势头最好的一种变现方式。

这种变现方式也在一定程度接过了安卓 app CPA 的接力棒，成为了新的黑市移动流量变现的最重要的一环。



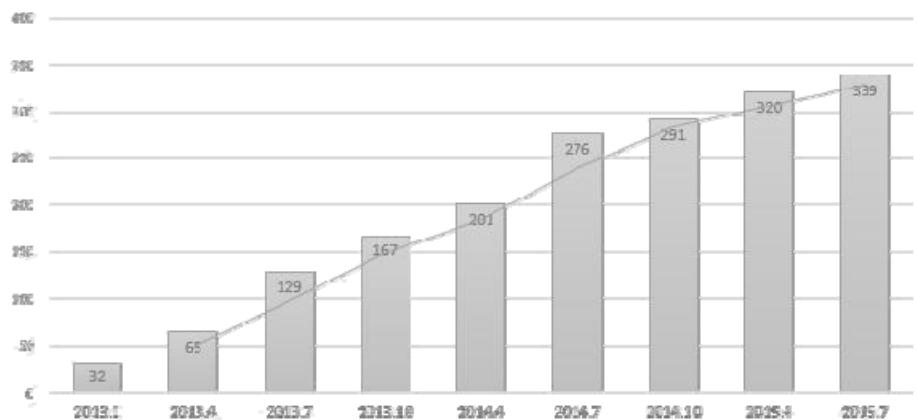
E. 独立移动电商支付分析与数据

微店类变现在支付环节上，一种是通过支付宝、银行卡等直接付款，但是更多的还是利用移动支付平台，目前地下产业链中移动支付平台也迅速发展。也有一些可以利用手机短信付款，话费付款等 sp 业务付款方式。

从模式上来，帮助这个平台上的客户收款，然后抽取一定的提成也是最典型的模式。但是也有一部分地下平台会扣款或者卷款跑路，属于黑吃黑也并不是对我们影响的风险。

但是值得一提的是，这类支付平台有一些存在于主流产业中，甚至已经拿到风投。其生态系统的构建和相关安全策略，肯定也会受到地下产业链的冲击。

2013年至今，微店类电商平台活跃用户数与平台数据
(通过对第三方移动支付平台的分析数据，并不代表真实数据)



Data Powered By **TOMs**
Insight

游戏地下产业链分析与相关生态

4

A. 相关地下产业链整体深度分析

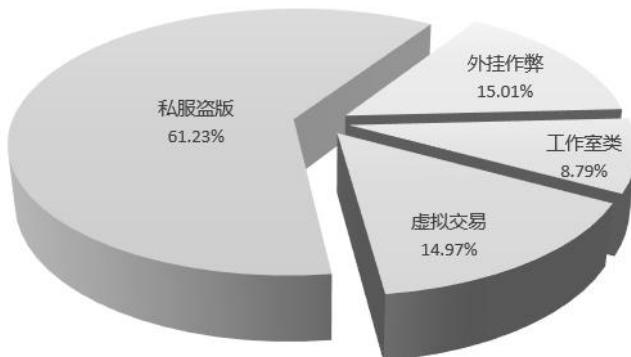
游戏是在国内除了电商以外最大的直接变现盈利终端，而且电脑游戏从诞生的第一天起，就和一些地下产业链有着千丝万缕的联系，这一方面是从文化上来说很多黑客喜欢游戏，也是从篡改游戏开始学习入门，另一方面和游戏的利润空间也不无关系。

游戏在国内发展到今天，端游、页游、手游都迎来过自己的辉煌或者高速发展，而与此同时，围绕这些游戏的地下产业链也在大肆的发展。

目前来说，游戏外挂作弊、游戏工作室、虚拟资产黑市交易、和私服盗版，是目前地下产业链中的几种形式。游戏地下产业大概能消耗地下流量的 11%。从流量变现终端来看，私服盗版由于直接面向终端流量用户，吃掉了 6 成的流量供给。

而工作室类由于是生产部分，并不需要流量支持，虚拟交易则由于特殊性，仅仅是通过一些小圈子来传播。而外挂的流量确是有另外的目的所在。

监控流量流入地下产业链游戏产业中行业具体细分
(2015年8月份数据)



Data Powered By **TOMs**
Insight

B. 游戏外挂作弊产业链数据分析

游戏外挂作弊产业在地下产业链中非常奇葩，几乎变成了一个黑客比拼技艺的地方，就如之前的 0day 组织的 64k 动画大赛一般。而且黑客们选择游戏外挂，总是针对自己最喜欢的游戏，来实现自己觉得最牛逼的作弊功能，在这个上面有更多的主观感情色彩，而并不是利益本身。

早期的端游外挂都是出售给最终用户的，而目前的外挂都会极其的保密，仅仅提供给一些游戏工作室使用，几乎很难在黑市渠道上寻找其踪迹。

那为什么外挂作弊还能消耗掉大概 10% 的游戏地下产业流量呢，说起来也许都很难置信，这些流量用作个人品牌宣传，被黑客圈子称之为：明挂。即明知道这些外挂宣传出去，很快就会被游戏厂商修复，但是还是为了炫耀或者宣传个人品牌，引流量来曝光。而这些所谓的明挂，也仅仅是浮出水面的而已。

C. 游戏工作室相关的产业链分析

游戏工作室并不是指的 cp，而是那些代练工作室，通过使用大量的机器，配合外挂，和人力，快速的聚集游戏的虚拟货币或者道具物品。在湖北的一个城市，游戏工作室几乎成了大多数年轻人从业的首选了。

游戏工作室很难说是完全的黑产，毕竟并不违法法律，可以半公开，仅仅是被游戏商所禁止。但是从另一个角度说，对于特定的游戏，少量工作室的存在能带动游戏内玩家的消费和活跃度，并不是什么坏事。

游戏工作室的核心资源是外挂，就如直接所说，黑客制作的外挂主要提供给游戏工作室，一个好的外挂可以让效率提高几倍，几十倍甚至几百倍。没有好的外挂资源，只能雇佣大量的人力成为小型工作室，而好的外挂和黑客的支持，可以让工作室变成如比特币挖矿般的自动和高效。

游戏工作室上游的是收货商，收货商在一定程度上可以营销一款游戏货币的黑市价格，来控制旗下的游戏工作室资源，整体调控来获得更大的利益。早期的收货商由于被游戏厂商憎恨，极其低调。最近几年由于游戏行业竞争激烈，还有一些主流游戏室竞争也会雇佣收货商“打毛”

竞争对手游戏货币的做法，导致这个行业也慢慢的浮出水面。但是更多数的收货商还只是专注于黑市上的虚拟交易。

D. 游戏资产交易与黑市交易分析

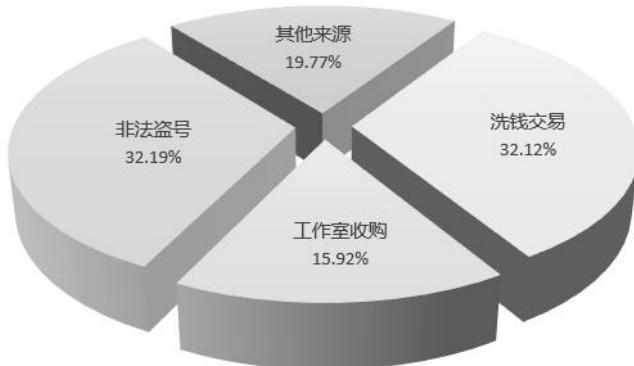
如果仅仅是收货商卖出来的游戏资产交易，虽然被游戏商禁止，但是还不至于违法。但是纯粹的黑市上的游戏虚拟资产交易，更多的是来自于盗号。我们之前有分析过信封号，在第一部洗信的时候，洗掉账号内所附带的游戏虚拟资产，是信封号最重要的一个环节。

盗号的过程也是各种手段层出不穷，不仅仅通过技术，还有各种骗术也层出不穷。甚至包括以下线下的行为。

另外由于游戏虚拟资产很难交易很难追踪，也成为一些网络洗钱的温床，也是黑卡盗刷产业链中很重要的一环。

下面的数据是黑市游戏资产交易分布：

2015年10月，地下产业链黑市交易游戏虚拟物品来源具体细分
(数据来源专家网络+抽样分析，算法模拟)

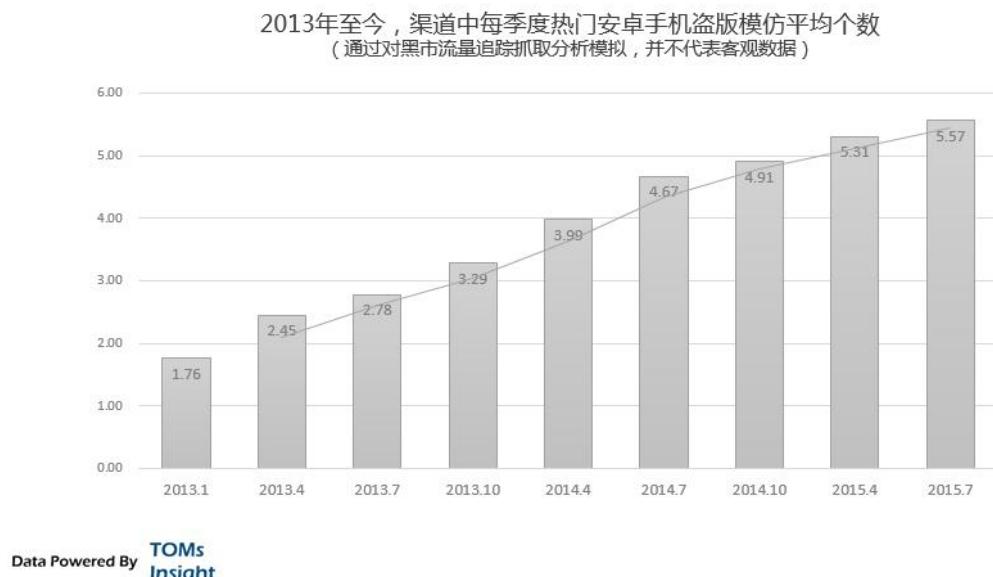


Data Powered By **TOMs**
Insight

E. 游戏私服与移动游戏盗版分析

曾经，在端游流行的年代，私服游戏几乎成为地下产业暴利的代名词。但是当游戏产业全面进入页游之后，私服显得没有那么重要了，由于复制成本低，有时候很难把私服和一块新游戏分离。而也由于玩家选择的多样性，和游戏策划本身的急功近利，私服的优势也没有那么明显。纯粹的打出来私服的名头也并不是噱头。

而更有创新性的是手游的盗版，由于安卓渠道的混乱和 Java 非机器码本身容易反编译。而地下游戏产业中 80% 的流量消耗大户，也来自于这些盗版的游戏。



博彩类变现相关地下产业链分析

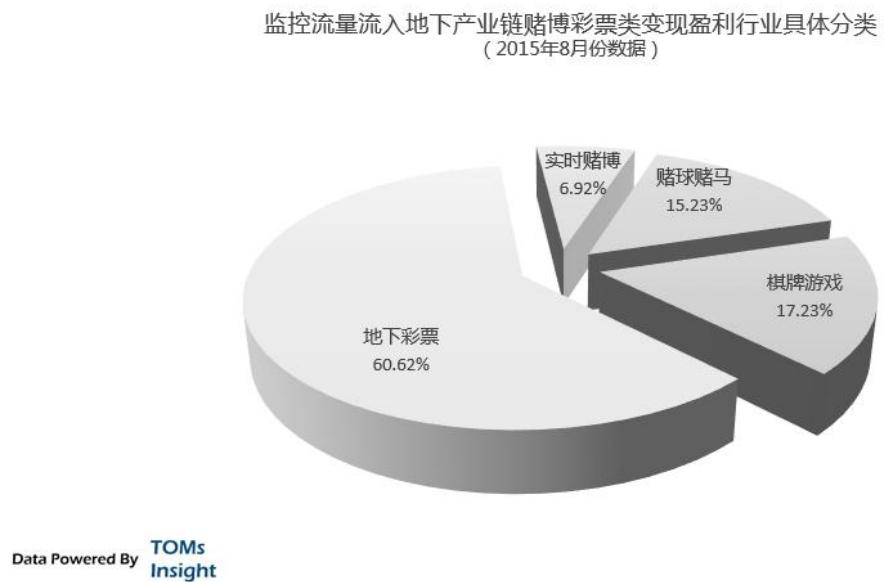
5

A. 相关地下产业链整体深度分析

互联网上根本用户需求，好像从互联网诞生那天起就没变过。比如典型的 3G 需求：Game、Girl、Gambling（游戏、美女、赌博）。而作为变现商业模式最直接的博彩，更是作为互联网的第一代 Key Application，都很难说是互联网推动了博彩，还是博彩推动了互联网。

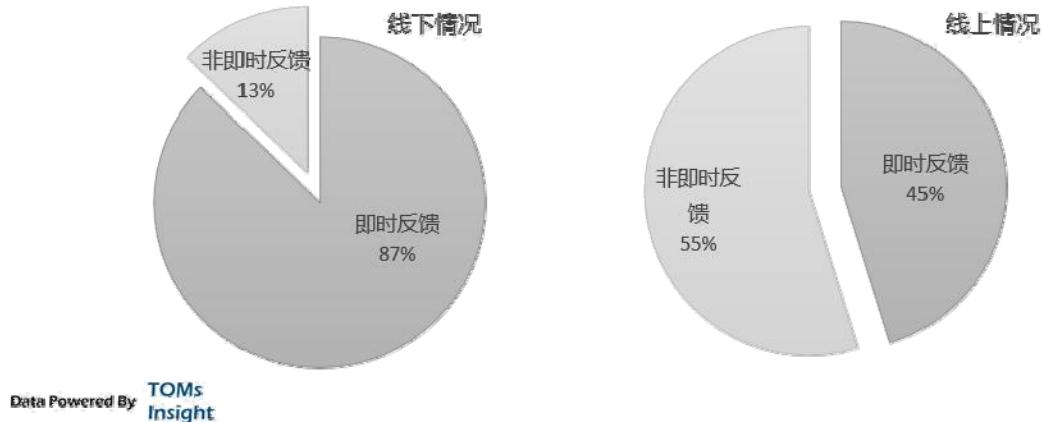
赌博在国内严格禁止，但是彩票的却在被限制性合法。而从游戏中衍生出来的带有赌博性质的棋牌类游戏，却又在各种渠道中流行，屡禁不止。

博彩类的地下产业链变现大概可以分成地下彩票、赌球赌马、棋牌游戏、实时赌博。如果从流量来看，地下彩票竟然吃掉了一半以上的流量，而实时赌博几乎没有多少份额。



这个比例是非常的奇怪的，因为传统的博彩业即时反馈类型大概要占据 9 成的份额，而就算是比较适合非即时反馈的互联网，非即时反馈大概也只占据 55%而已。但是在国内的地下产业链中，实时的赌博几乎没有多少市场。

即时反馈类与非即时反馈类营收对比
(拉斯维加斯五大博彩公司数据监控统计)

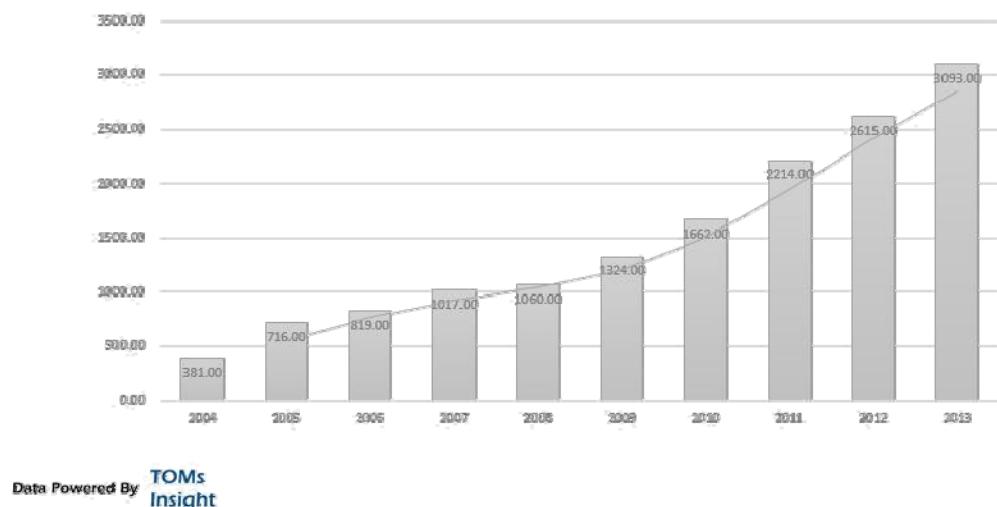


这很大程度上是由用户的接受度造成的：几千亿每年的官方彩票的发售，提高了地下彩票的接受度，也造成了地下产业链的博彩业现状。

B. 网络彩票地下产业链深度分析

主流的彩票业在国内经过二十几年的发展，已经成为了一个非常成熟的产业，特别是近十年的高速发展（10倍销售额），更让销售网络遍布全国。

2004年到2013年中国国内彩票总销售额，10年间的变化趋势

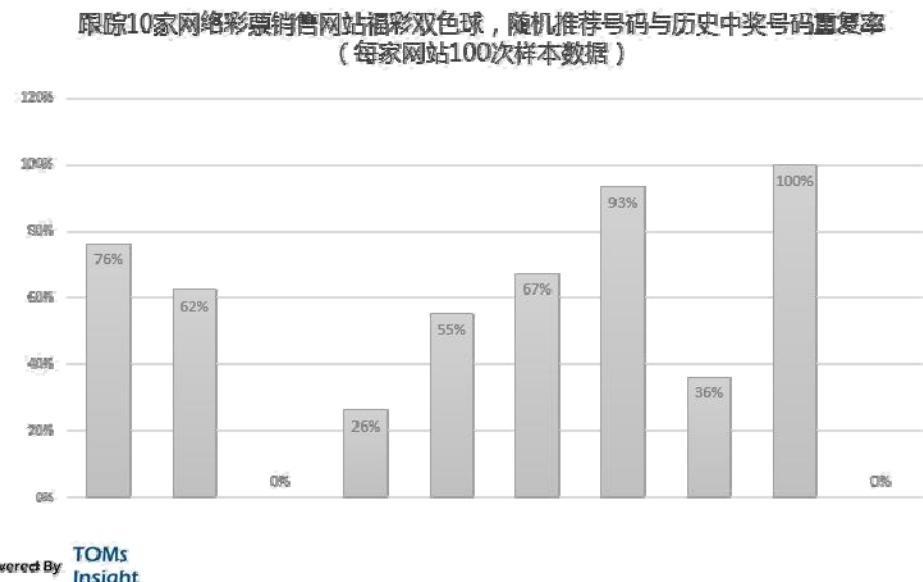


互联网作为彩票的销售渠道，是典型的利用流量切入传统行业。由于彩票的总发行费用只占销售额的 15%，还包括两大彩票中心的运营成本，其实网络彩票的可能拿到的利润极低，只能占据销售额的 5-7%，甚至更低。

由于网络彩票仅仅是代购，那么用户在网络上购买彩票后，代购的互联网公司要去国家的体彩或者福彩中心购买对应结果的彩票，在行业里面叫：出票。但是对于地下彩票行业来说，出票并不是必须的。

下图是我们跟踪 10 家网络彩票销售网站（非上市互联网巨头）双色球产品，随机号码与历史中奖号码重复率，就是说我们有时候经常在网络上买彩票，喜欢随机几注，但是随机出来的数字，大多都是和历史上的中奖数字重复。

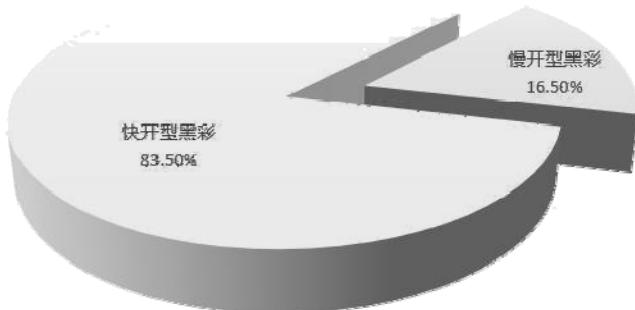
对此可能有人会说彩票是独立事件和历史结果无关，但是毕竟双色球历史上从来就没出现过完全一样的中奖号码。我们仅用此来分析相关网站的设计，推测是不是出票。



另外，还有一种彩票，和国家发行的彩票没有任何关系，完全是由私人坐庄，私自控制返奖率，被称之为“私彩”或“黑彩”。黑彩有很悠久的发展历史，从互联网并没有流行的时候就已经开始了。最早从香港传入南方内地，后在东北三省发扬光大，慢慢全国流行。在南方一些城市，在之前一些年代甚至出现过全城玩黑彩的一些黑暗历史。

目前行业内比较保守的估计官方彩票和黑彩的销售比例大概四六开，也就是说“黑彩”在国内保守估计大概有 5000 亿的规模。黑彩以快开型彩票为主，快开型彩票的官方彩票 2013 年全部产品加总销售额 631 亿，占整体彩票业的 20.4%。

55个互联网“黑彩”彩民讨论群舆情监控，关于“快开型”和“慢开型”参与占比



Data Powered By **TOMs**
Insight

但是在互联网“黑彩”中，快开型彩票几乎占据 80%以上。以“重庆时时彩”为例，白天 10 分钟一开，夜场 5 分钟一开，一天就能 120 期。而黑彩以快开型为主，通过利用彩票这种赌博在中国的认知度，也同时进入了更接近即时反馈的赌博品类。

经过几年的发展，国内各种各样的黑彩层出不穷，各种骗局极其高明。目前大概有下面几类：吃票、大客户模式（通过黑市上购买数据，找到特定的客户，推荐号码给客户，然后中奖，打造信任，让客户一点点的深入，最后赚一笔大的跑路）、散户模式（通过大流量引入大量的客户，针对每个客户都有特定的算法开票，逐步引入）、平台群（开大量的黑彩平台）

而黑彩的竞争也到了白热化：DDOS，黑市数据、病毒、黑链引流等等，十八般武器都进入到这个利润极大的黑产中。甚至百度搜索“时时彩黑彩”都能找到大量平台和软件出售！

而彩票类赌博，也成为了地下产业链变现盈利的最主要终端之一。

当然黑彩中还有别的形式，比如模仿“中福在线”（目前在百度上打广告的“中福在线”均属非法），比如更接近赌博形式的玩法。

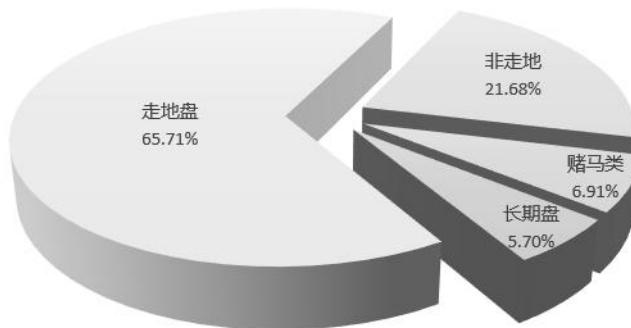
C. 网络赌球地下产业链深度分析

赌球其实和彩票模式一样，由于官方有各类体育型彩票，所以用户已经接受了足够的教育。赌球的模式和之前提到的地下产业链中的彩票变现以及如出一辙。

但是地下产业链中的赌球有一种叫走地盘的玩法。走地盘又叫滚球盘，就是对正在进行的比赛开出的盘口，博彩公司会根据比赛进行时间以及赛场局势发生的变化不断变更盘口。比如：一般走地每 10 分钟就会调一次盘，因为随着时间的推移盘口自然要有变化，不可能 A 让 B 球半，到 85 分钟了还是球半吧。除了时间因素外，比赛时发生的一些情况也会造成盘口的变化。比如：红牌，球员受伤等等。

走地盘一方面让用户很有参与感，另一方面由于更接近实时性，更接近赌博的原始需求。在地下产业链中，走地盘几乎占据了网络赌球的大部分份额。

监控流量流入地下产业链赌博彩票类中赌球赌马类变现盈利行业具体细分
(2015年8月份数据)



Data Powered By **TOMs**
Insight

D. 网络棋牌游戏赌博产业链分析

游戏产业对赌博行为禁止的非常严格，特别是棋牌类游戏，其中一个最核心的就是 check out 严格禁止，就是说你可以买筹码，玩游戏，但是赢的筹码不能兑换成现金。这是国内所有棋牌类的游戏非常严格的规则。

但是很多地下产业链中都会有对热门游戏的相关兑换产业，主要渠道就是在游戏中通过故意输的方式来转移筹码，而通过支付宝等支付渠道支付。

网络棋牌类还牵扯到实时在线赌博，但是此类由于危害性大，被严禁制止。但是此类的变现价值也几乎是所有的地下赌博类里面最大的。

E. 其他赌博形式产业链相关分析

由于赌博的变现暴利性，与地下产业链中各种数据安全都有错综复杂的联系，比如对病毒木马，挂马、各种黑市流量，各种黑市数据分析，甚至对单用户的数据跟踪等等。我们在本报告的第四部分会有相关分析。

赌博也是地下产业链变现盈利产业中对最终端用户危害最大一种，所以尽量的让用户远离任何形式的赌博，也是互联网用户需要的安全保证之一。

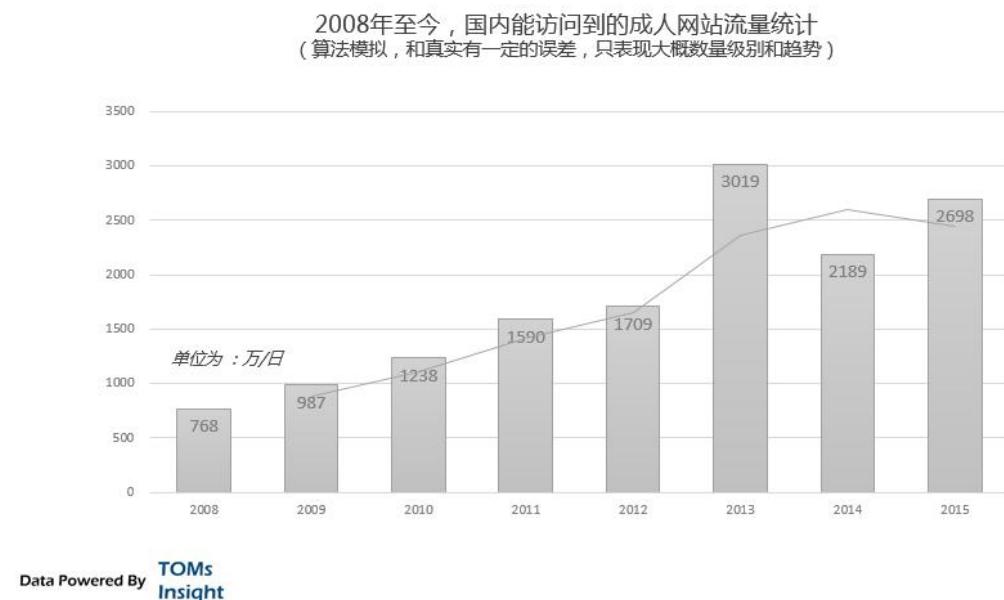
网络色情及诱惑相关产业链分析

6

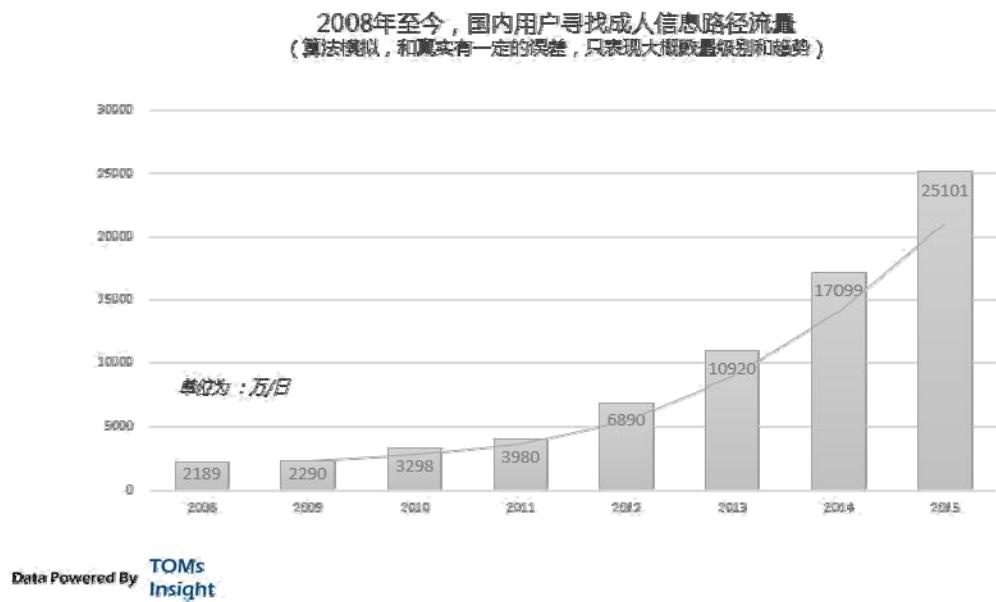
A. 相关地下产业链整体深度分析

谈到网络色情和诱惑类，大家可能想到的第一个就是色情网站。确实色情网站作为聚焦点可以成为聚集流量和用户的利器。我们在本报告第二部分第3章中介绍了色情网站在中国的流量聚合和通过网络联盟再分发的方式，以及路径流量分析。

但是色情网站毕竟严重违法，在国内法律的一次次打击下，国内能访问到的色情网站的规模一直没有发展壮大，几千万pv的水平根本没法和需求相提并论。



甚至在寻找成人内容的路径流量都要远远大于成人网站流量本身。所以在地下产业链中，与其铤而走险的去做色情网站，还不如去做路径内容，通过流量分发的形势变现。这也是目前地下产业链中的现状。



但是还会有一些人铤而走险的去做色情内容，既然如此，变现方式肯定会比流量分发要高很多才能对得起这个风险。我们接下来分析。

B. 色情网站产业链变现模式分析

色情网站一般有几种直接的变现方式：会员制、交易平台、裸聊、一夜情模式。

会员制可能大家都会很了解，把一些高质量内容做成会员收费内容，一般按月收费。对于色情网站来说，内容来源也会有上游产业链，但是一般由于色情站的特殊性，很多人愿意分享，也导致了内容成本较低。所以对于优化好的色情站来说，会员制是一种要比流量分发盈利水平高出很多的方式。

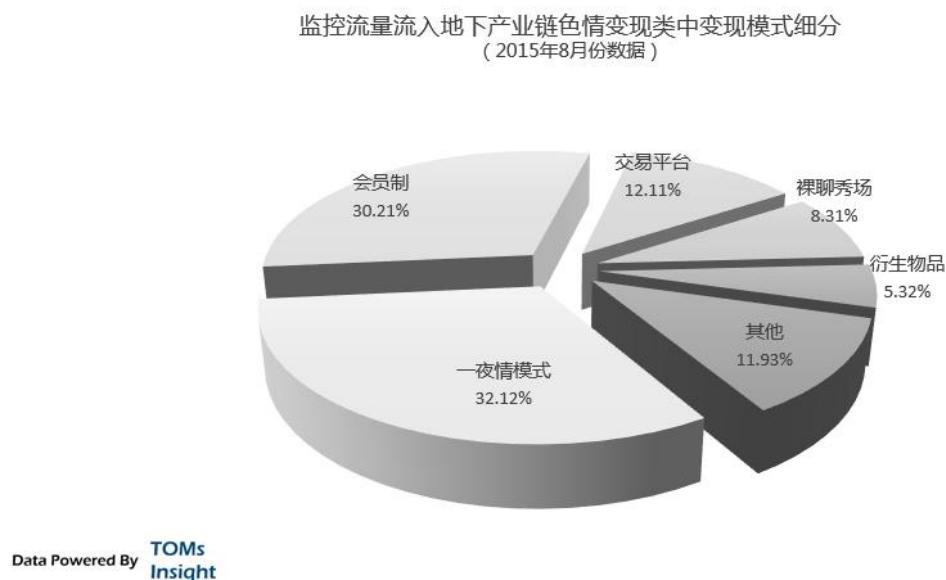
另外一种是交易平台。即提供一些线下的非法色情交易平台，或通过会员费，或和线下的色情组织合作，达成分成协议。这种模式盈利水平更高，但是由于风险更大，而且无法形成流量放大性规模，并不被广大的地下产业链接受。

裸聊有些平台会做到极大的规模，但是和交易平台一样，无法脱离线下，风险较大。没法有流量放大效益，所以逐渐的没落。特别是 2014 年的净网行动，严重的打击了色情网站和相关的

变现产业，使地下产业链中的这部分更加萎缩。

一夜情模式我们最后分析，但是这也是色情网站中使用最多的一种变现手段。即提供一个一夜情的平台，欺骗用户感觉自己所在的城市好像很多人要在找一夜情，而且注册登录后就会看到不断的邀约，吸引充值。但是充值后才会发现一切都是骗局。

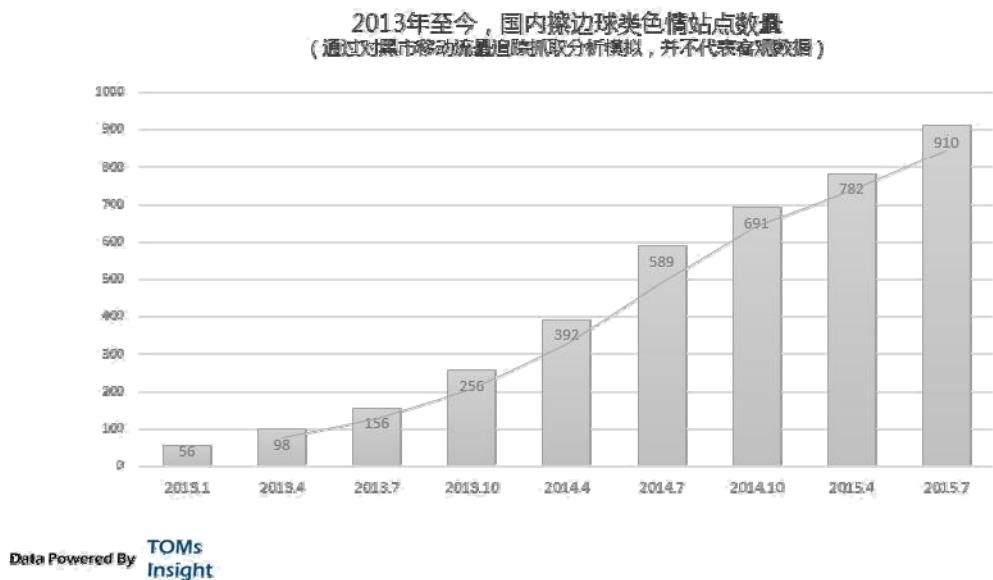
一夜情模式成功到已经超出了色情网站变现的范畴，在地下产业链或者黑市中，很多人都会把“一夜情模式”形容那种利用信息不对等完全匹配用户心理诉求的骗术。



C. 擦边球类型色情网站变现分析

擦边球类型的色情站点从 2013 年开始兴起发展，特点是内容原创，制作精美，但是色情程度却比传统的色情站点要低很多。

传统的色情站点的内容主要来源与日本、欧美的成熟成人产业的作品，而擦边球类型站点，内容都是原创，打造小而精的品牌，作品几乎打着法律的擦边球，有时候很难分辨的清楚到底算是色情淫秽作品还是艺术作品。



由于风险更小，而且易于传播，再加上国内压抑的相关需求。擦边球类的站点在 2013 年以后飞快的发展，而相关的变现也使用更加直接的会员制。保护一定的内容而且可以避过相关的风险。

而由于原创内容，所以还开辟出来衍生物品的售卖，仅仅是这块售卖，反而占据了色情网站之间变现超过 5% 的份额，可见相关的火爆。这是目前色情内容变现里面一个创新程度非常高的领域。

D. 地下秀场网站产业链深度分析

秀场类网站最近几年一直很火，还有相关的上市公司。地下秀场也跟随主流的秀场网站一直发展，所谓的地下秀场网站，也无外乎尺度更大，有夜场、单聊等等之说，算是裸聊的一种衍生品。但是配合秀场类网站摸索出来的优化变现经验，也有一定的发展。

但是和裸聊一样，由于秀场类网站风险太大，再加上不断的打击已经没落。反而是一些地产产业开辟了录像秀场的模式，即用录像代替了人开辟地下秀场网站，当然也是骗的过水流量用户，不过也能在地下流量采购上，形成一点规模。但是秀场类在移动端，却是另外的一幅场

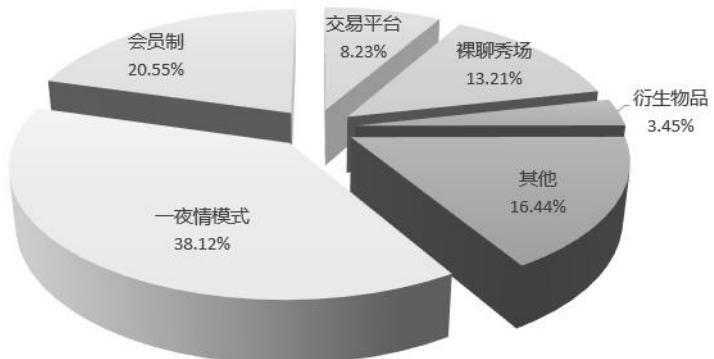
景。

E. 移动端色情应用相关深度分析

上述所有的模式，几乎都有在移动端应用中体现。移动应用由于私有性更强，几乎是完美匹配色情网站的各种模式。特别是约炮概念的炒作，让一夜情模式在手机客户端上更是发挥的淋漓尽致：附近的人、摇一摇、雷达等各种产品形态无缝迁移。

而且移动应用更容易躲过监管，风险更小。再加上微店模式催生了各种付款网管的产生，也让相关的地下产业环境变得更优化。而且由于用户体验的更加优越，也让秀场类变现在移动端得到了非常不错的发展空间。

监控移动流量流入地下产业链色情变现类中变现模式细分
(2015年10月份数据)



Data Powered By **TOMs**
Insight

网络培训与传销相关产业链分析

7

A. 相关地下产业链整体深度分析

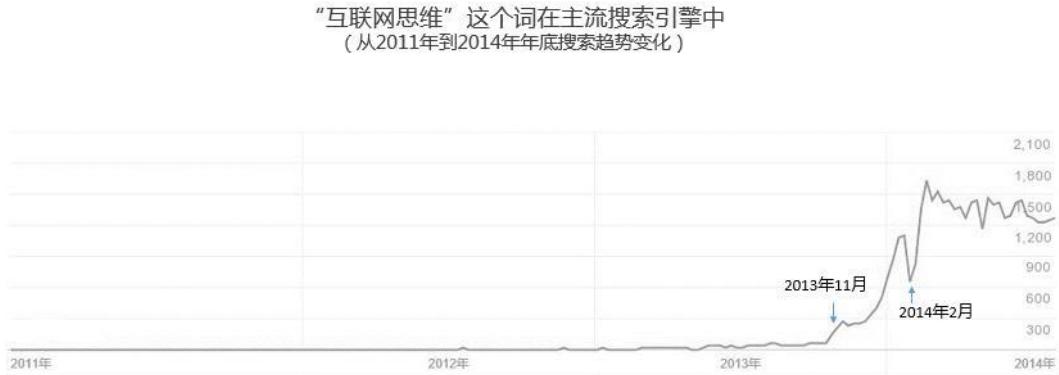
地下产业链也是一个很有意思的地方，在这个江湖里面，最牛逼的是开创新的变现方式，被人尊敬的是那些黑客们，当然如果你有能力搞定一个暴利品牌也是被人敬仰的。如果不及的话，也可以去做色情变现，去做路径引流，等等等。

但是千万不要去做网络培训。在互联网地下产业链中的网络培训，就好像美国监狱中的强奸犯一样，被人唾弃和不齿。我们也不知道这个文化氛围是怎么形成的，估计是网络培训是以忽悠为主，没什么技术含量，在相对讲究 Geek 文化的地下圈子里面，没人能瞧的上。

但是不管如何，网络培训毕竟在变现盈利产业链中占据重要一环，我们还是来分析一下。

B. 网络培训包装与推广深度分析

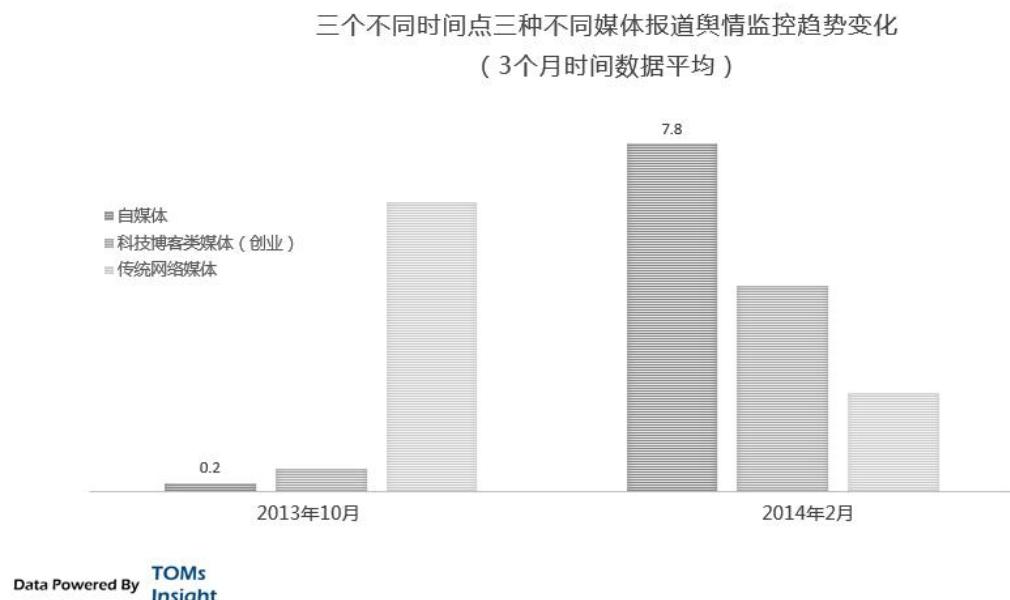
其实网络培训的主流产业很地下产业在内容本身上很难分的清楚，主流产业是通过包装一系列的词和概念而获取权威性，我们先看看主流的互联网培训如何包装“互联网思维”这个词。



Data Powered By **TOMs**
Insight

关键的两个时间点：2013年11月和2014年2月。2013年11月，中央电视台推出系列报道“改革发展新景象”，而这里面有一个非常重要的主题报道：“互联网思维带来了什么？”在这个报道里面，介绍了小米、海尔等公司的互联网模式，把一些互联网上的创新方法提到了“互联网思维”的高度。

这对于互联网培训公司是一个极其好的意识形态切入点和极佳的炒作概念。于是从2014年2月开始，互联网培训公司开始抱团忽悠，我们看下图三种不同的网络媒体（自媒体、新科技媒体、传统网络媒体）在这三个时间点上的关于互联网思维报道的变化：



培训公司已自媒体人为带头大哥开始在2014年2月份开始传播，而传统媒体更紧跟主流意识形态早已经在2013年10月开始报告过一轮并且热度降低了，而科技博客媒体在其中位置。

这是一次典型的培训公司的包装行为。

而地下培训产业由于面向的用户群体更加草根，所以在包装上也独具特色：“魔鬼超级营销人、兄弟们网络科技CEO、微营销界疯子、微营销创新品牌缔造者、在线教育界隐士复出、移动互联网界超级实战家、2011年自主创业，创办过67家公司，每天有1.5万人走

进微创 新营销兵法讲堂，微营销 O2O 移动商城发布 6 天即有 4.7 万商家入驻。公司每年营收达 10 余亿，10 个互联网界大佬有 9 个听过我们的课！“

这些是不是看起来很眼熟，如果是，那你也被地下网络培训产业所波及过。

仅仅如此并不是地下产业的网络培训的本质，我们接着分析。

C. 培训内容定位与用户数据分析

地下网络培训的内容更多的是定位在一些比较虚的、热点、能带来实际效果的一些内容分享，其实这些和火车站、机场书店的那些营销大师、沟通大师、生意大师系列没有多少不同，只是把内容转移到互联网上而已。

对于地下产业链的网络培训来说，更多的也是利用地下流量，吸引过水用户，完成变现。如果仅仅如此，网络培训变现也占不了地下变现大概 7% 的规模，关键是网络培训还和传销结合在一起了。

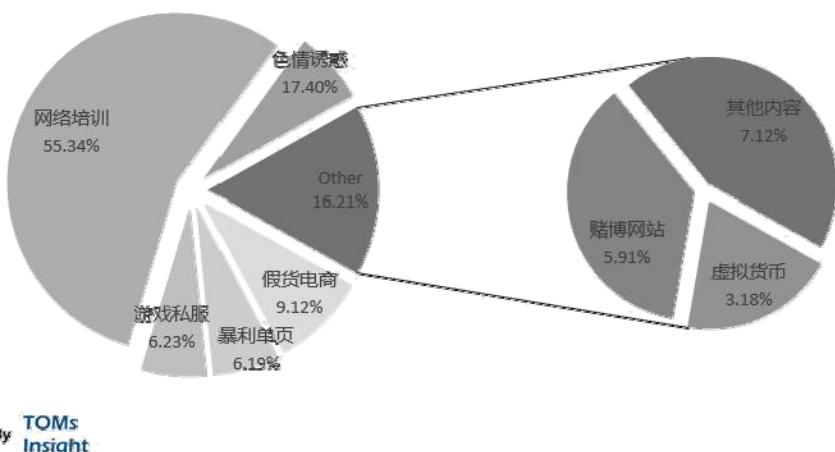
D. 网络传销地下产业链深度分析

网络传销与传统传销是完全一样的模式。传统传销为非法，受到工商部门的密切关注和严厉打击。网络传销使用了隐秘的不公开的手段，它的得利方式同样是交纳会费（或说是享受产品），然后再拉人进入作为自己的下线，如此炮制，这种方式与传统传销没有本质的区别。

所以其实网络培训本身并不能多赚钱，而变现方式确实下线的会费，材料费，体验培训费，代理费等等各种名目的费用。而培训大师有时候也只是这个网络组织的工具而已。

我们从舆情分析也能看出，大量发展下线的声音充斥着比较低调的黑市，占据了几乎 6 成言论的网络培训几乎成了最高点的黑产。而这也也在一定程度上解释为什么这也是最被人唾弃和鄙视的黑产了吧。

通过关键词分析地下产业链各种变现盈利类型的舆情
(2015年10月份，监控一定量的黑市大号微信群，QQ群言论分析)



E. 传销结合的网络培训商业模式

另外由于和传销相结合，地下网络培训的培训内容，更加以发展下线为导向而不是真正的内容本身，所以就如病毒一样复制，很多培训师都是当年传销出身，有着激情的口才和一定程度上的心理控制水平，所以地下产业链中的网络培训和主流培训的本质区别就是传销的模式。

但是如今主流网络培训也在借鉴，比较赚钱速度远远不能和传销模式相提并论。而且这种模式也在往其他主流互联网产业中渗透，很值得我们注意和警惕。

比特币与山寨币相关产业链分析

8

A. 相关地下产业链整体深度分析

2009 年，比特币（ BitCoin ）的概念由神秘网友中本聪（至今未露面）提出，在开源社区设计，开始只在 Geek 和黑客圈子里流行。到 2013 年，比特币的价值飞涨，引起了媒体的广泛关注，比特币也走进了大众视野。

比特币不依靠特定机构（去中心化），依据特定算法计算产生（挖矿），使用整个网络节点构成的分布式数据存储来确认并记录交易（免监管），使用密码学确保货币流通各个环节安全性、货币所有权、和流通交易的匿名性。比特币总数量将被永久限制在 2100 万个。

比特币的 p2p 技术并不是新鲜事物，这也是互联网的精髓之一：2002 年开始出现的各种基于 p2p 的 BT 下载软件，让很多人真正明白互联网的信息平等贡献的魅力所在。但是把此思想使用到虚拟货币上，还是让人感觉创新的魅力和思维的惊艳。

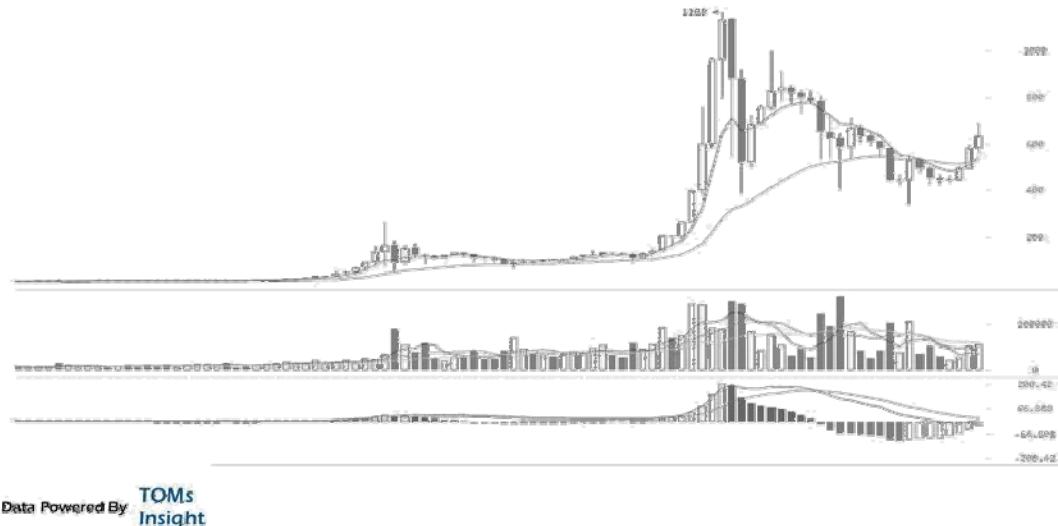
但是我们冷静下来，回归本质。用 100 多年前的货币学经典的费雪方程式来观察下比特币： $MV=PT$ 。式中，M 表示一定时期流通中货币的平均数量；V 表示一定时期单位货币的平均周转次数即货币流通速度；P 表示商品和劳务价格的加权平均数；T 表示商品和劳务的交易数量。费雪方程式在金融学有着物理学相对论的地位，解读上也有很多争议，不过确定的是，货币的价值、流通性和实体经济的交易数与价值是需要匹配。

但是对于比特币来说，这个方程式里面三个变量都被锁死或者降低：M 流通数（越来越多人在持有比特币而不是交易），V 流通速度（没有相对应的真正流通渠道和环节），T 商品和劳务交易数量（比特币覆盖的商家并没快速增加），所以比特币的价值也在升高。

越来越多的人选择持有比特币，等待升值，在交易市场上买卖，而不是真正的去消费，降低了市场上流通的数量。亦而降低了费雪方程中的 M，继续降低 P，所以比特币的价值继续升高。这是一个泡沫形成的过程，所以比特币价格将非常不稳定。

下图可以看到从比特币交易市场产生到现在的 K 线。

从2011年开始比特币在国内外主流几家交易市场上K线表现与相关指标监控



B. 比特币交易平台商业模式分析

从 2012 年以后比特币的交易市场雨后春笋般的出现，首先是国外，接下来是国内。而且相关的新闻和争议也开始越来越多，慢慢的开始有交易平台跑路的情况，而由于缺乏监管和暴力性，相关的变现模式也快速的黑产化。

比特币的交易平台主要通过三个手段变现盈利：交易手续费、沉淀资金，非对等交易。

交易手续费和沉淀资金可能大家都比较熟悉，而且这些这是正规的盈利模式，并不算黑产，我们接下来主要分析下非对等交易。

非对等交易：即由于交易平台缺乏监管，无法保证交易的真实性，导致的虚假交易。举个例子。小 A 今天随便找了一家交易平台，充值了 3500 元，买了一个比特币。下午到了 3000 元的时候，小 A 卖掉了。同样，假设 3500 的时候是另一个用户小 B 卖给的小 A，然后 3000 元的时候也是小 A 卖给的小 B。那么，这个交易平台上交易的是什么呢？这个交易平台上沉淀了那一个比特币么？没有，小 A 和小 B 都根本没见到那个比特币，因为都没有把比特币提现到自己的钱包。再绝对点，有一个交易平台，一天交易了一万次，全部都是小 A 和小 B 这样的情况，就产生了不对等的虚拟交易。再夸张一点，假设这个交易市场一天交易次

数不是一万次，而是十 万次，交易金额几个亿。再加上搬砖用户在不同的平台直接的流动、
和预期性导致的不同市场

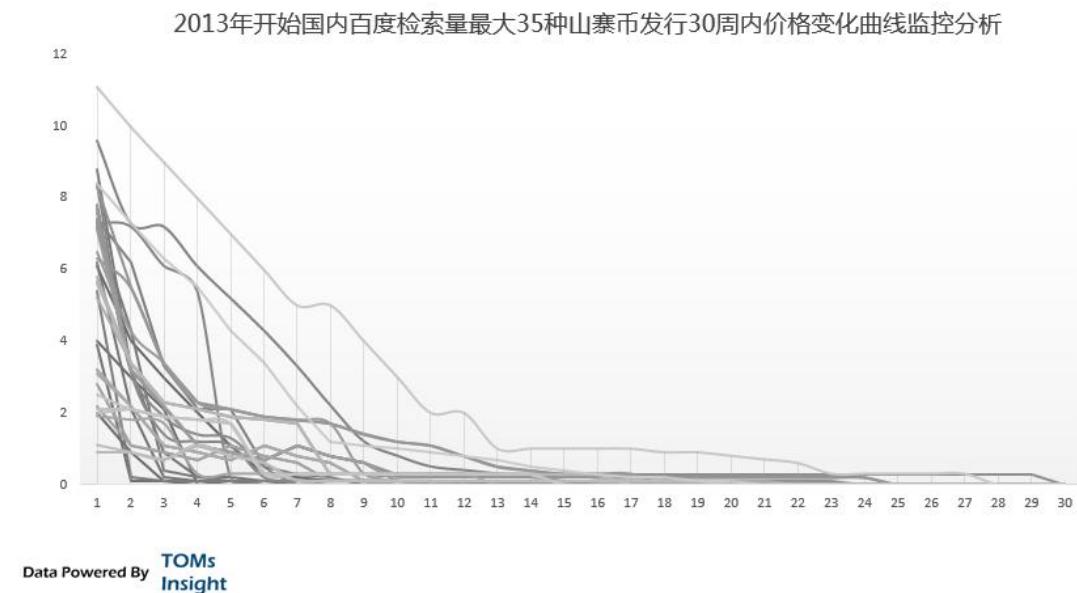
联动，完全可以做多做空整个比特币世界。虽然，比特币的数量是有限的，但是在一个交易平台上的比特币，交易数量可以是无限的。

好比股票交易，股市里交易多少股票是与实际的数量一致，这个一致性是由证监会监管，交易所一天一结算的任务就有保证股票和实际数量等同。而比特币的市场，是失去相关监管机制的。也就早就了这个黑产变现盈利模式。

C. 国内山寨币商业模式深度分析

比特币的交易市场就好比没规矩的地下赌场：不开赔率，散客之间的下注数字不公开，信息不对等。但下注对象比较是比特币，有些黑产想创建完全自己的赌博物品。

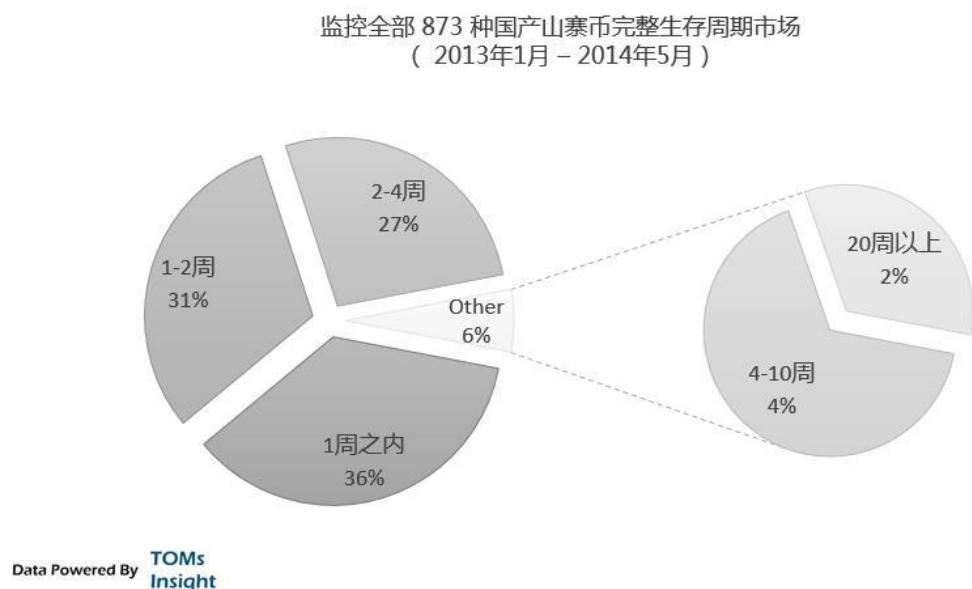
最先山寨币出现在国外，但是更火的确是国产虚拟货币，它们在业内被统一称为“山寨币”。例如：元宝币、烧烤币、马克思币、泽塔币、红币、等等。由于比特币的算法和程序完全开源，所以仅仅需要稍微改动，就可以创造一个新的币种，成本极其的低。



山寨币，其实和比特币有很大的不同，由于目的明确，所以几乎每一个山寨币都留有各种各样

的后门，有的有严重的预挖（先给自己留一部分，再发行），这已经不再拥有比特币的去中心化特征，更有甚者可以随意更改数量，甚至随时发行货币数量。再加上交易市场也是自己的，这已经完全类似私服游戏了。

发行一个新的山寨币，骗一圈钱，马上关门（1个月内），占据了95.3%，这在黑产里面也属于急功近利的类型了。



D. 周边相关地下产业链深度分析

比特币特别是山寨币在地下产业链中的地位不仅仅如此，这是第一次国内的地下产业链涉及到金融行业，虽然是虚拟货币，也让黑产中沉寂的Geek们兴奋不已。

这种虚拟货币的模式在很多黑产变现中得到了推广，并且让很多黑产的从业人员开始进入到p2p金融的领域。我们在此报告并没有分析p2p金融，但是黑产对p2p金融的渗透已经从2014年年初开始。天然的黑市流量，更快更大的变现模型，再加上终端用户即是客户，缺乏监管，p2p金融在黑产中的发展，也是一个水到渠成的事情。

E. 技术与模式变种影响分析洞察

去中心化的技术也给黑产技术领域带来了变更，由于其去中心化技术对逃避监管和打击有着非常好的效果，这也成为 2014 年开始很多地下产业链变现盈利终端中的创新技术，比如在很多赌博网站或应用中，就已经开始使用去中心化的技术来保证赌资的安全性。

比特币的商业模式和技术创新，给地下产业链中变现盈利环境提供了大量的创新空间，但是在主流互联网创新中却没得到很好的借鉴，这也能是更值得我们反思的一件事情。

移动变现数据与移动化趋势分析

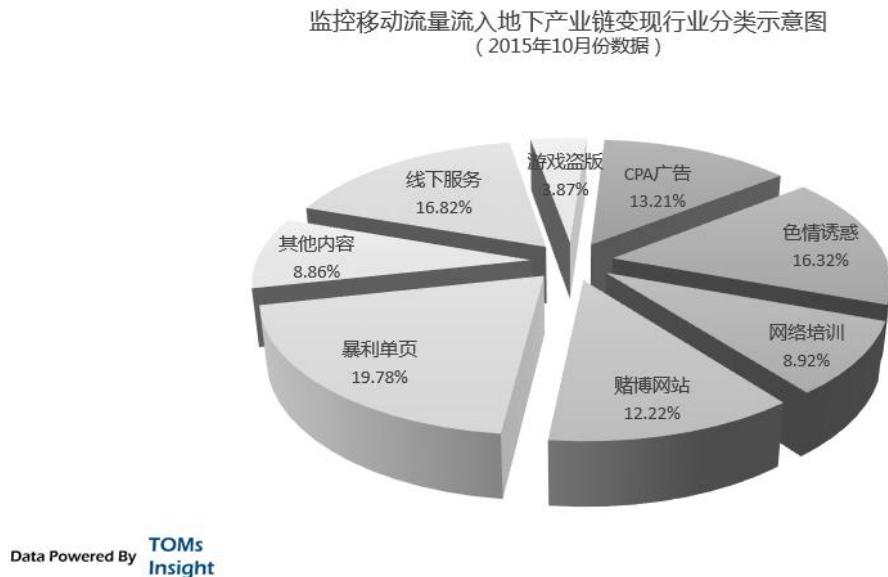
9

A. 相关地下产业链整体深度分析

之前我们已经分析了不少移动端变现的问题，但是由于整体互联网行业移动端发展的趋势，我们还是单独拿出来一章节再分析。在此，我们不再专注特定的一种变现方式，而是广义的移动端变现盈利。

广义上说，任何用户从手机上上网而之间进行消费的，从而变现的，都可以称之为移动变现。移动端流量和 PC 流量相比，由于屏幕的限制，明显有内容展现少，但是停留时间长的特点。而移动端的付款，相对于 PC，有优有劣：没有 PC 的方便程度，但是也会有短信付款这样的快捷方式。

从整体来看，移动变现已经摆脱了 CPA 形式（其实算是流量再分发，并不能真正算成变现盈利终端），开辟了以线下服务为主，暴利单页为辅的变现新模式。



由于移动端的 O2O 属性更强，可以获取的用户的地理位置，对于民营医疗、美容机构、职业教育等本地类服务有着极强的吸引力。而移动用户本身的行为变化，也是一个极大的利好。

B. 移动流量变现盈利的发展趋势

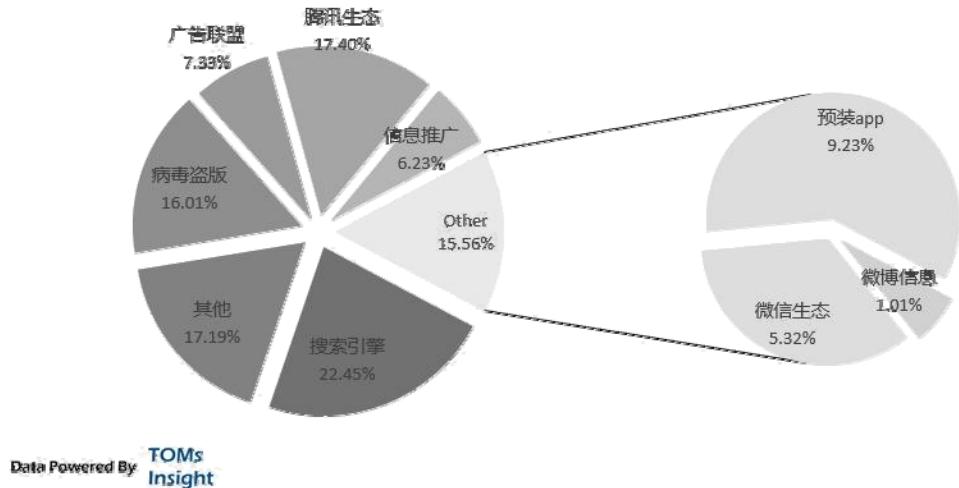
地下产业链的移动流量变现从 2013 年的流量分发 cpa 为主发展到目前暴利单页电商和线下服务为主，不得不说比主流的移动互联网产业要走的更快一些。移动变现一直都是互联网公司研究解决的课题，很多互联网巨头对此投入了很大的人力物力，但是从地下产业链而看，不论是更切合用户需求，顺应用户行为的暴利单页，还是利用地理位置信息，更好服务用户的线下变现，都能更准确的把握用户心理。

从发展来看，任何形式的互联网模式都需要有最终的变现终端，移动流量已经找到了相应在变现终端，而只会更多的发展出更创新的、合理的终端模式。反过来看，主流的移动互联网还处于比拼日活或者用户量的阶段，反而在步伐上落后了些。

C. 移动流量变现盈利的来源分析

从移动流量获取来源分析，搜索引擎仍然占据了重要入口，特别是在搜索引擎生态中的移动流量更容易分离，让来源规模直接得到大幅度提升。而由于病毒盗版的在技术上更容易更猖獗，再加上自带渠道，也让病毒盗版成为第二天的移动流量黑市来源。而由于线下服务变现的高比重和发展，搜索引擎流量可能会越来越爆发出价值，而百度最近的股价最近的优异变现，也不能不说是对市场预期的乐观。

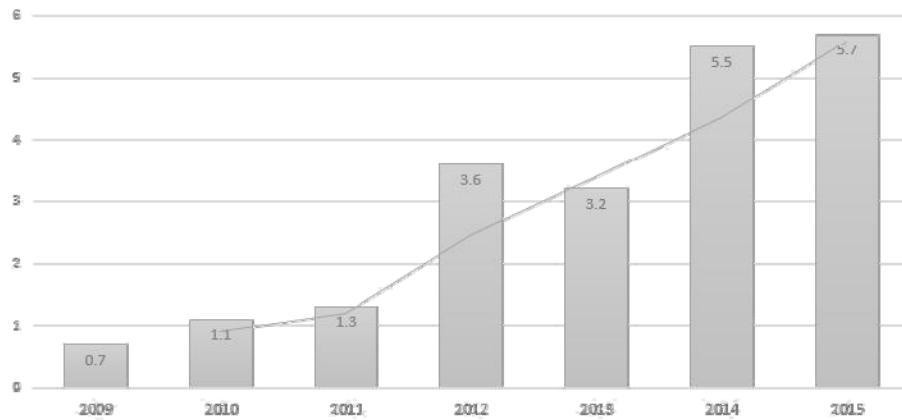
2015年6月-12月地下产业链移动流量各种来源比例
(通过地下产业链的变现模式，反推追踪流量来源计算)



D. 移动流量变现盈利的交易分析

地下产业链中的移动流量变现更多的依赖流量方，很少可以自己供给流量的。这是和主流移动互联网产业的创新的一大区别。而对于移动流量的采购，有时候也可以看出来整体的移动流量需求的趋势：

2009年至今，地下产业链移动流量购买CPM价格
(抽样统计及算法预估，一些CPA通过算法估算成CPM)

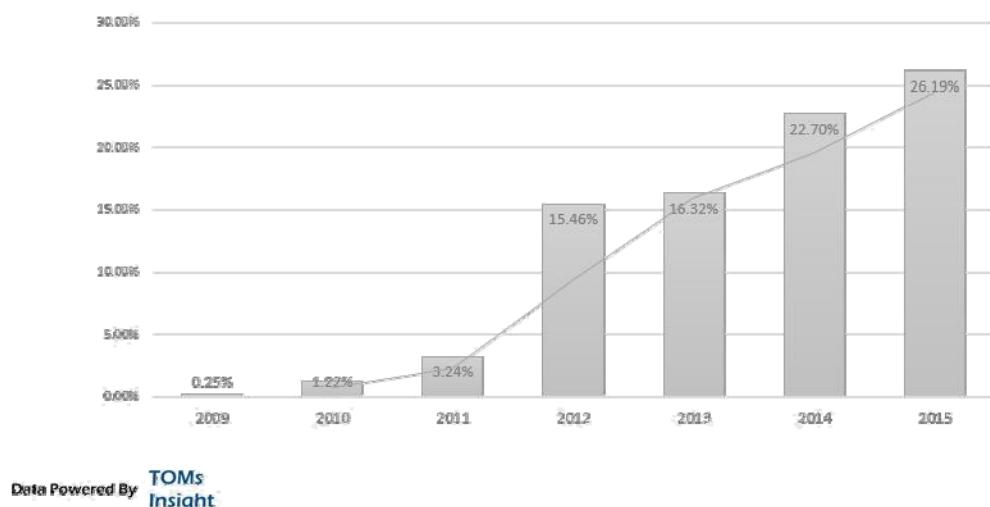


Data Powered By **TOMs**
Insight

E. 移动流量变现盈利的深度数据

最后，在地下产业链中的移动流量获取分发的整体比重，也从 2010 年的 0.25%，提高到了目前的 26.2%，而我们也可以估算出相关的移动变现盈利产业的增幅大小。

2009年至今，地下产业链流量分发中移动流量占比
(通过地下产业链的变现模式，反推追踪流量来源计算)



总结与洞察启示

在主流的互联网创新圈子中，盈利模式好像是一个很难开口的话题，甚至成了私下约定俗成不谈的一个问题。这在一定程度上和互联网圈子资本的变现方式有关，而更多的是长期以来的观念传承：先有用户、先有影响力、先有市场站位等等，然后就会有高额的收入回报，预期就是美好的。烧钱模式一直持续，甚至到上市后还找不到合理的盈利方式。

变现盈利不被主流互联网圈子重视，或者没人专注在此研究，成了一种很流行的现状。并且此风越刮越烈，好像变现盈利是一种很不互联网的行为，好像变现盈利和互联网的快速发展是相违背的，好像上市被并购才是互联网创新的目的，反而忽略的商业的本质。忘记了自己的初心，盲目的追风甚至是为了创新而创新。

地下产业链的变现盈利，更直接粗暴，由于其风险性和非法性，反而要求在短时间内尽可能多的变现。这让地下产业链中的变现产业几乎把所有的专注点都放到优化上。不可否认，这种优化是通过伤害用户作为代价的。但是作为主流互联网风气的另一个极端，在很多程度上，都非常值得我们学习与借鉴。

另外，由于地下产业链的变现在一定程度上推高了流量的价格和相关的服务价格，让很多创新者并不能客观的认识行业中的一些现象，盲目的去竞争或者去进入一些流量已经被推高的细分产业，或者地下产业链变现集中的细分行业，也会承担更多的成本风险和竞争风险。而此时，正确客观的去看待分析地下产业链也是必要的。

四、数据信息安全相关产业链部分

流量分发和变现盈利构成了互联网的基本形态，但是和其他行业一样，周边的服务产业和相关衍生产业在一定程度上更决定了整个行业生态环境的发展。

互联网地下产业链更是如此：为了规避风险和专注创新，拉长产业链条，更精细化的合作也是其发展趋势和方向。与此同时，所有周边衍生服务，几乎都围绕着数据信息安全来做文章，这是互联网地下产业链的技术核心，同时也是对终端用户影响最大的一部分。



数据信息安全相关产业链部分整体分析



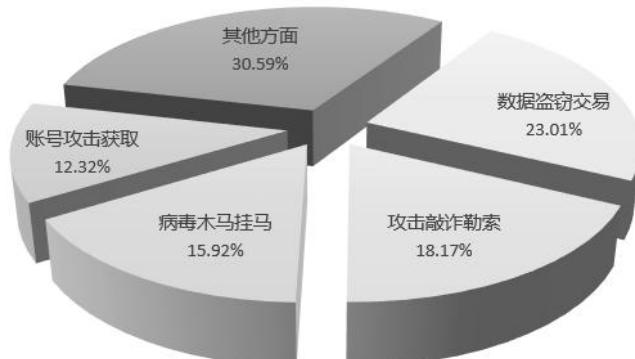
A. 数据信息安全产业链整体情况

地下产业链最早的起源是黑客，而黑客却是一种极端的 Geek 精神。我们很难形容这种意识形态，但是几乎全部的黑客都会把自己形容成海盗：自由、冒险精神，藐视规章制度、有过硬的航海水平、寻找宝藏。很多黑客认为网络本身应该是完全自由的，就好比大海是属于任何人的。这种网络海盗的思维形成了最早的一批黑客。

但是在国内的情况会变得更加特殊，由于国情决定了经济发展的不均衡和贫富差距，大量的技术天才并不是为了追求自由来到这片海洋，而是纯粹的财富。于是一次次刷新道德下线，而这些人也从硅谷黑客变成了纯粹的生意人。

国内互联网地下产业链发展到今天，黑客技术更多的是为黑产服务，而成为产业链中的一环。黑客技术能够成为很多地下产业链的核心资源，能对黑产的生产力有几何级的放大作用，也是很多黑产商业模式能够成立的关键。我们可以从下图看到黑客技术在地下产业链中的大概使用分类：

2015年10月地下产业链黑客技术使用方向分类
(通过抽样调研、专家网络、舆情监控、统计模拟整体情况，并不代表客观真实情况)



Data Powered By **TOMs**
Insight

当然，与此同时，数据信息安全也会对终端用户、主流的互联网产业造成很大的风险和影响，甚至对一些主流的互联网创新造成毁灭性的打击。

B. 细分产业链之间生态关系分析

我们通过六个细分产业链来分析地下产业链中的数据信息安全部分，分别是数据窃取与非法交易、网络攻击与敲诈勒索、病毒木马与挂马、人海战术与挂马产业、账户安全与认证以及网络诈骗。由于很多相关的模式以及融合在别的产业链中，已经在报告之前的部分中分析过，本部分着重在相关行为本身的分析。

在此部分，病毒木马与挂马、账户安全是地下产业链的基础服务，数据窃取、敲诈勒索、网络诈骗是目的所在，也是一种变现手段，人海战术与打码相关是一种方法。其本质各不相同，但是都在错综复杂的融入了地下产业链，成为理所当然的服务。

同时，和之前的流量获取与变现不同，数据信息安全很多时候都影响了主流的互联网产业，造成很大的风险和相关的隐患。由于情况的多样化，我们在此不会具体分析风险和隐患，但是希望能给大家带来相应的警示和洞察力。

C. 数据信息安全的黑市深度数据

地下产业链的黑市上，交易最火爆的其实并不是流量，而是数据信息与账号。数据信息与账号作为很多黑产的基础，是很多产业链必要的生产资料。

比如如果要大量发垃圾邮件，需要发送人的邮件地址，和用来发邮件的地址；通过盗版的 app 获取移动流量，需要大量的安卓市场账号以及 Google Play 账号；刷淘宝信用需要淘宝账号；注册微信公众号就需要手持身份证照片，等等。

更深度一些的，深度赌博平台可能需要一个用户的详细信息，甚至征信报告；精准的黑市流量需要直接从主流的互联网网站的数据库中直接获取；信封号产业链中有些人为了盯一个有价值的号或者有足够装备的号会收集信息很久并潜伏，再到构建社工库，等等。

这些交易几乎是黑市中最深度的部分，另外还有一些定制性交易，直接指向某一特定的网站或者数据的数据获取，有更大的牟利空间。而另一方面，最基本的用户信息，普通的身份证信息，电话号码、邮件信息，则以更快速的方式传播，反推到主流的互联网领域、甚至传统行业，有时候已经很难弄清楚到底采购者是谁了。

数据窃取与非法交易产业链分析

1

A. 相关地下产业链整体深度分析

用户数据泄露一直是主流互联网行业媒体的焦点，从最近的京东撞库事件，到之前的 csdn，一些快捷酒店的用户数据泄露，网站和黑客在用户数据上一直在进行着旷日持久的攻防战。

而数据窃取与交易这个细分领域也几乎是地下产业链隐藏的最深的一部分，很多在互联网地下产业链中沉寂了多年的大佬都并不了解此道的相关信息。而不断的爆出来的信息类似 csdn 的脱库事件，其实对于地下产业链来说，都已经没有任何价值的数据而已。

而绝大多数被盗窃后的网站数据，并不会公开与众，只是交易后进入到地下产业链的其他环节而已。所以目前到底有多少网站的数据已经被窃取我们没法客观的分析。在黑市中，大家说起来类似的问题，常用的一个词是“十墓九空”，也许这个说法有点夸张，但是也可以参考。

我们从 09 以来，通过黑市的专家网络调查，对互联网每年的流量排名前 100 的网站（刨去没有用户账号机制的）进行调查，结果如下：



如此高的比例，让人惊讶。但是从社工库里面的数据信息来看，几乎 8 成比例的数据泄露，也并不是空穴来风。

B. 数据窃取相关产业链深度分析

数据窃取产业虽然隐藏的非常深，但是发展历史悠久，地下产业链也随之成熟，对于如何把数据变成货币，已经有了非常完整的程序的分工协作渠道。从手段上来说，也包含技术入侵、社会工程学以及高级持续性威胁（APT）。

而其模式却相对简单的多，一般只包括：脱库、洗库、撞库这几个阶段。

在地下产业术语里面，“脱库”是指入侵有价值的网络站点，把数据库全部盗走的行为，因为谐音，也经常被戏称作“脱裤”。在取得大量的用户数据之后，黑客会通过一系列的技术手段清洗数据，并在黑市上将有价值的用户数据变现交易，这通常也被称作“洗库”。最后黑客将得到的数据在其它网站上进行尝试登陆，叫做“撞库”，因为很多用户喜欢使用统一的用户名密码，“撞库”也可以是黑客收获颇丰。

在早期的数据窃取过程中，这几个阶段几乎都是由同一个团队、甚至单个人来完成的。发展到今天，已经完全细化成产业链，很少有人从脱库、洗库一起做了，而变成定制化，或者交易化模式。

所谓的定制化，就是先有下游客户指定的某一家网站，然后聘请黑客去脱库，脱库后获得佣金的模式，在定制化模式中，有很强的黑产规矩即数据属于下游客户，而黑客不可以再次出售，或者在一定的窗口期内不能再次出售。

交易化模式即黑客去某一家网站脱库，脱库后直接在黑市上寻找下家，在这种模式下一般可以反复出售，但是由于风险较大，而且数据真实度和新鲜度不一定能得到保证，又充满了骗局，越来越没落了。

C. 数据交易相关产业链深度分析

除了贩卖数据本身得到金钱上的利益之外，黑客还会把得到的数据进行整理，制作成社工库（Social Engineering Data）。社工库可以对其他网站进行撞库攻击，撞库攻击实质上就是，以大量的用户数据为基础，利用用户相同的注册习惯（相同的用户名和密码），尝试登陆其它的网站。

这是一个放大的效应，由于社工库的日益庞大，信息的日益完善，再加上时间的沉淀，很多数据都可以慢慢地浮出水面，可以获得相当多的信息。目前有一些公开的社工库，信息全面性和对于用户隐私的了解已经让人震惊，但是这才是仅仅公开的社工库，对于黑客们来说其实已经是没有什么价值的信息。真正地下产业链中的社工库的数据信息丰富程度要远远更大。

利用社工库，和黑客之间的数据交换，可以让数据再次变现。一是通过虚拟资产：用户账号中的虚拟货币，游戏账号，装备，都可以在黑市上出售；或者是金融犯罪：金融类账号比如支付宝，网银，信用卡等账号和密码用来进行金融犯罪诈骗。

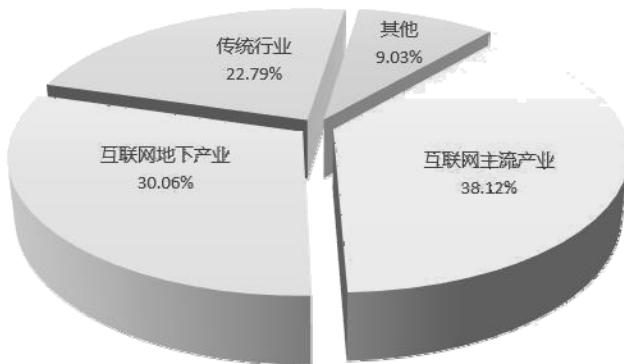
最后，全面的社工库基础数据，也是精准的流量获取来源，成为流量获取分发的地下产业链的基础服务和大数据服务商。

D. 数据购买下游产业链深度分析

我们看完了黑客对数据的洗库，但是之前有分析，这些数据其实都是下游的客户定制的，而下游客户定制某特定一家网站的脱库，是怎么盈利呢？

大多数时候，都是竞争对手或者上下游企业采购，而且大多数都是主流互联网产业链中的客户，甚至是传统企业客户。其实这个模式很简单，想一想在生意场上，这家网站的数据库对谁谁有利，谁就可能是潜在的定制客户，只不过由于很多主流互联网企业或者传统行业很少了解这个地下产业，所以就会有一些中间人，来做中介促成相关的生意，而这些中间一般情况就是黑市里面的买家或者定制客户了。

地下产业链数据窃取定制客户来源 (2015年7月调研)
(黑市专家网络调研获取数据，与实际情况可能有所出入仅供参考)



Data Powered By **TOMs**
Insight

E. 数据黑市交易情况与相关洞察

从 2013 年以后，数据的黑市交易更加隐蔽，而且呈现严重的分层：一些大的数据盗窃团伙早已经完成早期的数据积累构建非常完善的社工库，对于一般的数据定制需求都不会再接，会专注于更深度变现更强的金融诈骗；而一些小的数据盗窃团伙还在不断的相互交易、交换数据、而且相对高调的浮出水面，其实危害反而没有那么大。

而且出于用户交互方面的考虑，越来越多的终端支付或者金融产品的安全策略略浅，再加上更丰富的网络电商活动，导致沉寂在黑产中的数据危害也越来越大。这可能也会是更多的互联网产品的设计时需要考虑的问题所在。

网络攻击与敲诈相关产业链分析

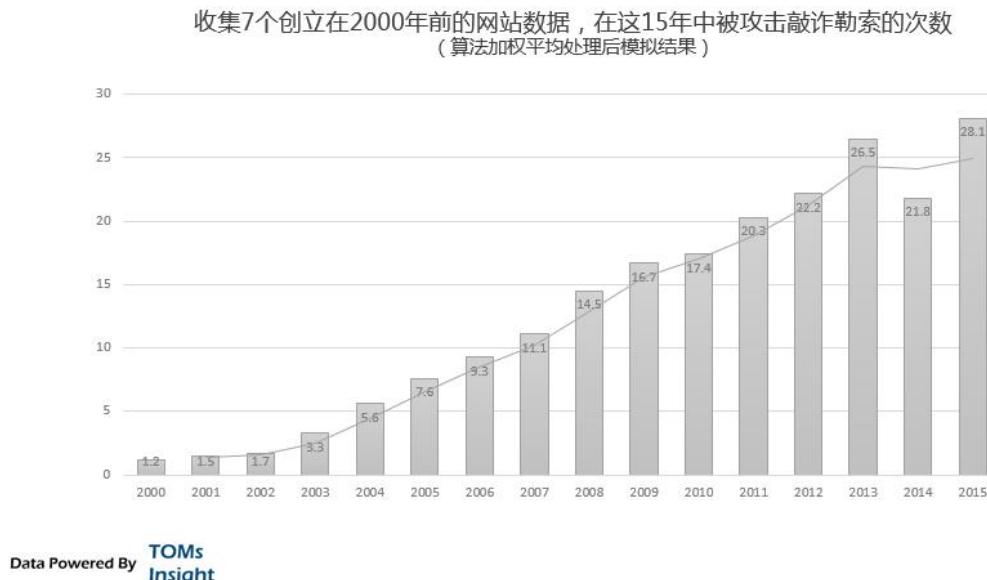
2

A. 相关地下产业链整体深度分析

对于所有的中国互联网中小企业主、创业者、站长来说，网络攻击敲诈勒索都是横着眼前的一道非常现实的关卡。为什么我们要把“敲诈勒索”要和“攻击”放在一起呢，敲诈勒索的法律定义是“以非法占有为目的，对被害人使用威胁或要挟的方法，强行索要公私财物的行为”，现实社会中由于人与人之间关系的复杂，可以通过各种方式来抓住把柄、或者依仗势力进行威胁要挟。而对于互联网而言，一切反而回归到最简单，那就是先攻击，后敲诈勒索。

在 2002 年之前，网络攻击敲诈勒索行业发展缓慢，主要是那个年代的中国互联网经济还处于烧钱状态，直接变现机会很少。稍微成点规模的敲诈也就存在于网络新闻领域（后面我们会具体分析），所以那个年代的互联网记者地位那也是相当高。但是 2002 年以后，网游和电商的发展让互联网有了直接变现的渠道，所以也导致了攻击敲诈勒索行业也迎来了自己的辉煌。

下图是我们调查了 7 个创立在 2000 年前的网站，在这 15 年中被攻击敲诈勒索的次数，由于网站类型和规模不同，我们通过算法处理加权平均，仅仅供大家参考趋势的变化（可以看出 2014 年净网行动还是很有成效）：



到了最近几年，这个产业已经形成规模，从低端到高端都有细分产业链的形成。大概分类成：人肉型、信息型、技术型、创意型等其他类型。接下来我们逐一分析。

B. 人肉型攻击敲诈勒索深度分析

人肉型是指那些纯凭人工完成的攻击，这也是中国互联网的一大特色。近几年有一些人肉型攻击者，通过 QQ 群、YY 群组织几千人甚至几万人的大规模团伙，有组织有纪律的去完成任务，形成极大的力量并有独到的优势来骗过代码。

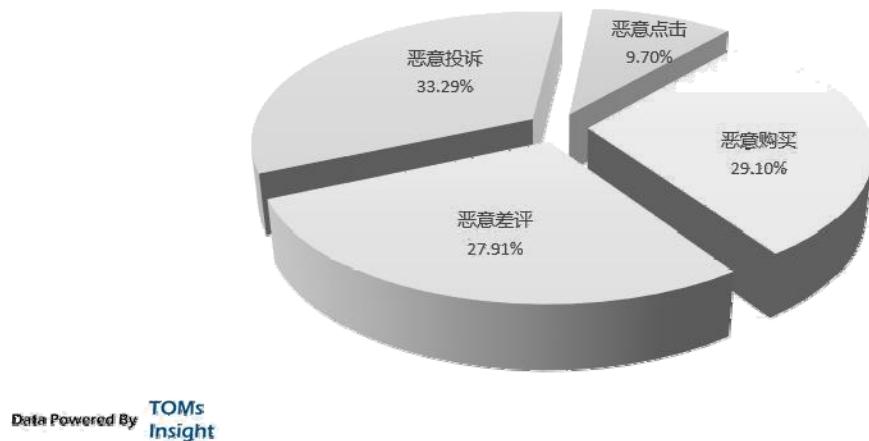
恶意购买：针对货到付款的服务，特别是百度生态圈的竞价单页、或者是一些特殊垂直行业电商网站（例如成人用品），通过物流公司的代收费业务，货款由物流公司代收。人肉攻击团伙采用下假单的方式，由于找不到用户，只能把邮包再退出来，一发一退对于受害者来说就是几十元的成本。接下来攻击者就会去受害者和谈，一次性或者每月收“广告费”、“公关费”、“营销费”、“顾问费”等打着各类名义的敲诈勒索费用。

恶意差评：差评师主要存在淘宝网，大家可能比较熟悉。差评师对卖家伤害很大，皇冠级别的卖家来说几个差评起不了多大作用。而对于心级卖家来说，几个差评基本上就宣布店铺倒闭了。交纳了保证金的卖家都是诚心想要把网店做好，为了自己的生计，多数卖家会选择忍气吞声的交钱。差评师会注册很多小号，拍店铺商品的时候十分爽快，但买回之后，问题就一连串地找上门来，称要给你选差评，店方老实地给了钱还好，对于店方比较强硬的，差评师们死缠烂打，团伙作案，大规模作案，直到就范为止。

恶意投诉：恶意投诉主要针对京东、亚马逊等平台的第三方加盟店，这些平台并不存在淘宝那么核心的信用等级机制，但是非常看重加盟店的信用口碑。攻击者一般会用几十个甚至上百个 ID 去受害者店铺去购买，然后去平台投诉买到了假东西、不开发票、存在欺诈、服务不到位等等。由于投诉众多，平台一般还是会审核整治，甚至撤掉资格。由于成为京东、亚马逊等平台的加盟店都会有一定的资质审核和保证金要求，所以店主更多的时候也希望息事宁人，交保护费了事。

恶意点击：恶意点击是针对网站的广告投放。比如说 CPC 广告，是按照点击计费，百度的 CPC 广告每一次点击都几元甚至几十元。攻击者采用人肉战术，每天几百几千人去点击受害者网站的广告，直接造成大量的广告费用浪费；再比如在 app 分发领域的 CPA 激活，攻击者定向下载 app 再卸载掉，造成极大的广告费用浪费，对中小创业者来说是致命打击。

2015年H2电商行业数据，四种类型人肉型攻击敲诈勒索所占的比例
(随机调查918家网站，样本有限比例仅供参考)



C. 信息型攻击敲诈勒索深度分析

人肉型攻击敲诈勒索几乎没有什么技术门槛，就是组织大量的人有纪律的捣乱。而接下来信息型的攻击敲诈勒索，就开始有一些门槛了。

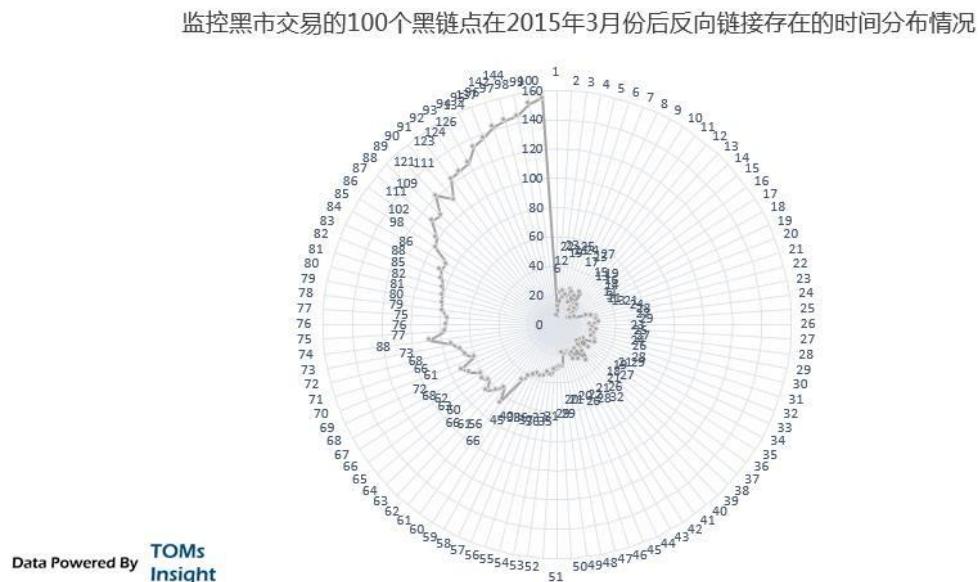
媒体负面信息：媒体通过负面消息敲诈好像已经不算什么黑市的分析范畴了，已经成为了一个行业常态，所以我们在此也不再拿出来多说什么。值得一提的是，大多数媒体负面消息并不是媒体本身所为，而是一些记者、编辑。在黑市上，很多网络媒体的记者、编辑直接明码标价负面新闻，而大量的攻击者在黑市上去购买这些发文权，有目的的去攻击，最后敲诈勒索的也是这些攻击者，记者编辑只是产业链中最底层的一环，而网络媒体只是被利用而已。

水军负面信息：水军负面消息是用大量的 ID 去发帖子、博客、知道问答、微博等，在网络上给某一特定受害者造成负面影响。在 2010 年之前，这些信息主要都存在与论坛上，但是在 2010 年以后，攻击者很少采取用这些的大量水军负面消息了。攻击敲诈勒索关键是为了钱，受害者交了保护费后就需要放过，不然怎么能有连续收入。但是水军负面信息，发起来容易，删起来难。比如天涯论坛信息后不能删帖，必须版主完成，而水军采取发帖机发帖，删除有很大的难度。目前升级成 SEO 负面消息手法。

SEO 负面信息：SEO 负面消息主要是指攻击者利用搜索引擎，我不发你很多负面消息，只需

要在百度上搜索你的品牌或者关键词，前几页都负面信息即可。这足够造成破坏，而且这些前几页的负面信息都是攻击者可以控制的，说删就删，而主要技术是使用黑链。攻击者简单的通过程序模版加数据抓取，制作一批新闻类、博客类的网站，通过关键词优化和黑链技巧，快速的把自己网站上的一些新闻在每一个特定的关键词上（一般是受害者品牌相关词）优化到前几页，这样，完全可以控制信息，收钱后秒删。

下图可以看出来，大多数黑链目前链接存放时间都在 40 天之内，而这个时间绝对只能是恰好 做好优化后就删除，这些黑链的作用也很明显了。



D. 技术型攻击敲诈勒索深度分析

技术型攻击敲诈勒索和之前都不一样，攻击者利用黑客技术，敲诈勒索的金额放大很多倍。当然，这些技术的运用，也有更大的成本，这里面就包括网络攻击的第一常规性武器：DDOS。

DDOS 攻击在国内有两种情况，一种是黑客控制大量肉鸡网络（被黑客控制的电脑）进行攻击，或者是拥有带宽资源的 IDC 机房背地攻击。后者多出现在一些很特殊的情况下，而对于网络攻击敲诈勒索，主要是前者。

在这个产业链中，黑客一般不会直接参与攻击敲诈，只提供肉鸡网络的使用权；DDOS 攻击服务提供商租用肉鸡网络进行攻击；而攻击者去购买 DDOS 服务。所以这种三层模式中，攻击者的成本是相当的高，特别是一些有规模的网站都有足够的带宽去扛 DDOS。所以与之对应，一旦到了 DDOS 攻击的地步，相对的敲诈勒索金额也会随之增加了。

对于一些特殊行业的 DDOS 的攻击敲诈是可以产生暴利的，特别是讲究实时运行的网站，例如之前一段时间火热的比特币交易平台，或者电商网站的抢购时段。

DDOS 的攻击黑客是不屑于参与的，但是黑客也会直接充当攻击者，主要是对网站的用户数据进行入侵并获取，即我们之前说的脱库。一旦获取了网站的数据库，就会直接联系改网站进行“赎回”，并威胁一旦不赎回，就会进行“撕票”。“撕票”的意思就是公开受害者网站的用户数据库，由于此威胁是一次性的，有些网站还真的不会赎回数据库，例如历史上有过几次著名网站的数据库泄露，也是属于“撕票”。

E. 其他攻击敲诈与周边黑产分析

以上是目前基本的攻击手法。但攻击敲诈勒索行业发展至今，开始出现了各种创意型的手段，各种组合拳的运用，让人防不胜防。比如“在黑市上购买数据，针对一些个人深度数据的攻击与个人敲诈勒索”，“对那些可以 QQ 登陆的网站，通过大量的信封号消息，留下这个网站的名字栽赃”等等。

而和攻击敲诈勒索相关的产业，比如说网络中间调停人之类的奇怪产业链也开始渐渐出现，虽然没有形成规模，但在也在一个发展的通道上。

病毒木马与挂马相关产业链分析

3

A. 相关地下产业链整体深度分析

计算机病毒（Computer Virus）是能自我复制的一组计算机指令或者程序代码。而木马（Trojan）这个名字来源于古希腊传说，是目前比较流行的病毒文件，与一般的病毒不同，它并不“刻意”地去感染其他文件，只是向施种木马者提供打开被种主机的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。

在互联网发展起来之前，病毒更讲究传播性，和破坏性，当时的病毒的使用目的和目前也很大的不同，更多的是一些比较宏观的破坏作用和一些地下产业链变现。到了互联网时代，已经很少有纯粹的病毒了，更多的是以木马的性质存在。而也有一些木马带有病毒的性质，可以自我复制或者通过网络自动传播。在此我们只分析目前流行的木马型病毒。

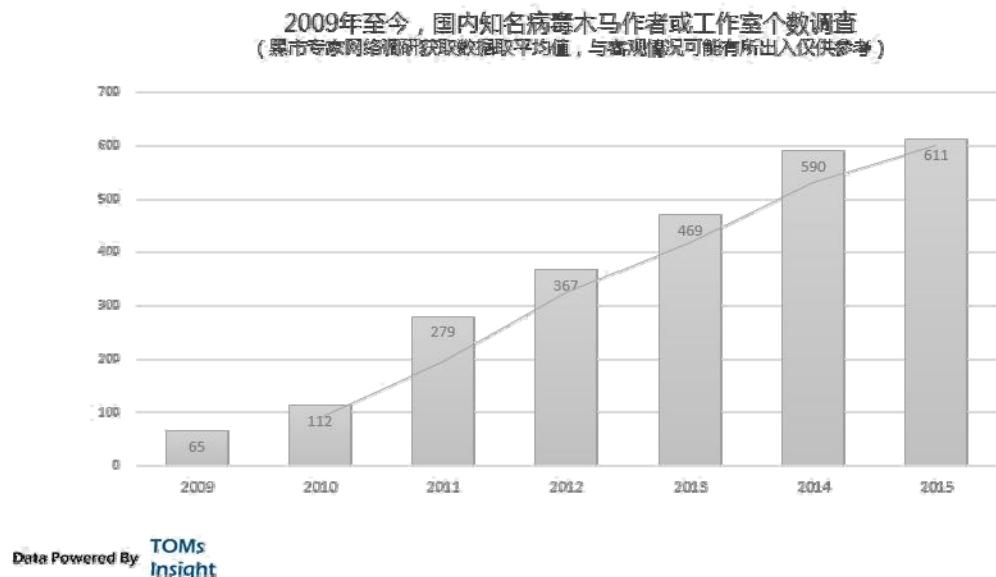
首先是病毒制造者，在黑市上被称为造枪。一般是一些黑客或者黑客工作室，针对不同的目标开发不同种类的病毒木马；接下来是卖枪，只指销售病毒木马；再下游是拿箱子，是指购买木马的盗窃实施者；再下游是挂马，一般由代理的形式将木马通过各种方式，大多是植入一些网站，或者在黑市采购流量，尽可能多地传播出去；最后是开箱子，把盗取的数据信息拿出来，通过分销打包转卖给买家，或雇人洗信；最后相关的数据信息在黑市出售，流到我们之前介绍的各种细分产业链中。

而主要变现方式和之前的数据盗窃的变现类似，通过虚拟资产：用户账号中的虚拟货币，游戏账号，装备，都可以在黑市上出售；或者是金融犯罪：金融类账号比如支付宝，网银，信用卡等账号和密码用来进行金融犯罪诈骗；最后剩下的数据可以完善社工库。

B. 病毒木马制作者深度解析分析

由于对病毒木马作者的打击力度较大，所以从业者一般都异常低调。其实大多数病毒木马的作者并不是大家想象的那些拥有多么高深的技术，由于国内网民对安全防范意识普遍不高，很多比较低级的木马反而也可以占据一定的市场。

互联网地下产业链最近几年的繁荣，当然也吸引了一些高手加入到这个行列，据我们在黑市的专家网络调查，大家普遍的认为很多作者或者工作室都是一些知名的安全公司从业人员兼职或者离职后所创，巨大的利益也让很多人抛弃了道德和法律约束。

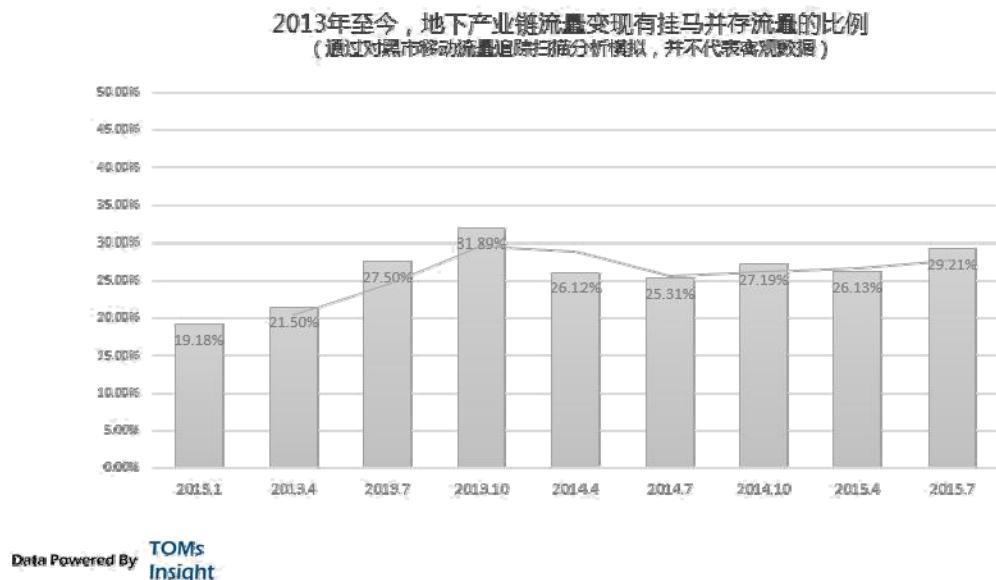


C. 挂马地下产业链深度数据分析

我们在本报告第二部分变现内容中，分析流量变现仅仅是直接变现部分，而并没有分析挂马，但是事实上挂马一直是地下产业链中的流量附加品，什么叫流量附加品呢，就是假设我们通过黑链 SEO 获取了一定的流量，这些流量可能会导入地下博彩产业变现，但同时这个网站上也会挂马，由于挂马并不影响其他变现，所以是一种并存的方式。

而这一种并存也几乎成了地下流量的一种很常态的行为。但是由于挂马很多时候被用户安装的各种杀毒软件发现，影响到其他变现方式，所以虽然是常态但是也不是大规模使用。

我们可以看一些从 2013 年以来，地下产业链流量变现中并存的挂马比例：



D. 病毒木马交易与代理模式分析

在病毒木马地下产业链中，制作木马的黑客并不是出于产业链顶端，而一般都是由卖枪的，或者是拿箱子的，有时候甚至大的挂马工作室。

这也是目前黑产发展到如今的一个现状：技术仅仅是代表核心竞争力，而形成规模需要产业链中各种角色的配合完成，在这个过程中势必需要有可以协调处理各方面利益，发展自己的网络，提供相关的资金，有能力承担风险，而且有一定的地下产业链资源的人出面。一般来说专注技术的黑客在这些工作上并不擅长。

层层代理的分销模式可以让很多利益稳定并且沉淀，也是一种积累方式。而同样这种积累方式也构成了新的竞争门槛，形成了软性的核心竞争力。

E. 手机病毒木马相关产业链分析

关于手机的病毒木马，我们在此前的报告中已经分析了很多内容。但是在此我们需要特别一提的是，这些病毒木马，除了引流、静默 cpa、做数据、暗扣以外，还有一些是搜集手机上的相

关信息，去完善社工库，而达到更大的盗窃目的。

这种病毒木马会潜伏很久而且由于不屑于做那些引流静默扣的事情，让用户很难发现，并且会对用户造成更大的危害，这种类型的比例也在不断的增大。



人海战术与打码相关产业链分析

4

A. 相关地下产业链整体深度分析

人海战术也可以称之为肉战，有时候我们很矛盾，我们不能说他是黑产，但他又是地下产业链中的一环，甚至是核心的方法论：通过组织低廉的人力成本，可以让很多在技术上几乎不可能的事情变成可能，比如会绕过几乎所有产品的安全保护打码机制。而且人海战术也能在攻击敲诈勒索上，刷单产业中，起到关键性的作用。

组织大量的人，也是地下产业链中一种自我优化的过程，很多情况下优秀的组织者被沉淀形成竞争力，而很多主流的产业链在这方面的趋势却没有那么明显，也需要我们反思。

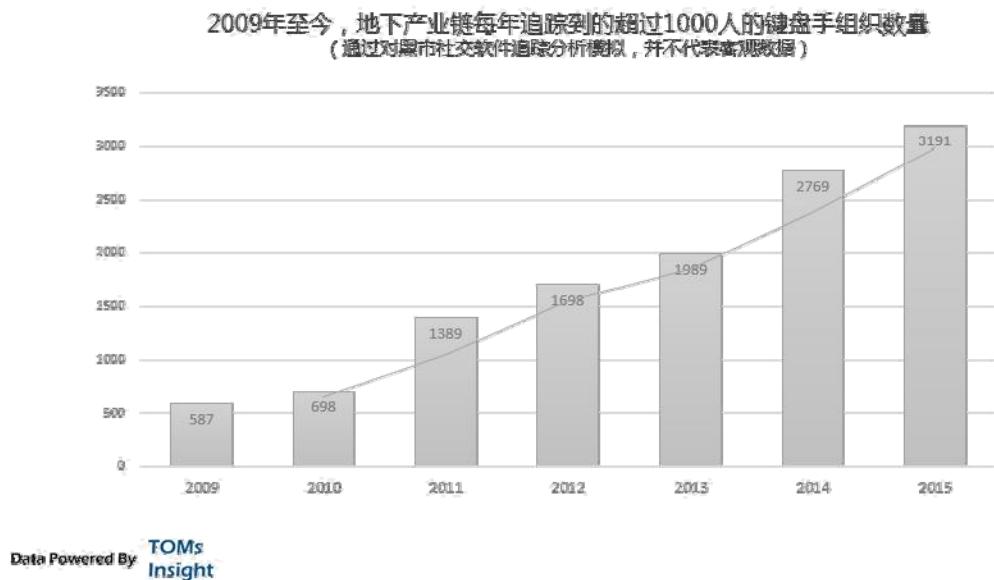
B. 人海战术商业模式与深度数据

人海战术最早大概在 2005 年出现，一些互联网从业人员通过 QQ 群等社交工具聚集到一起，有组织的规模化做同一件事情，最早一般是发帖子、投票。

起源的时候并没有多少盈利性的考虑，但是到了 2009 年以后，组织者发现这样的组织可以为很多人互联网产业服务，不仅仅是地下产业链，还有主流产业也需要相关服务。

这样的组织最底层的一般叫：键盘手，只是做大量的重复性工作。一般 50-100 人形成一个小组，然后几个小组再形成一个大组。组织者负责接货，派活。一般一个任务会被最上层的组织者分解，都了键盘手中，仅仅是重复性的劳动来代替程序而已。

通过我们的分析和追中，2014 年可以统计到的超过 1000 人的键盘手组织有接近 3000 之多，而相关的从业人员，也有几百万之巨。



C. 人海战术模式应用产业链分析

在人海模式应用的同时，有很多键盘模拟软件也出现了。这些模拟软件在设计上很简单，只是通过写一些脚本来模拟人规律的对计算机的操作。但是这些模拟软件却又大大的提高了键盘手的工作效率，或者可以代替键盘手的一部分工作。

另外，一些软件可以把键盘手的服务建立在云端，非常方面用户的使用，甚至把这块服务做出功能模块化，可以添加到各种软件中。例如典型的打码软件，里面的打码破解功能几乎可以看成一个自动化解码的功能，但是后台确是无数键盘手的人工行为。

大量类似的软件都是由易语言写成，而易语言也在地下产业链中的低技术产业中，充当了极其重要的地位。我们接下来就看一个人海战术的典型应用。

D. 打码相关产业链深度分析洞察

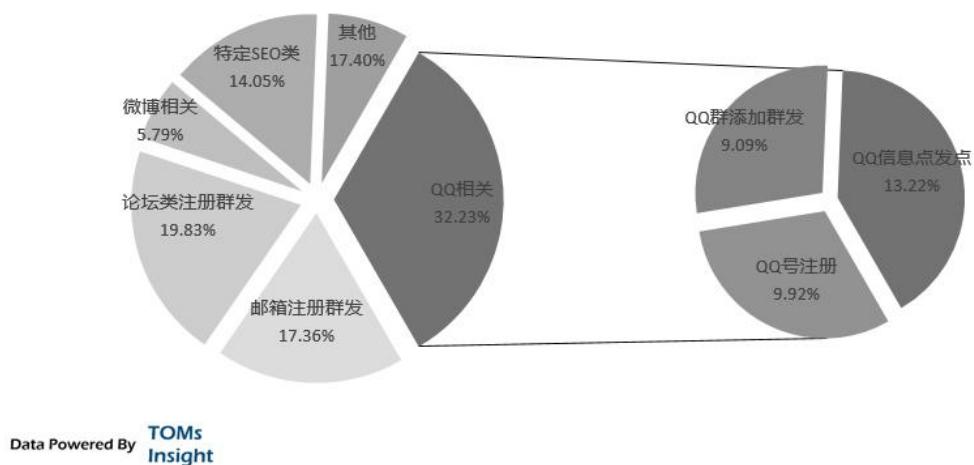
关于验证码，我们每个人应该都非常熟悉。几乎所有网络应用的注册、提交信息或者交互信息时都要求输入指定图片上的七歪八扭的文字，这是为了防止使用特定程序模拟用户行为。例

如：论坛灌水、批量注册 ID、各种刷票、等。我们每个人都有输入验证码的经历。验证码，这个源自卡内基梅隆大学的发明英文名是 CAPTCHA（下文统一称之为 CAPTCHA），是一个很高大上的名字的缩写：Completely Automated Public Turing test to tell Computers and Humans Apart（全自动区分计算机和人类的图灵测试）。区分计算机和人类的图灵测试。

从 2000 年 CAPTCHA 出现开始，人工智能领域就有无数科学家和黑客致力于破解它。十多年来，大量的团队和公司都在这个上面不断的尝试，但是魔高一尺道高一丈，验证码也不断升级，变得越来越复杂，复杂到有时候我们人类也需要几次尝试才能识别正确。破解 CAPTCHA 也就成为了一个神一样存在的目标。但是中国的互联网地下产业链的精英们早在 2003 年就已经彻底攻破了 CAPTCHA。发源自中国，推广到全世界有效的破解方法“打码模式”出现了。

所谓的打码模式，其实很简单，就是用人工的方式去破解。破解组织制作了打码软件，当在网上需要输入 CAPTCHA 时，打码软件自动的把歪曲的图片信息送到键盘手面前，一个熟练的键盘手一分钟可以输入 20 个以上的 CAPTCHA。这就是最早的打码破解模式。接下来起源于中国的这种人力破解的方式传到了全球各地，各大第三世界国家很多人靠打码为生（不完全统计有 100 万以上的打码工人存在），而这种工作也有了一个全球通用的名字：CAPTCHA Human Bypass。

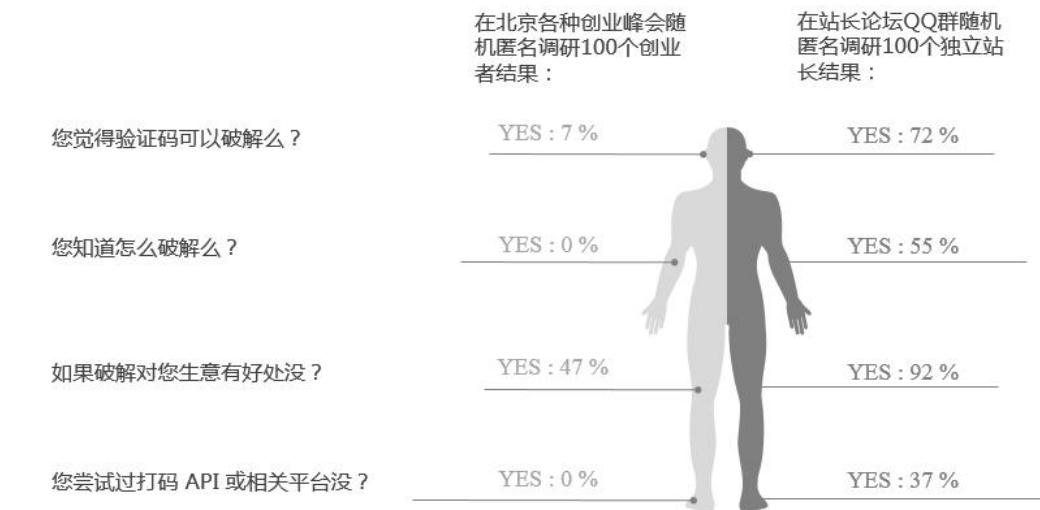
国内打码应用类别数据分布
(监控某地下产业链打码 API 一个月内 (2014.7) 订单 CAPTCHA 数)



E. 周边相关地下产业链深度分析

人海战术在一定程度上其实并不算黑产，这种方法如果并不是用在破解，而是用在一些主流的互联网产业中，其实还是有一定的意义：一方面通过人力创新做到技术突破，另一方面也解决了一定的就业问题。

而在地下产业链中，也有不少人把此方法论运用到一些主流的互联网营销推广等领域，也有不错的效果，毕竟，对于很多创新者来说，更接地气的解决办法也许是新的思路。



Data Powered By **TOMs**
Insight

账户安全与认证相关产业链分析

5

A. 相关地下产业链整体深度分析

账户安全与认证细分产业链也是属于地下产业链中的服务产业。由于互联网应用越来越多的要求手机认证、实名认证等，各大互联网企业也想尽办法去通过技术审核，甚至人工审核。给地下产业链带来的很多障碍，而账户认证就成为了一个必要的地下服务。对目前的地下产业链来说，账户认证是一个非常重要且实用的服务。

目前网络应用的注册大多采取手机认证和身份证认证的方式，所以一般的账户认证服务即提供手机号识别服务和身份证识别服务，而由于身份证识别牵扯身份证号码、照片、手持身份证照等，相关的交易也变得非常活跃。

由身份证牵扯出来的银行卡办理服务、甚至信用卡服务，在最近也变得越发猖獗火爆，而背后的金融诈骗，也和此产业链有紧密的联系。

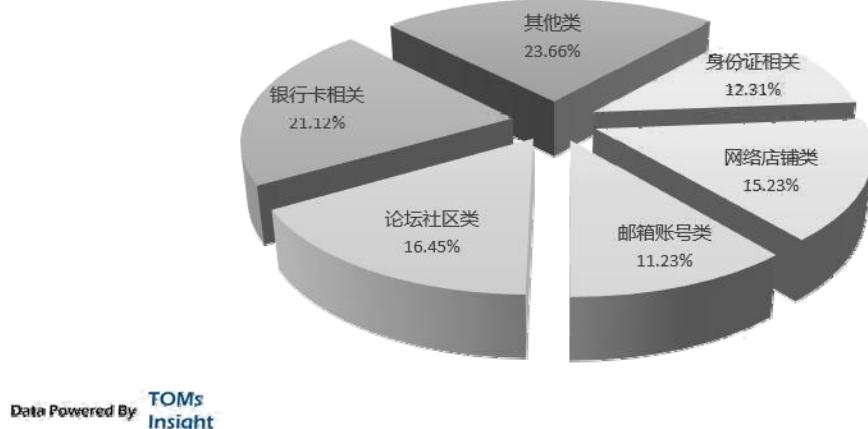
B. 账户黑市交易情况的数据分析

账户认证服务之上是账户交易，几乎所有的有价值的网络账户都有黑市交易情况，在此我们谈论的并不是那些被盗取的账户，而是新注册的干净账户。小到几分钱的邮箱账户，大到几百元的淘宝+支付宝+银行卡一套账户，甚至还有各种企业级账户的交易，五花八门。

这些账户大多使用在地下产业链，但是对主流的互联网产业也有一定的冲击作用，而很多初入互联网的小白也会被一些此行的骗术所迷惑，这对很多微型创业者来说也是一个很大的风险。

大多数生产者也是由人海战术的组织者组织键盘手完成的，这仅仅是注册环节，信息环境获取却是另外的情况。

地下产业链账户交易情况不同种类分析
(2015年10月，通过对一些黑市交易群组的舆情监控，仅供参考)



C. 身份认证识别地下产业链分析

早期很多网络应用仅仅需要一个身份证号码，这对于地下互联网产业来说根本就不算是重要数据，社工库里面估计有大半个中国的身份证号码信息。但是最近几年，主流互联网产业也不断的加强认证，仅仅是身份证号码远远不够，更多的是需要身份证照片，或者手持身份证照片。

我们以微信的公众平台举例，注册的时候需要身份证信息验证外，还需要对应的身份证本人手持身份证的照片，需要人和证件都很清晰，并人工审核。

对于这样的信息，身份识别产业里面有大量的“收件人”，所谓的收件人，其实只是带着一个相机，去偏远的农村或者山区、或者人口密集的地方去搜集，以一张手持身份证 50-100 元的价格去采购，很多信息不发达地区没有安全意识，为了几十块钱就会乐于去做；也有一些收件人，或冒充社区工作人员或者公安工作人员，去人工密集的地方去采集，几乎没有任何成本就可以获取大量的手持身份证。然后在网络上以更高的价格出售。

当然也有一些用这样的身份证照片作为模板，PS 更换号码信息来骗过人工审核，成本更低也几乎是无限量的供应。

D. 手机号识别与认证产业链分析

手机号验证码已经几乎所有网站的标配，但是破解注册码的成本也越来越低。手机号验证码和垃圾短信群发一样，使用一种叫“短信猫池”设备，虚拟管理大量的手机号，这些手机号可能已经被卖出或者未被卖出，由于和电信运营商联系较多我们在此不展开分析。

短信猫池可以帮助键盘手方便的通过手机验证码服务，甚至有一些服务商把相关服务放在云端让键盘手使用起来更方便简洁。而这也让各大网站的手机验证成了防君子不防小人的游戏。

E. 周边相关地下产业链深度分析

身份识别服务本身的危害并不大，但是最近几年开始出现通过掌握被害人信息，代办信用卡然后套现的一些情况，这类牵扯到了金融套现，对于被害人本身也危害很大 -- 不知不觉的就有大量的欠款。

而除了代办信用卡外，大量相关信息也在不断的充斥着社工库，引出别的地下产业链，特别是一些很有创新的诈骗方式，也是最近的趋势和需要我们警惕的。

网络诈骗与相关地下产业链分析

6

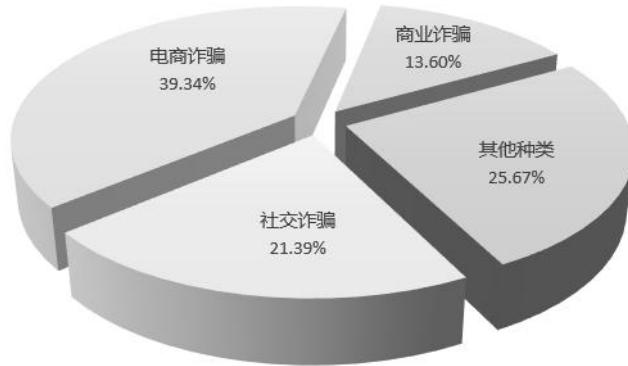
A. 相关地下产业链整体深度分析

网络诈骗是一个历史悠久的地下产业链，几乎从互联网诞生的第一天就存在，在某种意义上来说仅仅是诈骗行业找到了一个新的渠道。并不像有些地下细分产业链是互联网发展的新产物，网络诈骗在很多情况下只是诈骗行业的一个分支，利用互联网产品生态的设计、安全漏洞、信息不对等、用户心理等得到诈骗的目的。互联网更多的只是充当工具和渠道的作用。

在发展上来看，早期的网络诈骗更多的是电话诈骗和短信的延伸，但是发展到今天，由于网络越来越多的暴露个人信息，和数据信息安全的地下产业链发展，反而推高了整个诈骗行业的水平，让网络诈骗形成了一个新兴的、有技术含量的、并几乎与整个地下产业链都有错综复杂联系的地下产业。

网络诈骗主要可以分成社交网络诈骗、电商诈骗、商业诈骗或者其他种类等。而从模式上来说，一方面网络诈骗是网络盗窃的补充，另一方面是传统的诈骗手段的传承，并利用技术进行升级创新，其手段层出不穷。而由于社工库的日益完善、和对网络诈骗的打击力度，诈骗更多的从撒网博傻往深度发展，给网络用户造成更大的伤害。

地下产业链网络诈骗不同种类分析
(2015年11月，通过对一些黑市交易银行卡及黑市专家网络调研分析，仅供参考)



Data Powered By **TOMs**
Insight

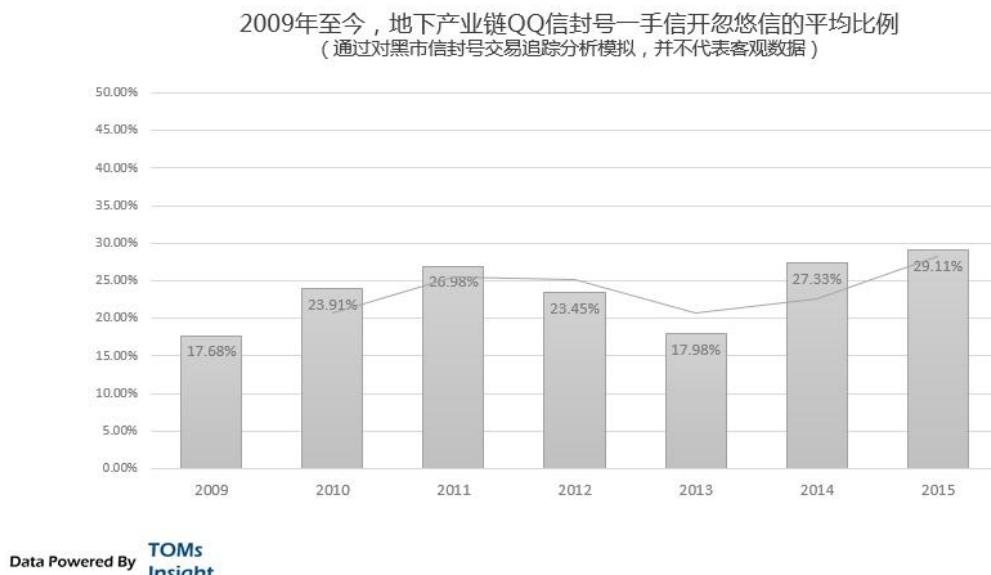
B. 社交网络诈骗及相关深度数据

QQ 由于庞大的用户基数和比较可见的社交关系，成为了社交网络诈骗的第一选择。和之前的短信诈骗模式的大海捞针不同，社交网络诈骗由于可见的并且信任的关系，让无数用户上当。

QQ 另一个优势是可以集结电话诈骗的话术随机性和短信诈骗的非实时性和范围，换句话说，不仅仅可以光撒网，而且还可以根据用户的反馈进行变现话术应答，在这诈骗行业是非常受欢迎的渠道，所以在地下产业链中，QQ 诈骗也在不断的吃掉短信、电话等诈骗的市场份额。

QQ 诈骗主要是利用之前我们分析过的 QQ 信封号，获得用户名密码登陆，用来诈骗用的信封一般在黑市上被称为忽悠信，以此类推有：海外留学忽悠信、女生忽悠信、18-23 岁忽悠信等 等，也可见网络骗子的分工细致和无耻的手法。

我们可以通过下图看出：信封号第一手开什么信可以代表什么变现最直接最重要，而竟然大概有 30% 的比例在不洗掉虚拟资产的情况下都开忽悠信，可见 QQ 诈骗的高利润性和在信封号产业链中的地位。



而如果我们把第一手信定义成洗过信（转移出虚拟资产），这个比例竟然可以高达到 90%。



而由于 QQ 信封交易的猖獗，QQ 诈骗门槛越来越低，渐渐的让更多用户都有了安全防备心理 和相关的意识。QQ 诈骗也随之发展，形成了更高级的一种形态：即潜伏形态。

这种骗术更多的是由网络盗窃行业发展而来，正如我们之前所分析，一些黑客脱库后完善社工库，在社工库上进一步分析，完善，利用数据技术，甚至通过木马分析一些用户 QQ 聊天的巨大内容，寻找有价值的目标，和相对更信任的关系网络。而一旦时机成熟，再去诈骗。

这种模式风险会更小，而且由于诈骗目标相对较大，收益更大。在这种模式下，完成技术分析工作的一般是黑客，但是最后完成诈骗的却一般不是，黑客按照客户要求去分析，最后把可以完成某种特定诈骗的目标连通相关信息出售（黑市称脚本）。

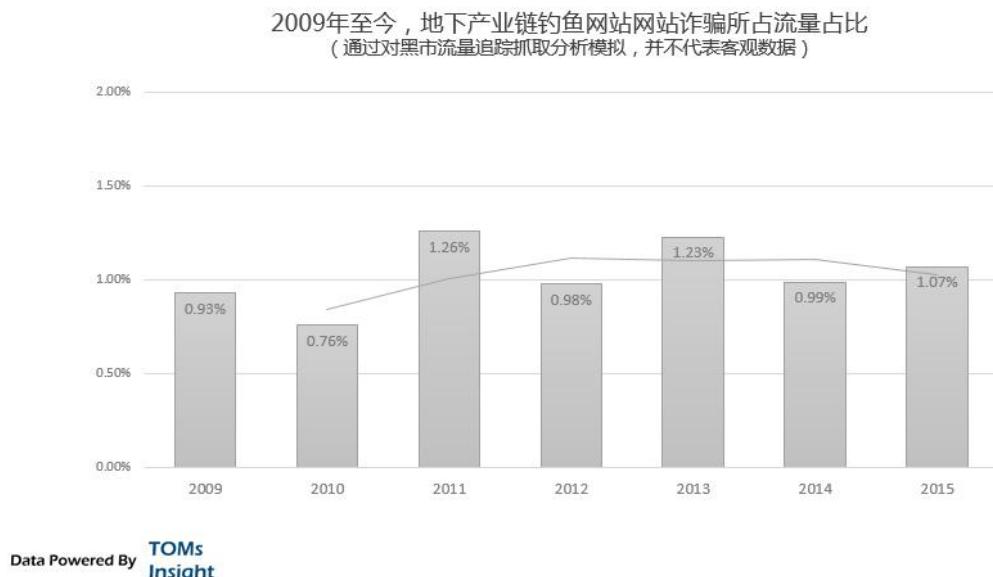
这种模式的 QQ 诈骗更多的是团伙完成，一般隐匿的更深，比那些买信封号广撒网的也要有更大的危害。而对于黑客和黑客工作室来说，这些更多的是无法完成网络盗窃的副产品，有时候反而会产生更大的价值。这种模式在最近 1-2 年发展迅速。

C. 电商购物诈骗及相关深度数据

电商购物类诈骗占据网络诈骗的主流，虽然危害性不如社交类网络诈骗，但是受害用户的波及面要远远大于。电商类诈骗其实在地下产业链中是一个模糊的概念，我们可以把暴利单页都称之为电商类诈骗，毕竟这种暴利程度已经可以算是诈骗的范畴；或者我们仅仅把那些纯粹的骗局称之为电商类诈骗。本章之前数据仅仅是指的后者。

在地下产业链中，最近几年已经越来越少使用纯粹的电商类诈骗了，一是由于打击力度较大风险较高，而是和暴利单页相比，其实利润也不会高出太多，而且没有持续性；另一方面由于各大流量生态的安全策略渐渐普及，所以慢慢在地下产业链中被暴利单页所取代。但是还是会有一定量的纯粹诈骗。

所谓的纯粹诈骗，一般是指的钓鱼网站、不发货电商、和一些中奖的电商骗术。



钓鱼网站的出现总是有时效性，特别是在双 11 等比较火热的阶段，或者是某一单品发布的火热阶段，不会持续的出现。而不发货电商和一些中奖的电商骗术类似，也是利用某一特定时期的热点来活动。客观上来说，在地下产业链中，很多暴利单页已经具备了电商类诈骗的属性，而且由于更容易的流量采购，更小风险，所以具备网络诈骗性质的暴利单页已经是新的方向。

D. 商业诈骗和其他种类诈骗分析

2013 年之后，商业属性的诈骗和金融类的诈骗越来越流行，由于互联网金融的概念的普及性，让很多对互联网不了解人放松的警惕，同时比特币山寨币等类似的互联网玩法一夜暴富的榜样作用，让更多的受害者有弱点可循。

商业类诈骗更多在在小圈子内传播，比如深度的锁定用户，利用社工库数据或者一些黑市的数据，针对性的设计骗术和骗局。而由于其针对性较强，创意也层出不穷。也有时会利用地下产业链的流量和人海战术将至范围扩大，但是由于其风险较高，更多的还是隐匿在小范围圈子内。

商业类诈骗愈发有合法性的倾向，比如 2014 年后火热的 p2p 金融跑路现象，其很多在设计初始即有此计划，甚至也有相当一部分创始人有很多地下产业链诈骗经验，仅仅是换了一个包装性质和内容而已，此类更具危害性。

E. 黑市交易与上下游产业链分析

网络诈骗在地下产业链中和网络盗窃行为类似，但是和盗窃的技术核心不同，更偏向骗术创意和对数据信息的利用。虽然在地下产业链中的占比不大，但是由于其危害性和明显行，很容易暴露出来，被舆论谴责也被各大互联网企业重视。

所以纯粹的网络诈骗越来越少，开始更多的把模式融入到其它地下产业链中，特别是变现盈利部分，使之变现能力越来越强，而风险也越来越小。最近几年地下产业链中出现了一些“创意顾问”、“优化顾问”的角色，也是更多的利用一些传统骗术，来“优化”地下产业链的各个细分行业，放大盈利变现的程度，屏蔽风险。而对用户的危害也愈发严重。

总结与洞察启示

数据信息安全是大多数互联网行业认识的典型的地下产业链，也是因为如此，获得了更多的关注和防范。但是最近几年，数据信息安全的地下产业链飞速发展，变得有创新性。同时和更多的产业链相融合，变得防不胜防，给互联网用户造成了极大的危害，也给互联网创新者带来更多的风险和挑战。

我们需要认识数据信息安全领域，一方面避免直接的被攻击风险，同时互联网主流创新者打造产品生态环境时需要考虑的最重要的因素，毕竟任何创新都不能活在真空的环境中。与此同时，保护最终互联网用户的利益和权益，对于互联网创新者来说，不仅仅是自己身上的责任，在某种意义上来说也是机会所在。

五、 总结性分析洞察与结论

地下产业链并不是消极的事物，在一定程度上讲，地下产业链更接近用户需求，更能还原互联网的本貌。在中国的传统行业都有一定的所谓黑市门槛，即属于潜规则范畴或者是不为人知的行业秘密，读懂了这些，才能算从根本上了解了这个行业。

对于互联网创新者来说，地下产业链代表着最接地气的用户需求和商业模式，可以给我们一定的用户需求理解、商业模式启示和相应的洞察力。另外，从地下产业链角度切入，纵览整个中国互联网产业的各细分领域，可以给我们更好的大局观和启示。这也是本报告的意义所在。



1. 地下产业链相关的风险影响分析

地下产业链会给主流的互联网行业带来一定的风险，这些风险一部分是由黑产本身决定的，但是更多的是地下产业链和主流产业链的竞争关系。由于互联网的用户资源有限，而地下产业链的手法更接近用户的原始需求，特别是流量获取分发方面，会给主流的互联网创新带来相当大的挤压性竞争：资源的总数是一定的，地下产业链获取的越多，主流互联网就会越少。这种竞争在整体性上并不明显，但是放到某一个个例上，却可以放大的非常厉害。另外由于这种竞争关系，也会让地下产业链主动的去攻击，更加放大相关的竞争效应。

地下产业链的数据信息安全相关产业，由于其生存的本质，也给主流的互联网造成很大的风险，这部分一般会被大公司重视防范，不断升级自己的产品生态链的安全策略。但是对于中小企业或者新鲜的创新者来说，有时候一次攻击敲诈就是毁灭性的打击。一方面我们需要继续曝光相关的黑产，不断的打击。但是更多的我们也需要有自我防范意识，了解相关的风险，控制在自己可以接受的范围之内，这也是创新者应该学会的自我保护。

2. 地下产业链相关的商业模式分析

地下产业链相关的商业模式更多的注重实际效益和生意本身，在对浮躁的主流互联网产业有相当强的学习借鉴的意义：目前主流互联网行业创新太多的变成资本游戏，在商业模式打造上不接地气，追逐概念和创新本身，而忽略了稳健的发展节奏和更成熟的发展心态。

从这个意义上来说，地下产业链的商业模式更像一个成熟的传统行业，讲究现金流和采购销售的分配，一定的风险接受能力和快速的复制。这些都是目前主流的互联网所欠缺的。同样是互联网行业，这么大的差别我们不能去主观的评价优劣，但是却值得我们反思。

3. 地下产业链相关的用户需求分析

地下产业链几乎最核心的竞争力就是对用户需求的把握了，由于讲究的是快速变现，对人性的把握和用户心理的痛点的研究，几乎成了这个行业的最基本的技能。主流互联网产业更喜欢的是创造需求和不是去发掘，这些创造的需求很难说是真实的还是虚幻的，而地下产业链对需求的把握更多的是从实际出发，通过不断的优化定位，在尝试中得出结果。

在主流的互联网行业，我们试图去抓住一部分人群的需求，我们努力的去分析：用户心理画像、大数据建模，抽丝剥茧去寻找真相，但是真相却离我们越来越远。信息技术的精髓，是对世界万物包括需求的抽象。当我们处于互联网前沿创新的时候，也许我们需要始终记得，我们是在抽象这个世界，而不是去描述这个世界。

4. 地下产业链相关的行业发展分析

地下产业链不断的发展，似乎还比主流互联网产业更快一些。几年前地下产业链也非常浮躁：在游资推动下，大家大肆获取流量，尝试各种方法变现，一旦有路数几乎一夜间就扎堆起来，攻击和诈骗几乎是广撒网，数据服务很少有人问津。这种局面在最近几年很难看到了，除去浮在水面上的一些刚入行者，大佬们都在做深度的研究和积累，潜伏下来等待机会。

而主流互联网产业，好像在资本的推动下，走着几年前地下产业链的老路。也许我们应该沉下心来了，不再关注快速轮转的热点，潜下心来积累自己的核心竞争力和相关资源，真正为用户拿出精彩的服务和创新，才是未来的发展之路。不然在竞争中会越来越占劣势，如果一个行业的创新者都没有其地下产业链的耐心，那么我们确实应该反思反思了。

5. 地下产业链相关的发展机遇分析

最后，地下产业链的发展肯定会继续，也会在猫鼠游戏中不断的进化，我们可以师夷长技以制夷，学习和借鉴的同时，坚决的打压防范，并且通过一些法律手段的去严惩。

本报告仅从学术角度研究，并不进行法律探讨。任何非法的事物必将受到法律严惩。