百度安全
有AI更安全

# 互联网安全报告：态势分析与生态治理

百度安全

2019年4月

# 目录

# 1 概要

人工智能时代，各行各业数据量的急剧扩增、广泛可连接、愈发丰富的数据维度及应用场景，在驱动人工智能发展的同时，也为公民个人信息的保护提出了挑战。中国《网络安全法》及欧盟GDPR（通用数据保护条例）的相继出台，对于关键信息基础设施运营者的企业而言，在保护公民个人信息安全、维护网络空间良性生态层面提出了全新的要求。

另一方面，新技术、新业态催生了传统网络安全格局的深刻变革，传统安全边界与框架范畴不断外延，对互联网发展与治理带来巨大的挑战。以前沿技术加入到全网信息安全生态综合治理当中，以开放协作的心态加强与政府、行业、学术机构的多层次协作，对于企业而言，使命感日益凸显。

日前，百度安全发布《互联网安全报告：态势分析与生态治理》，展示了百度安全在过去一年内，在搜索生态治理全网违法违规信息、加强公民个人信息保护、协助公安机关打击网络黑产的成果。据百度安全监测，2018年全网日均新增检出恶意网址①1456.6万，同比增长89.96%，百度安全拦截恶意网址全年总量超411.6亿次，同比增长102.86%。其中，针对涉嫌窃取公民个人隐私类恶意网站及盘踞其上的网络黑产开展重点监控打击工作，全年累计下线“涉嫌窃取公民个人隐私”恶意网站34万，全年累计下线“涉嫌窃取公民个人隐私”网址达1490万。

与此同时，百度安全也特别关注到暗网中文社区中有关个人隐私信息非法交易的滋长，并尝试对相关数据进行监测和分析，为防御策略的制定和对违法活动的打击提供支撑。

网络黑产多元化升级且呈体系化运作的趋势，意味着政府、行业、学术机构的协作模式，将从传统的触达拦截、单点防御、网络安全意识和防护技能的宣传普及，上升到狙击黑产全方位、持续、高压的态势打造。在这个过程中，威胁感知、过程还原，追踪溯源，成为高效、精准打击黑产的关键技术环节。2018年，百度安全持续从产业链的上游环节，协助公安机关对网络黑产进行重拳打击，“滤网行动”二号、三号相继侦破，这是继“滤网行动”一号中协助北京公安局海淀分局破获首例“手机访客营销”新型侵犯公民个人隐私黑产团伙之后，百度安全在加强公民个人信息保护、协助公安机关打击侵犯公民个人隐私类违法犯罪行为的最新进展。此外，在公安部“净网”2018专项行动中，协助北京公安局海淀分局破获一起特大售卖公民个人信息案件，涉案各类数据信息上亿条。

面对当下层出不穷且日益复杂的网络生态安全问题，百度安全始终倡导通过新一代技术研发与开源，实现对安全问题的快速响应与持续对抗。2018年，百度安全加强人工智能、大规模图数据库等新一代技术在全网信息安全生态综合治理中的应用，并通过技术开源，携手政府、行业、学术机构等多方力量共同推进网络黑产打击、网络安全生态综合治理，践行企业社会责任。

① 网址：互联网资源的位置和访问方法的简洁表示，是互联网标准资源的地址，用户可以通过网址找到所需的网站、文档和图像，《报告》中以“网址”作为监测与治理基本单位

# 2 2018年互联网安全治理整体情况

## 2.1 网络黑灰产类型日趋多元且呈体系化运作，安全攻防对抗不断升级

2018年，网络安全态势依旧严峻。据百度安全监测，2018年全网日均新增检出恶意网址1456.6万，同比增长89.96%。百度安全分析认为，一方面，电信网络诈骗、跨境赌博、破坏计算机信息系统功能、侵犯公民个人隐私等违法犯罪行为日趋多元且呈体系化运作；另一方面，流量劫持、恶意挖矿等诸多法律上尚未定性的灰产区域，具有显著的行业周期特征，吸引黑产分子不断升级技术手段，试图突破层层封锁，以获取巨大的经济利益。网络空间攻防对抗不断升级。

从恶意网址服务器IP地址国内地域分布来看，其中浙江、广东是恶意网址占比最高的省份，分别占比为22.60%、18.20%，香港、天津、北京、江苏占比依次降低，TOP6地域合计占比将近80%。

百度安全将恶意网页按照违法、欺诈、风险分类建模并重点监测。接下来，将针对三类恶意网址的现状态势及背后黑灰产业链条作具体分析。

图1：2018年恶意网址国内地域分布概况

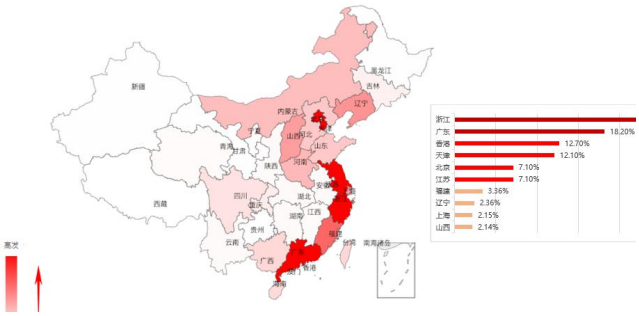
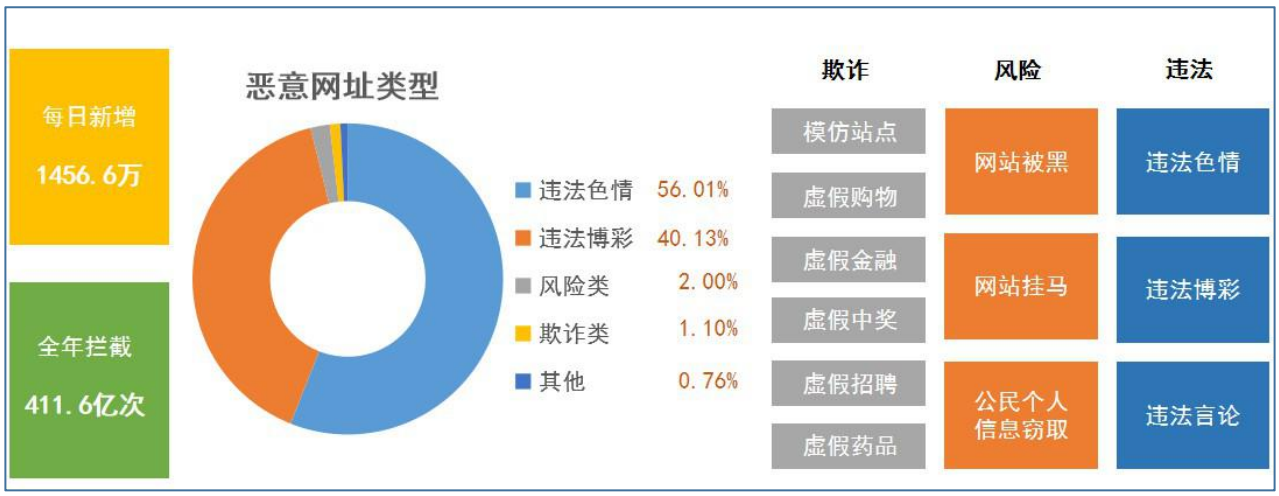



图2：2018年全网恶意网址整体概况



## 2.1.1 世界杯成赌球盛宴：网络博彩、色情业暗潮涌动的地下江湖

伴随历届世界杯而生的，是全球赌博产业的狂欢盛宴。俄罗斯世界杯亦不例外，期间涌现的大量地下赌场和非法赌博网站，不仅成为诸多非法分子的谋取利益的手段，同时存在极大的公民个人信息安全隐患。在2018年全网新增恶意网址中，据百度安全监测，**以博彩、色情为主的违法类恶意网址占比高达96.92%，占比率同比大幅上升，新增总量同比增长116.72%。**

互联网赌博主要源自境外的渗透。自地下博彩诞生以来，庄家利用与玩家之间的信息不对称，亦或通过暗箱操作等欺诈手段获取非法利益的现象屡禁不止，而网络赌博与非法洗钱有着紧密的关系，无论是赌博在线投注充值的资金流出，还是非法所得收益的层层“洗白”，都严重扰乱了我国社会经济秩序和金融管理秩序。为了躲避监管与黑产打击，国际赌博集团大多采用境外设立网站、境内推广的模式。数据显示，美国、东南亚已成为当下非法赌博网站服务器托管最主要的区域。

**赌博黑色产业链呈成熟的体系化运作，且内部分工明确。**

· 首先，博彩公司境外搭建博彩网站，网站服务器的托管和运营都在海外。推广客服负责吸引更多的人参与进来，推广的途径涉及**社交工具**、**直播平台**、**竞彩App**、**群发短信**等。此外，还会通过黑产技术为博彩网站导流，涉及**流量劫持**、**网页篡改**等；

· 然后，一旦用户进入博彩网站，在线客服则会使出各种方式游说用户注册会员、账户充值；

· 第三步，是将投注充值资金的“洗白”过程，为规避金融监管，黑灰产利用通常所说的虚假身份信息“四件套”（身份证、银行卡、手机号、U盾），亦或金融、贵金属投资和频繁的网银转账，将非法资金隐藏其交易来源及性质最终流入博彩集团的口袋。其中，“四件套”大多通过黑市购买而来，也不乏网络黑产通过技术手段入侵社交、视频、酒店、物流、游戏、电商等领域知名公司的服务器拖库、撞库而来。

· 接下来，赌博公司将非法收益继续扩大运营规模，招聘更多的人，发展更多层级代理和参赌人员，同时不断升级作案技术与工具与境内安全机构展开技术拉锯战。

图3:三类恶意网址变化趋势（单位：百万）


2018年全网日均新增检出恶意网页**1456.6万**，同比增长**89.96%**

**违法类**恶意网址新增总量同比增长**116.72%**

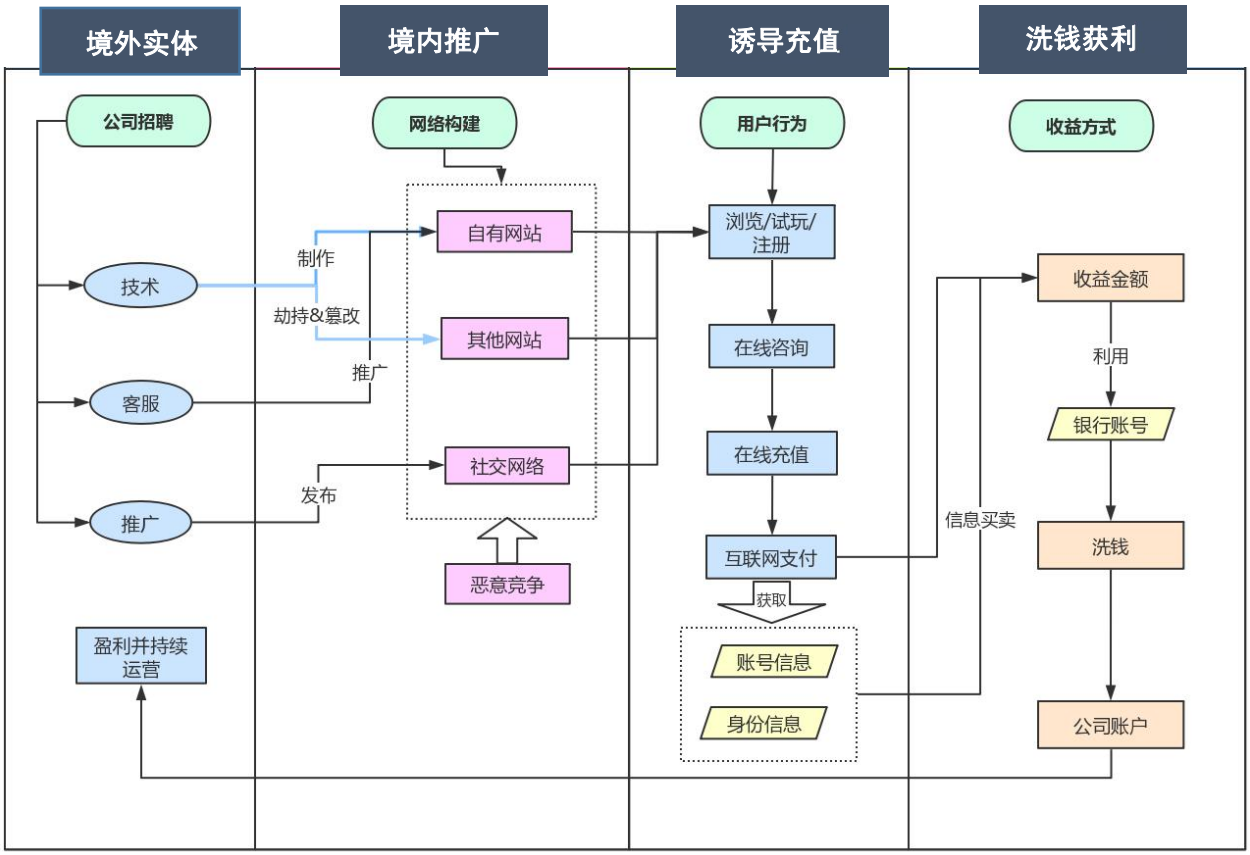
**欺诈类**恶意网址新增总量同比下降**60.53%**

**风险类**恶意网址新增总量同比下降**61.49%**

值得注意的是，大量的研究发现，色情网站和博彩网站密不可分，博彩网站是色情网站的利益归宿之一，色情网站则为博彩网站带来巨大的引流效果。网民为获得色情网站部分权益，或企图赚快钱一夜暴富而点击色情平台上的赌博网站广告的同时，正逐步深入黑灰产设置的层层圈套中。此外，色情网站捆绑聊天也是博彩推广人员惯用的方式，转化率很高。

图4：虚假身份信息“四件套”


图5：博彩黑色产业链



## 2.1.2 追溯网络诈骗源头：欺诈类网站成隐私窃取黑灰产重要载体

大数据时代，网络诈骗分子不仅能精确说出我们的姓名、身份证号、家庭住址，甚至精准“预测”衣食住行各类需求，令人真伪难辨，若干年前莘莘学子因此离世，社会反响强烈，亦令国内打击电信诈骗黑色产业链走入新阶段。值得指出的是，以往由于电话、短信往往是诈骗产业链条的起点，因此业内习惯性称之为“电信诈骗”，近年来伴随移动互联网、云计算、人工智能等新兴技术的兴起和大数据的广泛应用，犯罪分子欺诈手段及渠道更加多元，我们研究与监控的范畴，由传统的“电信诈骗”延伸至“通信及网络诈骗”的范畴。

据百度安全监测，**诸多通信及网络诈骗案件背后，与隐私窃取类黑产、非法信息交易具有千丝万缕的关联**。2019年“315”晚会所爆出以探针盒子为代表的第三方公司非法获取用户隐私信息的手段，只是当下层出不穷的用户隐私窃取手段的冰山一角，此外，全球知名公司重大数据信息遭遇拖库撞库、欺诈类恶意网站、公司“内鬼”数据外泄、第三方大数据公司非法获取、新型隐私类黑灰产等均是网络黑灰产实施公民隐私窃取的重要手段。

由于欺诈类恶意网站具有极大的迷惑性、诱导性，且涉案金额巨大，成为当下各类隐私窃取等违法犯罪行为的重要载体。这类恶意网站伪装成**金融、电商、航空、游戏、招聘**等各类“离钱近”领域的网站界面，其中不乏仿冒知名网站域名及页面，诱导用户访问输入身份证、银行卡、验证码等关键信息，既而窃取用户隐私，亦或诱导用户在线充值，造成用户财产损失。

**举个例子**，黑灰产通过社交工具或者伪基站短信散播某金融理财钓鱼网站，不明就里的用户点击进入一个在线聊天室，研习社精英论坛的气质，理财小秘书随即上线，极速开户，限时免佣，只需上传身份证正反面。提示开户“成功”后，用户被二次引导至某仿冒操盘页面，小秘书温馨提示入金操作方式，用户被三次引导至某仿冒银行页面或收款方为个人的第三方支付二维码。貌似与官方网站并无二致的界面与体验，背后正逐步深入黑灰产设置的层层圈套中。

不过，监管机构、关键基础设施运营者在过去一年中集中加强网络安全建设、协作共治的成果已初见成效，广大网络用户的网络安全意识和防护技能也在与日俱增。据百度安全监测数据显示，**2018年全网欺诈类恶意网址占比1.10%，同比占比率大幅下降，新增总量同比下降60.53%**。不过，在巨大的经济利益的驱动下，黑灰产不断升级作案技术与工具，作案手段日趋多元复杂，且呈跨区域、产业链化运作，网络攻防依旧处于一个不断博弈的过程，短时间内无法得到根治。

图6：黑灰产设置的某钓鱼网站层层圈套


图7：欺诈类恶意网址类型分布

### 2.1.3 全球性勒索病毒成分水岭，攻击者逻辑和规则正在改变

在违法、欺诈类恶意网址之外，尚有一类风险类恶意网址，涉及网站挂马、强制弹窗、强制插件下载、伪装更新下载、恶意篡改、恶意跳转等，**在2018年全网新增恶意网址中占比2.00%，同比占比率略有下降，新增总量同比下降61.49%**。这类恶意网址带有显著的互联网1.0时代的属性，尽管新增绝对数量逐年呈走低趋势，然而互联网并没有因此变得更加安全。

2017年全球性勒索病毒、僵尸网络病毒的大规模爆发是一个分水岭，我们深刻的感知到网络攻击者的逻辑和商业模式的改变，他们的攻击目标不再局限于个人电脑，而是侵占市政、医疗、交通、高校等公共设施，虚拟世界与实体经济的屏障已被打破，不仅涉及用户隐私安全、财产安全层面，同时延伸到人身、社会乃至公共安全层面，伴随与此，区块链技术和数据加密货币的兴起、暗网交易的日趋猖獗，则令传统的病毒经济链条更加复杂及难以追踪。风险类网站是各类病毒重要的注入载体和传播途径之一，百度安全近年来正逐步加大对该类恶意网址的监测与治理力度。

风险类恶意网址的另一特征，据百度安全监测显示，事业单位、教育、社交平台、视频娱乐等网站，因其网站权威性或流量庞大，近年来招致网络黑产虎视眈眈。网络黑产通过技术手段入侵这些网站，篡改正常内容以实现黑产展示，亦或重定向到博彩、色情网站以实现更大范围的黑产推广。监测数据显示，此类黑产擅长利用各类伪装技术来躲避监测，通常采用分区域、分时段、分访问途径区别呈现的策略，因其隐蔽性，网站运营者难以第一时间发现问题并上报，导致感染页面处理不及时。

图8：权威/高流量网站面临博彩类黑产威胁


## 2.2 重点治理三类恶意网址，从源头阻断网络黑灰产触达用户

**2018年，百度安全拦截全网恶意网页总量超411.6亿次，同比增长102.86%。**基于海量威胁情报数据与大数据分析能力，百度安全搭建全网网址安全态势感知系统，针对全网文字、图片、视频、代码等进行智能建模和7*24小时实时监控，对恶意网址采取**风险标注、风险拦截提示、搜索屏蔽、广告下线**等拦截措施，超过99%的恶意网址在触达用户之前实现精准拦截，既而从源头阻断网络黑灰产的蔓延，净化网络环境，保障数亿网络用户的搜索体验和公民个人信息安全。

2018年，百度安全加强了人工智能、大规模图数据库等新一代技术在全网信息安全生态综合治理中的应用。一方面，基于海量威胁情报数据，针对机器学习进行算法训练，构建网址安全检测智能决策模型，对既有机制形成有效补充，显著提升检测效率；另一方面，人工智能及大规模图数据库正在关联图谱分析领域发挥着重要作用，它能够从看似杂乱无章的关系中捕捉隐含相关性，从而更快速高效的感知恶意网址以及变种，审核政策更严，打击范围更广，在触达更多用户前实现精准拦截。

图9：对恶意网址风险标注、拦截提示、搜索屏蔽等

# 3 互联网隐私生态专项治理

在当下工业经济向数字经济转型的进程中，各行各业数据量的急剧扩增、广泛可连接、愈发丰富的数据维度及应用场景带来了前所未有的机遇。与此同时，虚拟世界与实体经济的最后一道屏障已被打破，数据安全成为网络安全一个非常重要的核心，不仅涉及用户隐私安全、财产安全层面，同时延伸到人身、社会乃至公共安全层面。中国《网络安全法》及欧盟GDPR（通用数据保护条例）的相继出台，对于关键信息基础设施运营者的企业而言，在履行主体责任、保护公民个人信息安全、维护网络空间良性生态层面提出了全新的要求。

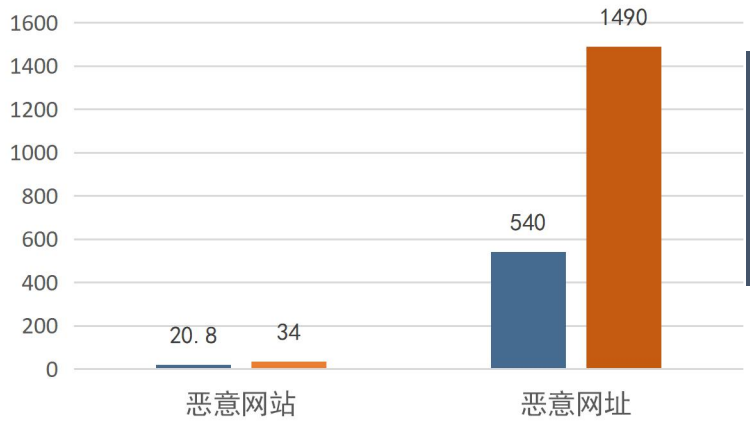
据清华大学经管学院互联网发展与治理研究中心联合百度安全、百度公益发布的**《中国互联网安全现状研究报告2018》**显示，伴随数据经济价值的不断上升，网络攻击者开始通过多种渠道和方式获取个人敏感数据，近年来个人数据泄露的重大事件数量逐年升高，往往所涉及到的人数较多，且泄露的数据一般较为敏感。**《报告》同时将“个人数据与隐私保护”列入我国当下网络安全生态系统的重点议题之一。**

## 3.1 基于搜索平台的隐私生态治理

百度始终重视数亿网络用户的搜索体验，将公民个人信息安全放在首位，致力于用前沿技术构筑安全的数据保护系统，以开放协作的心态率先加入到全网信息安全生态保护和治理当中。**2018年，百度安全全年累计下线“涉嫌窃取公民个人隐私”恶意网站34万个，全年累计下线“涉嫌窃取公民个人隐私”网址达1490万个，**基于对窃取隐私类黑产监控力度、打击范围的不断提高，同比增幅175.93%。

基于对互联网上涉嫌窃取公民个人隐私类黑产（下简称为：隐私类黑产）的长期监测研究，百度安全将此类黑产归纳为以下三个特点：

图10：下线涉嫌窃取公民个人隐私恶意网站&网址变化趋势（单位：万）




全年累计下线“涉嫌窃取公民个人隐私”恶意网站34万个，同比增幅33%

全年累计下线“涉嫌窃取公民个人隐私”网址1490万个，同比增幅175.93%

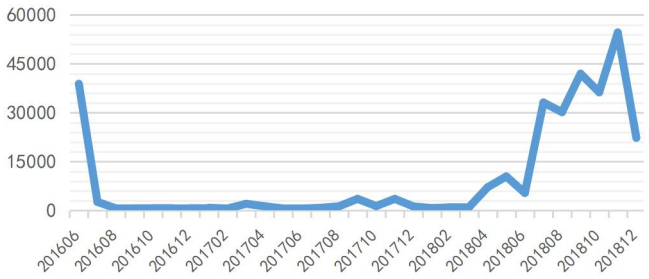
### 3.1.1 隐私类黑产攻防对抗尚处于博弈阶段，隐私生态治理将是长期的任务

自2016年发现国内首例新型“手机访客营销”隐私类黑产作案类型以来，百度安全针对全网涉嫌侵犯公民个人隐私类恶意网站及盘踞其上的网络黑产开展专项打击，对外配合公安机关在提供线索、黑产攻击溯源等层面开展大量工作，在多起非法获取公民个人信息案件的成功侦破中提供了坚实的技术支持；对内与风控体系、业务审核、法务等多个部门在技术、产品层面联动，实现**事前阻断（拦截下线、搜索屏蔽）——事后防御（处罚违规账号、黑产攻击溯源）**的保障机制。

然而，隐私类黑产依旧顽固，攻防对抗尚处于博弈阶段。据百度安全监测数据显示，尽管在集中时间段多部门基于搜索生态形成的高压打击态势下，后续隐私类黑产网站新增检出数量实现持续性的明显下降，但是短时间内根除难度较大，同时，伴随监控策略与感知维度的不断升级，在维持一段平稳期之后，伴随隐私类黑产窃取信息类型及作案手段多样化，隐私类黑产网站新增检出数量出现了反弹。隐私生态治理将是长期的任务。

百度安全目前已经实现对新型隐私类黑产类型及作案手段的实时威胁感知，并在新型黑产实现规模化并造成实际经济损失之前联合多部门进行专项打击，打击效率不断提升，尽可能的压缩隐私类黑产谋取非法利益的空间。

图11：涉嫌窃取公民个人隐私恶意网址检出趋势（日均）




### 3.1.2 隐私类黑产窃取信息类型呈多样化

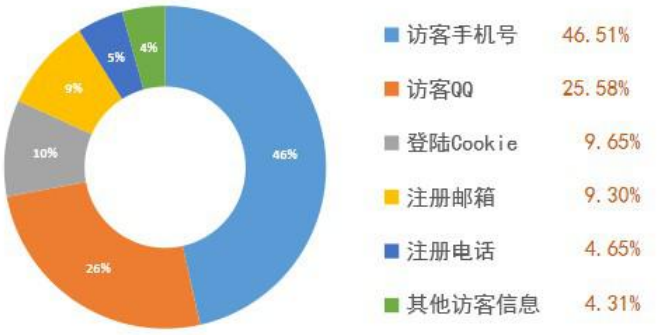
2018年，全球各大公司相继爆发出的重大数据泄露事件屡见报端，网络黑产通过技术入侵社交、视频、酒店、物流、游戏、电商等领域知名公司的服务器，窃取并批量出售数以亿计的用户个人信息以实现经济利益。在此之外，尚有诸多新型隐私类黑产在悄然滋生，公民个人信息在互联网上被窥视并公然收集，整个过程中无论从网络服务提供商到用户鲜有感知。“只要客户用手机访问网站，就可以轻松获取用户的手机号码！”不法分子的售卖广告词并非危言耸听，以“手机访客营销”隐私类黑产为例，黑产分子利用运营商系统漏洞，在用户访问网页期间非法获取公民手机号，既而将信息转卖给医院、教育培训、银行券商等机构，实现所谓“精准营销”。

百度安全认为，**该类隐私类黑产以其隐蔽性及长尾效应，相较传统恶意网址危害性更大，**不仅对广大公民个人信息造成侵犯，同时也对搜索及网络服务提供商的声誉造成了极大的伤害。

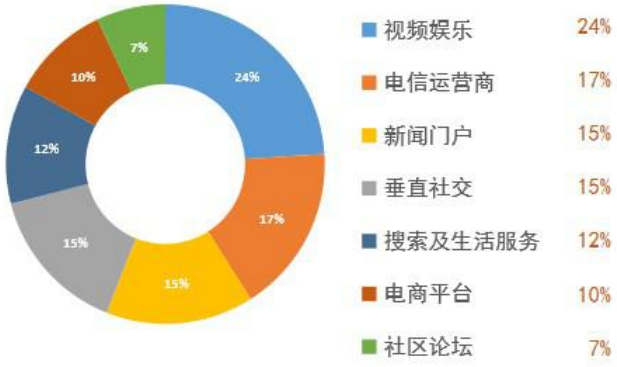
事实上，一旦网站被黑产利用安全漏洞植入恶意代码，用户在访问网站过程中的个人隐私信息就有可能遭到窃取。因此，**针对隐私类黑产窃取信息类型的研究，往往需要与网站安全漏洞结合。**继**手机号、社交账号、电子邮箱**之后，隐私类黑产盯上了公民在社交、视频、游戏、购物等网站上的**注册信息、交易记录、征信信息**等。图12展示了隐私类黑产窃取信息类型及利用漏洞行业分布，窃取类型中，**网站注册ID占比最高，高达57%**，其次依次为访客手机号、QQ、登录cookie、注册电话等（为清晰呈现，仅展示除注册ID之外类型占比）；利用漏洞行业中，**视频娱乐行业占比最高，为24%。**

层出不穷的窃取信息类型背后，据百度安全监测数据显示，**目前已被隐私类黑产利用的网站安全漏洞将近50个**，涉及国内**20多家**大型互联网公司及运营商网站。此外，以智能电视、智能路由器为代表的智能家居设备在发展进程中存在的安全漏洞也被纳入研究范畴，**通过恶意网址入侵AIoT设备，成为隐私类黑产的途径之一**。据2018年中国信通院泰尔实验室发布的智能电视安全报告显示，当下市面上多款智能电视存在越权操作、DNS劫持、用户敏感信息明文传输等安全漏洞，且漏洞修复率低，用户账号、登陆令牌、支付账户等重要个人信息面临威胁。

图12：隐私类黑产窃取信息类型及利用漏洞行业分布




隐私类黑产窃取信息类型



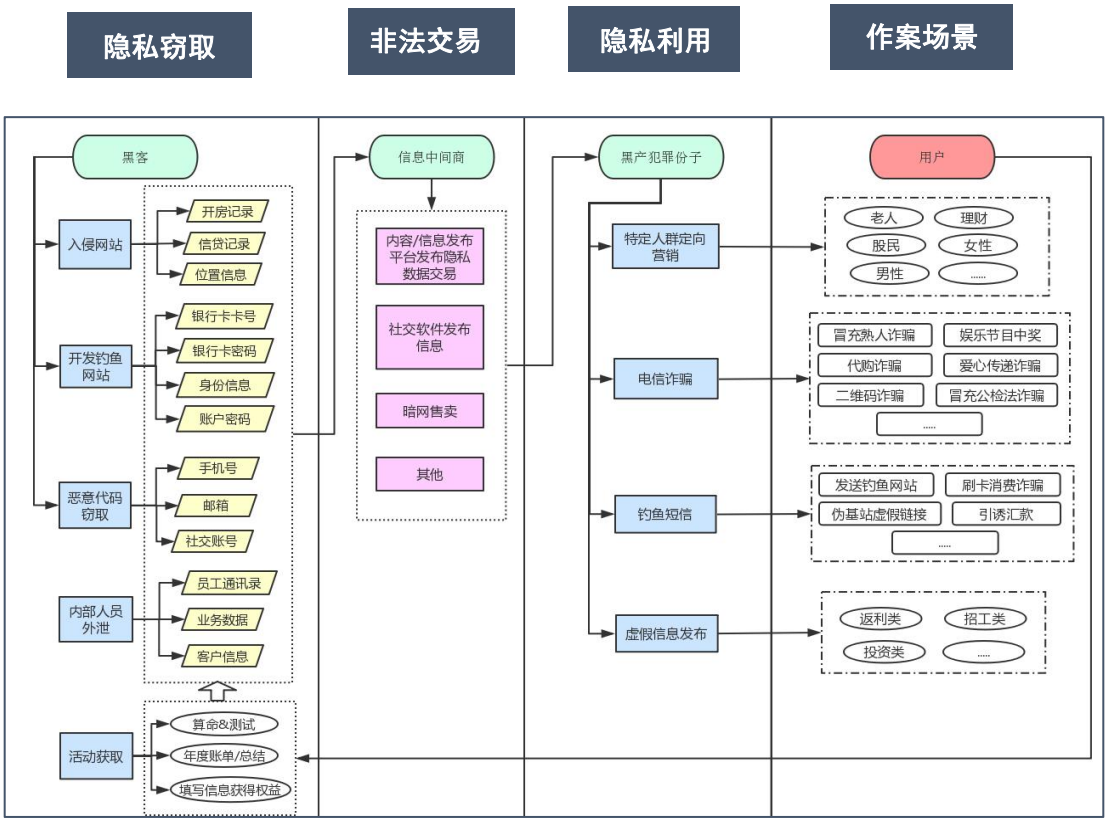

隐私类黑产利用漏洞行业分布

## 3.1.3 隐私类黑产作案手段日趋多元

公民隐私信息通过各类灰黑产渠道被获取后，进入交易流通环节。大量数据商贩在各类社交软件、UGC等内容平台发布相关隐私交易信息，或转卖给医院、教育培训、银行券商等机构，实现所谓“**精准营销**”，或转卖给电信诈骗、钓鱼网站团伙，实现“**经济收益**”，其中不乏暗网渠道。据百度安全监测显示，**目前在中文暗网社区，仅直接与个人隐私信息相关的非法交易便已达到将近50%的占比**，而大量企业数据的交易也大多与这些企业所掌握的员工及用户信息有关，敏感度较高的身份证、银行卡等证件信息、基本资料及各类通讯号码首当其冲，而**网购历史数据、酒旅信息、健康情况、信贷情况等都成为了不法分子交易的筹码。**

网络黑产通过“整合分析”将这些隐私信息“归档”到“社工库”进行贩卖，继而实施更精准的网络诈骗、定向营销、敲诈勒索等不法行为，鉴于其隐蔽性及扩张速度惊人，及威胁不容小觑。待数据流通到下游，便是大家众所周知的环节了。上、中、下游环环相扣，分工明确，且呈跨区域、产业链化运作，窃取技术、工具及作案手段日趋多元复杂。

图13：隐私黑色产业链




## 3.2 基于UGC内容平台的隐私生态治理

百度安全一直通过自动巡察、自主清理、用户举报等方式，持续对UGC内容平台上的不良信息进行重点监控打击工作。在2018年下半年启动的“用户隐私体验提升计划“中，百度安全联合数据隐私法务部，针对百度贴吧、百度知道等UGC内容平台开展专项治理工作，针对涉嫌公民个人隐私信息恶意披露、交易的违法违规信息集中进行下线清理、封禁账号、黑产打击溯源、警方联动等举措，同时驱动内容平台个人信息安全标准的建立。

**“黑产词”**是伴随黑产出现的产品同义词及违法产品本身的关键词的统称。黑产词通常会扭曲常用词含义，导致“外行人”无法理解其背后的含义，以此躲避监管和黑产打击。例如“菠菜”是“博彩”的另一种名称。百度安全近年来通过与高校合作，搭建 **KDES（ Keywords Detection and ExpandsionSystem ）**系统，并将该系统融入到内容生态治理之中，该系统已检测到近百万“黑产词”以及上千个黑产核心词，且随隐私黑产检测能力不断扩容。这些与黑产密切相关的威胁情报，能帮助安全研究者们更好的了解黑产规律，助力隐私生态安全保障。

# 4 互联网安全新战场：暗网非法交易

与往年不同，网络黑产在2018年还出现了一些新的变化和趋势。在这之中，中文暗网社区中相关非法交易的滋长便是其中一例。虽然起步晚，但中文暗网社区的扩张速度却相当惊人，小规模的“私聊买卖”形式也正在演化成具备一定运行和保障机制的“成熟”黑产交易平台，俨然成为各类个人隐私信息非法交易的聚集地，值得我们特别予以关注。

## 4.1 个人隐私非法交易

根据百度安全的监测显示，在中文暗网社区的线上交易中，仅直接与个人隐私信息相关的非法交易便已达到将近50%的占比，而大量企业数据的交易也大多与这些企业所掌握的员工及用户信息有关。

图14展示了在中文暗网社区中，有关个人隐私信息非法交易的具体类型。敏感度较高的**身份证**、**银行卡**等证件信息、基本资料及各类**通讯号码**首当其冲，而**网购历史数据**、**酒旅信息**、**健康情况**甚至“裸贷”等也都成为了不法分子交易的筹码。

企业数据的泄露和非法交易也同样是重灾区，根据百度安全对有明确指向性的交易标的统计，2018年下半年，在中文暗网社区中有相关数据被非法交易的企业便涉及超过上百家。其中，**十亿级和亿级的大规模企业数据非法交易量合计达到8起，千万级则达到13起，**与电商和物流相关的信息是暗网交易的主要对象；同时，社交平台、视频、游戏、酒旅及020服务等行业也榜上有名。

图14：中文暗网社区交易类型（个人信息部分。2018年）

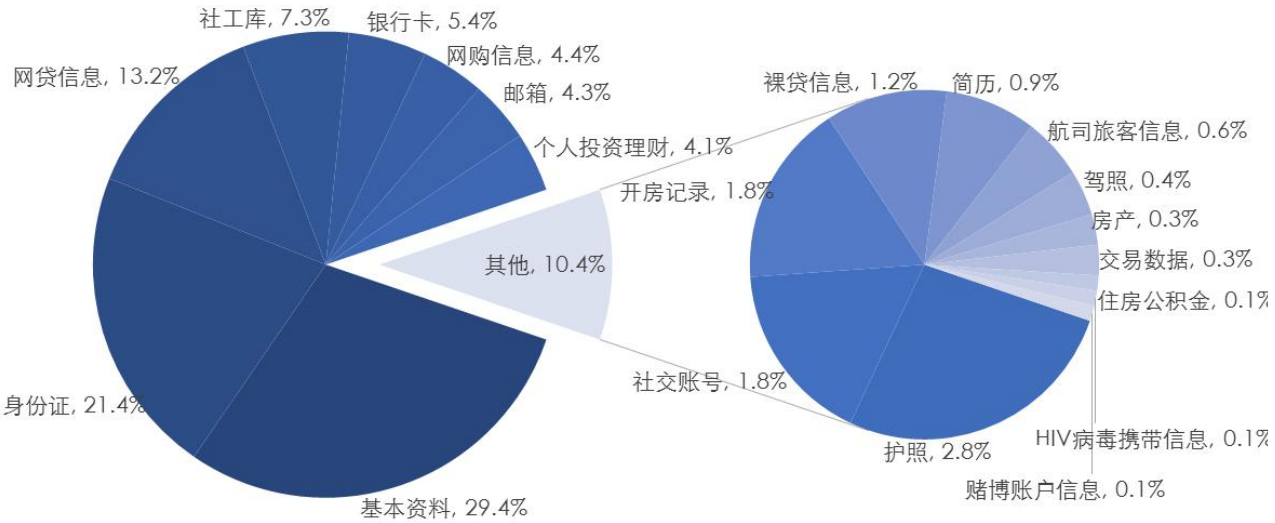
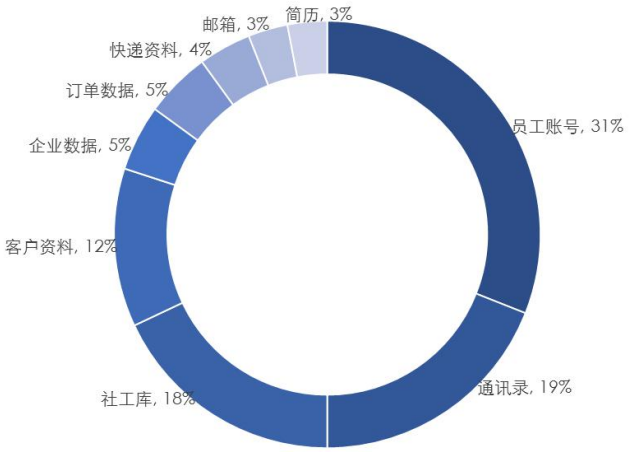


图15展示了有关企业数据非法交易中的主要“商品”组成，**企业内部员工的个人帐号等信息占比超过30%，通讯录及社工库数据分别近20%，企业客户数据达到12%。**事实上，尽管很多企业在网络安全方面的重视程度在近几年有所提高，但在内部信息和数据管理层面仍然存在着不少漏洞，从而也导致了企业自身与企业员工、客户信息泄露和品牌声誉的损失。

图15：中文暗网社区交易类型（企业数据部分， 2018年）




## 4.2 中文暗网社区非法交易量及价格监测

针对中文暗网社区交易类型的特殊性，自2018年下半年开始，百度安全对与个人信息和企业数据相关的非法交易进行了持续的监测。作为切入点，中文暗网社区中**“数据情报”**和**“虚拟资源”**两个论坛板块被列为重点监测对象，两者也是不法分子贩卖各类信息和数据的主要“根据地”。而通过对上述活动具体交易量及交易额的数据分析，将为相关监管机构的暗网治理和企业的防护策略制定提供有益的参考。

需要说明的是，为逃避监管，暗网交易中的“货币”以比特币为主，并通过“洋葱网络”通道和混币（Coin Shuffle）实现交易的匿名化。故在对其交易数据的监测中，其价格以比特币在交易时的兑换价格为准。同时，为更直观感知其在现实世界中的实际价值，我们也对上述交易价格进行了对应美元和人民币的换算。而由于比特币“汇率”存在较大波动，故我们在此根据百度安全对相关数据的监测时间为维度，即2018年下半年，以此时间段的比特币的平均“汇率”换算——约1比特币（BTC）：5000美元（USD）：34000人民币（RMB），这一换算数据仅作为参考，并非实际交易价值。

从图16中我们可以看到，对于中文暗网社区来说，2018年存在一个用户活跃度迅速提升的分水岭，即9月。成交量由几十上百跃升至千位及以上级别，但整体浮动较大，交易价格差异化明显，市场“成熟度”不高。

细分板块来看，在“数据情报”板块，**6月至11月相关交易总成交量为3698单，总成交额为25.7比特币，约合人民币87.37万元；月均成交额约为4.28比特币，约合人民币14.56万元，交易峰值出现在10月。**

而在“虚拟资源”板块，**6个月相关交易总成交量为12524单，总成交额为4.6比特币，约合人民币15.62万元；月均成交额约为0.76比特币，约合人民币2.6万元，交易峰值则出现在9月。**

图16：中文暗网社区两大板块非法交易数据监测

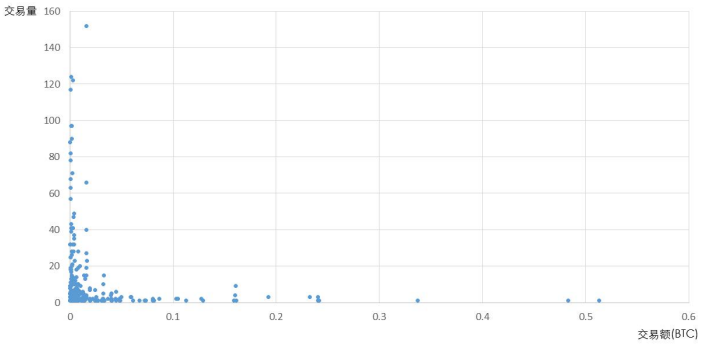
| 板块 | 月份 | 6 | 7 | 8 | 9 | 10 | 11 | 汇总 |
|---|---|---|---|---|---|---|---|---|
| 数据情报 | 交易量 | 6 | 39 | 167 | 1169 | 1529 | 788 | 3698 |
| | 交易额(BTC) | 0.29 | 1.46 | 4.25 | 7.01 | 9.27 | 3.42 | 25.70 |
| | 交易额(RMB/万元) | 0.98 | 4.98 | 14.44 | 23.84 | 31.51 | 11.62 | 87.37 |
| 虚拟资源 | 交易量 | 1 | 38 | 137 | 11566 | 561 | 221 | 12524 |
| | 交易额(BTC) | 0.01 | 0.05 | 0.31 | 2.20 | 1.02 | 1.00 | 4.60 |
| | 交易金额(RMB/万元) | 0.05 | 0.18 | 1.05 | 7.48 | 3.47 | 3.39 | 15.62 |

通过图17，我们可以更直观的看到交易成交价格的分布情况。而同样需要说明的是，考虑到有限篇幅下的呈现效果，在这份散点图的数据取用中不包括五笔交易量超过200单的交易，其交易量分别为10709单、764单、712单、680单和216单；也不包括一笔单价金额达到0.80719比特币的交易。

由此，我们可以发现，在中文暗网社区，目前主要的成交价格区间在0.00014至0.05比特币，约合人民币4.76至1700元，成交量则大多集中在30单以下。

而若从单笔最大成交量的交易内容考量，价格及成交量差异也较大。这一方由于其交易“商品”的价值不同，另一方面同样源于中文暗网社区交易体系的不成熟及其所带来的价格的不稳定性和随机性。

图17：中文暗网社区两大板块非法交易成交额价格分布




## 4.3 地下交易市场和黑色产业链

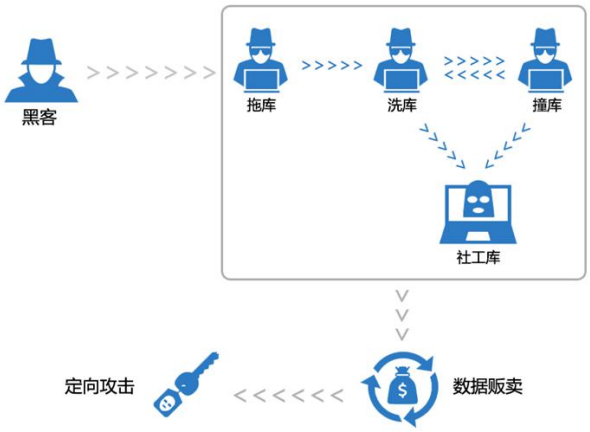
尽管从交易规模的角度上看，当前中文暗网社区非法交易在整体网络黑产打击方面的比重还不高，但由于其的隐蔽性和交易内容的敏感性，其威胁不容小觑。

根据百度安全的监测和分析，目前在中文暗网社区，以个人信息和企业数据组成的线上非法交易已经形成了一条黑色的产业链，而并非是零散的个人行为。不法分子在窃取这些数据后，通常会进行拖库、洗库及撞库等操作，“整合分析”后“归档”到“社工库”，并进行贩卖，以实施更精准的网络诈骗、定向营销、敲诈勒索等不法行为。

目前，中文暗网社区中的非法交易已为警方高度关注。就在2018年8月，浙江公安机关便成功抓获非法入侵浙江省学籍管理系统、并在暗网兜售浙江中小学生学籍信息的多名犯罪嫌疑人，这一行动也成为当年公安部公布的10起打击整治网络违法犯罪“净网2018”专项行动的典型案例。

警方的打击行动给了中文暗网社区中的非法活动以很大震慑，但对于我们自身和握有大量用户数据的企业来说，守住自己的安全防线，才是从源头上降低风险。

图18：中文暗网社区非法交易产业链



# 5 用创新技术狙击黑产，打造安全生态多方治理格局

2018全国网络安全和信息化工作会议上，中央提出要“提高网络综合治理能力，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局”。百度积极履行推进网络强国建设、加强网络安全和信息化工作中的企业主体责任，携手政府、行业、学术机构等多方力量共同推进网络黑产打击、网络安全生态综合治理，践行企业社会责任。百度安全作为核心技术研发机构，始终致力于从新一代技术的研发与开源，到为行业提供一体化安全解决方案，实现对当下层出不穷的安全问题的快速响应，以及对不断升级的网络黑产的持续对抗。

## 5.1 AI思维助力网络黑产打击

网络黑产多元化升级且呈体系化运作的趋势，意味着政府、行业、学术机构的协作模式，将从传统的触达拦截、单点防御、网络安全意识和防护技能的宣传普及，上升到狙击黑产全方位、持续、高压的态势打造。在这个过程中，威胁感知、过程还原，追踪溯源，成为高效、精准打击黑产的关键技术环节。

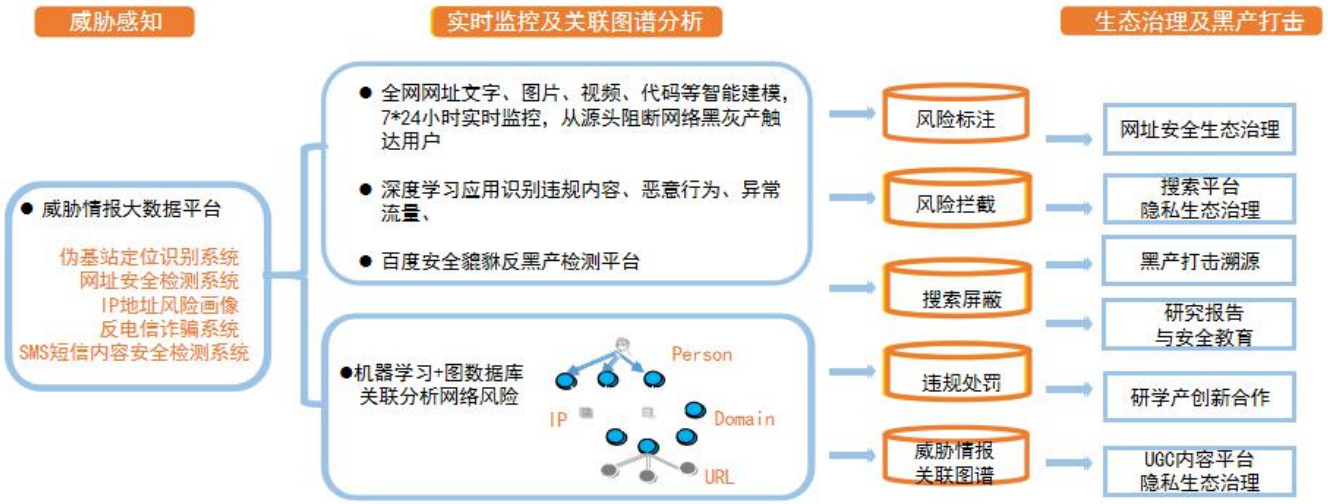
2018年，百度安全从产业链上游环节对网络黑产进行重拳打击。在保障公民个人信息安全、打击隐私类黑产领域，通过核心技术**助力公安机关相继破获“滤网行动”二号、三号，重创从黑产工具制作、多层级销售代理、到黑产工具购买者的整个产业链，逮捕犯罪嫌疑人4名，**这是继“滤网行动”一号中协助北京公安局海淀分局破获全国首例“手机访客营销”新型侵犯公民个人隐私黑产团伙之后，百度安全在加强公民个人信息保护、协助公安机关打击侵犯公民个人隐私类违法犯罪行为的最新进展。“手机访客营销”新型侵犯公民个人隐私黑产已潜伏多年，产业链庞大，涉及资金过亿，“滤网行动”对于该类黑产产生巨大震慑效果，各大手机号抓取黑产平台迅速关闭网站，删除数据。该案由公安部与最高人民检察院双重挂牌督办，入选公安部侵犯公民隐私十大精品案例。

保障公民个人信息安全、打击隐私类黑产领域另一成果，在公安部“净网”2018专项行动中，**百度安全协助北京公安局海淀分局破获一起特大售卖公民个人信息案件，涉案各类数据信息**上亿条。

打击网络诈骗黑产领域，2018年5月3日，在江苏江阴公安机关的主导下，**百度安全“天网”专项组助力警方捣毁一起“借壳”窃取百度推广账号黑产犯罪团伙。**该团伙通过发布钓鱼链接的手段，窃取百度推广广告主账号信息，继而冒充广告主的身份发布各类诈骗信息，以对各类不明真相的网民实施金融诈骗、个人隐私窃取等违法犯罪行为。百度安全在风险感知后，第一时间对于被感染推广账户予以拦截下线，通知广告主修改登录信息，并同步警方立案，协助警方溯源打击，提供了广东、海南等多省市的网上嫌疑线索，随专案组辗转广东、江苏、海南三省六地市，全面开展侦查工作，最终锁定多名嫌疑人，最终于2018年5月份在海南省儋州市将犯罪嫌疑人6名一举抓获。

打击黑产核心技术背后，得益于百度在人工智能、大数据、云计算等领域的迅猛发展，AI思维在全面改造和智能化传统行业的同时，也被运用在网络安全生态综合治理与公民个人信息安全保障层面。

图19：百度安全互联网安全生态治理智慧大脑



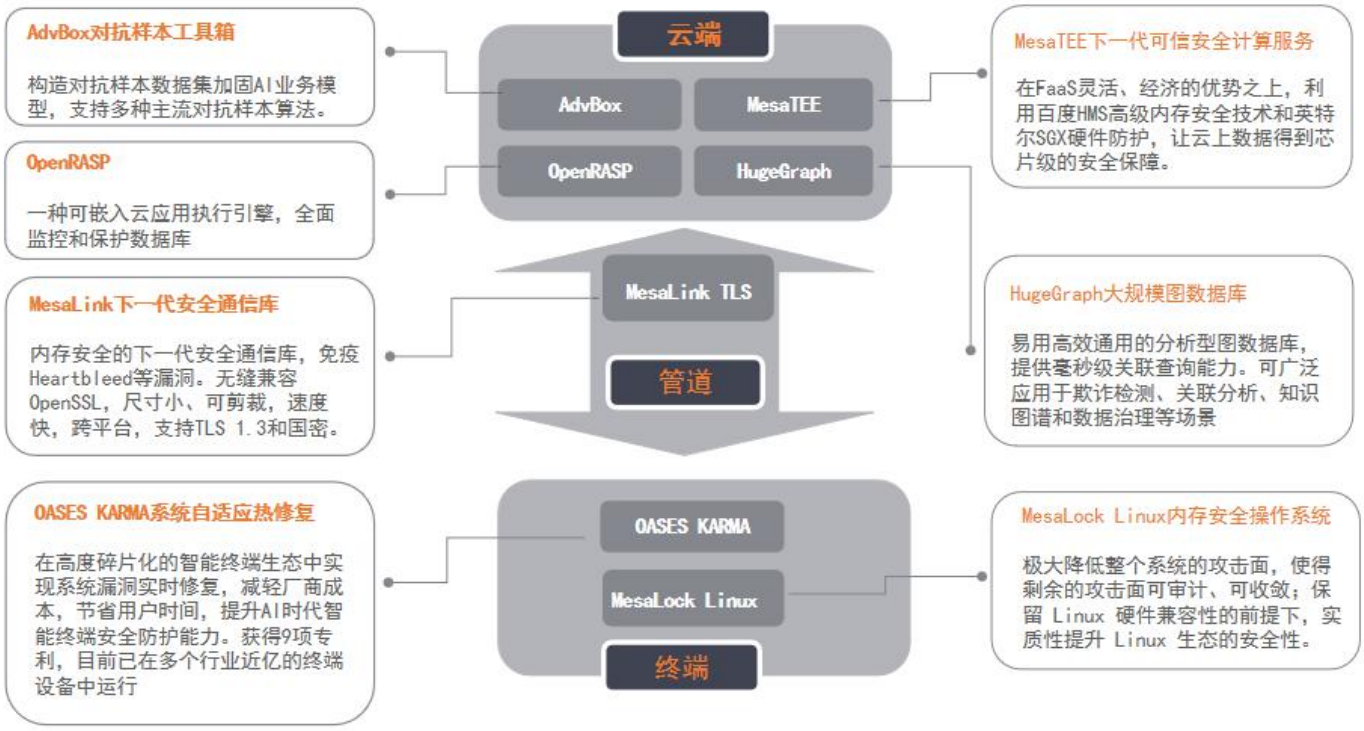

一方面，基于百度安全18年海量威胁情报数据与最佳实践训练出的”网址安全智能模型“具备全面感知、实时决策的特点，每日不知疲倦的执行千亿级别网页文字、图片、视频、代码的安全监测，处理速度以毫秒计算，准确率度高达99.67%，实现绝大多数场景下传统安全模式中大量人力维护的任务取代，恶意网站在人力维护模式下不断变换规则以逃避监测的伎俩，在人工智能面前变得无处遁形；

另一方面，人工智能及大规模图数据库正在关联图谱分析领域发挥着重要作用，应对新型黑产类型及作案手段日趋多元化的挑战，需要不断提升威胁感知与关联分析能力，百度安全从Web端、应用层、网络层等多个维度出发，针对网页访问、网站流量、代码意图等异常行为特征进行分析，采用深度学习和复杂网络分析的方法进行人工智能决策模型训练，辅助网址安全智能模型从看似杂乱无章的关系中捕捉隐含相关性，既而更加高效精准的感知并预警新型恶意网址及黑产类型，审核政策更严，打击范围更广。

## 5.2 “七种武器”全面开源，提升全网安全生态综合治理技术水平

2018年，百度安全发布**下一代人工智能安全技术栈（Baidu AI Security Stack，简称BASS）**，KARMA系统自适应热修复、MesaLink TLS下一代安全通信库、MesaLock Linux内存安全操作系统、MesaTEE下一代可信安全计算服务、OpenRASP下一代云端安全防护系统、AdvBox对抗样本工具包、HugeGraph大规模图数据库汇成“七种武器”，在保障百度内部生态数据安全、业务安全的基础上，向社会生态合作伙伴全面开源，解决云管端以及大数据和算法层面的一系列安全风险问题。

图20：Baidu AI Security Stack（BASS）下一代人工智能安全技术栈




当下，BASS下一代AI安全技术栈已经在网络安全生态综合治理、黑产打击与持续对抗等诸多领域展开实践。例如，内核漏洞热修复技术OASES KARMA已经广泛嵌入到智能电视、智能手机、智能车载系统的系统层中，避免“生态碎片化”导致的智能设备安全漏洞被黑产肆意利用，覆盖终端设备超过1亿部；下一代安全通信库MesaLink TLS有效规避安全界里程碑事件”心脏滴血”内存安全漏洞所导致的用户隐私泄露事件再次发生；下一代可信安全计算服务框架MesaTEE，利用Intel SGX技术，为云上数据的完整性和保密性提供芯片级的安全保障，对于数据隐私和云安全有着非常重要的意义；大规模图数据库HugeGraph已广泛应用到网址安全检测、威胁情报分析、业务风控、数据安全治理中，在百度安全协助公安机关破获多起电信诈骗、伪基站、流量劫持、用户隐私窃取等重大黑产案件中，提供了打击溯源的核心能力，全方位实现从警务数据整合到分析挖掘，助理智慧公安新业态。


百度安全在提升全网安全生态综合治理技术水平上的努力，还体现在产品化。在2019年央视315晚会中，部分APP通过不平等、不合理条款的授权协议，强制索取用户个人信息的行为被曝光。不仅是315，近年来频发的隐私信息泄露和数据违规使用事件都在发出预警——确保APP隐私合规，保障用户个人信息安全，是所有APP开发者和运营者的必选项。作为**业内首个对外提供服务的APP隐私合规一键式检测工具，百度安全隐私合规助手已为APP开发者和运营者带来了有效的解决方案。**从2017年启动研发到2018年内部测试，百度安全隐私合规助手已实现对百度旗下主要APP和SDK的接入，确保了百度产品矩阵在收集使用个人信息方面的合规性。2019年，百度安全将这一能力正式对外开放，助力APP开发者和运营者高效且低成本地完成APP隐私合规检测，规避隐私违规风险。

2019年3月，国家“APP违法违规收集使用个人信息自评估指南”正式对外发布，为APP收集和使用个人信息的红线界定提供了具体的规则和意见指导。针对“指南”中的新标准、新规范、新要求，百度安全隐私合规助手第一时间对检测模型进行升级和优化，实现了对其9大评估项、32个评估点的全面覆盖和规则对齐。目前，百度安全为国家计算机病毒应急处理中心定制研发的APP隐私监测服务，已在国家移动互联网应用安全管理中心（CNAAC）应用检测平台上线。

## 5.3 产学研创新合作

在过去一年中，百度安全结合国家科研体系框架开展了大量隐私保护研究工作，参与国家重点研发计划**“互联网环境下的隐私保护与追踪取证项目”**，保障了整体研发方向的正确性、创新性和权威性，并取得了包括**差分隐私（DP）**、**审计取证**、**安全多方计算（SMC）**在内的多项“产研学用”成果，在推动企业产品的技术进步和先进隐私保护技术的应用落地的同时，也为理论研究提供实地验证环境。

展望2019，百度安全将以开放协作的心态加强与政府、行业、学术机构的多层次协作，持续通过创新技术的研发与开源参与到网络安全生态多方治理格局当中，在为用户创造价值的同时，也运用人工智能实现更有力量的网络黑灰产打击和公民个人隐私保护。同时，百度安全将开展数据经济时代隐私保护的前瞻性研究，驱动相关标准建立，为未来立法贡献行业实践与智慧，推动人工智能时代行业大数据的安全与融合。

## 关于百度安全

百度安全是百度公司旗下，以AI为核心、大数据为基础打造的领先安全品牌，是百度在互联网安全18年最佳实践的总结与提炼。业务由AI安全、移动安全、云安全、数据安全、业务安全五大矩阵构成，全面覆盖百度各种复杂业务场景，同时向个人用户和商业伙伴输出领先的安全产品与行业一体化解决方案。

百度安全以技术开源、专利共享、标准驱动为理念，联合互联网公司、安全厂商、终端制造商、高校及科研机构， 推动AI时代的安全生态建设，让全行业享受更安全的AI所来带来的变革。