

零售行业黑产进化手册

代码漏洞到AI诈骗作恶升级



前言

在互联网重构商业的二十余年里，零售业经历了从PC时代的门户展示，到移动时代的场景渗透，再到如今AI时代的智能跃迁。这是一个商业效率狂飙突进的黄金时代，也是一部与阴影中的对手——黑灰产——不断博弈的战争史。

如果您是一名资深的零售从业者，你或许曾经历过这样的时刻：



这本《零售黑产进化手册》，不是一本枯燥的技术文档，而是一份来自战场的“情报档案”。我们复盘了从拨号上网到大模型时代的三次黑产进化浪潮，剖析了每一个时代的攻击手段与防御逻辑。我们希望通过这本手册，帮助每一位零售人看清对手的底牌，在未来的商业战场上，不仅能跑得快，更能守得住。

PC时代

门户网站下的“原始狩猎”

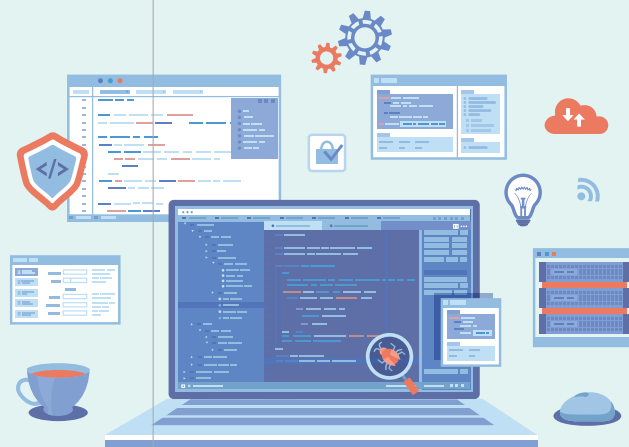
互联网的蛮荒年代，门户网站是信息核心载体，黑产的作恶手段也带着“粗放式”特征，技术门槛低但覆盖面广。

手段一

打接口，破解协议的“精准盗刷”

原理

黑产通过抓包分析门户网站、早期电商的公开业务接口，破解通信协议后伪造请求参数，绕开平台的身份验证、频率限制等风控机制，直接调用接口实施批量操作。



作恶场景：



批量盗取信息：

针对门户网站的用户登录接口、数据查询接口，伪造合法请求批量抓取用户账号、邮箱、手机号等核心信息，甚至通过支付接口漏洞窃取支付残留数据。



刷取平台福利：

瞄准电商、游戏平台的注册奖励、优惠券发放接口，构造自动化请求，无需人工操作即可批量领取红包、折扣券、虚拟货币。



恶意爬虫采集：

调用内容平台的视频、文章接口，批量下载无水印素材，或抓取商品价格、客户评价等商业数据，用于竞品分析或盗版传播。

获利方式：



信息倒卖：

盗取的用户信息按质量分级售卖，普通手机号每条 1-5 元，绑定支付信息的账号单条售价可达 50-200 元，百万级信息库可获利数百万元。



福利变现：

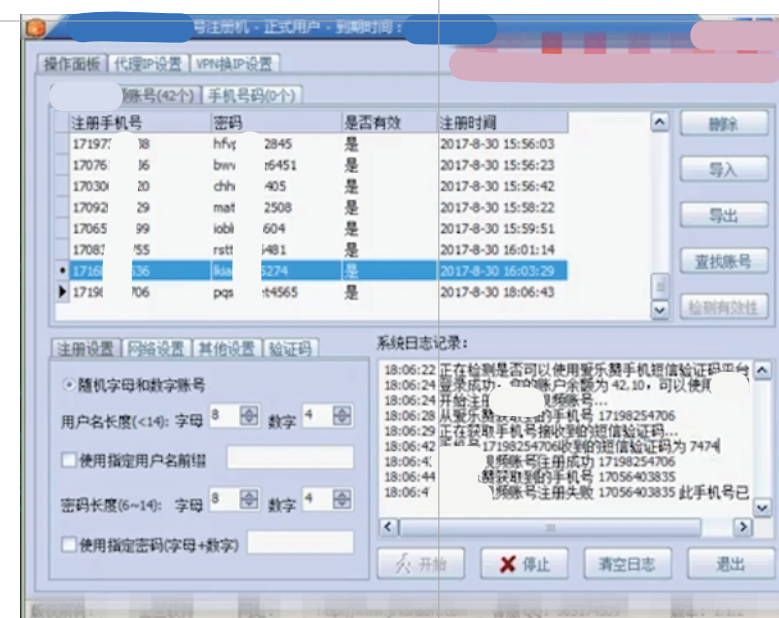
刷取的优惠券、虚拟货币通过二手平台、QQ 群转售，折扣券按面值 3-5 折转手，虚拟货币直接兑换现金，单工具单日可获利数千元。



数据转卖：

采集的商业数据、内容素材打包卖给竞品商家或营销公司，单份行业数据报价数千至数万元。

黑产工具操作：



一键开始，自动获取手机号和密码自动注册账号，接收短信验证码

手段二

ADSL 拨号：动态 IP 的“伪装作弊”

原理

利用 ADSL 宽带“断线重拨即换 IP”的特性，搭配拨号 VPS 服务器，实现 IP 地址快速切换，模拟不同地域、不同用户的访问行为，绕过平台的 IP 黑名单和频率限制。



作恶场景：



账号批量注册：

配合注册机工具，每注册一个虚假账号就切换一次IP，规避门户网站、电商平台的“单IP多注册”风控，批量生成海量“僵尸账号”。



恶意刷量投票：

针对门户网站的评选活动、电商商品评分、游戏排行榜，通过切换IP模拟真实用户投票、点赞、刷好评，帮助商家或参赛者刷取虚假热度。



撞库攻击试探：

用已泄露的账号密码组合，通过动态IP批量尝试登录不同门户网站，利用“一码通”的使用习惯，破解有效账号后盗走关联资产。

获利方式：



账号售卖：

批量注册的“干净账号”按用途定价，游戏账号每个 10-30 元，电商新用户账号每个 20-50 元，组建账号池批发给下游黑产可月入数十万元。



刷量接单：

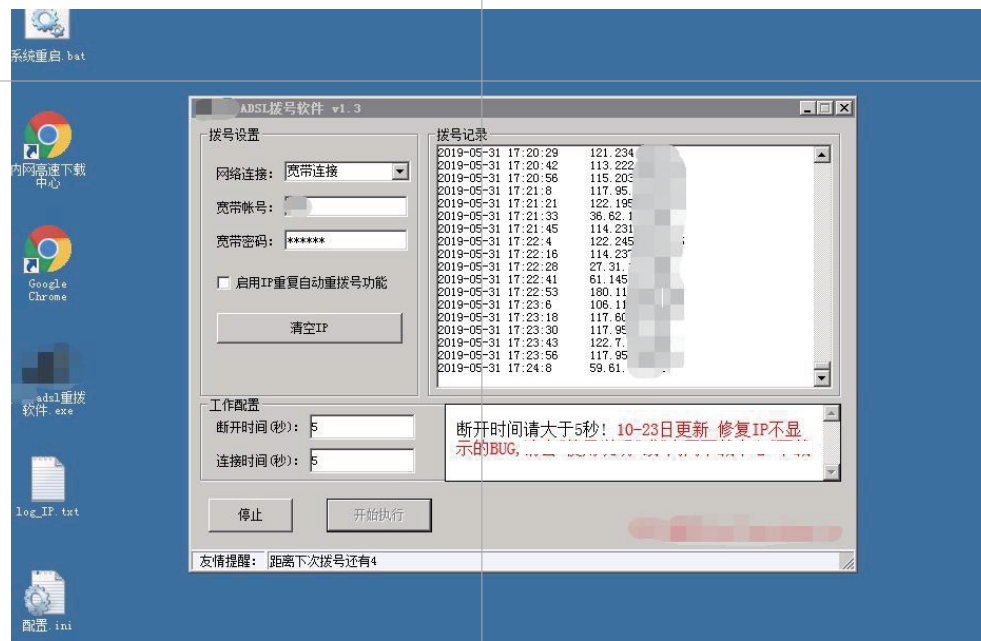
为商家提供刷评分、刷投票服务，单次活动收费按规模从几千元到几十万元不等，热门评选季单团伙月获利超百万元。



盗号变现：

破解的高价值账号（如绑定会员、虚拟资产的账号）直接转卖，或盗走账号内的余额、虚拟物品后折价出售。

黑产工具操作：



- 1、秒拨机桌面以及某拨号软件截图（黑产用户可在秒级切换IP）
- 2、风控难点在于，秒拨IP和正常用户IP取自同一个IP池，使用单一规则较难识别。

手段三

邮箱注册账号:海量养号的“基础燃料”

原理

利用邮箱的低门槛注册特性，通过接码平台获取临时手机号接收验证码，配合简单脚本实现邮箱账号的自动化批量注册，再通过点赞、浏览等简单操作“养号”，提升账号权重。



作恶场景:



搭建诈骗矩阵:

用海量邮箱账号注册门户网站账号、论坛 ID，批量发布钓鱼链接、虚假广告，或伪装成普通用户发布诈骗信息，降低被平台识别的概率。



参与活动薅羊毛:

针对门户网站的新用户抽奖、电商的注册礼、游戏的新手礼包，用邮箱账号批量参与活动，集中薅取平台补贴，账号越多获利越多。



垃圾信息轰炸:

用批量注册的邮箱账号给门户网站用户、企业邮箱发送垃圾广告、诈骗邮件，或在论坛批量发帖灌水，干扰平台正常运营。

获利方式:



账号出租 / 售卖:

“养熟”的邮箱账号按权重定价，普通账号每个 3-10 元，高权重账号（可发布广告、参与高价值活动）每个 50-150 元，批量出货利润可观。



活动套利:

集中薅取的新手福利、抽奖礼品，通过二手平台低价转卖，或兑换成虚拟货币统一变现，单日可刷取数百份福利。



广告代发:

为灰产商家代发垃圾广告、诈骗信息，按发送量或转化率收费，千条广告报价 50-200 元，规模化操作后收益丰厚。

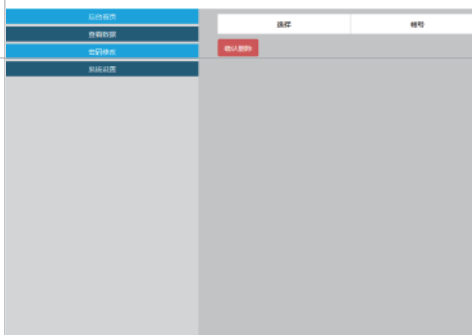
黑产工具操作:



钓鱼网站



输入账号密码



网站后台

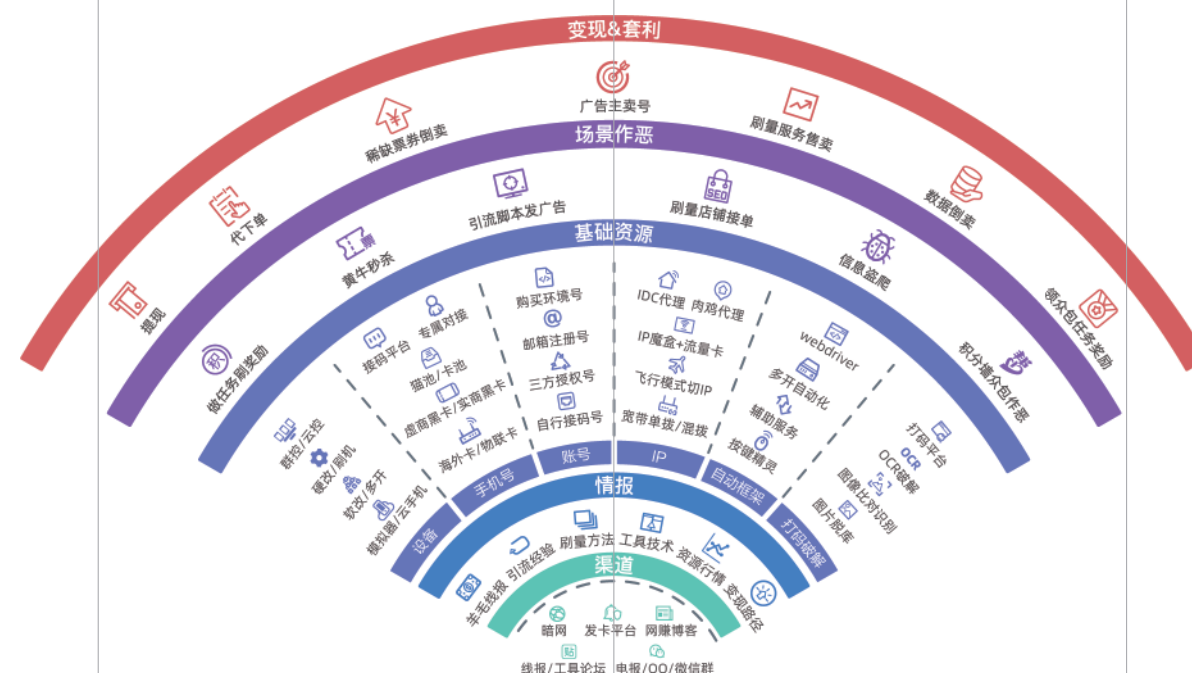
选择	帐号	密码
☐	123123112312	123123*

黑产已经获取账号及密码

场景渗透下的“精准收割”

移动设备的普及让互联网融入生活场景，黑产也从“广撒网”转向“精准围猎”，技术升级带来完整的获利闭环。

账号是黑产进入平台，伪装真人进行作恶的“唯一面具”，如何获取大量账号就成了黑产逐利的核心诉求。	
---	--



场景一

注册登录环节： 虚假注册与登录



作恶场景：

批量生成“僵尸账号”：

利用短信接码平台/微信接码平台，自动化批量注册账号。

篡改设备与秒播 IP 伪装登录：

修改设备参数、使用代理IP或虚拟定位，模拟不同地域、不同设备的登录行为，规避平台风控。

获利方式：

账号倒卖：

批量注册的普通账号以及“养熟”的高等级账号（有基础互动、无违规记录）通过不同等级，不同价格，打包批发给下游黑产。



骗取新人礼赠积分：

批量注册的新账号，获得平台赠与的新人福利（积分、算力，优惠券等）将账号进行分类，通过二级市场将手机号、账号进行转卖。



积分墙做任务：

黑产通过积分墙APP下发大量刷单任务，聚众真人进行登录注册，获取新人礼赠、优惠券，积分后，倒卖手号。

黑产工具：



短信接码平台



跑码群



安卓软改



安卓硬改/iOS重置



微信接码平台



首码手机号注册



混拨IP+电信



积分墙

场景二

运营活动： 薅取活动资源



作恶场景：



群控工具：

利用真机群控/运控与箱控，同时操控数百上千部手机，模拟真人滑动、点击、互动等行为，批量参与平台营销活动。



自动化任务脚本：

针对特定活动定制脚本，自动完成任务打卡、邀请好友、抽奖等操作，无需人工干预。



积分墙刷任务：

黑产通过积分墙APP下发大量刷单任务，聚众真人进行登录注册，进入平台薅取优惠、资源。

获利方式：



福利转卖：

刷取的会员时长、虚拟礼物、积分、等福利进行转卖，现金红包秒兑现，千级账号池单日可获利数万元。



活动代刷分成：

为普通用户或主播提供“刷奖”“刷礼物”服务，按获利金额的一定比例，收取分成。



账号增值售卖：

参与活动后获得高权益的账号，因附带会员、虚拟资产等价值，对手机号、账号分级、分类进行二级市场专卖获利。

黑产工具操作：



设备农场通过自动化脚本
大批量操纵手机进行作恶



启动按键精灵
自动完成App内的操作



积分墙发布真人任务

场景三

广告欺诈：
看似垃圾内容
根因是欺诈账号



作恶场景：

引流工作室向黑产购买大量虚假账号或成熟养号，自动化工具自动登录平台，在平台内执行自动化脚本引流，利用话术库自动生成随机话术，发布文本、语音、图片等导流广告。

获利方式：

- 

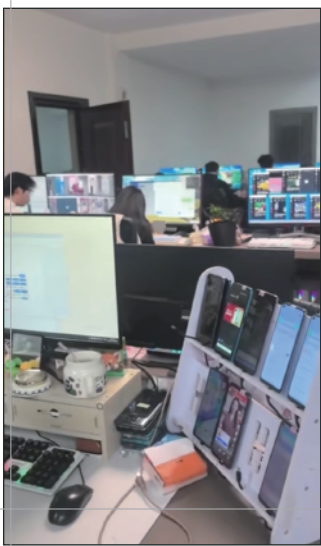
广告变现：
通过伪装账号，树立账号人设，吸引不同的类型粉丝，割韭菜。
- 

杀猪盘：
通过机器发送交友广告，引流至人工交流伪装白富美/高富帅，博取信任，诱骗投资，诈骗金额巨大。

黑产工具操作：



自动跳过-广告跳过工具



工作室刷广告

美妆行业经典案例

针对新零售行业，与互联网行业不同的是：黑产已从线上作恶发展至门店共同作恶，从黑产工作室纯技术作恶发展至众包真人作恶。

黑产通过作弊手段，掌握大量账号，规模化攫取品牌资源，低价倒卖品牌正装 & 中小样 & 美容服务等，破坏品牌价格体系与长期健康发展。

场景一： 薅取新会员试用装-黑产线上与线下配合作弊

通过线下黑产拍摄派样机二维码，线上黑产利用大量虚假设备+接码平台手机号完成规模化的派样机注册，获取大量品牌小样兑换码，以兑换码倒卖或小样倒卖的方式获利。

黑产路径



派样机



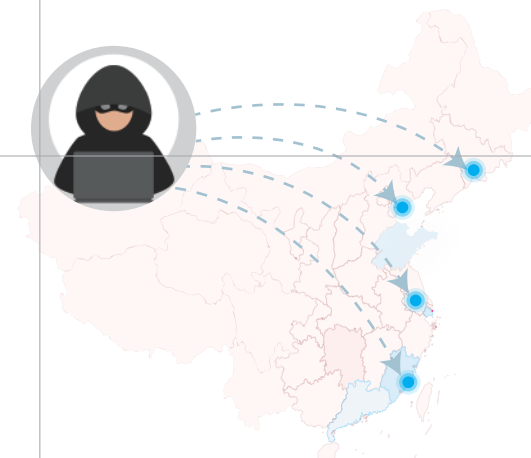
平台倒卖

场景二： 薅取新会员付邮费领取试用装 - 积分墙众包作案

黑产通过网站APP发布众包任务，提供众包用户返佣，使得大量众包用户协助下单，黑产规模化获取小样资源，以小样冲凑正装容量进行倒卖，冲击正装销量。

黑产路径

- 黑产发布众包任务
- 积分墙用户协助黑产下单
- 黑产规模化倒卖正装容量小样



下单购买小样

二手平台倒卖

场景三： 薅取到柜咨询的各类礼赠 - 积分墙众包与BC合作作案

黑产路径



发众包任务

为获取大量具备领样资格的会员账号。



接众包任务

线下背包批量领取并进行倒卖。



倒卖小样/新客礼

黑产直接倒卖卡券，BC可直接核销小样。

场景四： 专柜黄牛代下单 - 低价倒卖，价格体系收到冲击

黑产勾连全国大量柜台与BC超低折扣批量进货，违规获取底价产品，高卡级会员积分，大量礼赠小样。以不同形式不同渠道进行分发售卖。能做到柜台直邮，会员积分倒卖，回收代充，小样倒卖，获取高额利润。



全国进货

联系大量合作柜台和BC以低于品牌限制折扣进行批量进货



线上出货

将批量进货的正装以低于品牌活动价格进行出售，并支持线上付款后到联系好的柜台提货。

场景五： 散单代刷 - 内外勾结利用品牌高卡级会员获利

不为会员录入消费记录的操作，联合黑产将消费记录进行倒卖，代充至高卡级会员账号中从而提升会卡至高卡级会员。



线上交易

在社群中找好买家后直接将消费记录录入到买家的会员账号中。

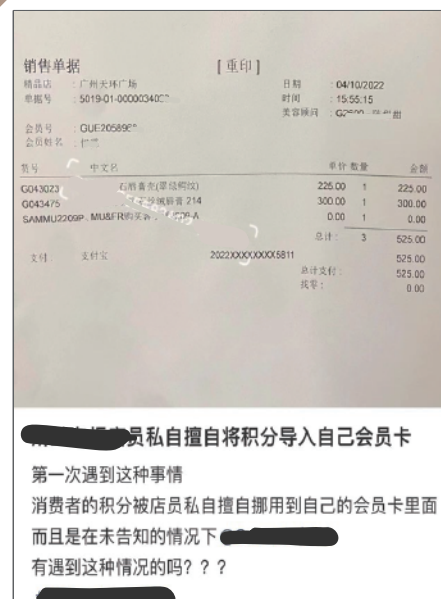


线上收票

联系全国柜台和导购进行消费记录回收。

真实消费者体验降低

消费者发现自己的积分被盗用后，品牌滞后处理消费者投诉，造成客户体验较差。



发现积分被盗，消费者发布至自己的社交平台，品牌和客户利益受损

软饮行业经典案例

场景：从瓶盖回收、二维码制作、平台化销售的完整产业链

黑产已经形成从瓶盖回收、二维码制作、平台化销售的完整产业链，上下游分工明确，实现利益各自利益最大化

黑产路径

普通用户
活动参与度

<70%

有效瓶盖
丢弃率

>30%

瓶盖回收端

回收瓶盖，制作url链接

出售

二维码发售端

平台化出售瓶盖内二维码

出售

职业羊毛党

利用大量资源扫码获利

获利方式

黑产
特性

瓶盖回收黑产
瓶盖回收端

- 具备大量瓶盖资源
- 缺乏瓶盖出售渠道

获利
方式

寻求下游
出售瓶盖资源

工作室黑产
二维码出售端

- 具备瓶盖出售渠道
- 缺乏瓶盖资源
- 缺少账号资源

依靠平台化
出售二维码获利

职业羊毛党
扫码获利端

- 乐忠于扫码博弈
- 充足的账号资源

依靠大量账号
资源扫码获利

工作室黑产仅依靠售码即能实现利益最大化

单次扫码
收益期望

0.50元

单次售码
平均价格

0.65元

! 单次扫码回报期望低于售码，且仍需投入额外的账号、人力成本。



1、平台发布
开瓶盖活动



2、收集大量瓶盖将信息译成二维码



3、通过扫码获取优惠



4、将优惠资源进行兜售

汽车行业经典案例

虚假拉新

活动信息

黑产总量：3131
成本：0.15¥

活动奖励

邀请好友注册可以获得积分

积分墙真人做任务

放单人：发布邀请人二维码
做单人：扫码注册

主要风险影响

- 产生大量低质账号
- 积分资源流失
- 商城优质商品流失

拉新一个账号获得50积分（0.5¥>黑产成本），每日可拉新10位，共计500积分

黑产手段

积分墙任务



任务作弊

活动信息

黑产总量：∞
成本：0.1¥（注册账号成本）
入口：某汽车app或者小程序

机刷脚本做任务

- ① 有软件的黑产可以自己使用，在软件中登录账号即可每天做任务获得积分。
- ② 黑产可以提供代挂服务。作弊用户将账号交给代挂黑产，黑产登录作弊人账号，每天可以自动做任务获得积分。

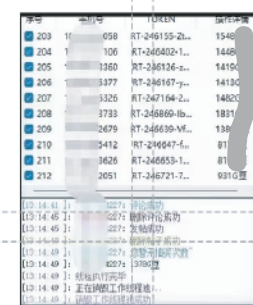
活动奖励

积分，一个账号一天可以获得100积分左右

主要风险影响

- 积分资源流失
- 产生大量低质账号
- 造成商城优质奖品流失

机器脚本界面



二手平台代挂服务



虚假线索

活动信息

黑产总量：971

成本：0.2 ¥

入口：活动链接、活动二维码

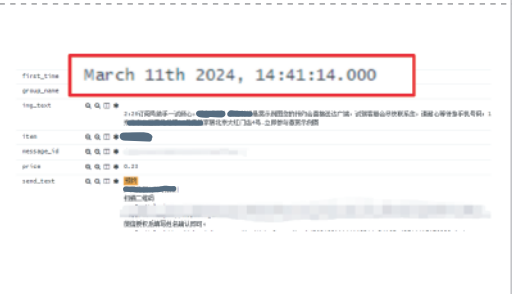
机刷脚本做任务

放单人：发布活动入口

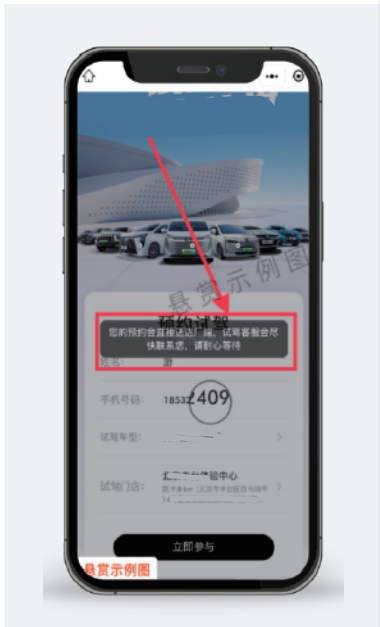
做单人：进入活动入口填写资料预约试驾

主要风险影响

- 线索营销投入浪费
- 产生大量虚假用户反馈



扫码填写信息



活动奖励

线索量KPI（活动方）

黑产手段

协同做单人完成回访任务

AI时代

智能伪装下的“隐形诈骗”

移动互联网时代发现的黑产工具、作恶手段还在持续危害平台健康，然而AI 技术的爆发式发展，让黑产完成了“智能化”蜕变，作恶更隐蔽、欺骗性更强，技术门槛和危害程度同步飙升。

无论是AIGC应用算力被薅取，会员权益被瓜分售卖，还是黑产利用大模型工具，而产生的新型风险，都表示我们着与黑产进入了全新的战场。

AIGC应用 被偷走的算力



批量在各大积分墙平台发布任务，真人完成任务后返回截图与手机号信息，区分手机号绑定账号的不同等级价值与会员权益，到二级市场价值售卖获利。



通过黑产工具，批量获取大量新账号，薅取新人专享算力，到二级市场进行批量售卖。



通过黑产资源和工具进行虚假助力和机刷日常签到，无限制免费薅取平台算力资源。

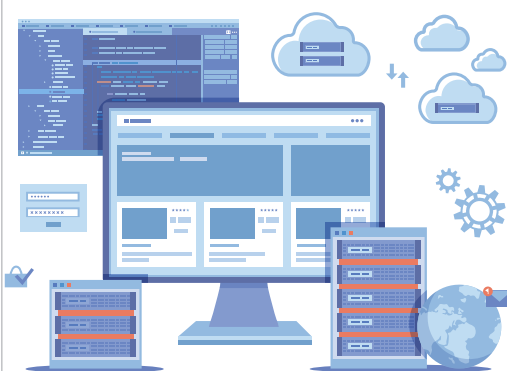
[illegible]

积分墙任务，通过真人注册



通过二手平台兜售，几乎可以支持全部平台功能

提示词注入攻击



在AI客服接听客诉电话后能自动发放平台补贴优惠券场景下，黑产利用AI客服背后大模型漏洞，进行提示词注入攻击，致使AI客服吐出大量优惠券。



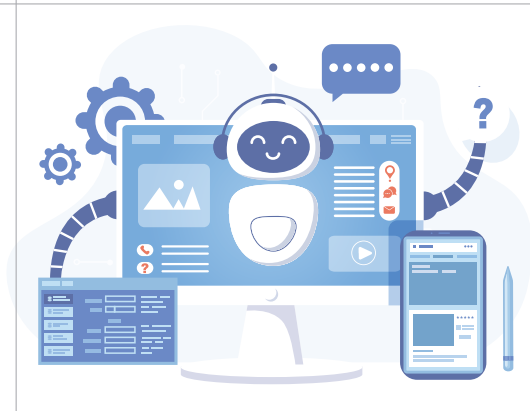
通过提示词注入攻击，利用AI生成非法内容，提供行之有效的违法犯罪行动方案

[illegible]

部分注入攻击提示词

新场景三

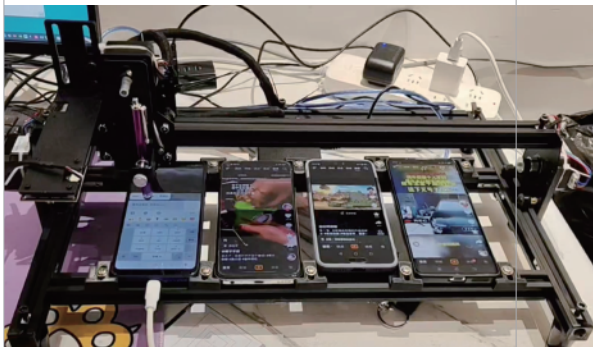
AI聊天工具



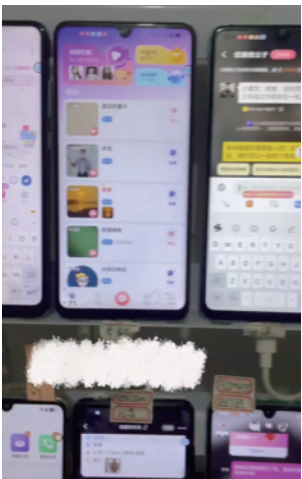
作恶场景:

1V1聊天场景下，在私密聊天室中男性需向女性主播支付一定的聊天费用，黑产通过自动化聊天工具，训练好的聊天模型，利用大量的设备与账号，同时在平台挂机，利用工具和聊天大模型的特性，敛取大量财富。

黑产工具操作:



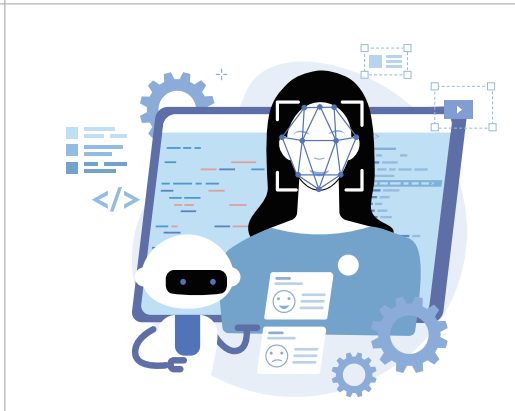
机械臂聊天工具



黑产利用AI自动化聊天

新场景四

AI换脸工具



作恶场景:

在AI客服接听客诉电话后能自动发放平台补贴优惠券场景下，黑产利用AI客服背后大模型漏洞，进行提示词注入攻击，致使AI客服吐出大量优惠券。

- 用 AI 换脸工具，置换明星人脸进行直播带货，视频切片，带货，割韭菜。
- AI换脸换声进行熟人诈骗。
- AI换脸进行支付认证，盗卡盗刷。

黑产工具操作:



AI换脸工具

行动指南

构建零售业的“数字防护系统”

黑产的进化从未停止，甚至在加速。从PC时代的“脚本小子”，到移动时代的“群控军团”，再到AI时代的“智能幽灵”，每一次技术的代际更迭，都成为了黑产收割零售红利的杠杆。

对于零售企业而言，这不仅是一场技术的较量，更是一场认知的博弈。面对这群“武装到牙齿”的对手，我们该如何应战？

从“被动救火”到“主动免疫”

摒弃“出现损失再修补”的滞后思维。在AI时代，黑产的攻击往往是毫秒级的，一旦破防，损失不可逆。零售企业需要建立“风控即业务基石”的顶层认知：

01 全链路视角：

黑产不再只盯着“领券”这一个环节，而是渗透在注册、登录、浏览、加购、下单、售后的全生命周期。风控防线必须前置，覆盖用户旅程的每一个触点。

02 数据驱动决策：

经验主义已失效。必须依赖多维度的用户行为数据（设备指纹、行为序列、关联图谱），用数据看透皮囊下的真实意图。

03 对抗性思维：

预设“系统一定会被攻击”，定期进行红蓝对抗演练，主动发现业务逻辑漏洞，跑在黑产前面修补篱笆。

构建“端云一体”的立体防御体系

思想的转变需要坚实的技术落地。我们建议零售企业从以下三个维度构建防御体系：

01 夯实基建（端侧防御）：

在APP/小程序端部署高强度的设备指纹和环境监测技术，精准识别模拟器、群控设备和改机工具，在源头掐断黑产的“作案工具”。

02 智能决策（云端大脑）：

引入AI风控引擎，利用机器学习模型实时分析用户行为。针对“真人众包”和“AI仿真人”，建立基于行为序列的异常检测模型，识别非人类的点击、浏览和交易模式。

03 联防联控（生态协同）：

黑产往往是跨平台流窜的。接入行业级的黑产情报库，利用手机号画像、IP信誉库等共享情报，让黑产在A处作恶，在B处寸步难行。

技术无善恶，但人心有方向。这不仅是一场保卫利润的战争，更是一场守护公平的战役。只有构建起强大的“数字免疫系统”，我们才能让每一次营销都触达真实的用户，让每一份福利都温暖真实的消费者。

零售黑产二十年进化全景图（PC - 移动 - AI）

PC互联网时代（门户/早期电商）	
核心特征 “原始狩猎” 利用代码漏洞，粗放式批量攻击	主要攻击目标 注册接口、抽奖接口、优惠券接口
核心作恶手段 1. 协议破解（打接口）： 抓包分析接口，绕过前端验证，批量发送请求。 2. 动态IP切换（ADSL）： 利用宽带拨号不断换IP，绕过频率限制。 3. 邮箱/手机号矩阵： 利用接码平台批量注册小号。	典型零售痛点 “一夜被薅空”： 促销活动刚上线，库存瞬间秒没，真实用户无法参与。
黑产工具进化 抓包工具、自动注册机、批量打码软件	防御核心逻辑 规则拦截： 基于IP黑名单、频次限制（如1分钟访问N次）、验证码拦截。

移动互联网时代（APP/O2O/新零售）	
核心特征 “精准围猎” 利用设备农场，模拟真人场景渗透	主要攻击目标 APP新客福利、会员积分、线下派样机、直播间人气
核心作恶手段 1. 设备群控（真机/云控）： 一人控制成百上千台手机，模拟真人点击。 2. 众包作恶（真人黑产）： 通过积分墙发布任务，雇佣真人去线下门店/线上领券。 3. 地理位置伪造： 篡改GPS定位，薅取特定区域的线下福利。	典型零售痛点 “虚假繁荣”： 注册量暴增但无留存；线下排队领小样的全是“黄牛”；直播间全是假人。

黑产工具进化 改机软件（一键新机）、群控系统、积分墙APP、GPS模拟器	防御核心逻辑 设备指纹与行为分析： 识别设备唯一ID，判断是否为模拟器/群控；分析点击轨迹是否符合人类特征。
AI智能时代（AIGC/大模型应用）	
核心特征 “隐形诈骗” 利用AI伪装，高拟真、智能化攻击	主要攻击目标 算力资源、智能客服补贴、高价值会员权益、品牌声誉
核心作恶手段 1. AI仿真人（Bot）： 模拟真人的浏览、点击节奏，养号绕过行为风控。 2. 提示词攻击（Prompt Injection）： 诱导智能客服吐出隐藏优惠券或敏感信息。 3. 深度伪造（Deepfake）： AI换脸过人脸识别，合成虚假买家秀/视频诈骗。	典型零售痛点 “真假难辨”： 评论区充斥AI生成的“完美好评”或恶意差评；无法区分是真人还是高智商AI在领券。
黑产工具进化 AIGC内容生成器、AI换脸/变声软件、自动化大模型攻击脚本	防御核心逻辑 以智御智（AI对抗AI）： 用更强的AI模型识别AI生成的特征；全链路行为序列分析；多模态内容识别。

用AI构建清朗可信赖的数字世界

联系我们：

400-610-3866

邮箱：pr@ishumei.com

官网：www.ishumei.com



数美科技公众号

了解更多风控前沿技术