威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

2022年黑灰产业研究报告

出品方：威胁猎人

THREAT HUNTER

以客户为中心 | 正直 | 求真

目录

Contents

前言

“从业者超 **200 万**，平均年龄 **23 岁**，市场规模高达 **1100 亿**”

这是来自中国互联网协会关于“黑灰产市场规模”的一项统计数据。

在巨额利益的驱动下，黑灰产从业者疯狂游走在监管边缘地带，黑产各类攻击资源高度市场化、模块化，产业链不同层级的团伙分工明确又配合严密。网络黑灰产业链在与各方对抗中不断升级，不少企业被迫卷入黑灰产的漩涡。

“知己知彼”才能打破攻防僵局，推动有效治理。黑灰产业链一直是威胁猎人重点研究的内容，威胁猎人发布**《2022 年黑灰产业研究报告》**（以下简称《报告》），客观呈现 2022 年黑灰产发展态势，深入分析黑灰产攻击资源、技术、场景并提出针对风险防治思路。

01

黑灰产发展现状

一、2022 年黑灰产发展现状

《报告》统计数据显示，2022 年国内的黑灰产业仍然非常发达，主要表现为：**规模更庞大、产业链结构更清晰、攻击更高效、覆盖场景更广泛。**

1.1 八亿余条黑灰产相关情报，2022 年黑灰产规模依然庞大

2022 年，威胁猎人情报平台监测到 **8 亿余条**黑灰产相关情报，黑产规模依旧十分庞大。2022 年黑灰产产业链整体结构可按照供需关系分为**资源、服务、变现**三个层级，并以此来区分产业链的上中下游：

资源层：作为上游，把控黑灰产作恶的底层基础资源；

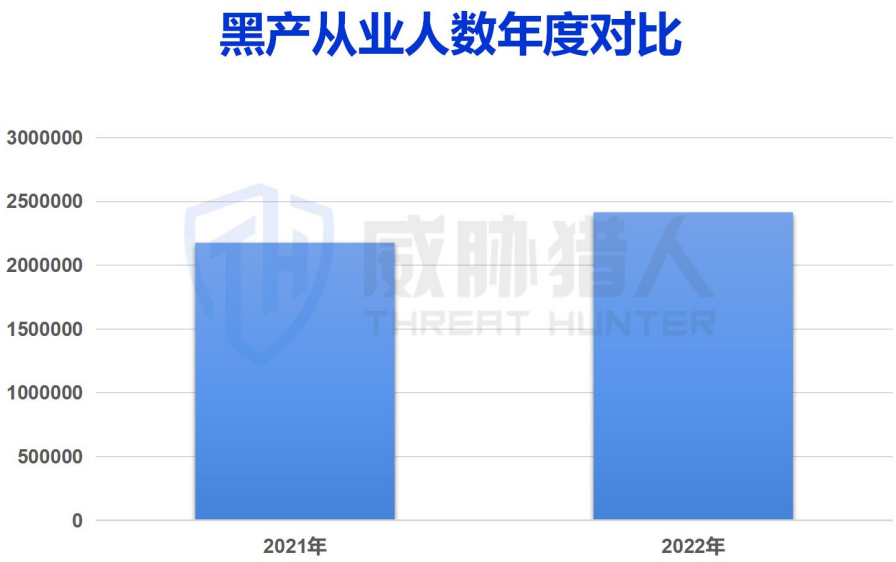
服务层：作为中游，整合上游资源和自身技术，为下游攻击提供各种服务支持；

变现层：作为下游，也就是实际黑产攻击群体，对业务进行攻击并最终实现利益变现。

黑灰产产业链组织及分工细致

1.2 2022 年黑灰产从业人员规模更广，较 2021 年增长 10%

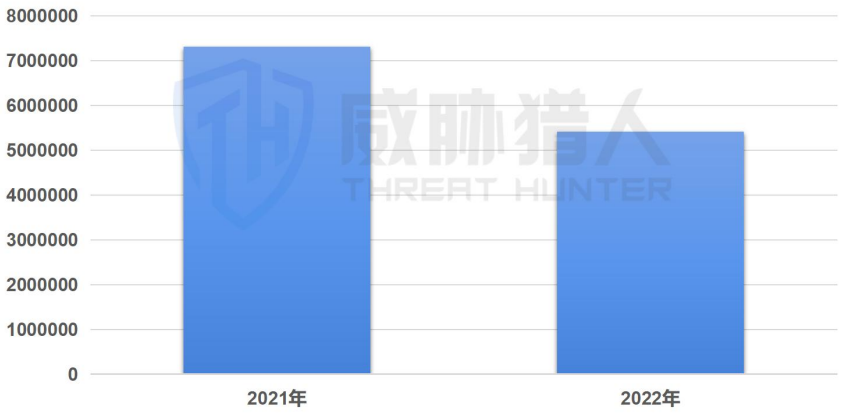
2022 年黑产从业人员规模更广，2022 年黑灰产从业人员数量较 2021 年增长了 10%左右。



1.3 受“断卡行动”持续影响，2022 年黑产资源新增数量减少

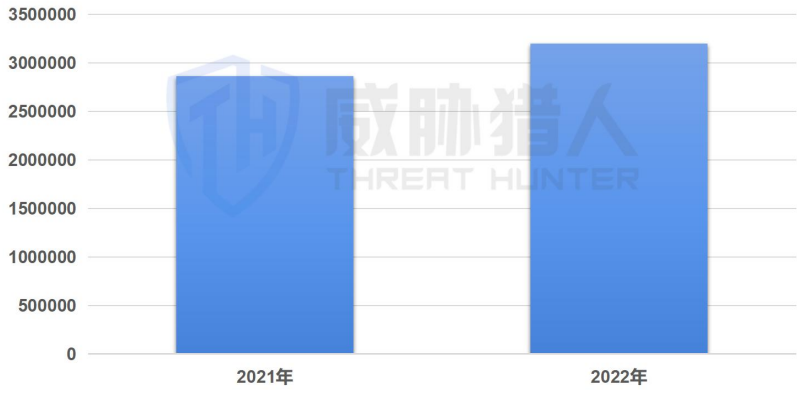
黑手机卡是十分重要的黑灰产资源。无论是营销作弊还是刷粉刷赞等，黑产都需要囤积大量账号，而账号的主要来源就是黑手机卡注册。2022 年“断卡行动”持续升温，黑产获取国内传统黑手机号的难度越来越大，**2022 年传统黑手机号增量较 2021 年下降了约 26%。**

传统黑手机卡年增量对比



黑 IP 同样是重要黑灰产资源之一，黑灰产利用海量黑 IP 绕过企业针对 IP 的风控，并隐藏攻击者的真实 IP。2022 年黑 IP 资源整体变化不大，**日活跃黑 IP 的数量较 2021 年增长了约 12%。**

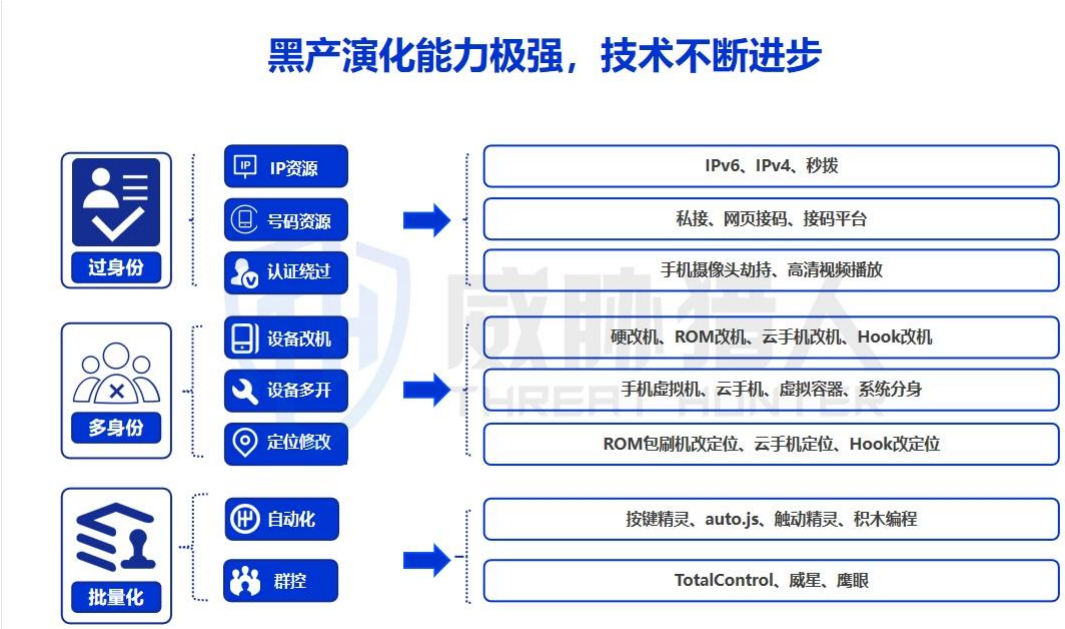
黑IP日活跃量年对比



黑银行卡是网络赌博、色情、诈骗等违法行为洗钱的重要资源。威胁猎人情报平台监测发现，2022 年新增的黑银行卡数量较 2021 年下降了约 20%，经研究推断，主要由于 2022 年“断卡行动”持续升温，各银行对于黑银行卡的治理取得一定成效。

1.4 黑产攻击服务划分为三大模块：“过身份”、“多身份”、“批量化”

威胁猎人针对产业链中游服务层进行深入研究及总结，将攻击服务划分为“过身份”、“多身份”、“批量化”三大模块，其中每个模块涉及到多种攻击技术。



过身份：利用伪造身份、人脸等方式**绕过平台认证**，可以注册虚假账号并正常参与平台业务和活动；

多身份：利用多开、改机、改定位等技术**伪造多个“正常”设备**，从而绕过平台对于单身份的限制；

自动化：利用**自动化脚本或群控工具**，批量完成注册、登录、点击等业务操作。

注：针对 2022 年黑灰产攻击资源、技术的具体分析，将在第二、三章详细讲解。

1.5 黑灰产作恶形势依旧严峻，涉及营销作弊、虚假刷量等 6 大重点攻击场景

2022 年黑灰产规模不减，作恶情况依旧严重。威胁猎人围绕营销作弊、虚假刷量、数据泄漏等 2022 年黑灰产重点攻击场景进行了深入研究，其中营销作弊仍然是黑灰产最主要的攻击场景，此外，刷量产业链不断进化，新型“高级账号”刷量悄然出现。

2022年黑灰产重点攻击场景

攻击场景	攻击对象
营销作弊	全行业
虚假刷量	社交、媒体资讯等行业
电商作弊	电商行业
信贷欺诈	金融行业
网络洗钱	银行、支付等行业
数据泄漏	全行业

注：更多黑灰产攻击场景分析将在第四章详细讲解。

02

黑灰产攻击资源分析

二、2022 年黑灰产攻击资源分析

2.1 2022 年黑手机卡资源增量波动较大

据威胁猎人观察，黑灰产通过**传统黑手机卡、拦截卡、海外卡**等方式为各风险场景作恶提供了充足的“弹药”，体现出黑灰产极强的对抗力和生命力。

2.2.1 传统黑手机卡

传统黑手机卡指非正常实名的手机 SIM 卡，渠道多样，有企业匿名卡、历史物联网卡、通信虚拟卡等等，主要特征是“在生命周期内被黑产固定持有”，即在这个期限内无论注册哪个平台，进行何种行为均可判断为恶意。

2022 年传统黑手机卡资源供给并不稳定，每月传统黑手机卡新增数量如下图所示：

经威胁猎人情报专家分析，增量波动较大的原因主要有两点：

1、受“断卡行动”的持续影响，卡商难以通过营业厅内鬼等渠道批量开新卡，不少卡商只能利用旧卡开展一些新业务；

2、传统黑手机号卡的最主要对接渠道——接码平台，在 2022 年受公安打击、平台跑路等现实因素影响，加剧了黑卡增量的波动。

面对监管平台的重拳出击，黑产团伙也出现了各种应对招数：

1、部分卡商发掘出新渠道进行批量开卡（如：**利用云平台号码隐私保护服务）**，因此部分时间段供卡量出现增长；

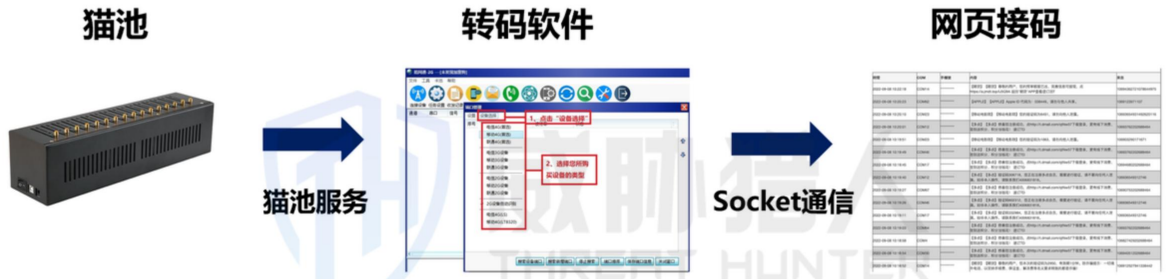
2、接码平台受多种现实因素影响，卡商逐步聚集到极少数**头部接码平台**，这些平台的服务器通常架设在海外，打击难度较大；

3、为了避免被轻易发现，越来越多的卡商采用**私密对接**的方式，2022 年私密对接的接码方式逐渐由“群接码”转变为“网页接码”。

群接码：卖家在 QQ、微信等社交软件中组建的群组容易遭到检测并封禁，因此需频繁组建或更换接码群，群接码较不稳定；

网页接码：有特定黑产团伙负责开发转码软件及网站，卖家可以通过软件生成专属链接，提供给买家用于接收短信内容（俗称接码房间），网页接码更加便捷和隐蔽，其原理如下：

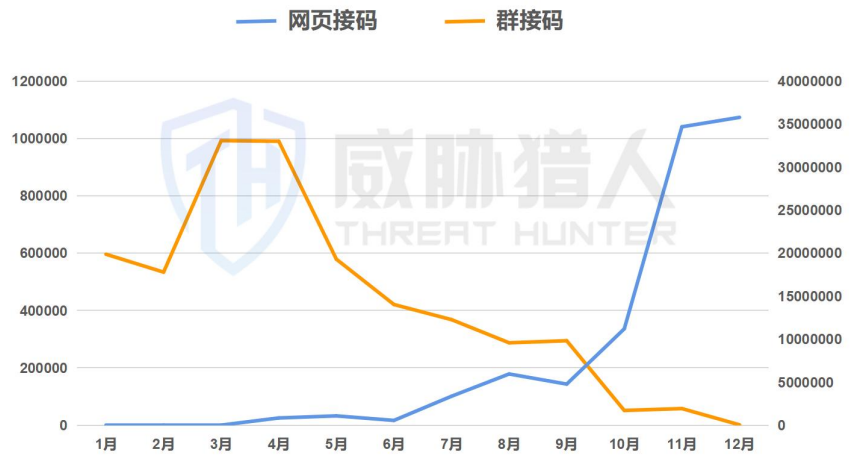
网页接码原理



利用猫池提供的服务，接收手机卡收到的短信　　通过Socket通信，将短信内容转发到指定网页

以下是 2022 年两种接码方式的走势对比，可以看出，**网页接码的规模持续增长，而群接码持续下降。**2022 年底，网页接码每月接收验证码的数量已达到**数千万规模**，而群接码几乎消失殆尽。

2022年群接码/网页接码走势对比



2.2.2 拦截卡

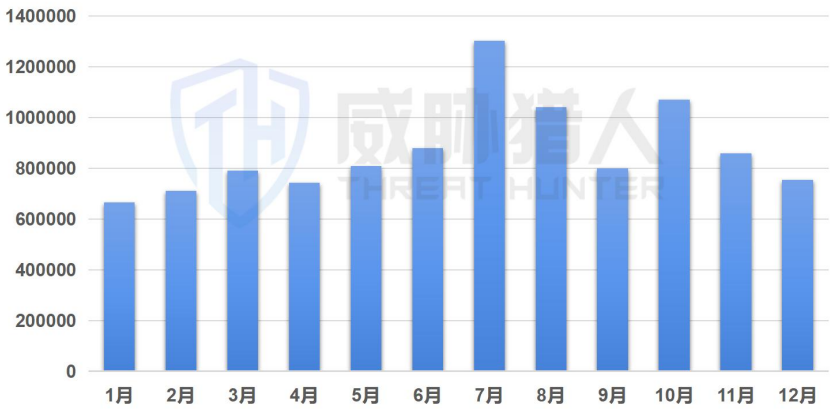
拦截卡主要特征是“手机号为自然人持有”，也就是“实名卡”，指在具备通信功能的移动设备上留下后门或植入木马，拦截正常用户手机设备收到的短信内容，利用其开展恶意行为，我们简称其为“拦截卡”。

威胁猎人调查发现，2022 年上半年拦截卡数量极少，主要因 2022 年初拦截卡平台集体跑路，从 2022 年 7 月份开始，陆续出现多个新的拦截卡平台并持续活跃，因此 2022 年下半年拦截卡数量明显增长。

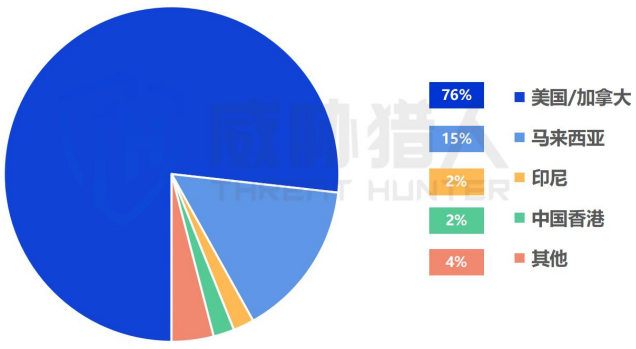
2.2.3 海外黑卡

海外黑卡无论是接码平台还是卡源都在海外，因此海外黑卡并未受到专项打击的影响，2022全年海外黑卡数量较为稳定，从海外黑卡的地域分布来看，主要集中在**美国、加拿大、香港、东南亚**等区域。

2022年海外黑卡每月增量

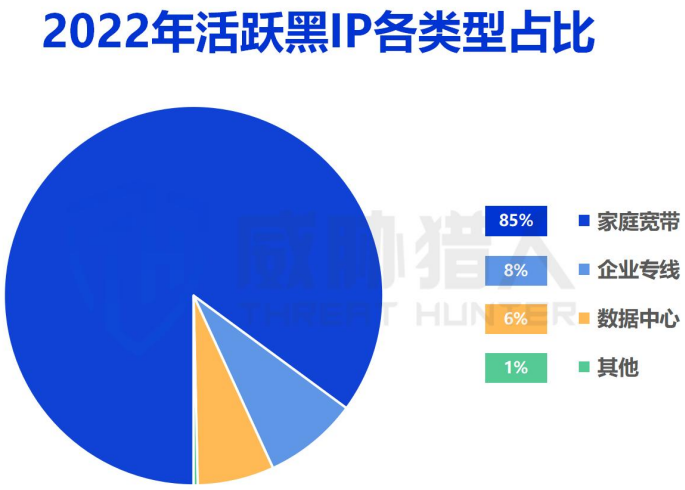


2022年海外黑卡地域分布



2.2 2022 年黑 IP 日活量稳定在 300 万左右，家庭宽带黑 IP 占比位居第一

2022 年黑 IP 资源数量较为平稳，日活跃的黑 IP 数量稳定在 300 万左右。威胁猎人研究员针对黑 IP 主要类型进行分析（排除掉 IP 类型未知的数据），发现家庭宽带类型的黑 IP 占比最高，超过 **85%**；其次是企业专线和数据中心，占比在 **6%-8%**左右；而移动网络和校园网络等其他类型的黑 IP，占比仅 **0.35%**。



家庭宽带：黑产所使用的**秒拨及动态代理 IP** 基本属于家庭宽带类型，主要利用“家庭宽带拨号每次断线重连，会重新获取一个新 IP” 的原理，**秒拨及动态代理 IP 价格便宜、数量大、切换方便**，因此成为了黑产大规模攻击的首选黑 IP 资源。

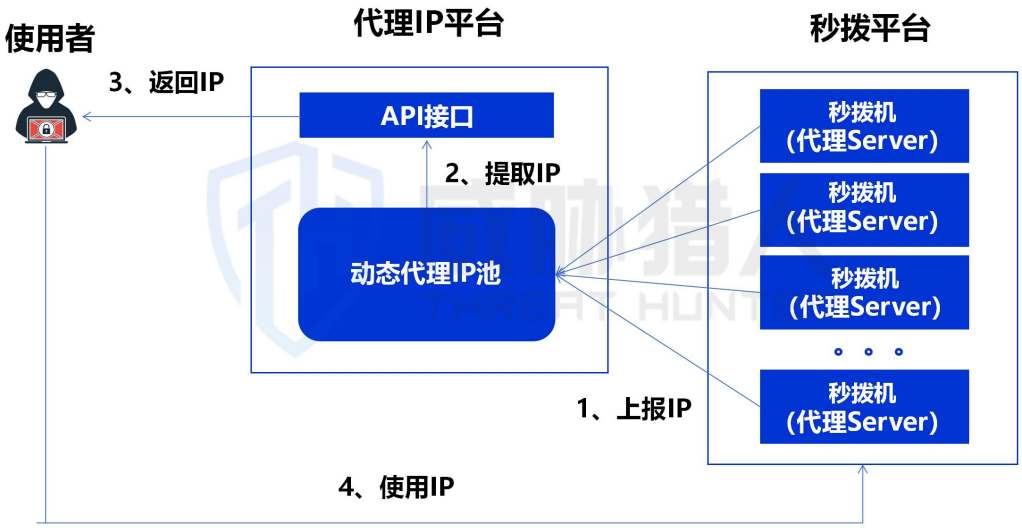
企业专线：企业专线类型的黑 IP 数量在近一两年有所上升，部分黑 IP 资源供给方通过企业身份申请企业专线 IP，并以优质池、独享池等方式进行出售。由于这些黑 IP **价格昂贵**，往往会被某些定向攻击的黑产团伙固定使用，**其识别难度更大。**

数据中心：数据中心类型的黑 IP 资源主要用于秒杀、抢购等营销作弊场景，该类场景往往需要**网速更快**的 IP 资源，因此资源供给方会选择租用机房，来满足部分黑产快网速 IP 资源的需求。

2022 年代理 IP 需求激增，黑 IP 的资源供给方以代理 IP 平台为主

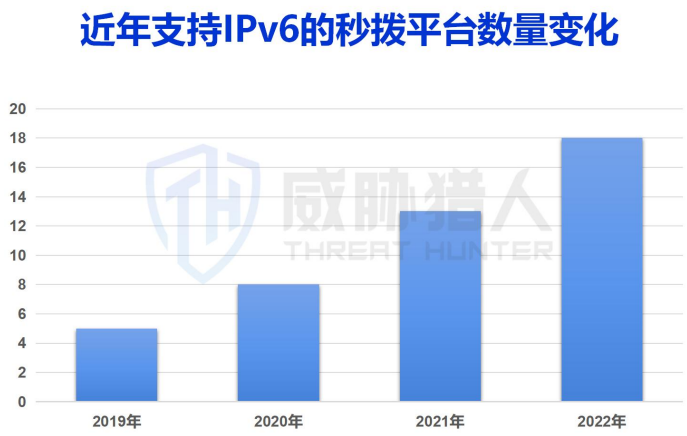
2022 年，黑 IP 的资源供给方主要是不合规的**代理 IP 平台**以及**秒拨平台**，其中以**代理 IP 平台**为主，随着各大应用开始展示用户 IP 归属地，代理 IP 的需求激增，无形中促进了代理 IP 平台的数量增长。同时，代理 IP 平台和秒拨平台联系紧密，很多动态代理 IP 都由秒拨平台拨出。

很多动态代理IP都由秒拨平台拨出



IPv6 日渐普及，支持 IPv6 的秒拨平台数量逐年增加

IPv6 在国内日渐普及，对黑 IP 资源供给方持续产生影响。目前，虽然代理 IP 平台尚未提供 IPv6 的代理 IP，但自 20219 年起秒拨平台已经提供支持 IPv6 的秒拨机，同时支持 IPv6 的秒拨平台数量逐年增加。



针对部分支持 IPv6 的秒拨机，经威胁猎人情报专家测试和分析发现：

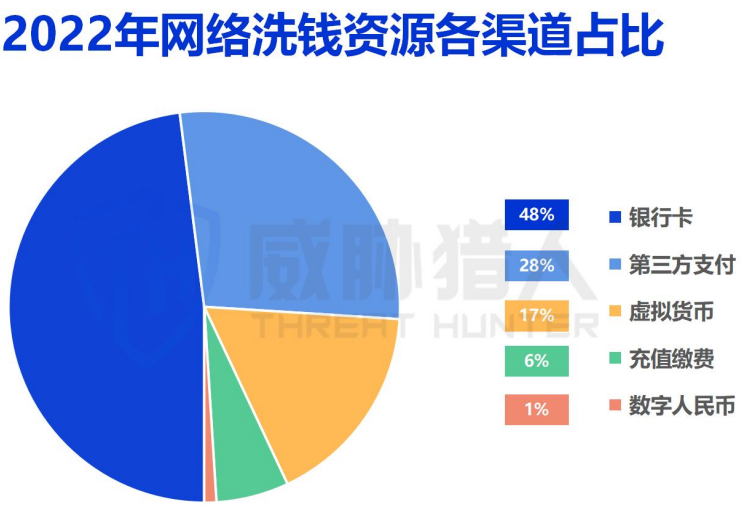
1、得益于 IPv6 远大过 IPv4 的地址空间，IPv6 秒拨机拨出的 IPv6 地址重复率非常低，攻击者完全可以做到每次攻击使用不同 IP 地址，这给黑 IP 的识别带来了新的挑战；

2、虽然 IPv6 秒拨机每次拨出来的 IPv6 地址不一样，但在地址分配上仍然遵循着一定的规律。威胁猎人通过观察到秒拨平台对 IPv6 地址分配的规律，结合捕获黑产使用的 IPv6 数据进行分析，形成识别规则，**构成一套 IPv6 风险识别算法**，能为企业检测出业务流量中 IPv6 流量在活跃时间内的风险值。

随着互联网的快速发展和普及，全球 IPv4 地址已濒临枯竭。而 IPv6 作为替代 IPv4 的下一代 IP 协议，在 IP 地址数量、安全性、移动性、服务质量等方面有着巨大优势，企业需要时刻关注黑产在 IP 资源供给侧的变化，并及时采取应对策略。

2.3 银行卡、第三方支付、虚拟货币成主要网络洗钱资源

据有关部门统计，目前我国非法赌博人数超过千万，每年境内流出涉赌资金超一万亿元，严重威胁国家经济安全。针对全网赌博、跑分等违法平台，威胁猎人情报研究员经过长期调查与数据分析发现，2022 年网络洗钱的主要渠道如下：



2.3.1 银行卡

银行卡仍然是最主要的网络洗钱渠道，尤其是针对网络赌博洗钱渠道。从 2022 年下半年起，黑银行卡呈现快速上升趋势，在世界杯期间月新增量超过 5 万。

2022年每月黑银行卡新增数量

通过对比近两年银行涉赌卡数量占比的排名变化发现，**排名上升最快的前 10 家银行中有 8 家是农村信用社**，由此可见，随着大行打压，赌资洗钱风险有所转移，农村信用社银行卡逐渐被赌博平台规模化利用。

近两年黑银行卡数量占比排名上升最快的前10家银行

	2022年排名	银行名称	同比去年上升
1	25	A省农村信用社	↑ 34
2	27	B省农村信用社	↑ 33
3	26	C市农村商业银行	↑ 21
4	28	Z省农村信用社	↑ 20
5	16	E省农村信用社	↑ 11
6	14	Y省农村信用社	↑ 10
7	8	G省农村信用社联合社	↑ 9
8	17	H省农村信用社联合社	↑ 9
9	24	K省农村信用社联合社	↑ 4
10	10	S市某银行	↑ 3

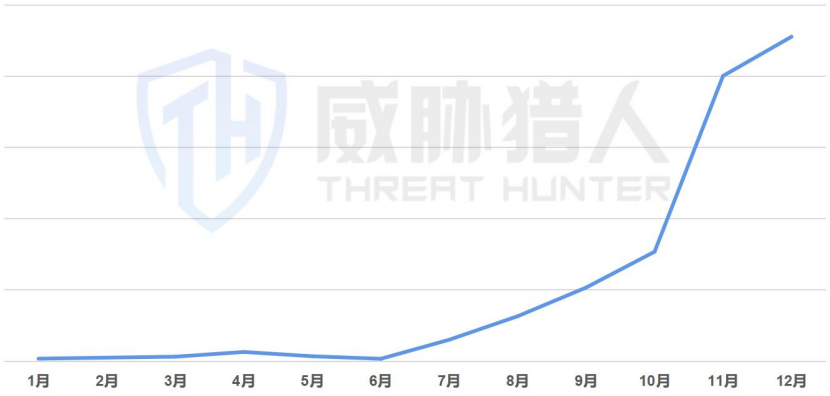
2.3.2 虚拟货币

由于匿名性、难以追踪等特点，虚拟货币长期被黑产用于洗钱等地下交易支付渠道。2022年，用于洗钱的虚拟货币活跃数量较为稳定，并于 2022 年 11 月世界杯小组赛期间达到峰值，月活跃量超过 5 万。

2.3.3 充值缴费 APP

黑产恶意利用某些 APP 的话费、电费等充值缴费功能，通过低价代他人充值缴费完成洗钱，2022 年，充值缴费的洗钱方式被更多黑产所利用。以代缴电费为例，2022 年下半年通过代缴电费进行洗钱的虚假账号数量呈快速上升的趋势。

2022年每月代缴电费洗钱热度走势



2.2.4 数字人民币

数字人民币钱包作为一种新兴的支付方式，从 2022 年 7 月起，普遍被网络赌博平台用于收款洗钱，呈现出明显上升趋势。

2022年黑数字人民币钱包每月活跃数量

数字人民币钱包主要分为四类，最低权限的**“第四类钱包”**属于匿名钱包，用户仅凭手机号便可开通，匿名账户之间可以任意转账，成为赌博平台绕过支付监管的新型充值方式。

威胁猎人调查发现，由于数字人民币“第四类钱包”无需绑定用户身份信息，有手机号即可注册，洗钱团伙会利用专门提供手机小号并接收验证码的平台，批量注册数字人民币钱包账户，或直接租用、购买普通民众的数字人民币账户，用于收取赌资。在将赌资进行转移后注销数字人民币账号，从而规避监管。

03

黑灰产攻击技术分析

三、2022 年黑灰产攻击技术分析

黑灰产在进行作恶时，会采用各类攻击技术进行批量、自动化攻击，以达到短时间内获得更多收益的目的，2022 年黑灰产主要攻击技术包括**改机技术、改定位技术、人脸认证绕过技术**等。

3.1 三大类改机技术依然活跃，定制 ROM 改机技术成为主流

改机是黑产大规模作恶所依赖的重要技术手段，主要指通过特定的技术，修改手机的品牌、型号、串码、IMEI、MAC 地址等设备信息，从而“伪装”成一台新的设备，黑产可以通过改机批量伪造新设备来绕过风控。目前，改机工具类型主要包括：**软件改机、ROM 改机、硬件改机。**

3.3.1 软件改机中，LSPosed 框架因隐蔽性高成为主要改机框架

软件改机：软件改机已经出现多年，其核心技术是通过抓取与设备信息相关的函数并修改函数返回值来达到改机效果。

软件改机一般都会用到 Hook 框架，Hook 框架包括 XPosed 框架、LSPosed 框架，其中 LSPosed 框架在近几年兴起并不断成熟，2022 年 LSPosed 框架已经成为了软件改机使用的主流框架，相比 XPosed 框架，LSPosed 框架更难以被检测。

以特征文件等检测点为例，LSPosed 框架相对不容易被检测出的原因如下：

检测点	XPosed框架	LSPosed框架
特征文件	Xposed对art虚拟机进行了修改，存在特征文件libxposed_art，以及开发包文件XpsedBridge.jar等	不存在
堆栈检测	Xposed对zygote进行了修改，存在特征堆：de.robv.android.xposed.XposedBridge.Main	不存在
主动类加载	Xposed 框架将自己的类加入到bootclasspath中，因此可以主动加载Xposed提供的API中的类来进行检测	不存在

此外 LSPosed 框架还有以下一些优势：

1、LSPosed 在设计之初就考虑到了对 XPosed 的**原生兼容**，所以已有的 XPosed 模块无需改动即可在 LSPosed 框架上运行。

2、对于开发者而言，LSPosed 依旧采用 Xposed 开发包开发模块，**没有额外的学习成本**，可轻易在 LSPosed 框架上开发想要的模块。

3、目前 LSPosed 框架**维护和更新比较稳定**，不用担心可用性问题。

3.3.2 定制 ROM 改机成为目前最主流的改机方式

定制 ROM 改机：从威胁猎人的攻防实践及客户实际测试效果来看，软件改机的成功率并不高，为了提高成功率，黑产也在不断开发更底层的改机技术，其中就包括定制 ROM 改机。

定位 ROM 也不是新技术，其核心原理是通过修改 Android 源代码进行改机。2022 年定制 ROM 改机技术更加成熟：一方面，有专业团伙负责维护各种品牌手机的 ROM 包（包括驱

动）；另一方面，有专业团伙负责解各种品牌手机的设备锁。在多方配合与成熟运作之下，无需从零打造“作案工具”。**目前，定制 ROM 改机已经成为了最主流的改机方式。**

与软件改机相比，定制 ROM 改机的优点如下：

1、ROM 改机所修改的源代码并未运行在目标应用进程中，因此防守方无法在检测上与之正面对抗；

2、ROM 改机无需 Root 手机，因此防守方无法通过检测 Root 环境来标记设备风险；

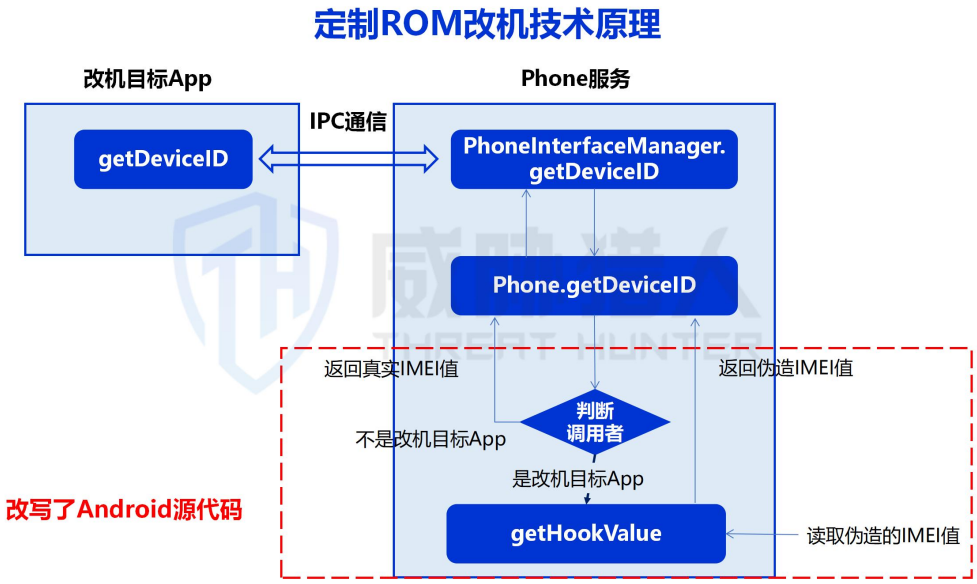
3、ROM 改机可以轻易修改设备的任意信息，且稳定性高。

定制 ROM 改机为何难以检测?

如果将**一台电器比作改机目标，**将控制其电源比拟为改机过程，软件改机则是“入室控制电源”，极易被检测发现，而 ROM 改机则是”直接控制发电厂”，从根源进行远程破坏，防守者很难与之正面对抗。

具体的技术原理如下：

我们以修改设备的 IMEI 值为例，解释定制 ROM 改机的技术原理。在 Android 系统上，获取 IMEI 值调用的 getDeviceID 函数，这其实是一个 IPC 调用。响应方是系统的 Phone 服务（对应的进程包名是 com.android.phone），并最终会调用到 Phone.getDeviceID 函数。通过改写该函数，根据 IPC 调用方的 uid 来判断是否是改机目标应用；如果是，则调用 getHookValue 返回伪造的 IMEI 值；如果不是，则返回真实的 IMEI 值。整个过程如下所示：



3.2 改定位技术中，“劫持系统位置服务”被黑产普遍使用

改定位，指修改设备可用于定位的信息，包括 GPS、wifi、基站等，从而将设备“伪装”到指定的地址。改定位技术被广泛运用于各种业务欺诈行为，如：

1.伪造虚假的司机出行记录骗取平台补贴；

2.将定位改到特定地点并通过社交软件的“附近人”功能进行色情引流；

3.限定地区参与的营销活动，通过修改定位突破限制获得活动资格等。

改 GPS 定位主要有以下几种方式：

1、比较初级的方式是将定位信息注入到目标 App，通过 Hook GetLastLocation 或 GetLastKnownLocation 函数，伪造返回的经纬度信息。这种方式比较容易被检测，黑产已经很少使用；

2、通过定制 ROM 技术也可以伪造 GPS 信息，原理和与改机类似，这种方式目前尚未被黑产普遍使用；

3、**目前，劫持系统位置服务被黑产普遍使用，**劫持系统位置服务通过 Hook 关键函数并伪造函数返回值，因不在目标应用进程空间而难以检测。

劫持系统位置服务被黑产普遍使用，其技术原理及具体步骤如下：

原理：在 Android 系统中，获取 GPS 信息会调用系统的位置服务；而该服务运行在 system_server 进程中，对应的 Java 类是：com.android.server.LocationManagerService，因此通过劫持 LocationManagerService 中的相关函数，可以达到伪造定位的效果。

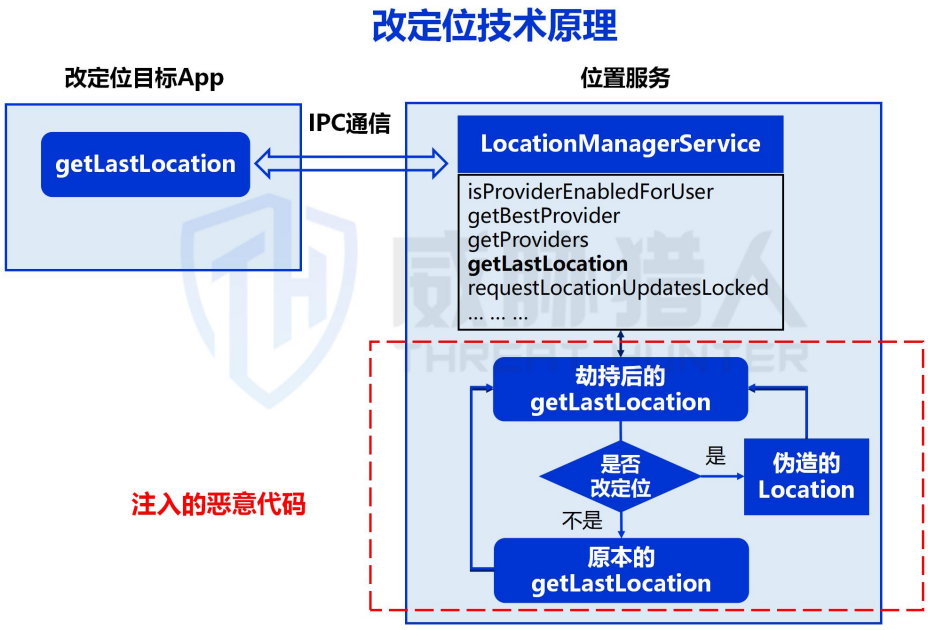
步骤：

1、向 system_server 进程注入恶意模块；

2、恶意模块的入口代码，通过 Class.forName 反射调用，找到 LocationManagerService 对象；

3、Hook LocationManagerService 对象的多个函数，其中就包括 getLastLocation 函数：

4、在劫持的 getLastLocation 函数中，判断是否需要改定位。如果是，构造一个 Location 对象，填充伪造的经纬度信息并返回；如果不是，则调用原本的 getLastLocation 函数并返回。



3.3 人脸认证绕过技术中，定制 ROM 劫持摄像头成常用攻击方式

人脸认证绕过，黑产俗称“过脸”或者“过人脸”，随着越来越多的应用进行实名认证同时使用人脸识别技术，黑产对于人脸认证绕过技术的使用更加普遍，具体包括定制 **ROM 劫持摄像头、云手机虚拟相机**等。

定制 ROM 劫持摄像头同样通过修改 Android 源代码来实现，由于这种技术改写了比较底层的 Android 源代码，因此难以被检测，成为了 2022 年黑产常用的劫持摄像头的攻击方式。

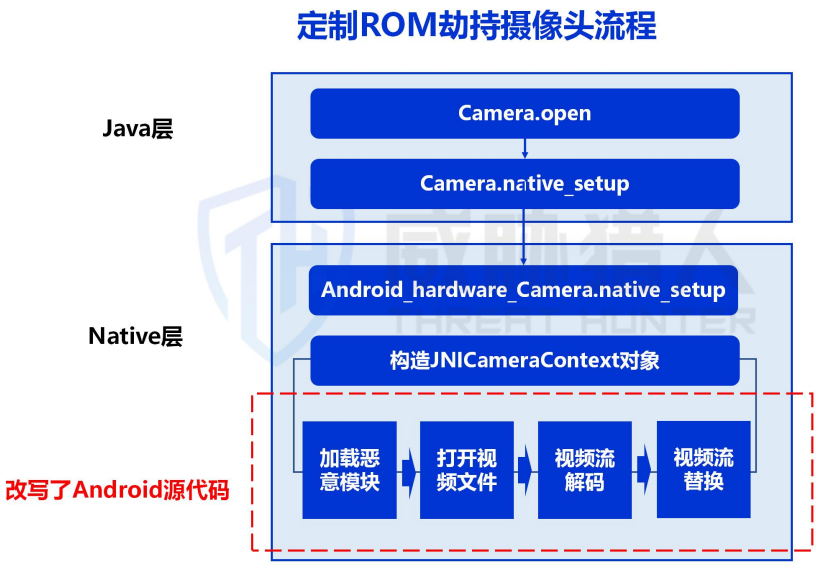
定制 ROM 劫持摄像头过程如下：

1、当应用使用摄像功能时，会调用 Camera.open 函数去打开前置或者后置摄像头，并最终进入 Native 层的 libandroid_runtime.so 调用 android_hardware_camera.native_setup 函数；

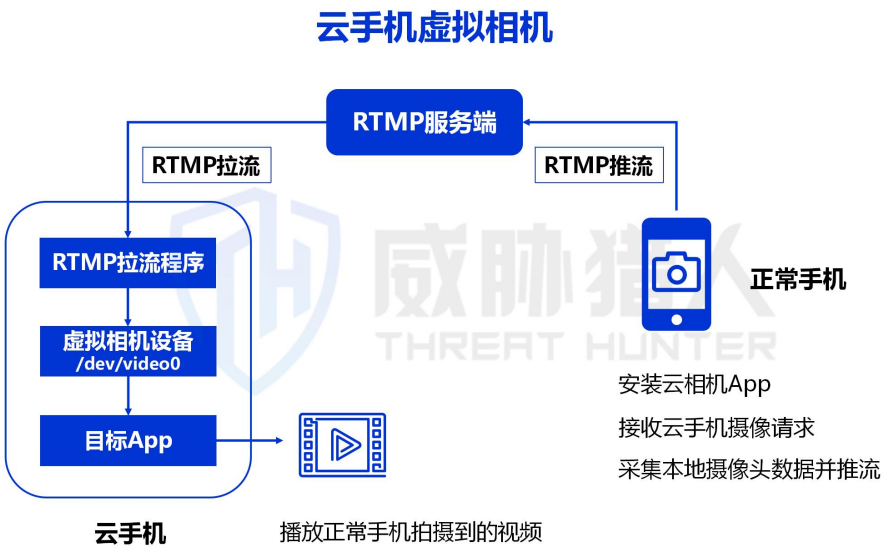
2、native_setup 函数中会并构造一个 JNICameraContext 对象（相机上下文），通过操作这个对象使用摄像功能；

3、劫持摄像头的定制 ROM 改写了 JNICameraContext 对象的源代码，再其构造函数中主动加载了一个恶意模块；

4、这个恶意模块集成了 ffmpeg 库（一款优秀的视频编解码库）。通过调用 ffmpeg 库，打开想要替换的视频文件，并对文件进行解码，将其转换成摄像头录制的视频流格式，并进行替换，最终达到劫持效果。



此外，威胁猎人通过蓝军攻防实践发现，**云手机虚拟相机也可以绕过人脸认证。**目前市面上出现了众多的**云手机平台**，其中大部分是基于瑞芯微(rockchip)的 RK 系列芯片开发，部分云手机平台开发并提供了“远程虚拟相机”的功能。从实际测试效果来看，**云手机虚拟相机绕过人脸认证的成功率较高。**



面对改机、改定位、人脸认证绕过等日渐猖獗的黑产技术，企业很难从单一技术角度与之正面对抗，可以从情报维度及时监测并分析使用该技术的各类黑产资源，及时进行针对性防御。

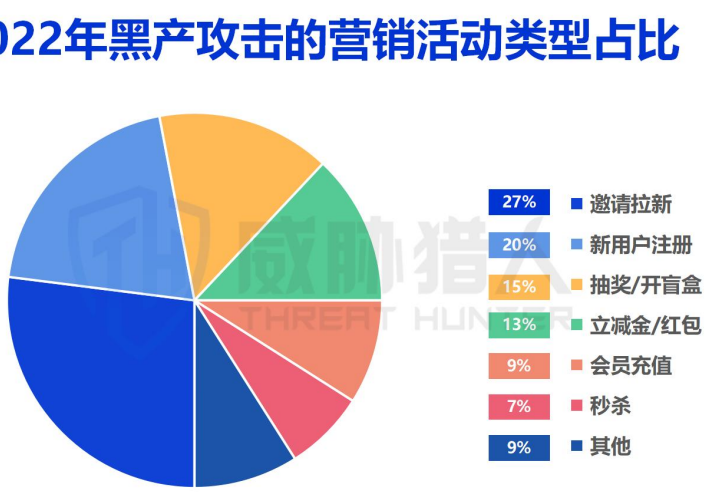
04

黑灰产攻击场景分析

四、2022 年黑灰产攻击场景分析

4.1 2022 年营销作弊仍然是黑灰产最主要攻击场景

企业开展营销活动时，往往会投入现金、实物或虚拟商品等各种奖励来吸引用户，但同时也吸引了大量的黑产参与活动并薅取奖励。2022 年营销作弊仍然是黑灰产最主要的攻击场景，攻击目标覆盖全行业，以下是 2022 年较为常见的活动类型：



2022 年各行业为刺激消费，立减金成重要营销活动类型

排名靠前的活动类型中，除立减金外，其他往年也都排名前列。立减金是一种发放给用户的现金券，在客户消费时可以进行抵扣。

2022 年各行业为了刺激消费，立减金成为了重要的营销活动类型，多家银行都曾推出各种形式的立减金活动。由于缺乏营销作弊的防控经验和手段，当活动参与资格及变现方式较为宽松简单，便极易遭到黑灰产的攻击。

以某银行立减金活动遭受到的作弊攻击为例

参与该活动的用户没，每人可领取 5 元立减金，黑产找到了该活动的变现路径，发起了大规模持续攻击，预估造成的营销费用损失将近 100 万，攻击全过程如下：

立减金活动攻击过程

活动规则	黑产攻击方式
一个手机号只能领取一次	黑产通过接码平台的黑手机卡注册了大量的账号
用户需要完成企业认证	通过爬取各种企业查询和信息公示网站，黑产囤积了大量的企业信息，包括企业名称、营业执照、企业法人个人信息等
5元立减金需要消费才能兑换	参与抽奖任务，每次金额5.16元，黑产实际只需支付0.16元，而抽奖任务可以进行交易从而变现

专业黑产团伙发起的规模化攻击对企业造成的损失极大，这种攻击往往需要具备以下两个要素：

1、大量虚假账号：单个账号营销作弊的收益往往不会太高，因此黑产团伙一般通过大量虚假账号来积累收益，虚假账号的主要来源就是黑手机卡，如何有效识别黑手机卡成为对抗营销作弊的关键；

2、自动化攻击：针对营销活动开发的自动化攻击工具，可以高效完成注册、拉新、助力等活动任务并薅取活动奖励，自动化攻击的主要方式有两种：

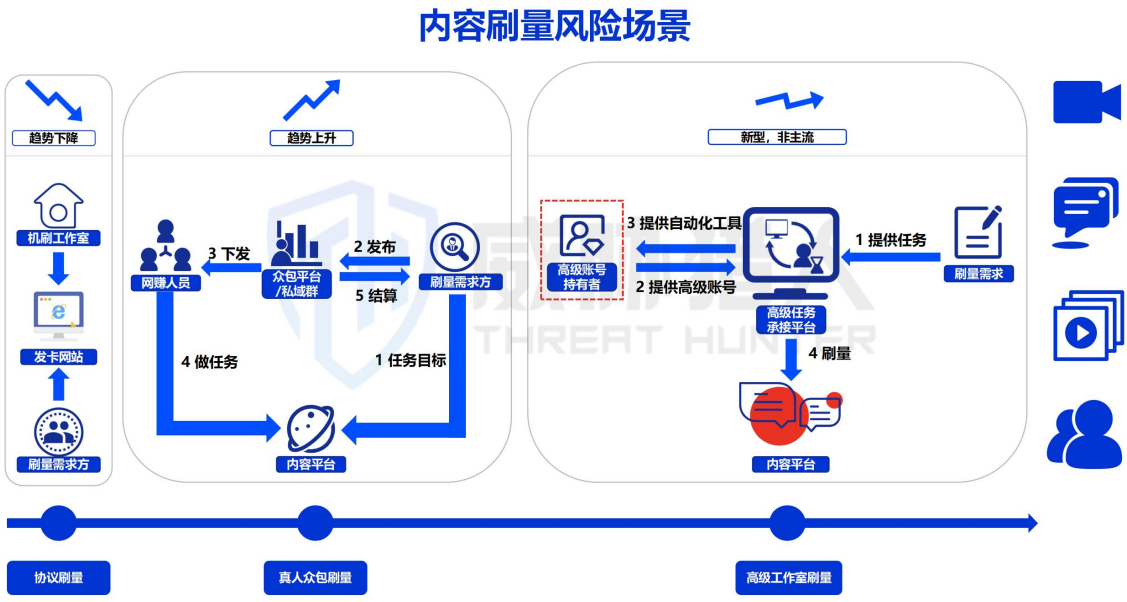
① **改机+群控：**通过改机技术伪造出多台设备，通过群控技术批量操控多台设备，对于这种攻击方式，如何有效识别风险设备环境成为关键。

② **协议攻击：**破解注册、登录以及跟活动相关的 API 接口，批量伪造接口请求。对于这种攻击方式，对 API 接口进行安全加固以及如何识别风险流量成为关键。

4.2 刷量产业链不断进化，新型“高级账号”刷量悄然出现

在如今“流量为王”的时代，刷量已成为互联网行业心照不宣的“潜规则”。由于各大内容平台以阅读量、粉丝数、点赞数等数据作为影响力的评判标准，内容发布者为了提高排名获得更高的曝光度，不惜制造虚假的流量数据。

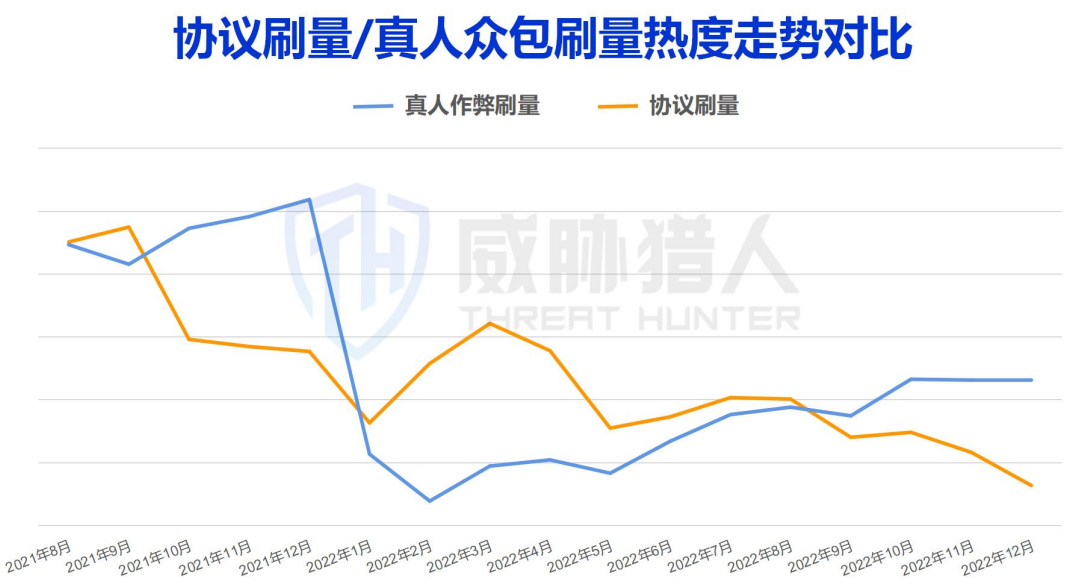
在流量思维的主导下，数据造假风气盛行。2022 年，内容平台虚假刷量热度依旧，刷量方式除了**协议刷量**和**真人众包刷量**之外，还衍生出了新型的**高级账号刷量**方式。



协议刷量：协议刷量是“流量造假”的原始手段，即直接采用“代理 IP+用户登录态”来模拟协议并编写代码，实现自动化刷量，简单、直接、技术含量低。

真人众包刷量：真人众包刷量指刷量者在“真人众包任务平台”或“刷量任务群聊”发布刷量任务，以任务赏金的形式吸引真人用户，并让其按照特定流程进行刷量。

协议刷量和真人众包刷量在 2021 年 8 月至 2022 年 12 月的热度走势如下，可以清晰看到协议刷量整体呈现明显下降趋势；而真人众包刷量在 2022 年初有明显下降，经研究分析主要是受到网信办“清朗”系列专项打击活动的影响，而在 2022 年 2 月以后呈现出逐步恢复并上升的趋势。



2022 年“协议刷量”明显下降，“真人众包刷量”稳中有升，经研究分析主要原因如下：

1、协议刷量的难度增加。随着各内容平台安全建设水位的不断提升，无论是协议的破解难度，还是绕过机器流量识别的难度，相比以前都大大增加，而且一旦被发现，会面临平台的严惩；

2、真人众包刷量效果远超协议刷量。真人众包刷量都是真人操作，难以从技术上进行识别。威胁猎人与国内某头部内容平台合作，进行真人众包刷量测试，实测成功率很高且平均速度很快，完成任务平均用时仅需 4 分钟；

3、真人众包刷量任务价格适中。目前真人众包刷量的任务类型主要为：下载、评论、点赞、浏览、收藏、关注、喜欢、投币等。这些任务的价格不算高，单价在 0.2 元/条左右，买家完全可以接受这个价格；

4、专项打击对刷量产业链影响较大。在监管部门专项打击活动期间对刷量产业链震慑效果明显，但由于刷量市场需求很强，专项打击过去一段时间后，不少真人众包平台很快恢复了刷量任务的发布，且任务数量持续上升。

2022 年，真人众包刷量成为了黑产刷量的最主要方式。此外，针对头部内容平台，黑产刷量衍生出了一种新型刷量手段：**高级账号刷量。**其刷量账号具有等级高、内容多、粉丝数量多等特征，如**“千粉号”、“万粉号”、“千粉千赞”**等，由于这类账号在平台上的可信度和影响力大于一般账号，因此在评分、排名等方面拥有更高的权重，从而可以达到更好的刷量效果。

高级账号刷量攻击的产业链示意图

4.3 机器作弊效果日益变差，真人作弊成电商作弊主要手段

2022 年电商场景因于平台风控日益完善，机器作弊效果日益变差，真人作弊成为黑灰产的主要作弊手段，而风险主要集中在**店铺刷单**、**黄牛代下**、**凑满减**和**恶意赔付**四个细分场景。

1、店铺刷单：店铺刷单指平台卖家付费委托刷单黑灰产，通过刷单工具、真人刷手等方式向指定的平台卖家购买商品、填写虚假好评来提升店铺销量、信用度和评分、获取平台流量。

店铺刷单不仅误导消费者的购物决策，引发店铺不公平竞争，还会严重影响平台的正常运营。2022 年度，威胁猎人监控到与电商平台相关的刷单线报超过 15 万，较 2021 年增长了 26.15%。

2022 年店铺刷单作弊的主要方式如下：

刷单手法	手法介绍
真人刷单	真人刷手接受任务后向指定的平台卖家购买商品、填写虚假好评来提升店铺销量、信用度和评分
直播引流刷单	主播在其直播间的商品橱窗挂低价值福利品而非商家主营商品，购买链接指向作弊商家，通过吸引真人用户购买+好评，来提高店铺整体排名，全程仅需店铺配合扫码即可。

2、黄牛代下：黄牛代下指黑灰产雇佣真人远程下单，来批量薅取活动限购的优惠商品，目前也形成了一个成熟的产业链。黑灰产实时监控各个商家的优惠商品，并通过 QQ 群、微信群等私域群组、报单网站发布代下方案，真人用户按照黑灰产提供的商品链接和地址下单，并赚取黑灰产提供的佣金，而黑灰产收到商品后进行转卖以获利。

黄牛代下导致大量优惠商品被专门的黑产团伙薅取，而正常用户基本享受不到优惠，企业白白耗损大量营销费用，久而久之正常用户甚至会流失到黑产的转卖渠道。

黄牛代下单流程示意图

代下产业链的的核心是：“下单发货到特定地址”。 黄牛中介在不同渠道发布的代下商品方案中，包含下单商品及统一的下单地址，而统一地址背后往往的大型的收货团伙/大货主，收拢来自全国大量分散的代下团伙的代下商品。因此，平台方可以收集分析此类下单地址，针对该类订单/账号实施对应风控策略。

3、凑满减：凑满减指羊毛党通过研究电商平台的满减要求，为以最优惠价格购买目标商品选择另外一款商品凑单达成满减条件，付款后再对凑单商品进行退货操作。可能引发凑单商品短时间内被大量退货的风险，以及商家数据异常和库存压力。

2022 年，威胁猎人检测到“凑满减”相关线报总量超过 68 万条，涉及到的黑产群组超过 1000 个，且整体呈上升趋势。值得注意的是，在电商平台大促活动期间，“凑满减”风险尤其普遍且后果更为严重。

以大促期间平台跨店“凑满减”为例：

大促期间，平台往往支持跨店凑满减，凑单商品大多可通过口令形式便捷传播、快速下单，同时平台及店铺支持无条件退款。同一个“凑满减”商品线报，往往会被不同的羊毛党生成不同的口令在社交群聊中大肆传播，因此凑单商品将会在短时间内面临大量退货风险。

4、恶意赔付：恶意赔付指黑灰产或职业打假人利用法律法规、电商相关禁止规则，通过向商家套话或向有关部门举报等方式，下单商品并恶意发起售后申请，向商家及平台施压要求索赔的行为。部分赔付教程通过引流、付费等方式被广泛传播及实操，极大影响了商家和平台的正常运营。

2022 年，威胁猎人通过监测相关黑灰产论坛及社群，挖掘黑灰产恶意赔付方案超 30 例，主要集中在头部电商平台。通过对方案进一步分析发现，当前的赔付方案主要围绕不发货、商品宣传违禁词、售假、三无、违禁品、食品安全等问题，寻找存在这些漏洞的店铺并发起恶意售后申请。

以某电商平台“三无产品赔付”方案为例：

该方案展现了赔付思路及操作流程，包括如何筛选赔付商品链接、下单、收货注意要点、赔付话术等，具体内容如下：

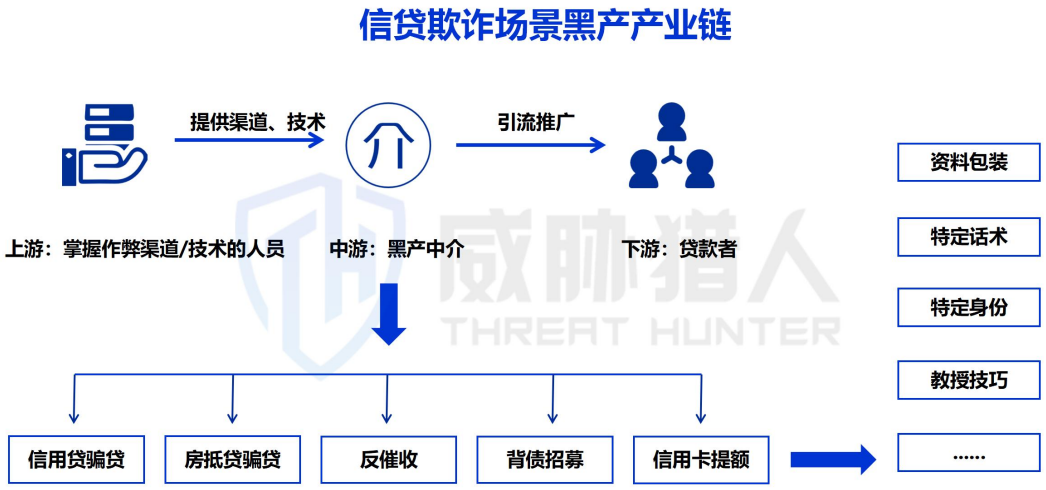
某电商平台“三无产品赔付”思路及流程

4.4 金融信贷欺诈给金融机构带来大额经济损失

随着金融+互联网的发展，金融行业通过数字化转型为用户提供灵活与便捷服务的同时，也面临着黑产不断迭代演变的各类欺诈威胁。其中以金融信贷欺诈最为严峻，给金融机构带来了坏账和大额经济损失。

金融信贷欺诈：黑产中介利用贷款审批漏洞为贷款者申请贷款，或通过特定话术等方式，为贷款者成功申请延期、减免利息，而中介从中赚取高额提成，这类作恶行为会造成信用机构资金损失、大额坏账。

当前信贷欺诈场景黑产产业链结构如下：



- 上游主要是掌握作弊渠道或技术的人员，负责提供撸贷渠道和技术；
- 中游主要是信贷中介群体，负责作弊方案的传播，并进行实际的代理操作
- 下游主要是骗贷群体，作为实际的贷款者，骗贷群体主要分为几类：

①因没有资质而被银行拒绝的用户；

②想进行退息、退费等操作的用户；

③被中介教唆或者恶意隐瞒而进行贷款的用户。

在信贷欺诈中，黑产的攻击场景可以细分为：**骗贷、反催收、背债招募、信通卡提额、退息退费**等，其最终目的多为通过伪造资质证明，达到过身份的目的。主要的欺诈思路包括但不限于伪造资质及银行流水、利用特定话术反催收等。

信贷欺诈的具体作恶思路如下：

-

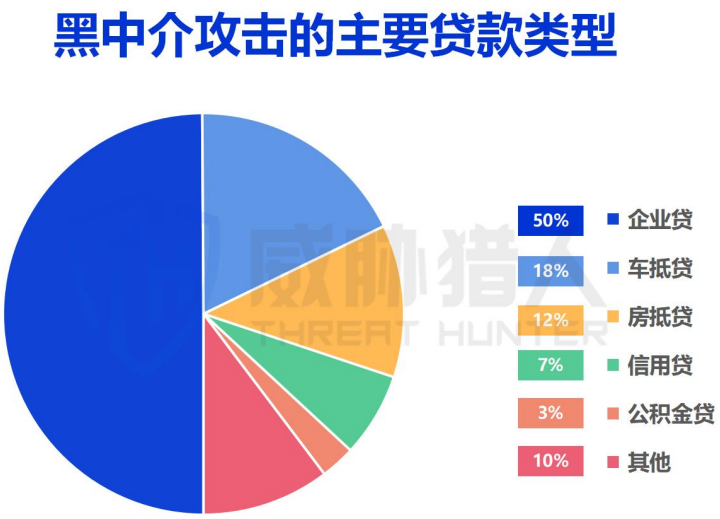
① 伪造贷款用户资质：黑产通过伪造资料帮助违约用户贷款，其本质是对申请人信息进行造假，常见造假项包括：工作单位、房产信息、公积金、工资流水等。

② 仿冒银行 APP 制作银行流水：黑产通过仿冒假银行 APP 伪造虚假流水，难以发现异常。该方法主要利用了不同银行间的信息差：假设黑产想去 A 银行申请贷款，并制作伪造 B 银行的虚假 APP 及虚假流水，申请过程中黑产会向 A 银行工作人员展示 B 银行的虚假 APP 及流水，因此 A 银行不仔细分辨的情况下很难发现异常。

③ 提供反催收特定话术：2022 年，大量的信贷客户由于疫情原因发生信贷逾期。很多黑产向这些客户提供反催收的服务，最主要的手法就是提供反催收的特定话术和具体方法，服务包括停息挂账、罚息减免、投诉赔偿、征信修复等。

黑中介攻击的主要贷款类型中，企业贷占比近 50%

2022 年威胁猎人监测到黑中介攻击的主要贷款类型包括企业贷、车抵贷、房抵贷、信用贷、公积金贷、社保贷、保单贷、创业贷、装修贷、税贷、流水贷、烟草贷、消费贷、学历贷等，**其中企业贷成为金融信贷欺诈者首要的攻击目标，占比将近 50%。**



4.5 2022 年捕获多个洗钱事件，预估涉案金额过亿

通过充值缴费 APP 进行洗钱的方式被众多黑产所利用，2022 年威胁猎人风险情报平台捕获到多个相关案例，**涉及 App 超过 10 个，预估涉案金额过亿。**

以捕获到的某**充话费洗钱事件**为例，黑产作案过程如下：

1、赌客在网络赌博、色情等违法网站上进行充值，选择支付方式为充话费；

2、赌客点击充值，则会跳转到某违规聚合支付平台；

3、与此同时，普通用户通过部分渠道购买打折/低价话费，进行话费充值；

4、聚合支付平台根据充值金额在某些 App 上发起等额的话费充值请求，生成订单并获取支付链接；

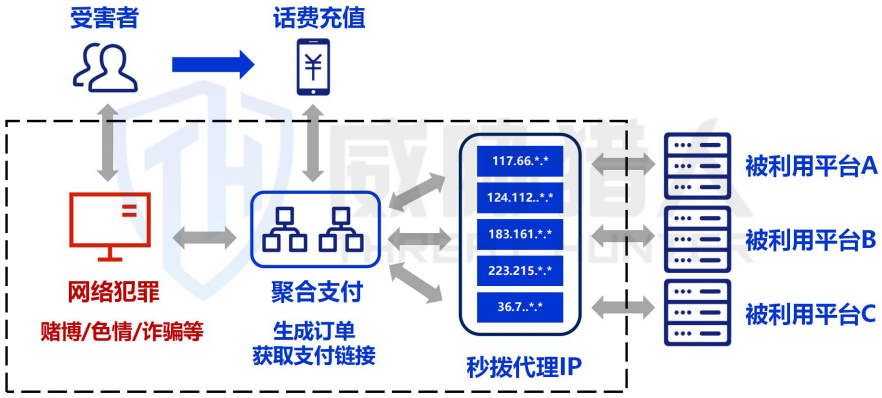
5、聚合支付平台将获取的支付链接返回到赌博平台；

6、赌客根据支付链接完成话费充值，成功“上分”。

于是普通用户的话费，就这样摇身一变成为了赌客的赌资。

威胁猎人情报人员发现，非法第四方平台通过聚合第三方支付平台、合作银行及其他服务商接口，对赌博平台提供综合支付结算业务。在此基础上，四方支付平台需生成大量充值订单，极易被充值服务平台识别为异常行为，为了规避充值服务平台的检测与监管，非法四方支付平台常采用“代理 IP”的形式隐藏身份，使网络赌博平台支付的违法行为更加隐蔽。

黑产绕过限制流程示意图



05

风险对抗思路

五、风险对抗思路

黑灰产日渐猖獗，让互联网、金融、电商、游戏等各行业深受其害。对于防守方而言，不能只是被动的防御，更需要持续的监测与响应，主动掌握黑灰产的动向。因此，**情报能力就变得尤为重要。**

无论是传统的黑灰产攻击场景，还是最近愈发严重的因 API 管控不当引发的数据安全问题，都可以**以情报为依托，建立风险管理的安全基线。**

利用丰富的黑灰产情报数据，企业可以：

在外部黑灰产治理中，通过全网多渠道监测及时监测、感知攻击风险，分析提炼出黑灰产具体动向、使用工具/物料等攻击信息，从而及时进行针对性防御。

黑灰产在发起攻击时必然会用到一些资源，比如 IP、黑产作恶工具等，利用威胁猎人丰富的**黑灰产情报数据**，提取黑产攻击模式及资源特征，与企业业务中的异常流量进行匹配，快速识别风险：

1、利用威胁猎人风险情报平台监测到的**风险 IP 标签**，对客户业务流量进行标记，一方面持续监测各业务 API 的风险 IP 访问趋势变化，另一方面通过对比数据，分析出正常用户与风险 IP 在该 API 下的请求行为序列的区别，判定该 API 是否有被攻击的风险；

2、针对攻击 IP，提供**风险 IP 画像**访问次数、地域、风险等标签信息，以 API 接口的方式实时输出攻击特征 IOC，之后再联动企业其他安全系统及时阻断攻击流量，提高阻断的效率 ，实现多点防御。

借助“情报”能力，企业可以从全局视角出发，全面、及时感知内部 API 资产风险与黑灰产团伙的轨迹与动向，精准预警并输出攻击者的 IOC 情报等，然后联动风控系统或 WAF 等快速处置攻击风险，面对日益严峻的黑灰产风险与挑战，做到从容应对，有力反击。

威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

关注“威胁猎人”

深圳永安在线科技有限公司

总部地址：深圳市南山区科华路3号讯美科技广场3号楼1609

官方服务热线：400-809-3699

官方合作邮箱：marketing@threathunter.cn

官网地址：www.threathunter.cn