威胁猎人
THREAT HUNTER

以 情 报 构 筑 数 字 化 安 全 基 石

黑产大数据

2023年互联网黑灰产研究年度报告

THREATHUNTER

目录

Contents

前言

2023 年，黑灰产从业人员人数超过 580 万，威胁猎人捕获到的国内作恶手机号数量高达 625 万，日活跃风险 IP 数量 602 万，洗钱银行卡数量 87 万。

从百万级黑灰产业链规模、大幅提升的攻击资源量级可见，2023 年是黑产攻防对抗空前激烈的一年，推陈出新的攻击资源和技术成为黑产攻击的“保护色”，因难以监测黑产攻击行为和溯源潜在风险，不少企业遭受严重损失，成为业务安全建设中亟需攻破的难点。

威胁猎人发布**《2023 年互联网黑灰产研究年度报告》**，针对 2023 年黑灰产业链进行了深入研究，从 2023 年互联网黑灰产发展现状、黑灰产攻击资源、黑灰产攻击场景等维度进行全面梳理分析，力求通过客观呈现黑灰产情报数据，帮助更多企业深入直观了解黑灰产业，有效防控各类攻击风险。

相关名词定义：

1、风险 IP：业内也称黑 IP，指存在攻击风险（包括代理、秒拨等恶意行为）的 IP；

2、风险手机号：存在被滥用盗用等风险的手机号，如被黑产用于接收短信，实施批量恶意攻击的手机号，通常从接码平台或发卡平台捕获；

3、风险邮箱：指被黑产用于恶意注册生成的临时邮箱，用以骗取用户重要信息、传播恶意程序等；

4、黑手机卡：指未进行实名登记或以假身份进行实名登记的，并被不法分子利用实施违法犯罪活动的电话卡；

5、猫池卡：指通过“猫池”这一网络通信硬件，实现同时支持多个号码通话、群发短信等功能的黑手机卡；

6、拦截卡：指通过病毒木马控制真实用户手机短信/验证码收发权限的手机卡，通常捕获自拦截卡平台；

7、洗钱银行卡：指被黑产用于非法资金清洗（将违法所得收入合法化）的银行卡，例如赌博及诈骗团伙通过银行卡消费、转账等方式转移洗钱资金；

8、洗钱数字钱包：指被黑产用于非法资金清洗的加密数字货币，例如通过数字人民币消费、转账等方式转移资金，利用数字货币的隐蔽性来逃避监管审查；

9、洗钱对公账户：指被黑产用于非法资金清洗的银行对公账户，因对公账户具有收款额度大、转账次数多等特点，使得“对公账户”常常作为黑钱转账的集中点及发散点；

10、改机：指的是通过修改手机设备信息，如手机型号、串码、IMEI、GPS 定位等，达成绕过厂商设备检测的目的；

11、改定位：指利用相关工具修改手机定位信息，例如通过修改地理位置信息参加地域性活动并进行营销作弊；

12、数据泄露情报：威胁猎人通过 TG 群、暗网等渠道捕获到的“未授权个人/组织敏感信息被公开交易或使用” 的情报信息，可能包含历史数据、重复数据等，往往量级巨大；

13、数据泄露事件：威胁猎人安全研究专家针对数据泄露情报的样例等进行分析及验证，确认为真实、有效的数据泄露事件；

14、暗网：指隐藏的网络，普通网民无法通过常规手段搜索访问，需要使用一些特定的软件、配置或者授权才能登录；

15、公民个人信息：指公民个人身份信息，包括但不限于姓名、身份证号码、出生日期、手机号码、家庭住址、银行账户信息等。

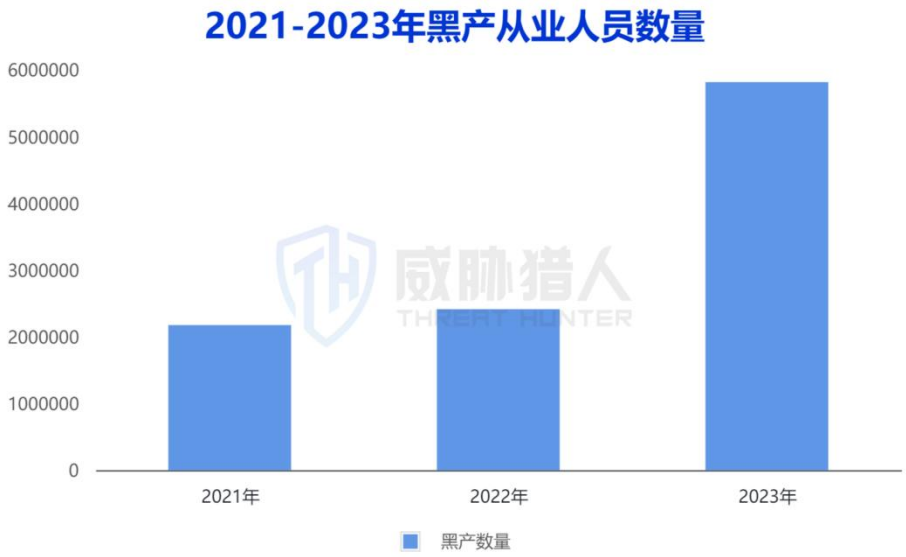
01

2023 年互联网黑灰产业发展现状

一、2023 年互联网黑灰产业发展现状

1.1 2023 年互联网黑灰产从业人员达 587 万，较 2022 年上升 141%

威胁猎人安全研究员调研统计发现，2023 年互联网黑灰产从业人数持续上升，从业人员数量达到 587.1 万，较 2022 年上升 141%。



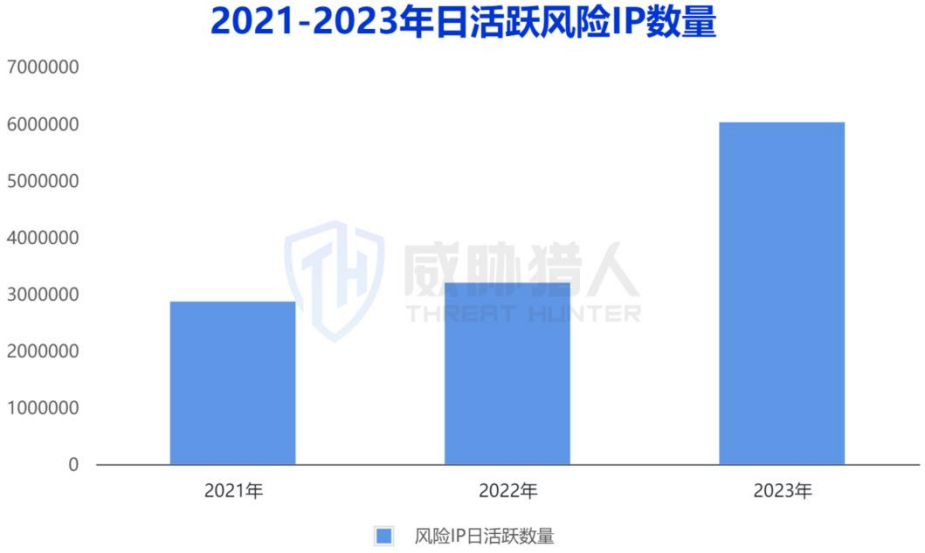
1.2 2023 年黑灰产资源整体情况

1.2.1 2023 年国内作恶手机号较 2022 年增长 15.44%

2023 年国内作恶手机号数量达到 625.5 万，较 2022 年上升 15.44%。

1.2.2 2023 年风险 IP 数量较 2022 年增长 88.47%

2023 年风险 IP 数量持续上升，风险 IP 数量达到 602.2 万，较 2022 年上升 88.47%。



1.2.3 2023 年洗钱银行卡数量较 2022 年增长 133.74%

2023 年洗钱银行卡数量持续上升，洗钱银行卡数量达到 87.4 万，较 2022 年上升 133.74%。

02

2023 年黑产攻击资源分析

二、2023 年黑产攻击资源分析

2.1 2023 年黑手机卡资源分析

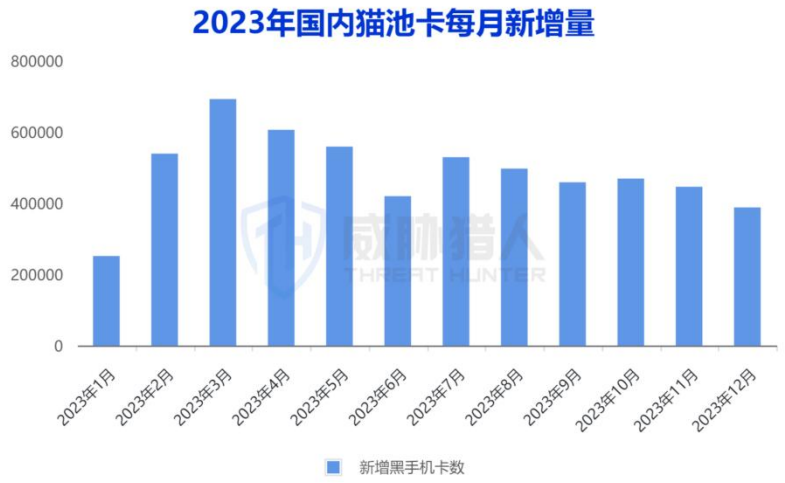
2.1.1 2023 年猫池卡资源变化趋势

（1）2023 年国内猫池卡数量较 2022 年增长 8.25%

据威胁猎人威胁情报运营平台数据显示，2023 年新捕获猫池卡 586.6 万个，较 2022 年上升 8.25%。从 2023 年国内猫池卡数量的变化趋势来看，1-3 月出现明显上升趋势，4-6 月逐渐降低。

经威胁猎人情报专家分析，出现这一趋势的主要原因是：

1-3 月某头部接码平台对接的黑产持续上传大量新的接码手机号，使得该时间段内的新增作恶手机号数量持续上升；4-6 月该头部接码平台遭遇持续性 DDos 攻击而无法正常运营，导致该时间段内的作恶手机号数量持续下降。

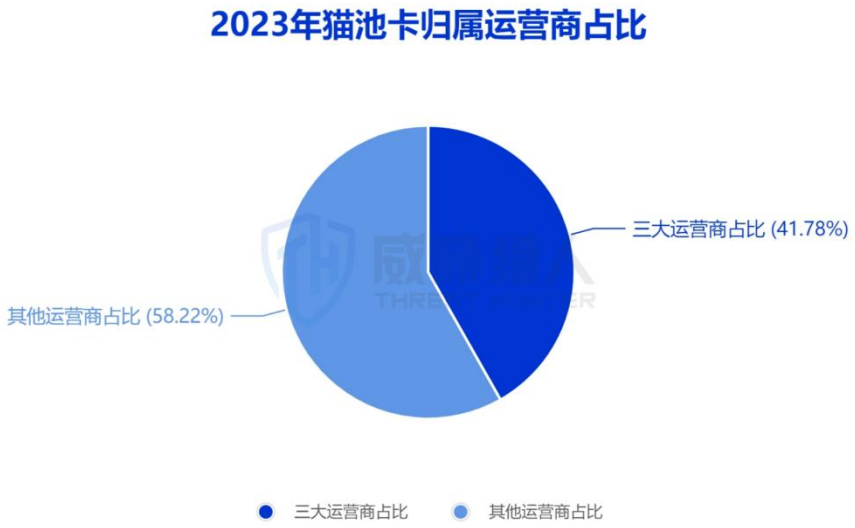


（2）2023 年猫池卡归属最多的三个省份为：江苏、山东、河南

威胁猎人情报专家对 2023 年捕获到的国内猫池卡进行统计分析，发现江苏、山东、河南三省为猫池卡归属地最多的三个省份；针对归属城市分析发现，南京、上海、北京三城市为猫池卡归属地最多的城市。

（3）2023 年捕获的猫池卡中，归属国内三大运营商的占 41.78%

2023 年威胁猎人威胁情报运营平台捕获猫池卡 618 万张，其中归属国内三大运营商的拦截卡占比 41.78%，归属其他运营商的占比 58.2%。



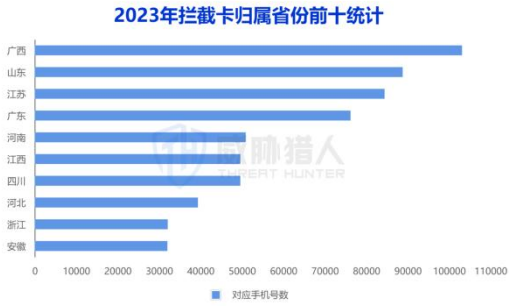
2.1.2 2023 年拦截卡资源变化趋势

（1）2023 年国内拦截卡数量达 38.9 万，并于 3 月出现大幅上升

2023 年，威胁猎人最新捕获拦截卡达 38.9 万，并于 3 月捕获到大量新增拦截卡，经过持续监测分析发现，其主要原因是：2023 年 3 月出现一个新的拦截卡接码平台，导致 3 月新增拦截卡数量大幅上升。

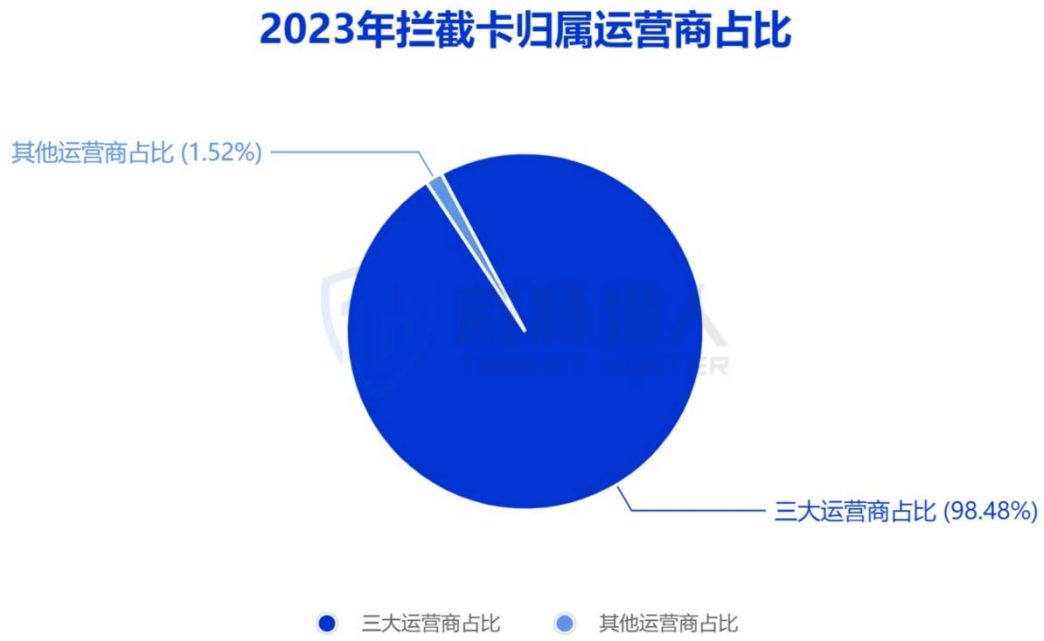
（2）2023 年拦截卡归属最多的三个省份为：广西、山东、江苏

威胁猎人安全研究员对 2023 年捕获到的国内拦截卡进行统计分析，发现**广西、山东、江苏**三省为拦截卡归属地最多的三个省份，与猫池卡归属省份存在一定的重合；针对归属城市分析发现，**南京、贵港、南宁**三城市为拦截卡归属地最多的城市。



（3）2023 年捕获的拦截卡中，归属国内三大运营商的占 98.48%

2023 年威胁猎人威胁情报运营平台捕获拦截卡 87 万张，归属国内三大运营商的拦截卡占比达 98.48%，归属其他运营商占比 1.52%。



值得注意的是，2023 年威胁情报运营平台捕获到的 192 号段黑手机卡数量达到 87.8 万，黑产大量使用 192 号段的黑手机卡进行作恶。从 192 号段黑手机卡数量的变化趋势来看，7 月、8 月及 10 月出现大幅增长。

经威胁猎人情报专家分析，7 月、8 月及 10 月新增量较大的主要原因是：

自第三季度开始，有 4 个供应渠道进一步增大 192 号段手机卡的投入规模，使得第三季度新增量进一步增加。10 月，部分黑产开始将目光投向非头部互联网平台并展开攻击，直到 11 月这些平台开始察觉到攻击情况并对其进行风控，192 号段的新增量开始逐渐下降。

2.1.3 发卡平台成为黑产投放高价值接码手机卡的主流渠道之一

从威胁猎人威胁情报运营平台捕获的数据来看，提供接码服务的发卡平台及发卡店铺数量呈明显上升趋势，同时通过发卡平台捕获到的接码手机号也呈现出明显上升趋势，由此可见，**“发卡平台”成为黑产投放高价值接码手机卡的主流渠道之一。**

高质量接码手机号：手机号入网时间短，在网状态正常，绝大多数都是黑产卡商通过特定渠道及技术新开的实体手机卡。黑产多利用此类手机号对热门 APP 业务进行攻击并实现获利，如热门的视频 APP、互联网社交 APP 或电商 APP 的注册和换绑业务。

（1）2023 年每月捕获的涉及接码的发卡平台及发卡店铺数量持续上升

自 2023 年 1 月起，每月捕获的涉及接码的发卡平台数量持续上升，截至 2023 年 12 月，活跃发卡平台达到 28 个。在这些发卡平台中，直接向黑产提供手机号接码服务的发卡店铺数量亦也出现大幅度上升，2023 年 12 月，威胁猎人共捕获该类店铺 322 家。

（2）2023 年通过发卡店铺每月捕获的高价值接码手机号数量持续走高

自 2023 年 1 月起，威胁猎人通过发卡店铺捕获到用于作恶的接码手机号数量出现大幅上升。2023 年 12 月，威胁猎人共捕获作恶手机号 12.9 万个。

威胁猎人安全研究员发现：**“黑灰产手机号接码服务愈发成熟，已呈现出明显分工趋势”**。例如手机卡商提供黑卡物料，代理商汇集多个卡商渠道，通过在发卡平台开设店铺的形式为黑产提供隐蔽的接码服务。

2.2 2023 年风险 IP 资源分析

2.2.1 2023 年风险 IP 资源变化

近年来国内互联网平台业务不断开拓海外市场，如何识别海外风险 IP 已成为各大企业亟需重视的问题。威胁猎人海外风险 IP 监测能力的提升，也为互联网平台优化海外风控规则提供了有力支持。

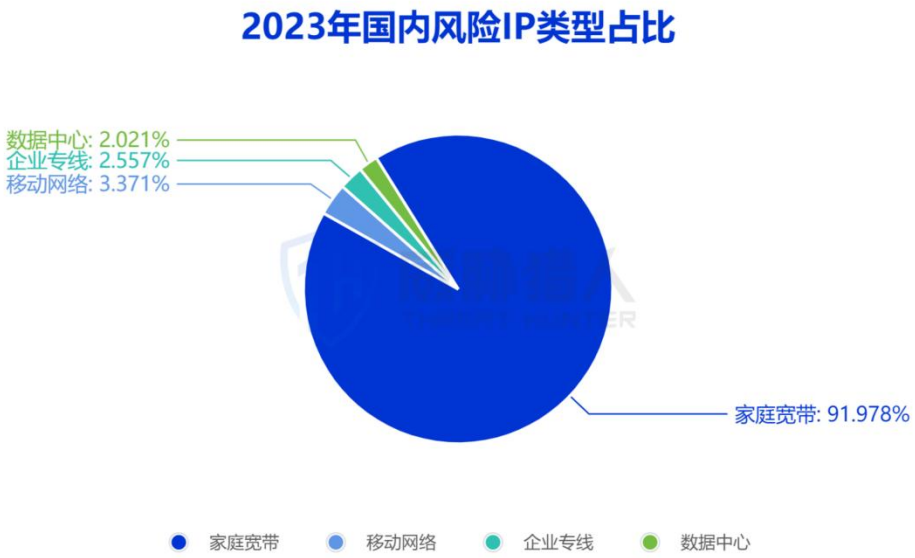
2023 年威胁猎人持续监测国内风险 IP5906 万个，国外风险 IP7172 万个。我们对国内及国外两种类型的风险 IP 分析发现：

（1）2023 年国内风险 IP 归属最多的三个省份：江苏、浙江、广东

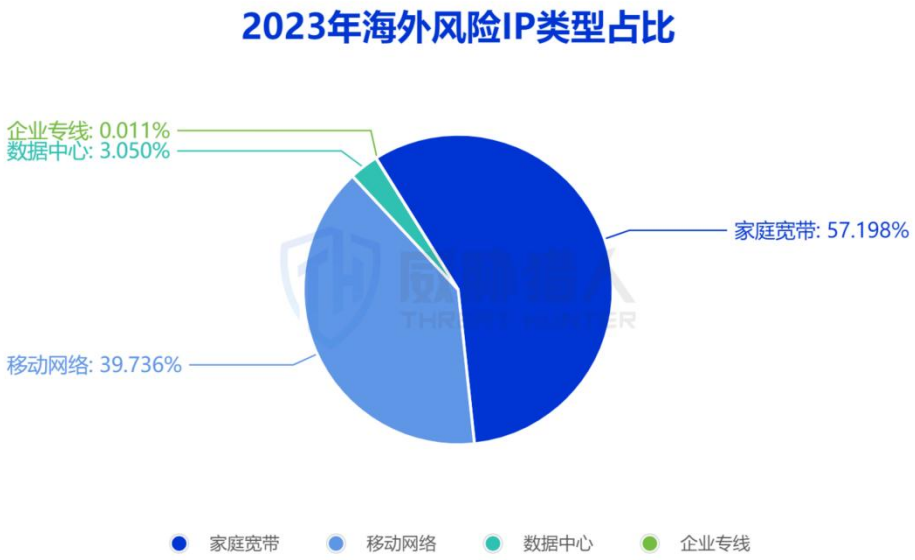
(2) 2023 年国内风险 IP 归属最多的三个城市：上海、重庆、苏州

(3) 2023 年国外风险 IP 归属最多的三个国家：巴西、印度、美国

(4) 2023 年国内风险 IP 类型中，家庭宽带类型占比超 90%



(5) 2023 年海外风险 IP 类型以家庭宽带、移动网络为主



2.2.2 黑产通过植入木马恶意使用正常用户 IP 的行为更加猖獗

威胁猎人发现，黑产通过在正常用户设备中植入木马，实现在其网络上建立代理通道，且每次使用时间很短，因此普通用户难以感知到自己的 IP 被盗用。从甲方风控视角来看，正常用户的 IP 被黑产恶意使用，这类 IP 属于“好坏共用-代理”IP。

这类 IP 由于大部分时间是正常用户进行操作，如点击、充值、浏览等行为均正常，少量时间会出现短暂的作恶行为。因此平台可能会认定该用户为正常用户，进而忽视其短暂的作恶行为，给黑产可乘之机。

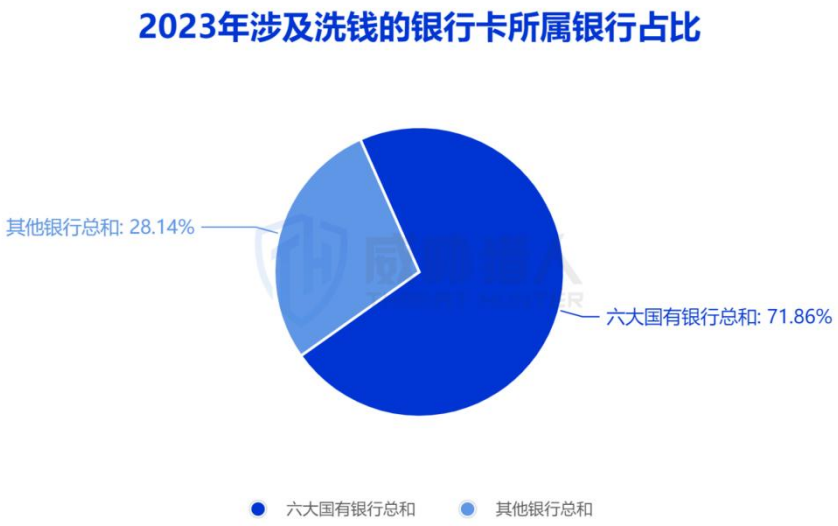
通过对代理 IP 平台的持续监测，我们发现黑产通过植入木马恶意使用正常用户 IP 的行为更加猖獗，以威胁猎人 2023 年 11 月及 12 月捕获到的数据为例：11 月捕获被劫持 IP 数量达 508 万，12 月捕获被劫持 IP 数量达 934 万，较 11 月增加 83.85%。

2.3 2023 年网络洗钱资源分析

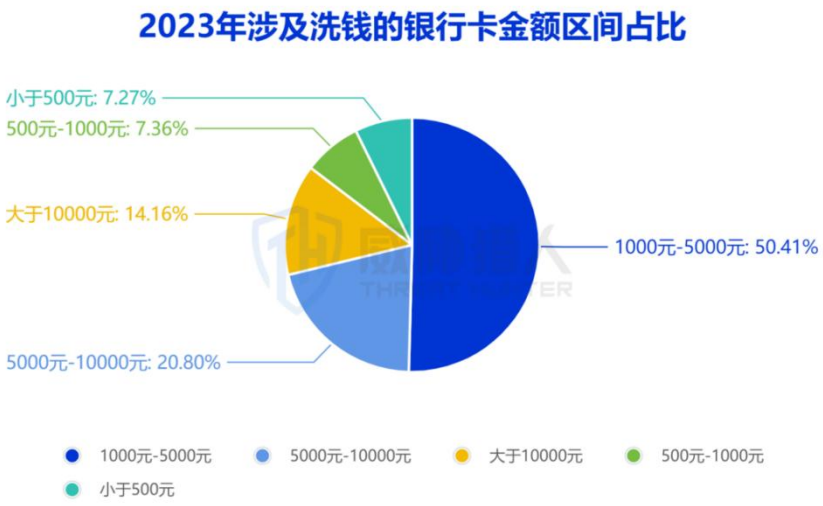
2.3.1 2023 年银行卡资源变化

2023 年威胁猎人共捕获洗钱银行卡 87.4 万张，对捕获到的洗钱银行卡进一步分析发现：

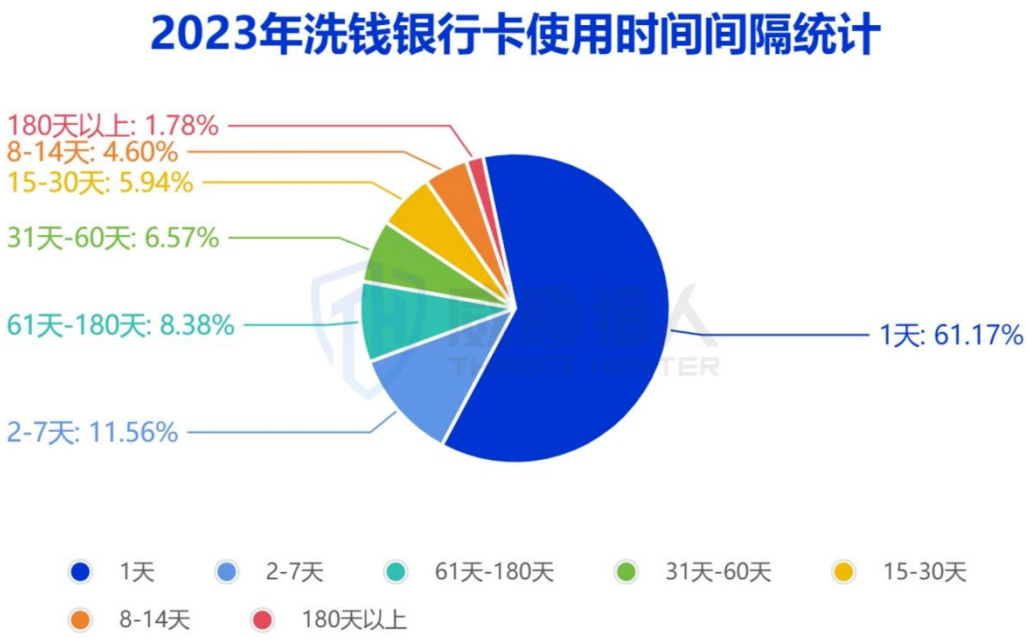
（1）涉及洗钱银行卡归属国有银行的占比远高于非国有银行



（2）银行卡洗钱金额的主要区间为 1000-5000 元



（3）洗钱银行卡使用时间间隔极短，过半银行卡再次使用时间不超过一天



2.3.2 2023 年数字人民币资源变化

随着社会公众对零售支付便捷性、安全性等需求日益提高，数字人民币支付正在成为消费新趋势。

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。

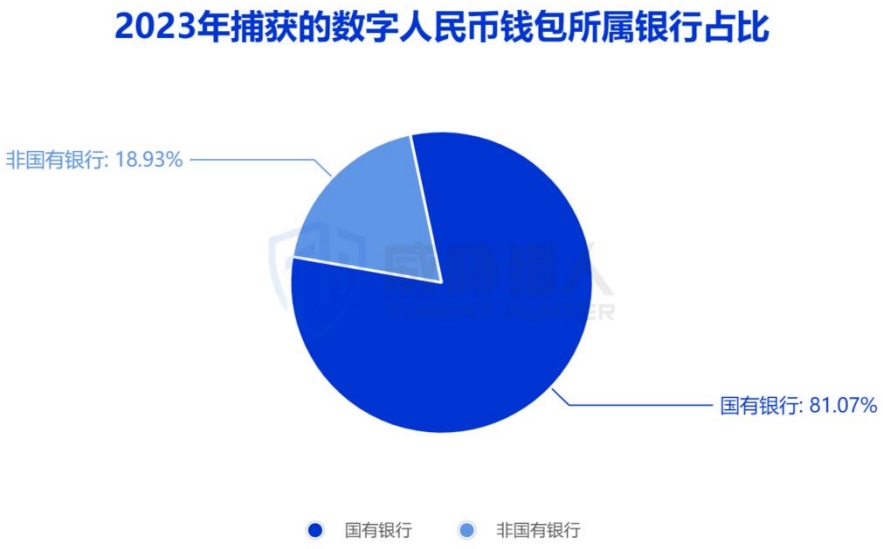
（1）2023 年捕获涉及洗钱的数字人民币钱包数量达 23 万，月增幅超 270%

2023 年威胁猎人共捕获涉及洗钱的数字人民币钱包 23.2 万个，同时发现黑产利用数字人民币进行洗钱的情况整体呈上升趋势，尤其是 9 月，月增幅超过了 270%。

经调查发现，9 月出现较大增幅的主要原因是：9 月出现大量支持数字人民币洗钱的第四方支付平台，使得利用数字人民币进行洗钱的情况变得更加高频。

（2）涉及洗钱的数字人民币支付中，归属国有银行的占比超 80%

目前，威胁猎人监测到数字人民币洗钱涉及银行数十家，其中国有银行占比超 80%。就支持开通数字人民币的银行用户数量而言，国有六大行的银行用户总数远大于其余银行之和，因此其潜在的数字人民币用户也相对较多。



2.3.3 2023 年对公账户资源变化

银行对公账户具有收款额度大、转账次数多等特点，这使得“对公账户”常常作为黑钱转账的集中点及发散点，在黑产洗钱链条中担任极其重要的位置。

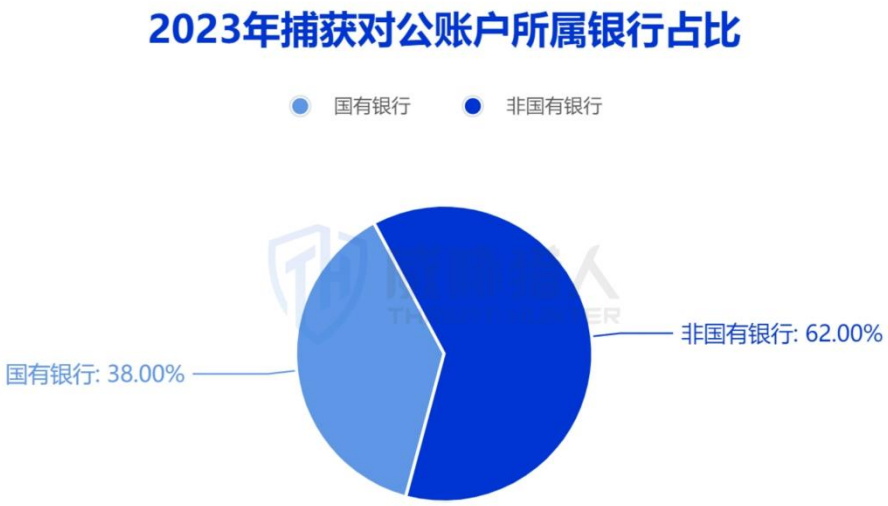
在打击洗钱犯罪过程中，银行对涉及洗钱的对公账户进行风控也是十分重要的一环。因为一个对公账户的收款额度往往在几百万到几千万不等，及时发现涉嫌洗钱的对公账户并进行针对性风控，往往能中断某个黑产团伙的某一洗钱链条。

2023 年威胁猎人持续覆盖及监测黑产在洗钱过程中所使用的银行对公账户资源，发现涉及洗钱的对公账户数量持续上升。

（1）2023 年捕获涉及洗钱的对公账户数量逐月上升

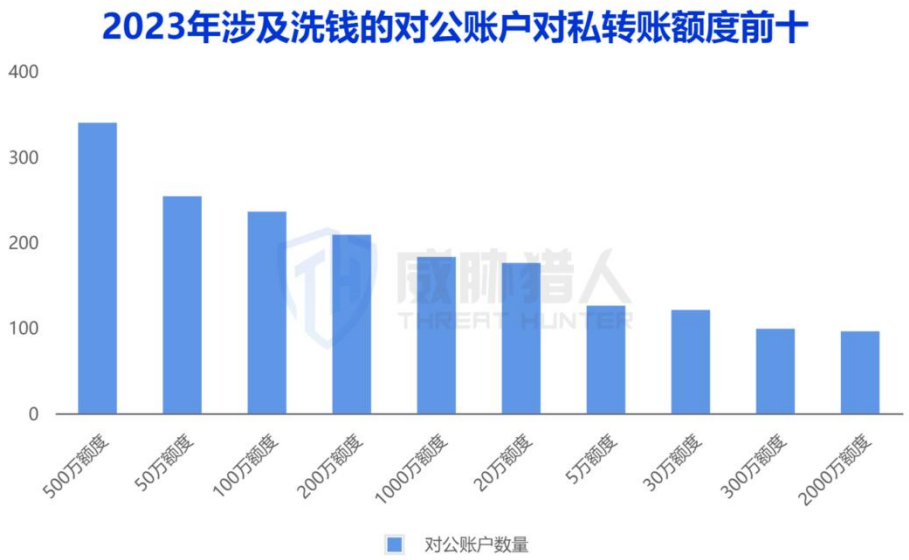
（2）2023 年捕获涉及洗钱对公账户的所属银行中，非国有银行占比超 60%

2023 年威胁猎人共捕获到涉及洗钱的对公账户 4782 个，涉及银行 695 家，涉及洗钱对公账户的所属银行中，非国有银行占比超 60%。



（3）2023 年捕获涉及洗钱对公账户归属最多的三个省份：广东、山东、河南

（4）黑产洗钱利用最多的转账额度为 500 万



2.3.4 2023 年黑产洗钱手法多达 19 种，影响平台众多

2023 年，威胁猎人安全研究员捕获到的洗钱手法多达 19 种，作恶手法不断迭代，受害平台众多。

洗钱方式	具体手法	受害平台
银行卡洗钱	（1）行内转账； （2）跨行转账； （3）小额多次转账； （4）单次大额非整数转账； （5）银行网点提现； （6）.....	（1）银行； （2）持有第三方支付牌照的平台； （3）虚拟货币平台； （4）直播平台； （5）短视频平台； （6）电商购物平台；
第三方支付平台洗钱	（1）支付平台收款码； （2）支付平台红包； （3）好友转账； （4）生活缴费（水、电、燃气、电话费） （5）电商购物； （6）.....	
数字人民币洗钱	（1）数字人民币钱包相互转账； （2）数字人民币钱包收发红包； （3）数字人民币提现银行卡； （4）.....	
对公账户洗钱	（1）个人银行卡转账对公账户； （2）对公账户转账个人银行卡； （3）对公账户转账对公账户； （4）.....	
直播平台、短视频平台洗钱	（1）直播打赏； （2）赠送礼物； （3）.....	
虚拟货币洗钱	（1）银行卡充值购买虚拟货币； （2）.....	

（1）对公账户洗钱流程介绍

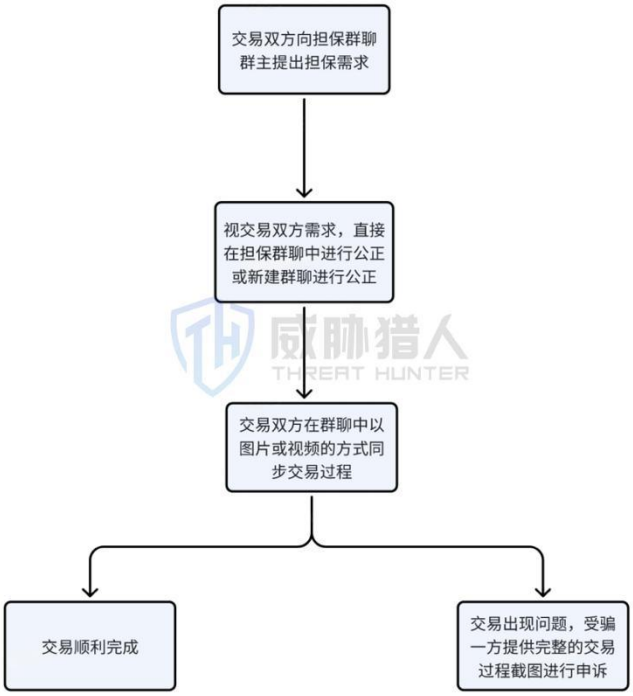
① 担保公群是什么?

为了加强渠道的可信度，确保数据交易顺利进行，交易双方往往会通过第三方平台保障交易过程的可信度及可行性，最常见的方式就是“担保公群”。

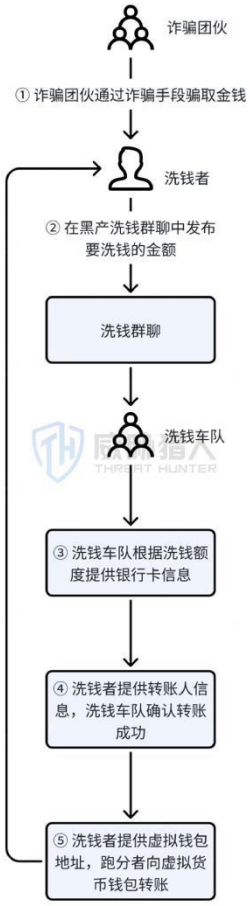
在交易时，买卖双方在交易前会在担保公群提供的虚拟货币账户中转入等价于交易金额的虚拟货币作为押金；通过第三方担保公群收取押金的方式，避免受骗带来的损失。


担保公群交易规则 必看
1 做事规则跑分要求必须提前跟合作用户沟通好！
2 出现问题如实交代，发现弄虚作假一律发红包扣押处理！
3 必须服务好每一名咨询的用户以及小白！
4 对接群 负责人创建 ！
5 禁止开启群禁言模式，晚上除外 白天必须是可以聊天的群频道！
6 严格禁止私下交易如代付，私下跑分，借钱！
7 公群只负责担保群内用户和指定项目，其他项目除外
8 特殊行业不同，隐私东西可以私下发，如：账户、个人信息、数据、群码等不可避免的隐私内容可以允许私下，但交流必须在群
9 需求方或者供应方正在与公群老板交易时必须在群内报备金额避免后来者持续不断的交易，这种情况下导致超押金让公群老板跑路的，没报备的不赔付
10 全部都有报备，导致多人累计超押金造成公群老板跑路，扣出压金的10%为管理处理手续费再按照报备的先后顺序赔付群内报备正在交易金额
11 发现超押经营或老板刻意要求私下交易将会对公群老板做出罚款押金的20%
12 公群老板把交易规则要求置顶群内，交易有争议按规则处理，没规则的老板大概率会输
13 公群退押问题：公群老板如要退押金，与客服报备后由负责人在公群公告并通知暂停交易，24小时无争议后方可退押
683 15:37


转发自频道 资源库
公群报备模版：
公群交易报备：
公群编号：xxx
交易方： @Xxxxxx（客户）
交易金额：Xxxx U（以实际交易为准）
交易日期：Xxxx_xxxx
交易内容：（xxxxx）
对接该群那位管理员：@Xxxxxxx
交易规则：
注意：之后避免公群超压，如有私下对接，合作之前找担保客服报备一下，此报备模板适应任何行业，可以根据行业不同适当修改调整，对接的管理员，需要该管理员回复才算，证明此交易真实有效
790 15:37


交易双方向担保群聊群主提出担保需求
视交易双方需求，直接在担保群聊中进行公正或新建群聊进行公正
交易双方在群聊中以图片或视频的方式同步交易过程
交易顺利完成
交易出现问题，受骗一方提供完整的交易过程截图进行申诉

② 黑产如何通过担保公群用对公账户进行洗钱?



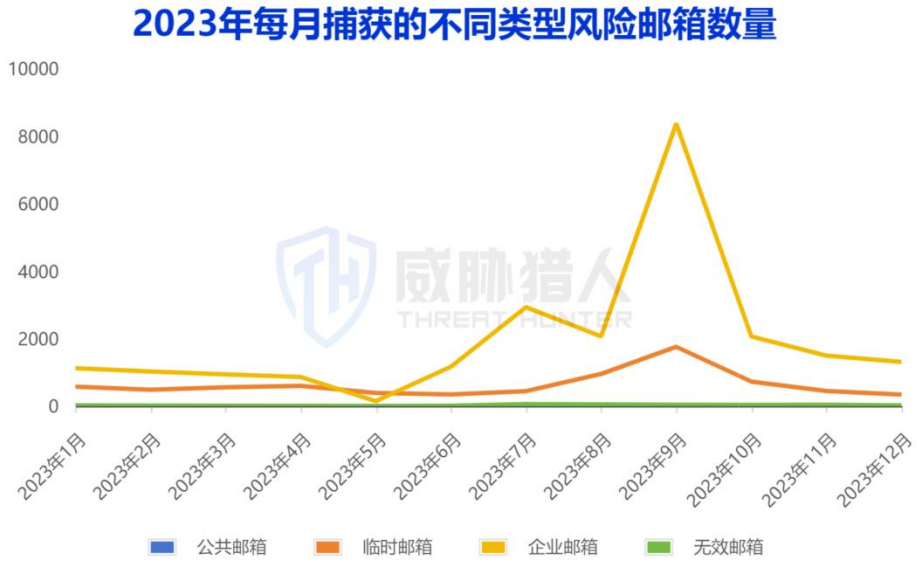
2.4 2023 年风险邮箱资源分析

2.4.1 2023 年风险邮箱资源变化

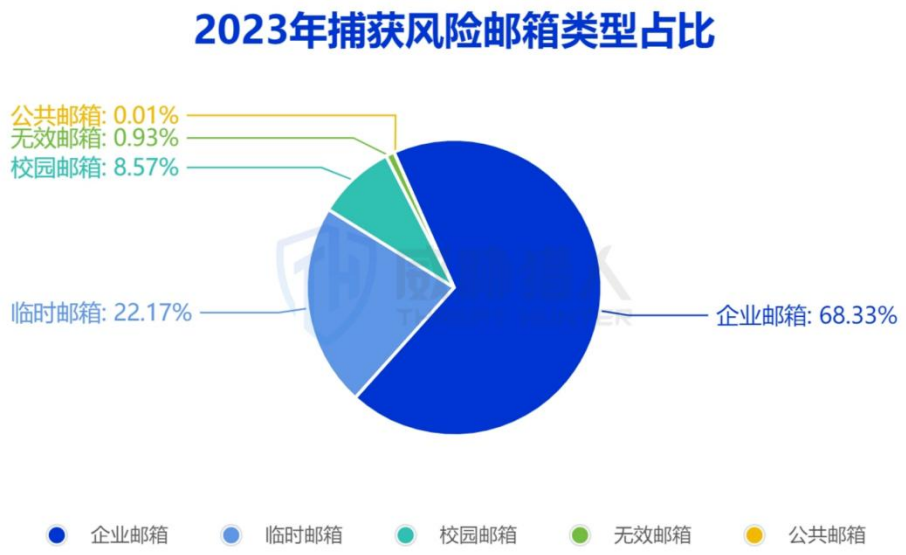
（1）2023 年 9 月捕获大量风险企业邮箱

从 2023 年每月不同类型风险邮箱捕获数量来看，9 月出现大幅上涨。2023 年 9 月，威胁猎人安全研究员通过已知的风险邮箱进行 MX 解析，关联出了大量的风险企业邮箱。

MX，即 Mail Exchanger（邮件交换记录），它指向一个邮件服务器，主要用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮件服务器。通常情况下，一个 MX 可以绑定多个邮箱域名。



（2）2023 年捕获风险邮箱中，企业邮箱占 68%以上



03

2023 年黑产通用型攻击技术

三、2023 年黑产通用型攻击技术

3.1 黑产应用 AI 技术大幅提升攻击效率，突破企业防御体系

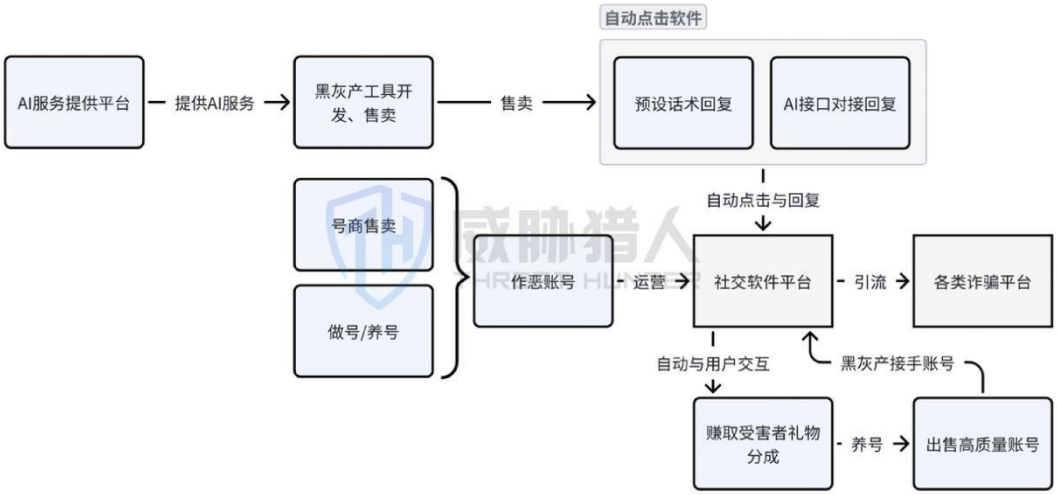
2023 年，AI 技术应用于网络安全的多个场景，AI 技术的深度应用也引起了大量黑产团伙的觊觎。威胁猎人研究人员观察到，不少黑产团伙利用文本生成、照片活化、人脸替换、验证码识别、语音生成等 AI 技术进行攻击并实施诈骗行为。

由于 AI 的智能、自动化能力，攻击者运用 AI 技术绕过企业现有防御，发起高度隐蔽、复杂、自动化的攻击，在同等时间内攻击尽可能多的目标用户，因此近年来利用 AI 技术实施网络攻击的事件快速增长。

（1）黑产在社交场景接入 AI 机器人，自动生成聊天话术

威胁猎人安全研究员在 2023 年第三季度发现，黑灰产在社交引流场景已经接入 AI 机器人，使聊天更智能。以捕获的一款自动聊天工具“AiTuLing”为例，该工具除了常规的“基于预设话术进行引流”外，还支持接入 AI 机器人，同时该工具支持市面上近百个社交平台的自动引流。

研究发现，黑产通过购买 AI 服务平台的服务，并在此基础上进行整合、开发及售卖，最终被更多作恶团伙用于社交平台自动引流及诈骗。

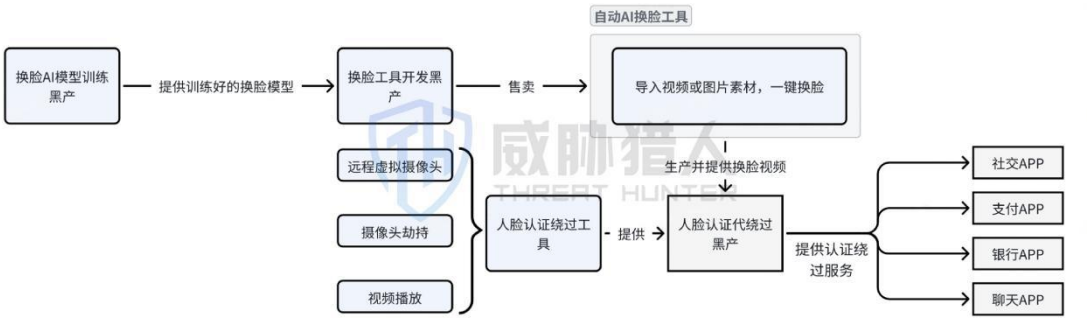


值得注意的是，AI 机器人的接入成本也极为低廉，最低只需 19.9 元/月即可；同时使用方法极为简单，只需填入相关账号并启动软件即可自动聊天引流，目前被大量应用于电商平台及社交群聊，一定程度上增加了对应平台的检测难度。

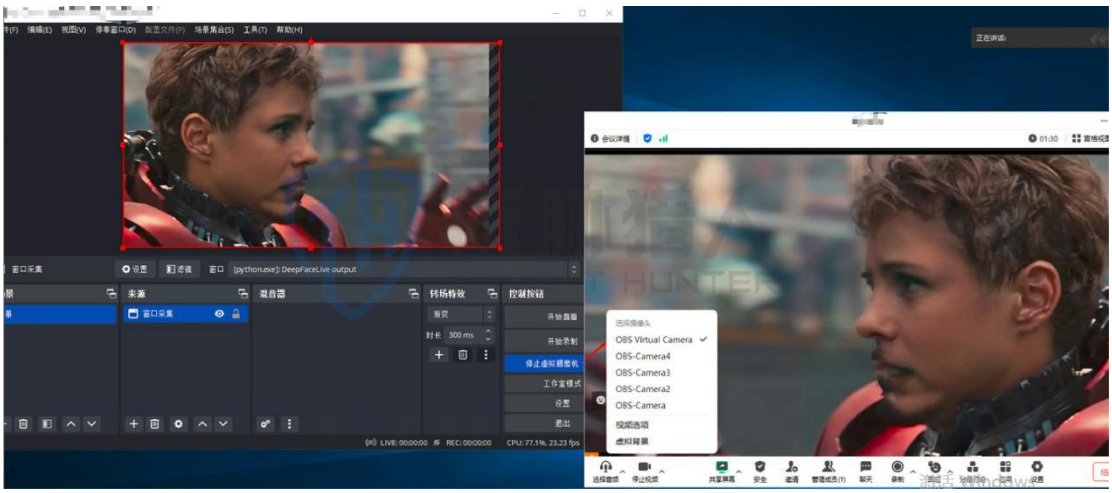
（2）黑产利用 AI 进行视频伪造，人脸验证需警惕

2023 年，黑产大规模利用 AI 换脸工具制作换脸视频提供代认证服务，以社交 APP 为例，黑产通常会购买大量的实名账号进行发言引流，当账号触发平台风控而需要进行人脸认证时，则需要借助 AI 换脸技术绕过人脸验证。

此外，利用会议软件+AI 换脸工具伪装成受害者熟人对受害者实施诈骗转账的案件频繁发生。案件中，诈骗者往往让受害者在手机上安装会议软件，并通过会议软件+实时直播换脸工具，伪装成熟人从而骗取受害者信任，进而实施诈骗。



威胁猎人对“视频会议软件模拟熟人进行诈骗”的案例复现如下：



3.2 提供云手机服务的平台持续增加，配套攻击工具更加完善

据威胁猎人研究发现，2023 年提供云手机服务的平台持续增加，且头部云手机平台已呈现出产业化趋势，这类平台除了提供云手机服务外，还提供配套的攻击工具，如代理 IP 服务、改机工具、改定位工具、Hook 框架等，极大提高黑产攻击效率。下表为某云手机平台提供的配套服务：

配套服务	具体作用
IP 代理	黑产进行批量攻击时，防止自身 IP 泄露及防止同一 IP 进行多次攻击而引起平台警觉。
设备大师	指通过相关工具，在手机设备不断生成新的设备参数。通过搭配接码平台进行接码，黑灰产能实现无限新用户注册，批量获取新用户奖励。
虚拟定位	指通过相关工具，修改手机的定位信息。通过改定位，黑产能参加存在地域限制的活动，如 A 地的黑产通过改定位能领取 B 地的消费券。
虚拟场景	模拟不同场景下，正常人的行为。如通过向陀螺仪、重力感应器、加速度传感器等设备传输虚假的参数，模拟正常人跑步。
自动化脚本工具	通过自动化脚本能把攻击行为程序化，能让无任何计算机技术的人亦能通过点击运行脚本这一简单操作，发起攻击。
远程虚拟摄像头	配套安装在真实手机上 APP 用于获取动态人脸/二维码信息数据，通过程序将收集到的数据实时上报至指定云手机
obs 推流直播	通过 OBS 软件，能把本地正在直播的内容或重复播放的视频推流到云手机上，方便在云手机上进行直播
应用信息转发	云手机内收到的应用消息转发至指定的微信公众号或者用户的指定地址（如服务器地址）
网盘服务	在云手机中安装网盘 APP 能便捷的上传或下载数据、文件
应用守护	提供应用自启动、定时重启和启动 RTMP URL 的功能。
ADB 调试	可通过远程 IP 及端口访问云手机，进行 ADB 调试
进程日志导出	一键导出云手机进程日志，方便进行程序的调试

相较于真实手机设备，云手机具备以下优势：

（1）购买成本低：购买真实手机需要几百到上千元不等，租用云手机只需花费几十元/月即可；

（2）使用方便且配套服务完善：云手机自带改机工具且具备虚拟定位、自动化脚本工具等配套服务。

以上云手机的优势使黑产的攻击作恶成本大大降低，同时节省了黑产安装、配置作恶环境所需的时间，提高了黑产的攻击效率，为企业风控带来了一定的挑战。

除安卓端云手机外，黑产使用 iOS 云手机进行作恶的情况并不少见，由于 iOS 系统对应用权限申请的严格限制，使得大部分互联网公司在 iOS 设备上获取设备信息的难度远大于安卓端设备，这在一定程度上可能会使得平台在 iOS 设备上进行风控识别的难度更高。

针对此类情况，威胁猎人建议企业应及时获取此类平台样本，进行相关样本分析和防御。

04

2023 年黑产攻击场景分析

四、2023 年黑产攻击场景分析

4.1 2023 年业务欺诈场景分析

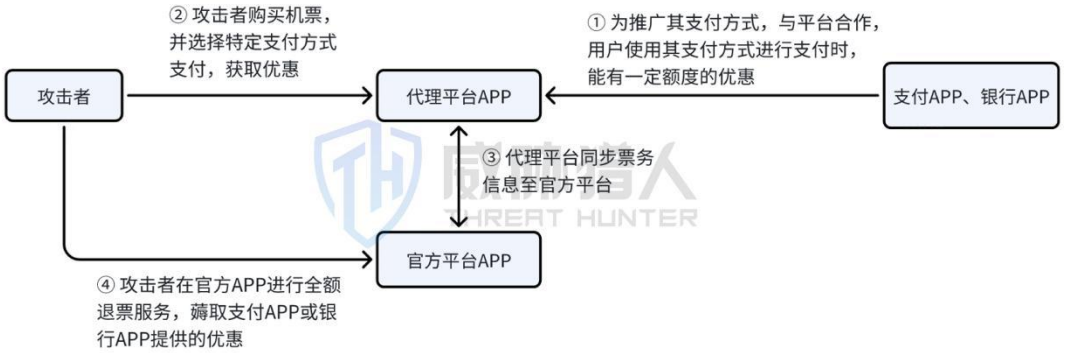
4.1.1 营销活动

（1）营销活动攻击情报 928 万条，涉及作恶黑产人数达 15.9 万

今年各企业平台营销活动遭受黑产攻击的现状依旧严峻，2023 年威胁猎人共捕获营销活动攻击情报 928 万条，监测到活跃的作恶社交群组 1.2 万个，涉及作恶黑产人数达 15.9 万名。

（2）大量黑产利用业务规则漏洞薅取用户优惠

2023 年 12 月，威胁猎人发现大量黑灰产和羊毛党通过“第三方渠道购买后在官方渠道退款”的方式来薅取银行、平台立减优惠，导致合作平台出现大量异常退款单的同时，活动立减金也被白白薅走。主要由于黑产利用了提供购买服务的第三方平台与官方平台之间信息不互通这一特点。



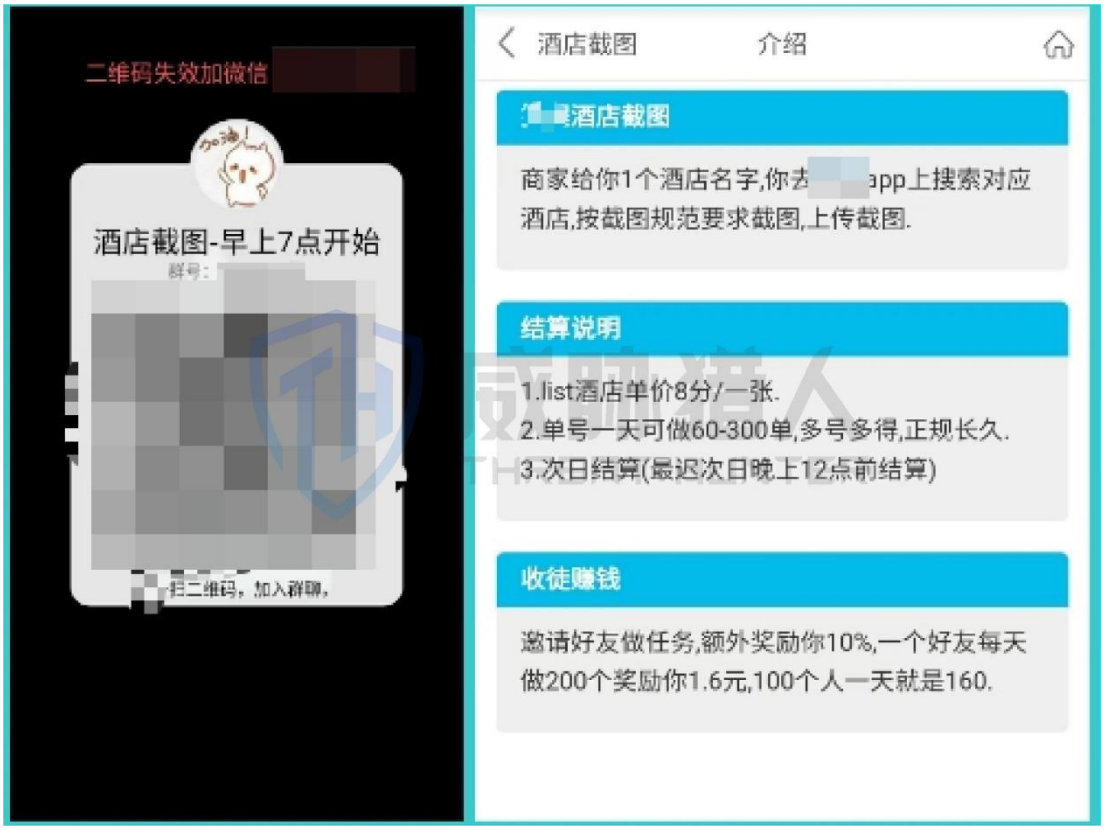
（3）众包平台“私域化”，作恶行为更加隐蔽

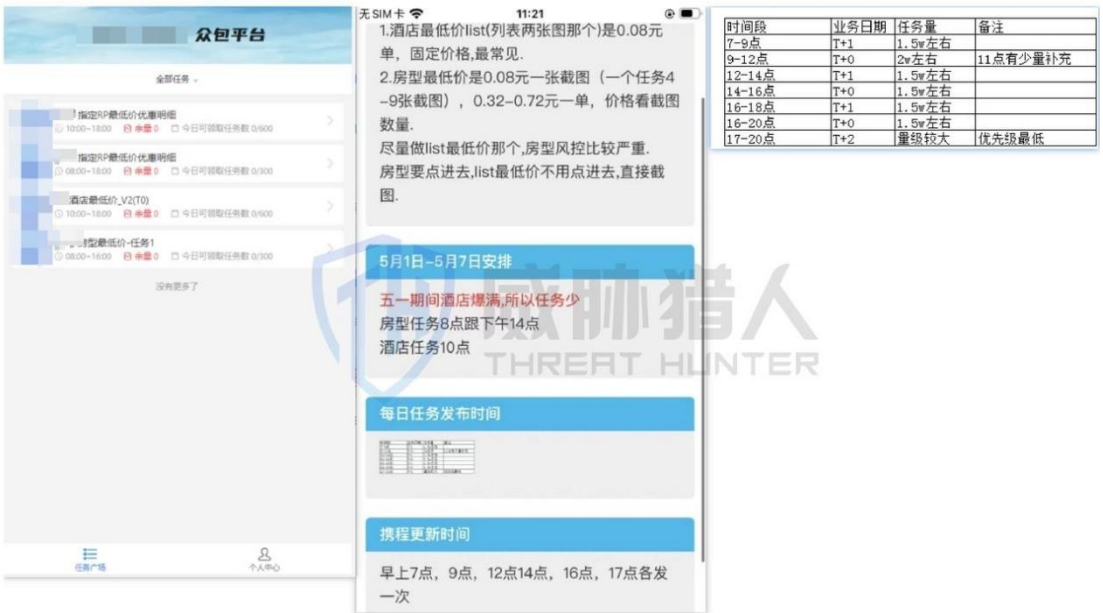
2023 年，威胁猎人研究人员发现，黑灰产为了避免众包平台被监测和风控，推出了更为复杂、安全的众包发布渠道。其复杂性主要体现在：

1、首先众包人员需要先进入特定的社交群聊才能获取到众包平台的网站链接；

2、而后众包人员需要访问链接并注册登录后，才能执行接单任务。

这种方式做单虽增加了执行时间和操作成本，但其隐蔽性使得平台的监测及风控难度大大提升。





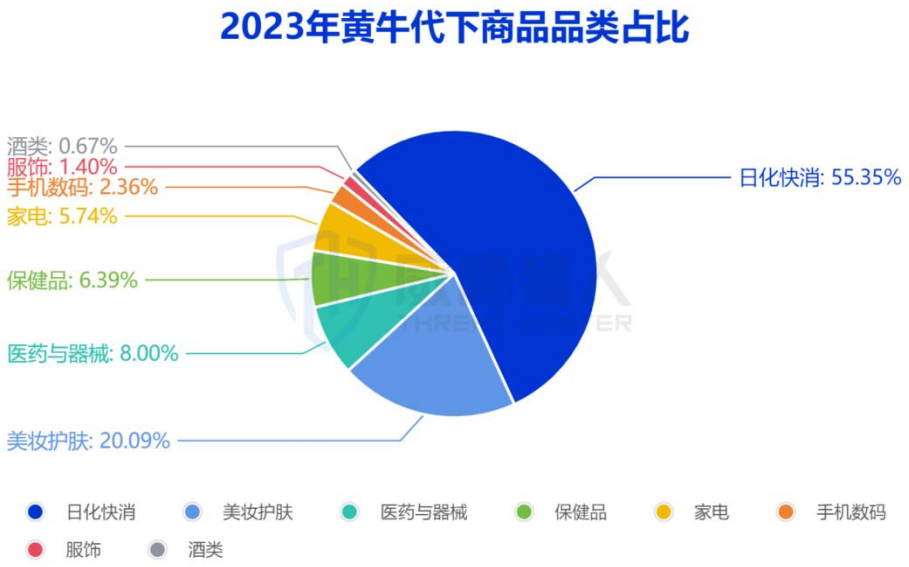
除了私域众包平台外，威胁猎人还观察到部分公开的众包平台也开始推出新的策略，防止平台被监测及风控，例如：

1、刷量任务中，刷量链接使用短链接代替真实的刷量链接；

2、拉新任务中，需注册、实名众包 APP，并领取任务后才能获取详细的任务步骤及教程。

（4）电商代下现状严峻，日化快消和美妆护肤品成为电商代下重灾区

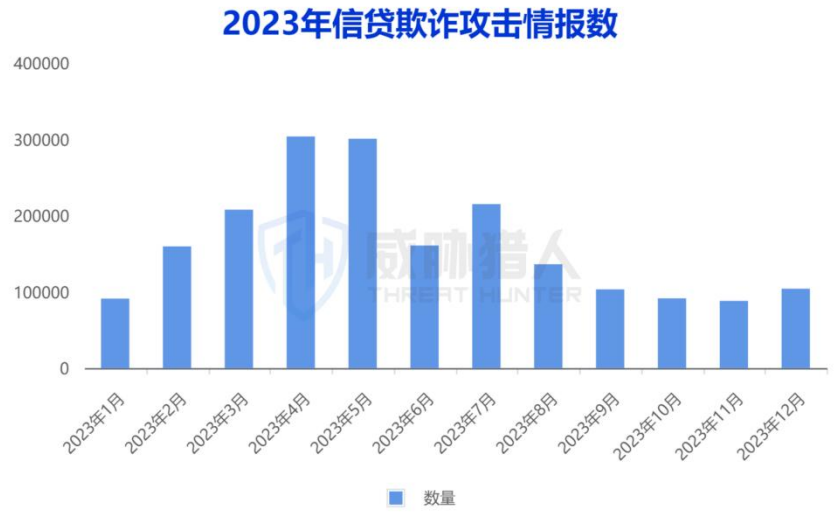
2023 年，威胁猎人捕获的代下方案中，代下品类 Top3 为日化快消、美妆护肤和医药器械类，分别占总数的 55.35%、20.09%和 8%，余下 16.56%的品类与保健品、家电、手机数码、时尚服饰、酒类等相关。



4.1.2 信贷作弊

（1）信贷欺诈攻击情报 196 万条，监测到活跃群组 4486 个

2023 年，威胁猎人共捕获信贷欺诈攻击情报 196 万条，监测活跃的作恶社交群组 4486 个，作恶黑产 2.8 万名；虽然 2023 年活跃的作恶群组数及作恶黑产数量变化相对平稳，平台仍需警惕信贷欺诈黑灰产的作恶情况。



（2）反催收手法及案例

反催收通常指的是一些组织或个人通过非正常手段帮助债务人恶意躲避债务的行为，帮助债务人延长还款期限、减免利息费用，或者通过其他方式减少债务人的还款责任。

例如反催收中介让债务人寄个人电话卡或者设置呼叫转移，由反催收团伙这边所谓的法务人员代替债务人进行协商沟通，达成减免利息和延期/分期还款等目的，最终基于反催收结果向债务人收取一定比例手续费，由此来获利。

经调研发现，在反催收作恶场景中主要存在四个主要角色：

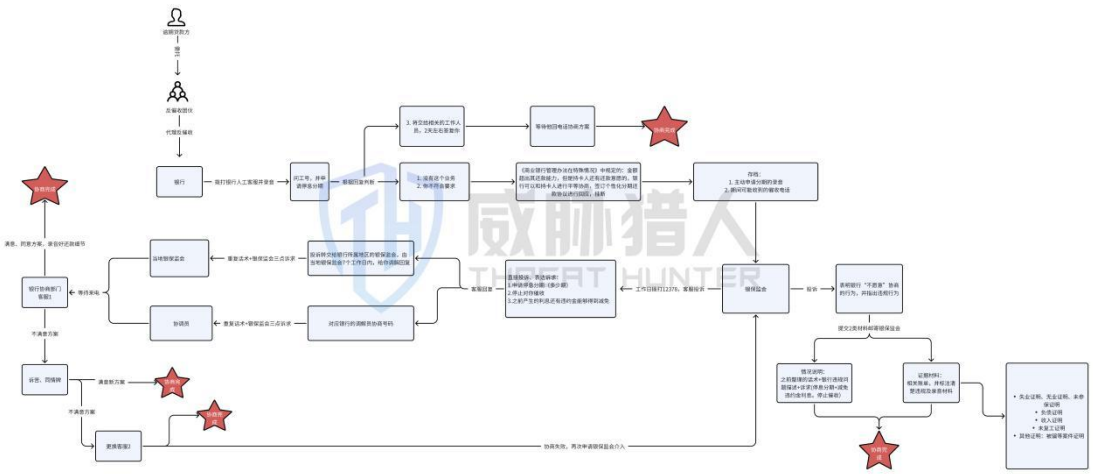
① **贷款者：**反馈延期停息需求，寻求反催收中介的帮助；

② **反催收中介：**在各类社交平台/渠道发布反催收业务广告，招揽已逾期的贷款者

③ **法务：**代替贷款者向网贷平台申请协商延期以及协商谈判

④ **借贷平台：**在法务的话术威胁下同意协商延期

以下是贷款逾期的延期停息操作的运作流程：

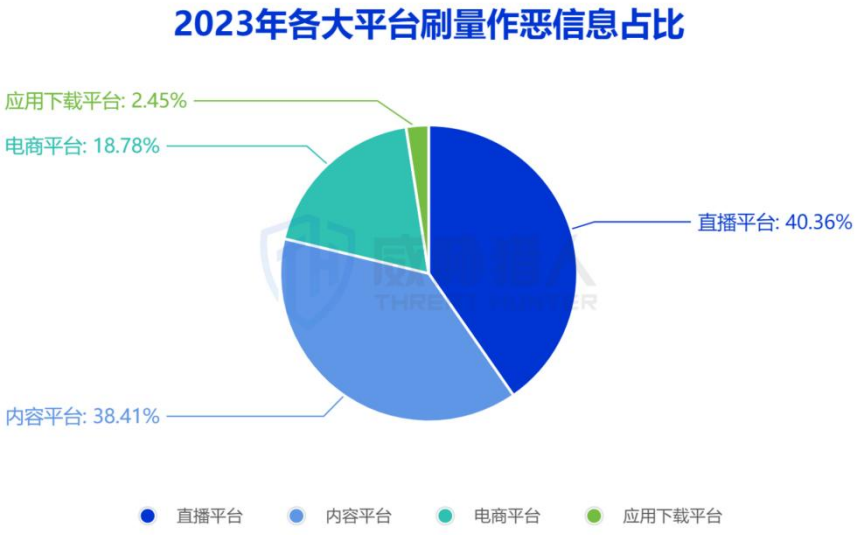


4.1.3 内容刷量

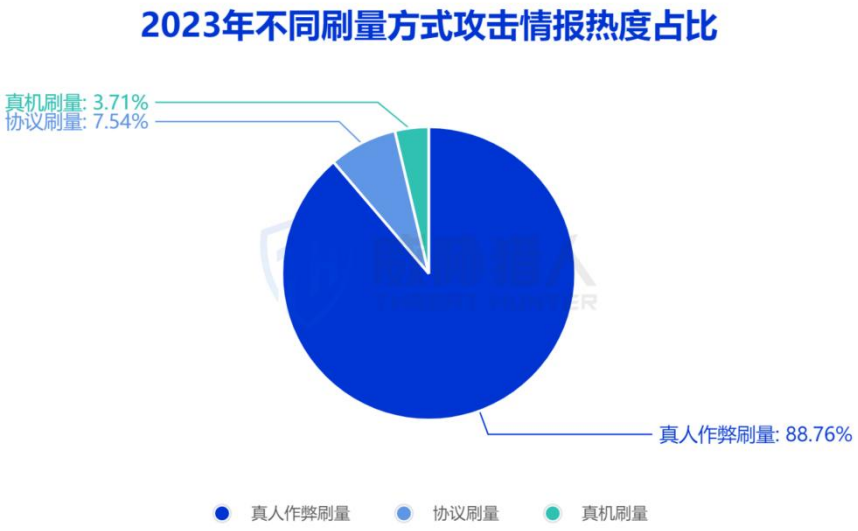
2023 年，整体刷量作弊情况依旧严峻，威胁猎人共捕获直播平台、内容平台、电商平台及应用下载平台刷量作弊攻击线报 42.5 万条，监测活跃的刷量作恶社交群组 4364 个，作恶黑产人数达 5759。

就刷量方式而言，随着各大平台对恶意刷量行为的识别能力提升，众多刷量工作室逐渐减少协议刷量及基于真实设备的群控刷量，转而使用真人刷量。

（1）直播平台及内容平台遭受刷量攻击最为严重



（2）真人作弊刷量仍为主流刷量方式



（3）刷量服务售后完善，黑产提供“补量”服务

随着各大平台对恶意刷量行为的识别能力提升，同一批次的刷量往往无法达到既定的目标数量。此时，黑产通常会进行补量操作，即“在规定的一段时间内，通过持续刷量，让文章或视频的浏览数、点击数保持在既定的目标数量上”。

4.2 2023 年数据泄露场景分析

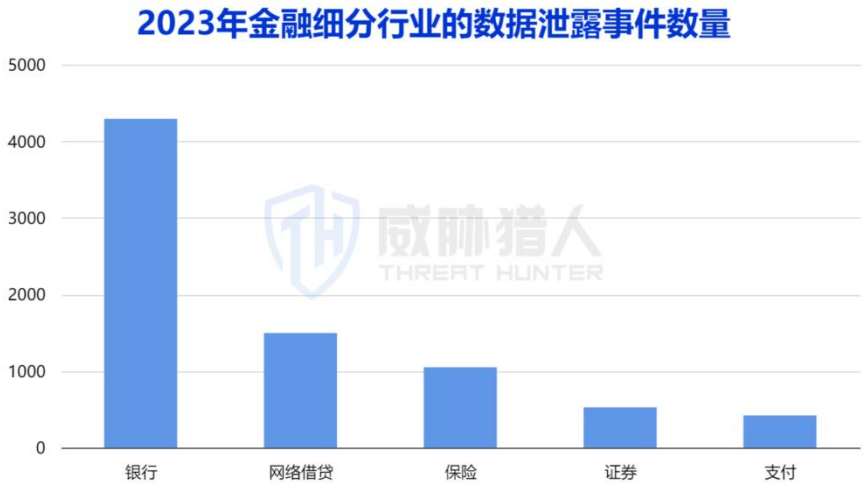
（1）2023 年监测数据泄露事件超 19500 起， 金融、物流、航旅等行业是数据泄露重灾区

据威胁猎人数据泄露风险监测平台数据显示，2023 年全网监测到的近 1.5 亿条情报中，分析验证有效的的数据泄露事件超过 19500 起。从行业分布来看，2023 年数据泄露事件涉及二十余个行业，数据泄露事件数量 Top5 行业分别为金融、物流、航旅、电商、汽车。

（2）金融行业数据泄露事件 8758 起位列第一，航旅行业跃居第三

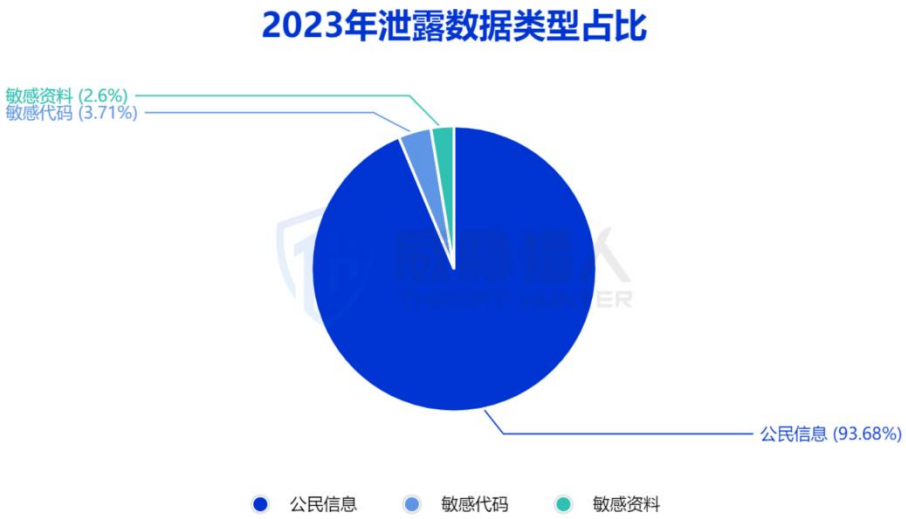
2023 年，金融行业依旧是个人信息泄露重灾区，数据泄露事件数量 8758 起，涉及银行、保险、证券等行业高净值人群信息，主要源于下游黑产用于营销推广以及诈骗的收益价值更高。

从金融细分行业来看，数据泄露事件数量发生最多的是银行业，全年共发生 4293 起，其次为网络借贷、保险、证券及支付行业。



（3）2023 年“公民个人信息”依旧是数据泄露的主要类型，占比超 90%

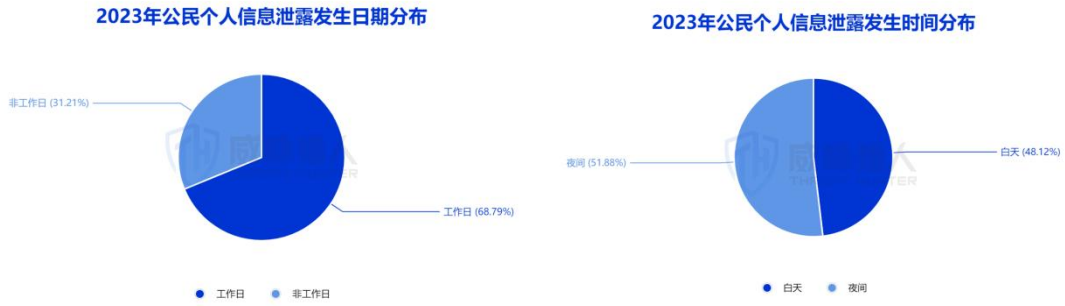
从数据泄露的类型来看，2023 年泄露数据类型主要有 3 种：公民个人信息共计 18347 起（93.68%）、敏感代码共计 727 起（3.71%）、敏感文件资料共计 510 起（2.6%）。



（4）公民个人信息在夜间交易的超过 50%，在非工作日交易的超过 30%

威胁猎人研究统计发现，2023 年公民个人信息泄露事件中的数据交易时间中，非工作日（周末、节假日）发生的事件数量高达 31.21%，夜间发生的事件占比高达 51.88%，超过一半。（夜间：18:30 至次日 09:30）

在防守最薄弱的时候，企业难以在数据泄露事件爆发时快速感知、及时响应，以至于错过最佳应对时机，给企业资金、品牌声誉及商业竞争带来重大影响。



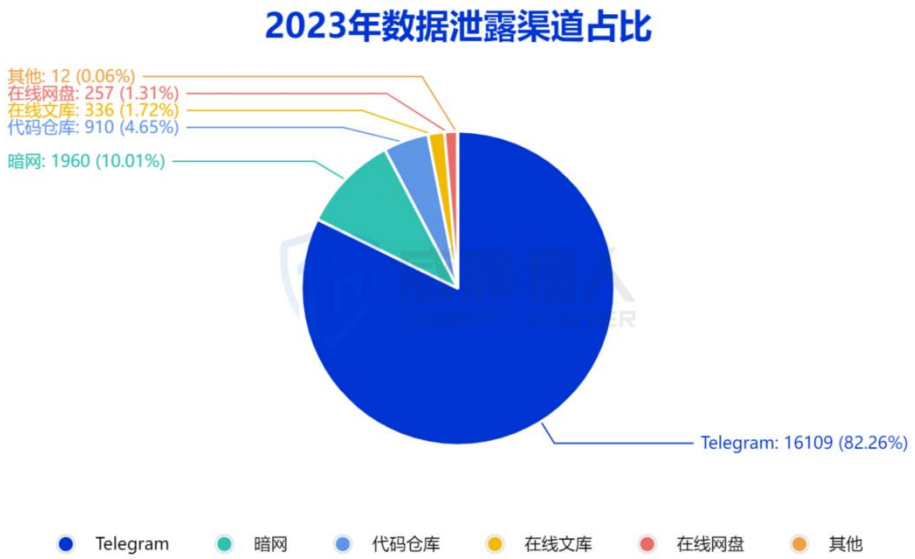
（5）数据泄露原因包括运营商通道泄露、内鬼泄露、黑客攻击等

从数据泄露的具体原因来看，2023 年数据泄露原因包括运营商通道泄露、内鬼泄露、黑客攻击、安全意识问题等。其中，因运营商通道泄露引发的数据泄露事件数量最多。

（6）Telegram、暗网是数据泄露的主要渠道，占比高达 92%

2023 年威胁猎人监测到的数据泄露事件中，发生在 Telegram 及暗网的达 92%以上，其中 82.26%集中在 Telegram，10.01%发生在暗网，主要原因是 Telegram 及暗网渠道的隐蔽

性较高，难以追溯到黑产本人，是黑产沟通和交易的首选渠道。此外，威胁猎人在代码仓库（如 GitHub、GitLab 、Postman 等）、网盘文库等渠道也监测到了数据泄露事件。



截至 2023 年 12 月，威胁猎人数据泄露监测情报覆盖了 Telegram 近 2 万个频道/群聊，在超过 1700 个频道/群聊中发现公民个人信息泄露风险事件。

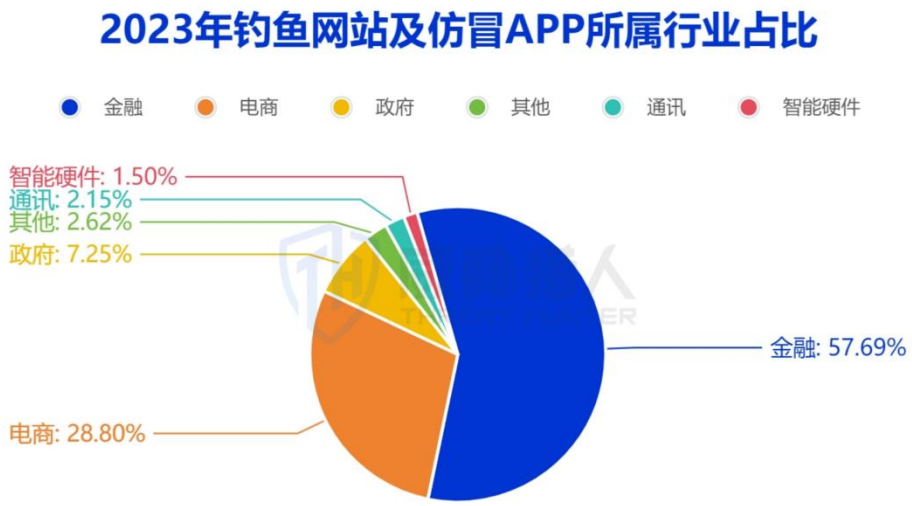
4.3 2023 年钓鱼仿冒场景分析

2023 年，威胁猎人共捕获到钓鱼网站 28794 例，涉及 234 家企业；捕获到仿冒 APP1295 例，涉及 67 家企业。此类网站及 APP 都是通过仿冒正常网站及 APP，获取用户信任并骗取用户的个人信息及钱财。

威胁猎人研究人员针对捕获到的案例进行分析发现：

（1）金融行业遭受的钓鱼仿冒情况最为严重

无论是钓鱼网站，还是仿冒 APP，金融行业成为黑产攻击的主要目标。由于金融行业的业务场景多涉及资金流转，且交易金额较大，故黑产往往在不引起受害者怀疑的同时，还能最大程度的获利。同时，大多数情况下，黑产为了尽可能取信于受害者，往往会选择行业头部企业进行仿冒。



（2）作恶手法以诱导下载仿冒理财及刷单 APP 进行转账为主

① 诱导下载仿冒投资 APP

此类型诈骗套路相对隐蔽，用户在注册时，需要相关介绍人提供注册码才能注册成功。

作恶的大致流程如下：

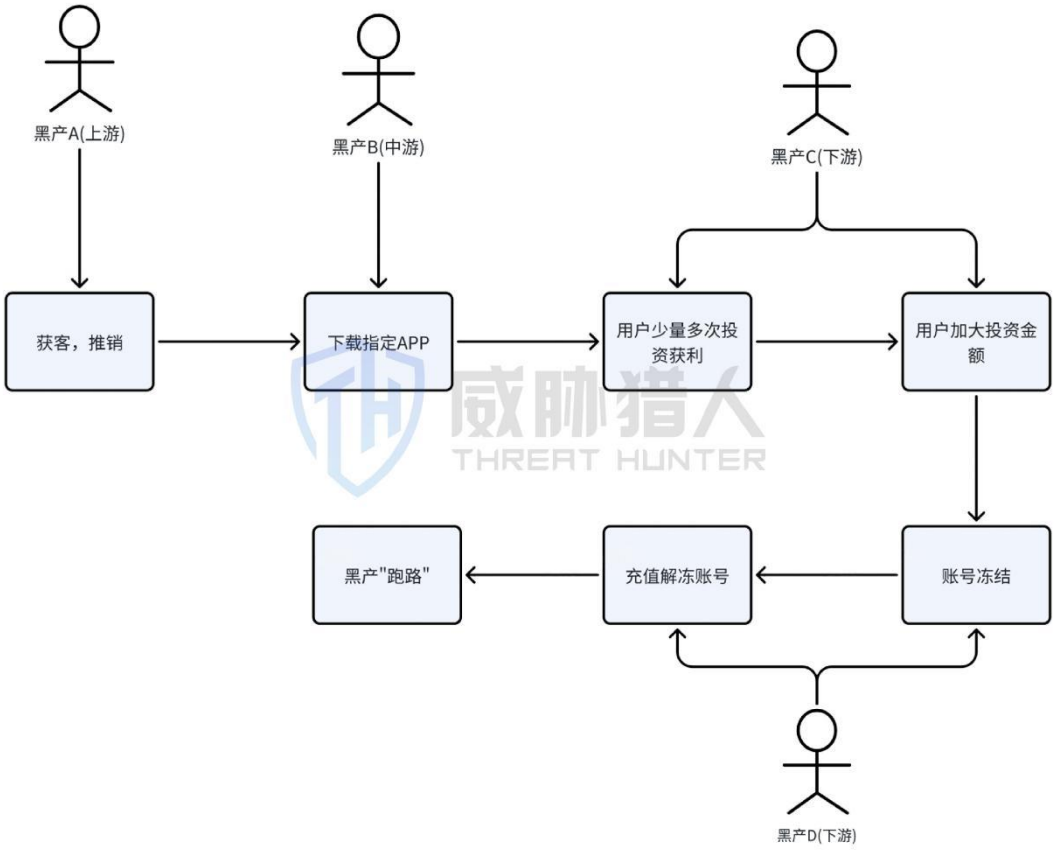
1、黑产通过技术手段实现精准获客，目标客群一般是拥有一定数额存款的高收入人群；

2、介绍人（黑产口中的“理财/投资/分析师”）通过夸大理财收益诱导客户下载指定 APP 进行理财或投资；

3、用户进行短期、多次理财投入，且每次都能获取到一定数额的收益；

4、分析师再次诱导用户加大理财（投资）投入，累计一定数额锁定用户账号；

5、客服再引导用户充值解冻用户账号，直到用户停止充值，平台直接“跑路”。



② 诱导下载仿冒电商刷单 APP

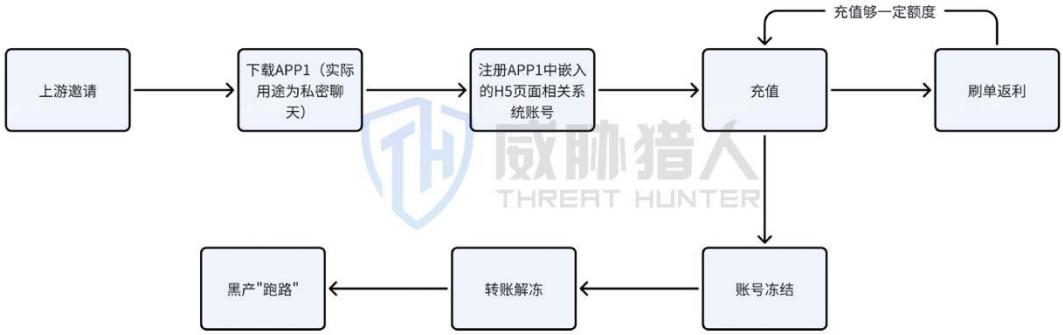
该仿冒类型表面上是仿冒电商平台的 APP，用户安装 APP 后会发现该 APP 实际上是仿冒社交平台的 APP，再嵌入一个刷单诈骗的 H5 界面（也就是刷单系统）。用户需要通过上游提供的邀请码才能注册账号，并进入相关的刷单系统。

作恶套路大致为：

1、刷单系统需要用户充值一定的金额才能进行接单，充值的金额越多，用户的等级越高，每日接单的数量和刷单返回的金额就越高。这种模式会诱导用户不断充值，充值到一定程度，账号就会出现冻结状态。

2、当用户寻找客服解除账号冻结状态，客服会引导用户多充钱解除账号异常后才能提现。

3、用户不进行充值或者发现平台异常后，用户的大量资金已经被黑产转移，平台也会“跑路”。



05

总结

2023 年黑灰产作恶情况愈发严峻，黑灰产从业人员数量、作恶资源量级连续两年呈现上升趋势，黑灰产获取作恶资源的途径更为隐蔽，无论是攻击资源、作恶手法还是作恶场景，都发生了巨大的变化，黑产攻防对抗也成为了各企业平台面临的极大挑战。从 2023 年互联网黑灰产趋势来看，**企业需要重点关注以下问题：**

1、在攻击资源方面，2023 年黑灰产整体资源量级大幅上升，应用方式更加高效隐蔽

2023 年国内作恶手机号较 2022 年增长 15.44%，风险 IP 数量较 2022 年上升 88.47%，洗钱银行卡数量较 2022 年增长 133.74%。

在应用方面也有了新的趋势，如发卡平台成为黑产投放高价值接码手机卡的主流渠道之一；黑产通过植入木马恶意使用正常用户 IP 的行为更加猖獗，这种“好坏共用”的 IP 更容易逃脱企业风控。

2、在攻击技术方面，AI 技术的应用大幅提升攻击效率，头部云手机平台呈现产业化趋势

2023 年，AI 技术应用于网络安全的多个场景，AI 技术的深度应用也引起了大量黑产团伙的觊觎。不少黑产团伙利用如文本生成、照片活化、人脸替换等 AI 技术进行攻击，进一步实施诈骗行为，包括在社交场景接入 AI 机器人自动生成聊天话术、利用 AI 进行视频伪造绕过人脸验证等。

2023 年提供云手机服务的平台持续增加，且头部云手机平台已呈现出产业化趋势，这类平台除了提供云手机服务外，还会提供配套的攻击工具，如代理 IP 服务、改机工具、改定位工具、Hook 框架等，极大提高黑产攻击效率。

3、在攻击场景方面，为逃避企业风控系统，出现了更多隐蔽的攻击方式

在营销欺诈场景上，2023 年威胁猎人研究人员发现，黑灰产为了避免众包平台被监测和风控，推出了更为复杂、安全的众包发布渠道。这种众包平台“私域化”虽增加了执行时间和操作成本，但其隐蔽性使得平台的监测及风控难度大大提升。

数据泄露场景上，威胁猎人研究员发现，公民个人信息泄露事件中的数据交易时间中，非工作日（周末、节假日）发生的事件数量高达 31.21%，夜间（18:30 至次日 09:30）发生的事件占比高达 51.88%。

夜间和非工作日时间是企业防守最薄弱的时候，大部分企业很难在数据泄露事件发生时快速感知、及时响应，以至于错过最佳应对时机，给企业资金、品牌声誉及商业竞争带来重大影响。

近年来，黑灰产不断优化攻击资源、迭代攻击技术，以确保持续、高效的获利，日益严峻的黑灰产攻防局势也意味着，各企业平台在感知黑灰产的攻击行为上存在一定的滞后性。

针对层出不穷的作恶事件，企业应及时了解其作恶流程及细节，并结合自身业务场景建立具体的风控规则。此外，企业也需要意识到与外部黑产的对抗是动态的、持续性的，可以**依托基于全网多渠道监测的黑灰产情报数据**，提取黑灰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，快速识别风险并进行针对性防御。

对抗黑灰产的道路任重道远，企业在外部“威胁情报”的助力下，能够全面、及时感知黑灰产团伙的轨迹及动向，在日益严峻的黑灰产风险局势中**精准打击黑灰产，更好地守护自身业务安全。**

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（品牌名：威胁猎人）

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