威胁猎人
THREAT HUNTER

以 情 报 构 筑 数 字 化 安 全 基 石

黑产大数据

2024 年互联网黑灰产趋势年度总结

T H R E A T H U N T E R

关于威胁猎人

威胁猎人 Threat Hunter（深圳永安在线科技有限公司）成立于 2017 年，以黑灰产情报能力和反欺诈技术为核心，专注于及时、精准、有效的业务欺诈风险的发现和响应。

公司围绕不同行业在数字化发展过程中面临的业务欺诈、数据泄露、钓鱼仿冒、API 攻击等风险场景，提供成熟多样的产品与服务，并多次入选 Gartner 技术成熟度曲线报告、IDC 威胁情报领域代表厂商。

公司总部在深圳，在北京、上海、重庆、新加坡等地设有分公司，并在深圳和重庆两地建立数字风险应急响应中心（DRRC），为客户提供 7*24 小时全天候数字风险应急响应和及时、优质的服务支持。截至目前，公司已为金融、政务、物流、互联网、科技、零售等行业的 300 多家客户提供安全服务，覆盖 85%头部互联网企业，每年帮助客户减少数十亿资金损失。

前言

2024 年，互联网黑灰产攻击依旧严峻。不管是在黑灰产团伙规模，还是攻击资源、攻击技术的应用以及攻击场景的演变，均出现了较大的变化。

在攻击资源方面，2024 年威胁猎人捕获全球新增作恶手机号 1600 多万例，日活跃作恶 IP1170 万例，较 2023 年大幅提升。为躲避风控监测，黑灰产不断升级技术寻找更加隐蔽的攻击资源，如通过在正常用户设备植入木马将其 IP 作为攻击资源、“商户洗钱”产业链快速发展等。

在攻击技术方面，2024 年黑产团伙对通用技术的应用也有新的发展，如滥用“子母机”绕过身份认证、利用“NFC 远程传输软件”进行境外洗钱、定制化云手机系统提升攻击效率等等。

在攻击场景方面，线上业务欺诈、金融贷款欺诈、品牌广告欺诈、API 攻击、钓鱼仿冒、数据泄露、电信网络诈骗等场景热度持续高涨。线上业务欺诈已进入深水区，全行业、全业务环节无差别攻击；“王星事件”更是进一步提升了公众对电信网络诈骗的关注度。

威胁猎人发布《2024 年互联网黑色产业链研究报告》，基于对 2024 年互联网黑色产业链的深入研究，从 2024 年黑灰产攻击资源、攻击技术、攻击场景等维度进行分析，客观呈现 2024 年互联网黑灰产的整体发展态势，旨在从情报维度帮助各行各业企业提升对黑灰产的认知，从而进一步完善风控策略。

目 录

01

2024 年互联网黑灰产攻击资源分析

一、2024 年互联网黑灰产攻击资源分析

1.1 2024 年作恶手机号资源分析

1.1.1 2024 国内作恶手机号新增数量超 800 万，较 2023 年提升 30%

据威胁猎人情报数据显示，近年来国内作恶手机号数量持续上涨，2024 年新增量级超 800 万，较 2023 年增长 30%。

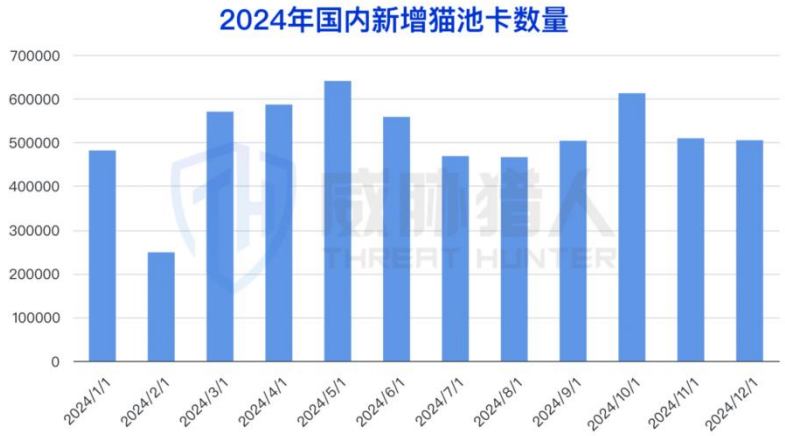
作恶手机号资源中，“猫池卡”和“拦截卡”占比最高，下文 1.1.2 和 1.1.3 将重点分析 2024 年“猫池卡”和“拦截卡”资源的变化情况。

1.1.2 2024 年「猫池卡」资源分析

（1）2024 年国内新增猫池卡 615 万，较 2023 年增加 4.86%

据威胁猎人情报数据显示，2024 年国内新增猫池卡 615 万个，较 2023 年上升 4.86%。

猫池卡：指通过“猫池”网络通信硬件实现同时多个号码通话、群发短信等功能的作恶手机卡。

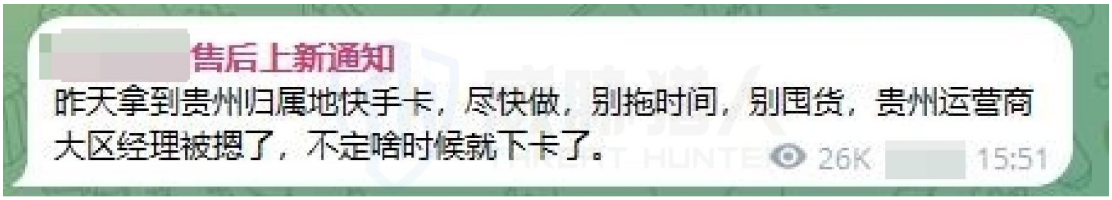


从 2024 年国内猫池卡数量的变化趋势来看，2 月、6 月到 9 月期间，新增国内猫池手机卡数量呈现下滑趋势。

经威胁猎人情报专家分析，出现这一趋势的主要原因是：

1、2 月因春节期间黑产交易放缓，攻击者活跃度降低导致数量显著下降，节后恢复稳步上涨趋势；

2、6-9 月期间，由于监管机构加强打击，多个发卡平台被关停，部分卡商被捕，造成供应减少，导致新增猫池卡数量下降。

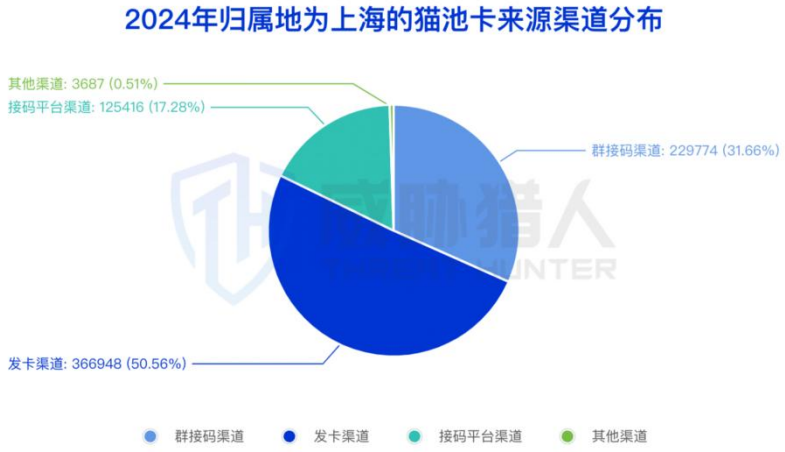


（2）2024 年国内新增猫池卡归属省份 TOP3：上海、北京、辽宁

威胁猎人情报数据统计显示，2024 年国内新增猫池卡归属地省份（含直辖市）主要集中在上海、北京、和辽宁省。

其中，归属地在上海的猫池卡数量同比 2023 年增长了 87.86%。威胁猎人关注到，今年上海的猫池卡在全年各月均保持较高数量，活跃在发卡平台的头部卡商今年也持续提供上海猫池卡。

通过对上海今年新增的猫池卡来源渠道分析，发现来自发卡平台的猫池卡数量占比超过一半：



2024 年国内新增猫池卡归属地 TOP10 对比 2023 年变化情况如下：

省份	2024年猫池手机卡新增数量排名	对比2023年变化情况
上海	第一	↑3
北京	第二	↑7
辽宁	第三	↑2
山东	第四	↓2
河北	第五	↑1
广东	第六	↑2
江苏	第七	↓6
湖北	第八	2023年未进入top10
福建	第九	2023年未进入top10
重庆	第十	维持

【关注】2024 年归属地为中国香港的作恶手机号持续增长，全年捕获 78.25 万例

值得关注的是，威胁猎人情报数据显示，自 2024 年 3 月起，归属地为中国香港的风险手机卡交易数量大幅增长，9 月份达到峰值。

由于下游诈骗黑产需求旺盛，中国香港手机号因可注册国内外应用、成本低、可用时间长等特点，仍被黑产大量需求。

对比其他境内手机卡，中国香港手机卡具备如下特点：

1、注册范围广：香港手机卡注册范围广，可注册 Telegram、WhatsApp 等海内外应用；

2、在线使用时间长：香港手机卡接码服务的在线使用时间相对其他境内卡更长，一般可保证一个月重复使用，而其他境内手机卡一般为数日；

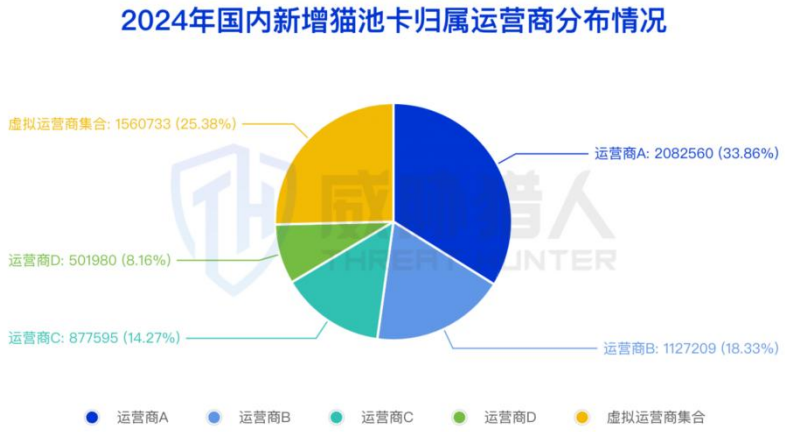
3、价格较低：香港手机卡的价格相对其他境内卡接码价格更低；

4、支持多种接码形式：香港卡支持多种接码形式，目前威胁猎人在接码平台、发卡网站、私域接码均发现了香港相关手机卡的作恶记录。

（3）2024 年国内新增猫池卡归属为三大运营商的占比为 76.42%，比去年提升 14.51%

威胁猎人情报数据显示，今年国内新增猫池卡的归属运营商主要为基础运营商，占比高达 76.42%，相比去年提升了 14.51%。

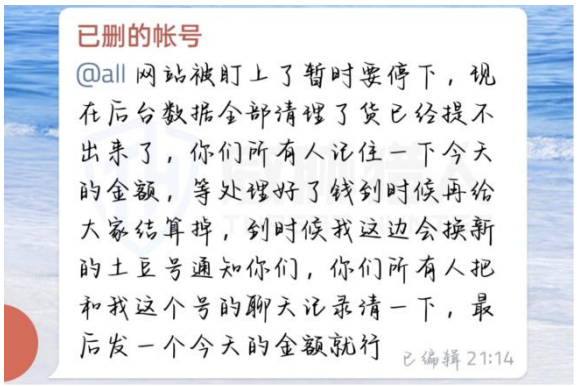
威胁猎人情报人员通过调研发现，今年三大运营商占比提升，主要是很多企业进一步提升对虚拟运营商手机卡的风险控制，导致黑产对国内三大运营商的手机卡资源需求增加。



（4）【关注】2024 年猫池卡发卡平台数量增加了 39.37%，但平台生存周期缩短

威胁猎人持续监控黑灰产作恶资源来源渠道变化趋势，发现作为猫池卡主要贡献渠道的发卡平台在 2024 年数量大幅增加，但生存周期缩短：

2024 年新出现了 171 个猫池卡发卡平台，同步 2023 年增长 39.37%，但其中有 24%的猫池卡发卡平台运营时间不足一周。威胁猎人进一步调研发现，今年发卡平台遭受了较强的监管压力，多个发卡平台以及活跃的猫池卡卡商因遭受监管打击而停止运营或活跃。



此外，威胁猎人对目前还存活的猫池卡相关发卡平台进行测试发现，一些黑灰产为了防止被监管打击，会采取一些较高的安全措施，包括但不限于周期性订单删除、使用加密货币支付、频繁修改接码地址、限制异常访问和支付等。

1.1.3 2024 年「拦截卡」资源分析

（1）2024 年国内新增拦截卡 196 万例，较 2023 年增长 405.50%

据威胁猎人情报数据显示，2024 年国内新增拦截卡大幅增加，共有 196.64 万例，较 2023 年增长 405.50%。

威胁猎人研究发现，一月份拦截卡数量大幅提升是因为去年年底新出现的一个拦截卡渠道，投放了大量拦截卡资源，2024 年该渠道贡献拦截卡数量近百万余例，占今年整体数量的 48.82%。但该渠道在 2024 年 6 月到 7 月期间暂停活跃，最终在 2024 年 12 月停止运营。

（2）2024 年国内新增拦截卡归属省份 TOP3：广东、山东、四川

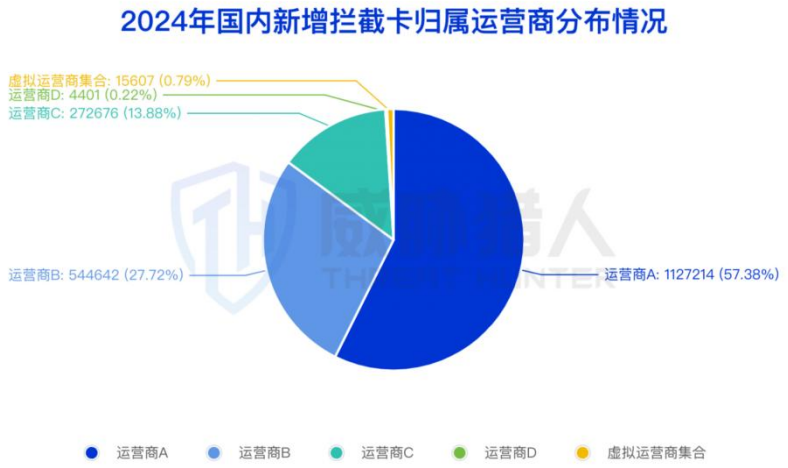
威胁猎人情报数据统计显示，2024 年国内新增拦截卡归属地省份（含直辖市）主要集中在广东、山东和四川。

2024 年国内新增拦截卡归属地 TOP10 对比 2023 年变化情况：

省份	2024年拦截手机卡新增数量排名	对比2023年变化情况
广东	第一	↑3
山东	第二	维持
四川	第三	↑4
河南	第四	↑1
湖南	第五	2023年未进入top10
安徽	第六	↑4
广西	第七	↓6
河北	第八	维持
江苏	第九	↓6
江西	第十	↓4

（3）2024 年国内新增拦截卡归属为三大运营商的占比为 98.99%

威胁猎人情报数据显示，今年国内新增拦截卡的归属运营商 98.99%为基础运营商，归属其他运营商的占比 1.01%。



（4）【关注】“群接码”模式简化黑产使用拦截卡的流程，并使拦截卡真实平台更隐蔽

威胁猎人研究发现，拦截卡的接码方式也逐渐从传统的拦截卡平台接码模式转变为“群接码”模式 。

这种模式下，拦截卡卡商隐藏真实号码，仅展示打码号码，只有黑卡购买者可获取完整号码完成接码作恶。

传统的拦截卡平台接码样例：

“拦截卡”的群接码模式接码样例

#	号码	时间	内容
26	1 3****5 2	2024-11-29 15:59:31	【 】验证码：(436991)，您正在使用短信验证码登录功能，2分钟内有效。转发可能导致帐号被盗，请勿泄露给他人
96	1 2****6 3	2024-11-29 15:55:03	【 】验证码：(732739)，您正在使用短信验证码登录功能，2分钟内有效。转发可能导致帐号被盗，请勿泄露给他人
97	1 2****5 5	2024-11-29 15:53:28	【 】验证码：(421760)，您正在使用短信验证码登录功能，2分钟内有效。转发可能导致帐号被盗，请勿泄露给他人

相比传统拦截卡平台使用专属接码工具接码，这种模式的优势在于：

1、**使用更便利，**卡商只需提供号码和接码链接，无需为下游代理或黑卡使用者开设账户或配置权限；

2、**更高隐蔽性，**卡商可通过“群接码”模式隐蔽真实的平台信息，不将平台的敏感信息暴露于使用者。

目前，通过“群接码”渠道日均捕获作恶短信记录 1269 例，作恶记录最高峰为 11 月，捕获作恶短信记录近 6 万例：

1.2 2024 年作恶 IP 资源分析

1.2.1 2024 年日活跃作恶 IP 有 1178 万，较 2023 年提升 95.68%

据威胁猎人情报数据显示，近年来日活跃作恶 IP 数量持续上升，2024 年日活跃作恶 IP 数量达到 1178 万，较 2023 年增长 95.68%

1.2.2 2024 年国内作恶 IP 资源分析

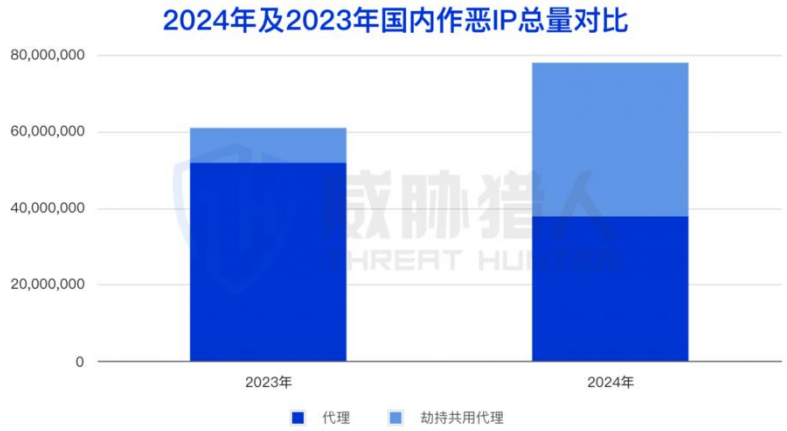
（1） 2024 年国内作恶 IP 有 7794 万个，同比 2023 年增长 31.96%

2024 年，威胁猎人共捕获国内作恶 IP7794 万个，同比 2023 年增长 31.96%。

威胁猎人研究发现，2024 年国内作恶 IP 的大幅增长主要是劫持共用代理 IP 数量急剧增长导致。2024 年，国内劫持共用代理平台发展迅速，威胁猎人捕获劫持共用代理 IP 数量超 4000 万，占比从去年 14.91%提升至今年的 51.47%，且超过普通代理 IP 的占比。

劫持共用代理 IP：指被黑产恶意劫持的正常用户 IP 资源。黑产通过在正常用户设备中植入木马，通过木马在正常用户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。

威胁猎人在 2024 年 1 月已把这类 IP 标记为“劫持共用代理 IP”风险标签



（2）2024 年国内作恶 IP 归属省份 TOP3：江苏、广东、河南

威胁猎人情报数据统计显示，2024 年国内活跃的作恶 IP 归属省份（含直辖市）主要集中在江苏省、广东省和河南省。其中，河南省量级提升最大，提升了 54.45%，排名也从 23 年的第六到了第三。

（3）【关注】黑产 IP 资源获取技术升级，利用正常用户的 IP 资源规避风控检测

随着网络安全监管及企业风控策略的增强，为规避风控检测和追踪，黑产也在升级技术尝试挖掘更加隐蔽的 IP 攻击资源。

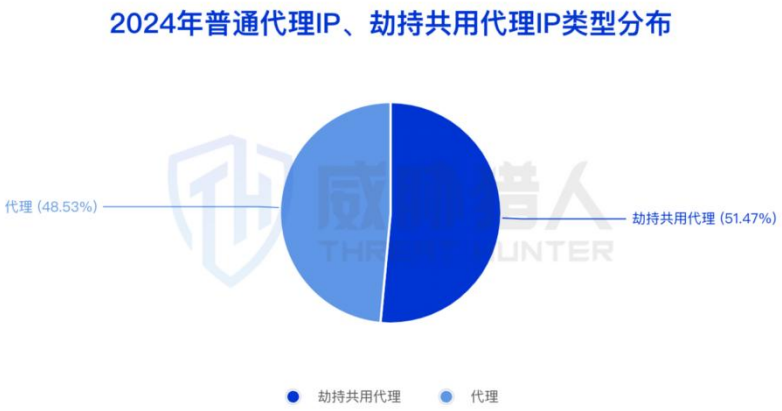
近年来，威胁猎人陆续发现正常用户与不法分子混合使用的作恶 IP 类型，并对其进行深入研究，于 2024 年推出「劫持共用代理 IP」、「云服务 IP」、「云手机 IP」等风险标签。

1. 2024 年劫持共用代理 IP 占比过半，成为攻击者主要使用的攻击资源

劫持共用代理 IP 是指被黑产恶意劫持的正常用户 IP 资源。威胁猎人发现，黑产通过在正常用户设备中植入木马，通过木马在正常用户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。

劫持共用 IP 大部分时间是正常用户的常规行为，仅少数时间被黑产劫持用于短暂恶意行为，因此平台风控会直接将其视为正常用户，忽视其短暂作恶行为，这就使得黑产使用劫持共用 IP 的成功率往往高于普通代理 IP，导致越来越多的平台转向劫持共用代理 IP 资源。

这类劫持共用代理 IP 在 2023 年底出现，2024 年快速发展、数量急剧增加，2024 年威胁猎人捕获劫持共用代理 IP 超 4000 万，同比增长 341.81%，且超过了普通代理 IP 的数量。

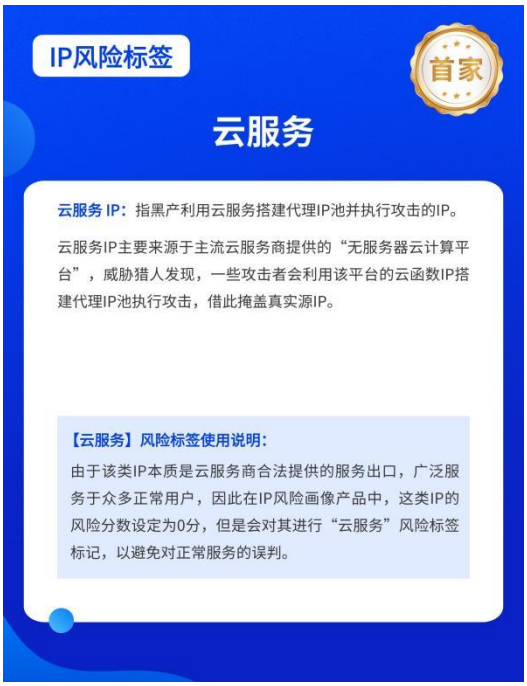


2. 黑产滥用云技术：云函数与云手机群控技术成黑产 IP 作恶新手段

云服务技术为各行业带来便利的同时，也在被黑产滥用。一些黑产将云技术成果转为作恶工具，如借助云服务搭建代理 IP 资源池、利用云手机的群控设置向企业发起攻击等。

威胁猎人发现，一些攻击者为了掩盖真实源 IP，会利用云计算平台的云函数 IP 搭建代理 IP 池执行攻击，或者利用云手机的群控配置执行批量攻击，威胁猎人将这两种方式产生的 IP 定义为「云服务 IP」、「云手机 IP」。

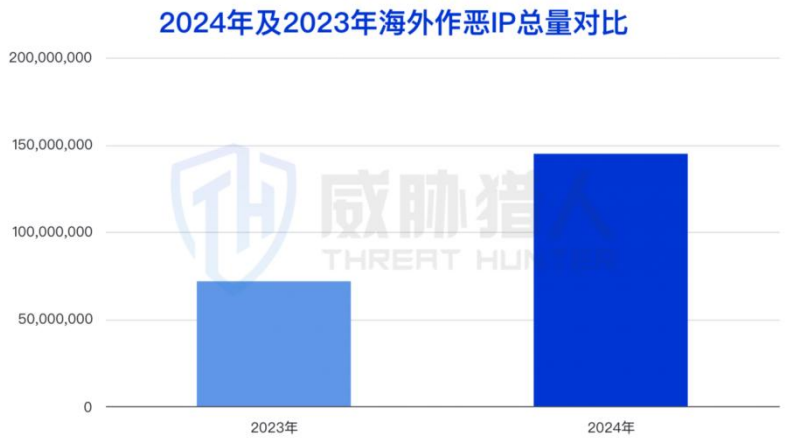
不管是云服务 IP 还是云手机 IP，都是广泛服务众多正常用户，因此平台风控一般会直接将其视为正常用户，忽视了它们的作恶行为。



1.2.3 2024 年国外作恶 IP 资源分析

（1）2024 年捕获国外作恶 IP 4479 万个，同比 2023 年增长 102.14%

2024 年，威胁猎人加强对海外作恶 IP 进行的监测，2024 年共捕获海外作恶 IP4479 万个，相比 2023 年提升了 102.14%。



（2）2024 年国外作恶 IP 归属国家 TOP3：巴西、美国、印度

（3）国内外作恶 IP 类型占比存在差异，国外移动网络占比远超国内

威胁猎人情报人员对国内和国外作恶 IP 类型进行分析，发现二者存在差异：

国内作恶 IP 主要以家庭宽带 IP 为主，占比将近 90%，国内作恶代理 IP、秒拨 IP 和劫持共用代理 IP 都与家庭宽带密切相关；

国外作恶 IP 虽然家庭宽带占比也是最大，但移动网络占比也比较高，超过 40%，进一步分析发现，这些 IP 主要来自流量卡，通过频繁切换飞行模式来实现 IP 变化。

1.3 2024 年网络洗钱资源分析

1.3.1 2024 年涉及洗钱的银行卡资源分析

（1）2024 年参与洗钱的银行卡中涉诈卡占比最多，占比 42.03%

威胁猎人对捕获到的 33.6 万张参与洗钱的银行卡进行分析，主要分为涉赌卡、跑分卡和涉诈卡三种类型，其中涉诈卡占比最大，达到 42.03%。

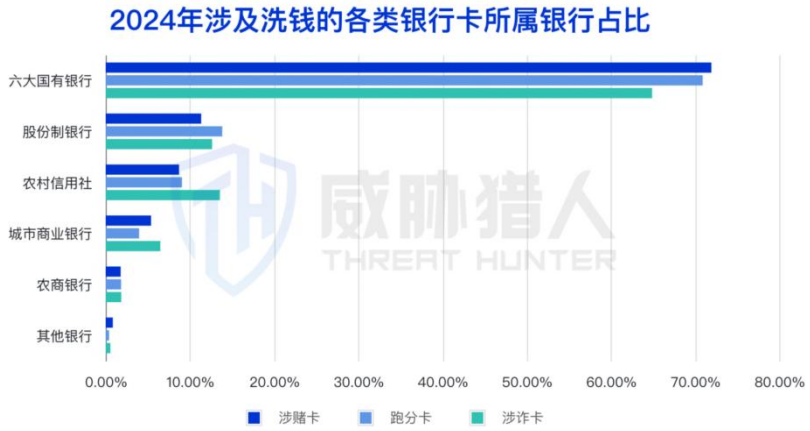
涉赌卡：活跃在赌博平台中，为赌博平台内收款使用的银行卡，常被用于赌博平台内进行充值收款行为，关联的资产涉及到赌博洗钱行为。威胁猎人通过人工和自动化结合的方式，从各类赌博平台中采集用于收款行为的银行卡账号信息。

跑分卡：活跃在跑分平台，为跑分份子使用的银行卡，常被用于各种非法来源资金的流通交易。威胁猎人通过自动化的方式，从跑分平台 APP 中获取到跑分订单中的银行卡账号信息。

涉诈卡：在各类匿名社交黑产群聊中，被诈骗团伙购买用于洗钱的银行卡，常用于诈骗类黑资金转移。威胁猎人通过自动化的方式，从各大匿名社交黑产群聊中发送的记录中，提取出诈骗团伙所使用的银行卡账号信息。

（2）2024 年参与洗钱的银行卡归属银行分布：六大国有银行占比最高

威胁猎人通过对三类洗钱卡的监测数据发现，归属为六大国有银行的洗钱卡占比最大。这主要是因为其覆盖范围广、客户基数大，因此也更容易被黑产利用作为洗钱工具。。这主要是因为其覆盖范围广、客户基数大，因此也更容易被黑产利用作为洗钱工具。



*其他银行包括：民营银行、开发性金融机构及其他金融机构

（3）2024 年参与洗钱的银行卡归属地区分布：广东省数量最多

威胁猎人研究发现，三种类型的洗钱银行卡归属地区分布上有相似也有差异：

相同点：

三种类型的洗钱银行卡归属省份 TOP10（排名有先后）都是广东、广西、江苏、湖北、山西、河南、重庆、四川、山东、云南，且 TOP1 都是广东省；

三种类型的洗钱银行卡归属城市 TOP10（排名有先后）都是深圳、广州、重庆、东莞、上海、武汉、晋城、郑州、成都；且 TOP3（排名有先后）都是深圳、广州、重庆。

差异点：

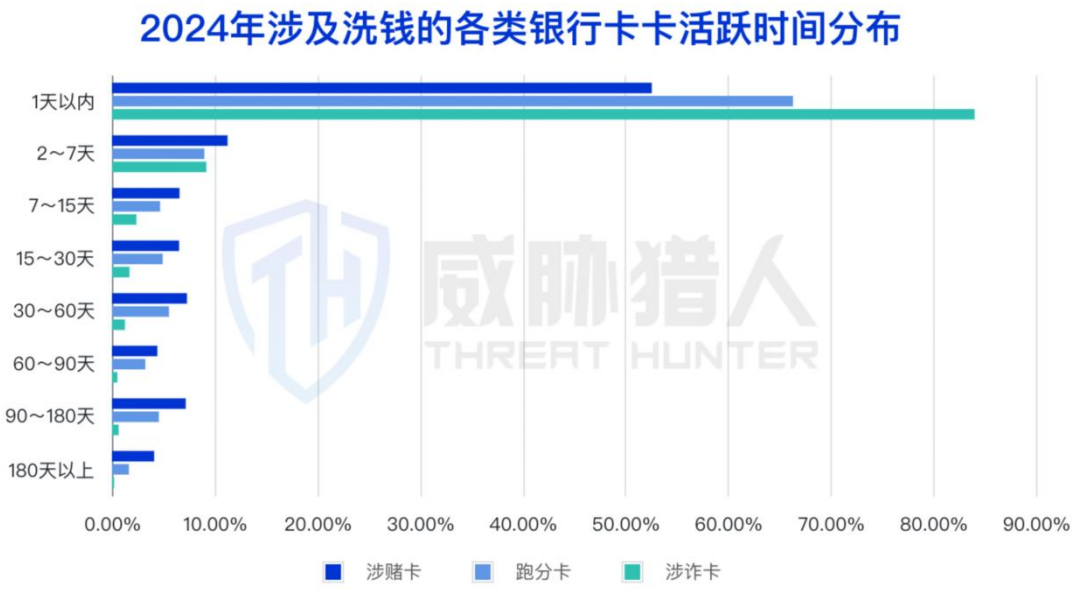
河南、山西、四川、云南和山东等地的涉诈卡数量均高于跑分卡和涉赌卡；

重庆的涉诈卡和涉赌卡最多，深圳和广州的跑分卡最多。

（4）参与洗钱的银行卡超过 50%活跃周期不到 1 天

威胁猎人研究发现，2024 年参与洗钱的银行卡，超过 50%的卡只在 1 天内活跃，其中涉诈卡在 1 天内活跃的占比达到 84.03%，高于跑分卡的 66.33%，和涉赌卡的 52.58%。

这也说明，洗钱场景下，黑产更倾向于快速完成交易，具有明显的短期、高频操作特点，尤其是在诈骗洗钱场景下更明显。

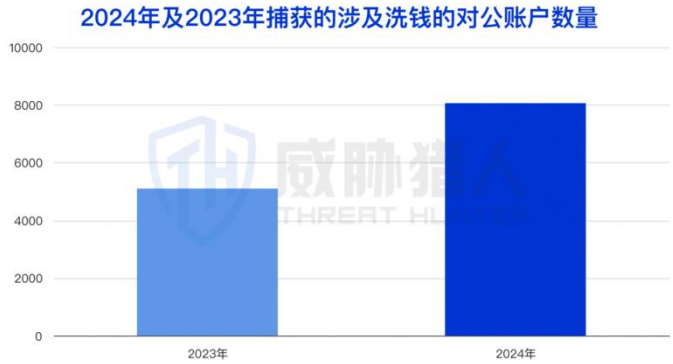


1.3.2 2024 年对公洗钱账户资源变化分析

洗钱对公账户：对公账户指以公司名义在银行开立的账户，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。

（1）2024 年新增参与洗钱的对公账户 8059 个，较 2023 年上涨 58.05%

2024 年，威胁猎人持续监测黑产在洗钱过程中所使用的银行对公账户资源，根据威胁猎人情报监测洗钱对公账户数据显示，2024 年，新增洗钱对公账户数量大幅上涨，同比 2023 年增长了 58.05%。



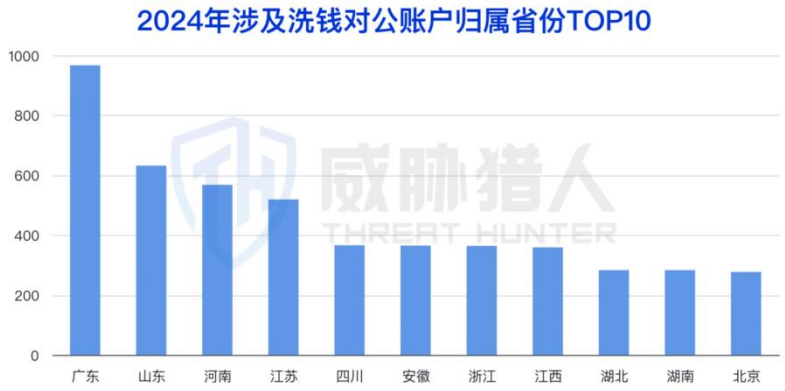
（2）2024 年涉及洗钱的对公账户所属银行中，城市商业银行排行第一

威胁猎人情报数据显示，参与洗钱的对公账户归属银行类型分布中，城市商业银行排行第一，占比 30.63%。

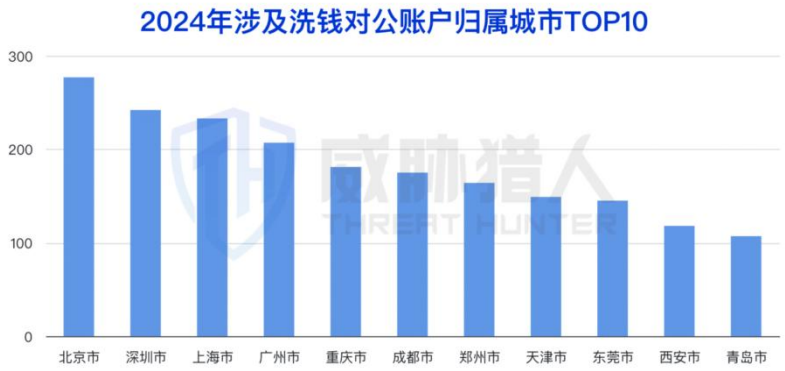
进一步分析发现，今年城商行对公账户数量较 2023 年上升 8.13%，农信社和农商行的对公数量较比 2023 年分别上升 5.48%和 3.48%，而六大国有占比下降 11.21%。

按照此趋势，黑产利用对公账户洗钱的过程中可能开始转向地方性银行，威胁猎人将保持关注。

（3）2024 年涉及洗钱的对公账户归属省份 TOP3：广东省、山东省、河南省



（4）2024 年监测到涉及洗钱对公账户归属地区最多的三个城市：北京市、深圳市、上海市



1.3.3 2024 年参与洗钱的商户资源变化分析

威胁猎人研究发现，洗钱团伙除了使用个人银行卡、对公账号等进行洗钱外，也会利用“商户账号”进行洗钱。

“商户”通常指具有合法营业资格的商户商家及商户账号。近年来，诈骗或洗钱团伙开始利用商户账户收取“黑钱”来洗钱，使用商家资质开通的收款账户基本没有收款额度限制，可支持花呗、信用卡等多种付款方式，相比传统洗钱方式会更隐蔽和高效。

威胁猎人在 2024 年针对“商户洗钱”产业链进行重点研究，发现目前已出现了“商户代收”（商家码）、“扫街码”、“商户反扫”、“商户代付”（核销码）等多种商户洗钱方式。

（1）“商户洗钱”成上升趋势，2024 年参与洗钱的商户及黑产团伙持续增多

威胁猎人情报数据显示，2024 年参与洗钱的商户数量持续增多，下半年相比上半年增长了 141.42%。

2024 年下半年，活跃的洗钱黑产团伙数量显著增加，同比上半年增长 81.91%。

（2）2024 年参与洗钱的商户归属地 TOP3 省份：广东省、浙江省、四川省

（3）2024 年参与洗钱的商户归属地 TOP3 城市：深圳市、成都市、广州市

（4）2024 年参与洗钱的商户所属行业分布 TOP3：零售业、批发业、餐饮业

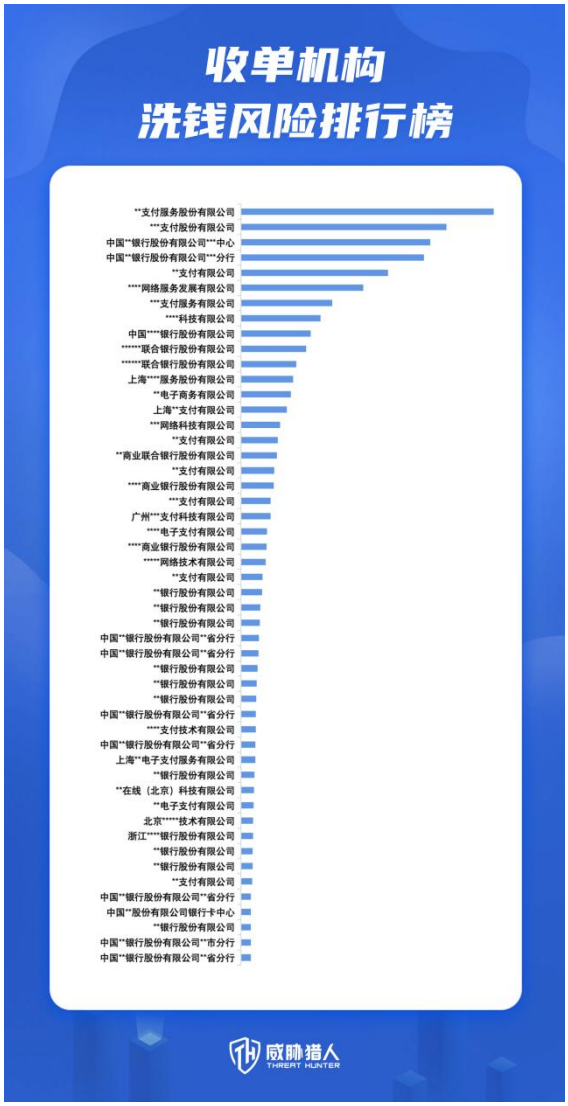
威胁猎人情报人员对参与洗钱的商户进一步分析发现，这些商户涉及 80 多个行业，其中零售业商户占比最多，超过了 40%，其次是批发业、餐饮业。这类行业具备资金流动频率高、交易对象多、资金结算快等特征，这些特征正符合黑产洗钱的要求，黑产利用此类商户洗钱更不容易触发风控。

（5）【关注】2024 年金融行业收单机构洗钱风险排名

威胁猎人研究发现，在“商户洗钱”产业链中，有一个核心的角色——收单机构。收单机构既有企业性质的第三方收单机构，也有银行自身作为收单机构角色。

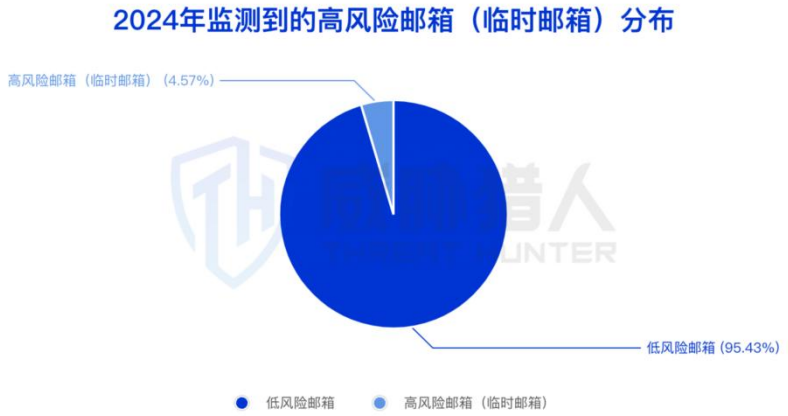
在威胁猎人监控的 300 多家涉及商户洗钱风险的收单机构中，银行自身作为收单机构的占比最多，达到 84.17%。

威胁猎人按照洗钱交易次数排名，将 2024 年涉及洗钱的收单机构整理输出 TOP50 排名：

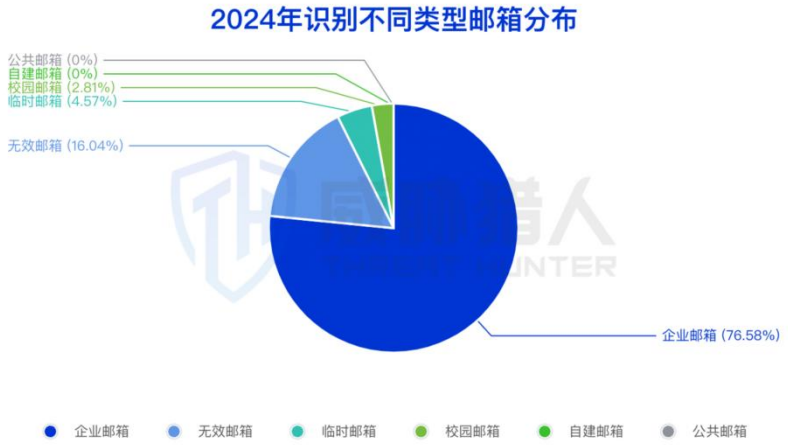


1.4 2024 年风险邮箱资源分析

2024 年捕获高风险邮箱（临时邮箱）域名数量 9334 个，占总量 4.57%。



从 2024 年不同类型邮箱数量来看，2024 年捕获邮箱 20.41 万个，其中低风险企业邮箱占总量 76.58%，高风险邮箱（临时邮箱）占比 4.57%，今年新增邮箱主要集中在企业邮箱。

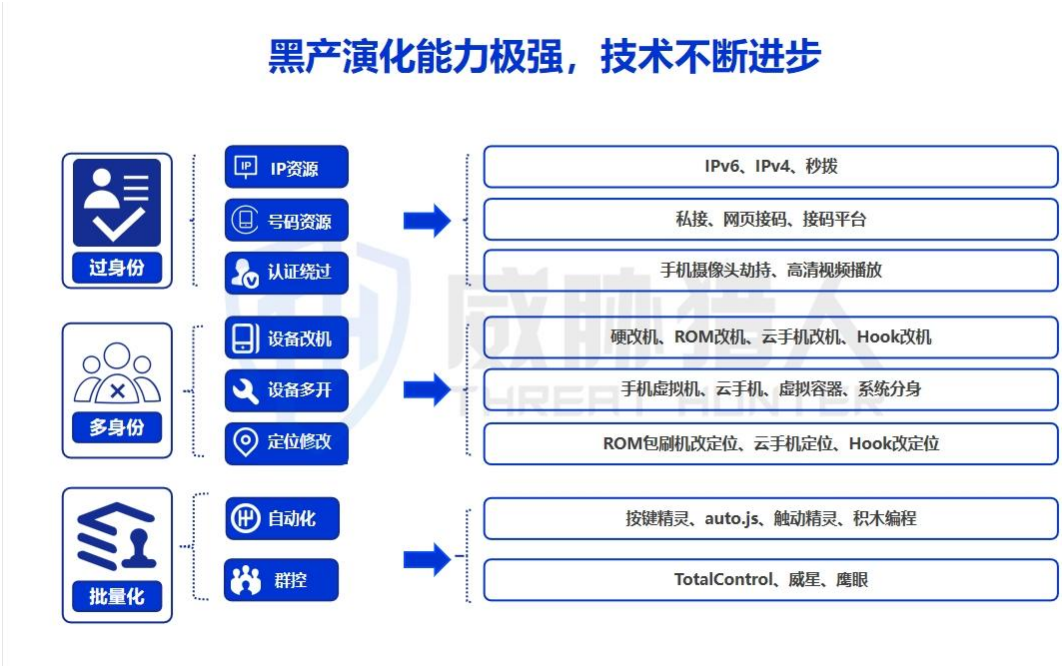


02

2024 年互联网黑灰产通用型攻击技术分析

二、2024 年互联网黑灰产通用型攻击技术分析

威胁猎人研究发现，由于各企业拥有不同的业务环境和风险控制措施，黑产组织针对这些企业所采用的恶意工具、攻击服务也呈现出多样性，但通过深入分析这些工具的底层技术特征，我们可以将攻击服务划分为“过身份”、“多身份”、“批量化”三大模块，其中每个模块涉及到多种底层攻击技术，这些技术是实现各类具体攻击行为的关键所在。



2.1 身份绕过技术演化：黑产利用“子母机”绕过认证，无资质人员也可平台接单

威胁猎人研究发现，2024 年黑灰产利用“子母机”技术，可使两台手机同时登录同一平台账号，利用这一技术，黑产可实现两个人同时共用一个平台账户完成平台相关操作。

“子母机”的应用逻辑是：黑产先用母手机登录账号完成身份认证，在通过代码劫持获取账号的Cookie、设备环境等信息，再将这些信息复制到子设备上，替换其原始文件，并让子设备读取新信息。

目前，出行、外卖等行业已出现此类工具的售卖，可能导致未经培训或资质不符的司机/外卖员违规上岗，不仅影响平台的服务质量，还可能危及平台用户的人身安全，给平台带来更大的损失和名誉受损。

【出行平台“子母机”示例】

以出行行业某 APP 为例：

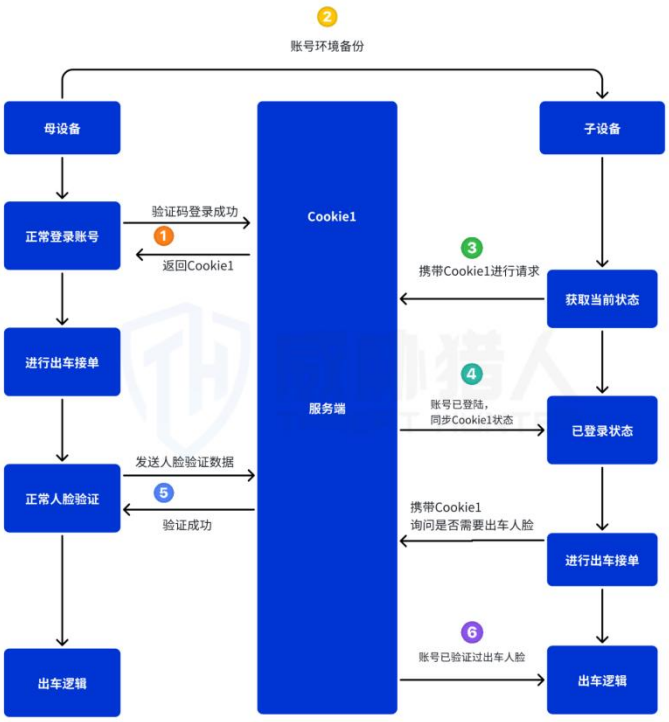
① 首先，在 A 手机上登录并认证完成了 A 师傅的平台账号；

② 然后，通过劫持等方式把 A 手机上的 cookie 和设备环境信息等，复制到 B 手机上；

③ B 手机此时掌握在 B 师傅上，但 B 手机上的信息，是 A 师傅的账号信息；

④ 每次人脸认证时，只需要在 A 手机上进行认证，即可在两台手机上都生效，A、B 师傅都可继续使用账号进行业务操作。

具体流程如下：



2.2 黑产利用“NFC”远程传输软件进行境外洗钱，达到转移违法资金的目的

威胁猎人研究发现，2024 年有黑灰产利用“NFC 技术”实现远程洗钱活动。

NFC（近场通信）是一种短距离无线通信技术，有效距离通常在 10cm 以内，广泛应用于移动支付（如 Apple Pay、Google Pay）、门禁卡、数据交换等领域。

所谓 NFC 远程传输，指的是先通过 NFC 技术读取设备信息，再借由网络远程传输这些信息。例如，设备 A 读取 IC 卡信息后，通过特定应用将信息发送至服务器或设备 B，设备 B 即可模拟该 IC 卡使用。

黑灰产正是利用这一技术，实现 IC 卡信息的远程读取与复原。即使手机设备 B 与 IC 卡物理上分离，也能执行如 POS 机支付等操作。

最典型的攻击案例便是洗钱：黑产将国内信用卡信息远程传输至国外设备，利用这些信息进行 POS 机消费，购买奢侈品、珠宝等，从而绕过信用卡交易的地理限制，完成洗钱行为。

以威胁猎人发现的某款传输 APP 为例：

① 该软件介绍“不受时间及国界限制，无论何时何地都能完成交易”、“可实体，可虚拟，支持所有钱包”：

② 国内（传卡方）、国外（接收方）两部手机都下载这个软件；

③ 使用国内的手机，去碰实体银行卡，此时会将银行卡的信息传到了国内的手机上；

④ 国内手机接收到到银行卡信息后，会通过手机上安装的软件把银行卡信息传输到国外的手机上；

⑤ 国外手机通过软件接收到银行卡信息后，即可正常刷卡使用。

图 A：国内手机(传卡方)去碰银行卡

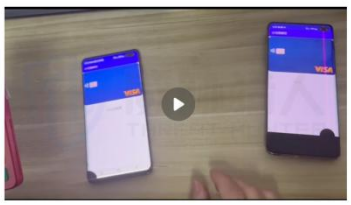


图 B：国内/国外手机都收到了银行卡信息

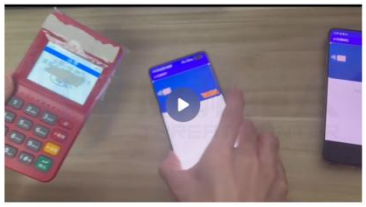


图 C：国外手机进行支付了操作

具体流程如下：

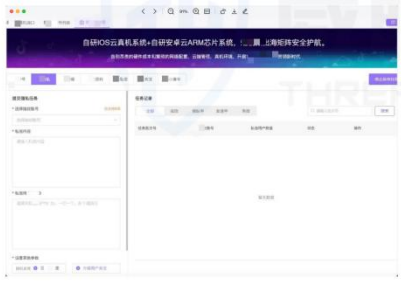
2.3 定制化云手机系统，进一步提升黑产攻击效率

威胁猎人在 2023 年发布的《互联网黑灰产研究年度报告》中指出，云手机平台的配套服务日益丰富，黑产技术呈现出集成化、服务化的特点。2024 年，我们继续跟踪观察发现，云手机平台不仅集成化、服务化趋势愈发明显，定制化趋势也愈发成熟。

服务化主要提供完善的基础攻击工具，让用户基于这些工具实施攻击。而定制化则是云手机平台针对特定 app 进行风控绕过、开发对应的作恶脚本，并集成到云手机系统中，供用户直接使用。

以某社交 app 为例：

黑产为其定制开发的云手机系统涵盖了注册、养号、引流变现等完整攻击流程的自动化实现。这不仅降低了攻击者的准入门槛，使新手也能进行傻瓜式操作，还让攻击者无需关注风控层面的对抗，从而极大提升了攻击效率。



03

2024 年互联网黑灰产攻击场景分析

三、2024 年互联网黑灰产攻击场景分析

3.1 线上业务欺诈场景

本报告中的线上业务欺诈场景不局限于传统营销活动欺诈攻击，只要是所有干扰业务正常运营，从正常的业务开展中牟利的恶意行为，都被称之为“业务欺诈攻击”，如营销欺诈、恶意引流、刷量欺诈、认证绕过等。

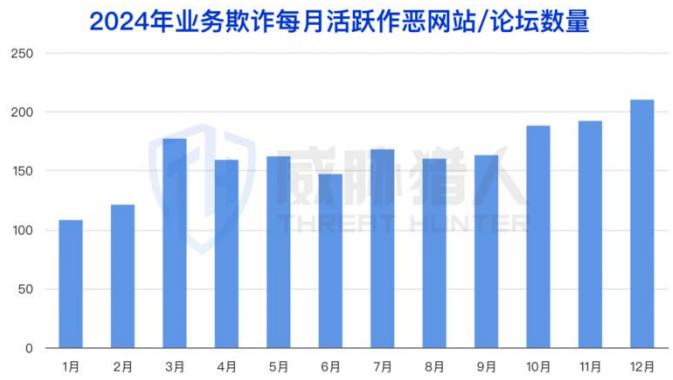
3.1.1 2024 年线上业务欺诈风险热度不减，相关攻击情报量近 3 亿

2024 年，威胁猎人共捕获业务欺诈攻击相关情报 2.72 亿条，监测业务欺诈作恶群组 12 万个，涉及作恶账号 223 万个。

2024 年 12 月业务欺诈相关情报出现暴涨现象，威胁猎人情报人员进一步分析发现，12 月增长量中超过一半源自匿名群聊上的情报信息，这一现象主要是因为一些大型赌博黑产团伙线上赌博活动频繁，以及跑分洗钱团伙通过多账号进行广告“招商”和暴力引流所导致。

2024 年，威胁猎人捕获业务欺诈活跃作恶群组数月均 3.2 万：

2024 年，威胁猎人捕获业务欺诈活跃作恶网站/论坛（暗网除外）月均 163 个，全年作恶帖子总量 926 万例：



2024 年，威胁猎人捕获业务欺诈活跃作恶账号数月均 32 万：

3.1.2 2024 年预警业务欺诈事件达 4158 起，涉及全行业、全业务

威胁猎人风险情报平台为客户提供风险情报挖掘和事件预警服务，支持将黑灰产原始线索深入分析并结构化为有效的攻击事件。在 2024 年，该平台已为合作客户预警了 4158 起明确的攻击事件，平均每月约 346 起。

通过对这些攻击事件进一步分析，我们发现业务欺诈攻击已经渗透到多个行业、多个业务。也就是说，线上业务欺诈针对不同行业、不同业务环节呈现“无差别攻击”，任何有利可图的地方都是黑灰产的攻击目标。

通过对攻击事件进行热词提取，我们发现当前业务欺诈攻击不局限于过去专攻注册登录、领券抢单等业务，内容发布、商品管理、订单交易、支付交易、售后支付、企业数据传输等各个环节均可能被黑产攻击获利。

3.1.3 业务欺诈已进入深水区，真人作弊愈发定制化、角色边界更加模糊

随着业务风控能力的不断提升，大多数典型的机器作弊行为已被有效识别。尽管一些高端黑产仍在使用定制化技术进行对抗，但越来越多的黑灰产开始转向真人众包作弊方式进行攻击。

从威胁猎人捕获到的情报信息来看，2024 年，真人作弊行为变得更加定制化，角色多样化，且界限模糊。主要体现在以下几方面：

（1）传统的任务型众包平台，即以“发布任务”和“领取任务”为主的模式，无论是平台数量还是任务数量，都在持续增长。

2024 年以来，威胁猎人共捕获到 889 万个众包任务，月均超过 63 万个，高峰时期甚至达到 100 万个。

（2）**黑灰产采取了更加隐蔽的众包组织形式，如通过众包私域群聊、开发专项 APP 来招募真人执行特定任务，这种模式类似于刷单真人群，很难被风控系统识别。**这些专项任务可能包括变相刷单、浏览酒店页面以增加浏览量、或使用真人账号挂机爬取平台商品数据等。

案例 1：以“酒店截图”众包项目为例，黑产开发了一款名为“指尖 xx”的 APP，通过该 APP 组织兼职人员完成酒店截图任务。

参与者按照 APP 提供的教程，针对指定的入住平台、日期、地区和酒店名称，截取酒店页面的价格信息并上传。APP 会自动通过 OCR 技术识别并提取价格信息，参与者随后可以领取相应的佣金。

案例 2：黑灰产以兼职名义创建群组，组织、招募真人使用其账号对指定电商平台商品链接进行访问，按要求获取商品对应件数、对应活动条件的到手价格上传表格。这就是一种“真人爬虫”行为。

序号	商品ID	商品链接	最大购买件数	1件到手价	2件到手价	3件到手价	备注	是否百亿补贴	1件到手价截图	姓名
12501	1006418	https://item 0703.ht	2	89.1	178.2			否		朱
12502	1009976	https://item 9272.ht	1	158				否		朱
12503	1008938	https://item 1043.ht	2	139	278			否		朱
12504	1000144	https://item 17.html	3	84	168	214.2		否		朱
12505	1006102	https://item 4008.ht	1	79				否		朱
12506	1003972	https://item 7866.ht	2	89.1	178.2			否		朱
12507	1003650	https://item 0260.ht	1	169				否		朱
12508	1010301	https://item 0917.ht	2	610.8			无货	否		朱
12509	1004096	https://item 1158.ht	1	149				否		朱
12510	1000483	https://item 89.html	1	139				否		朱
12511	1008800	https://item 9279.ht	2				下架且无价	否		朱
12512	1000961	https://item 97.html	2	89	178			否		朱

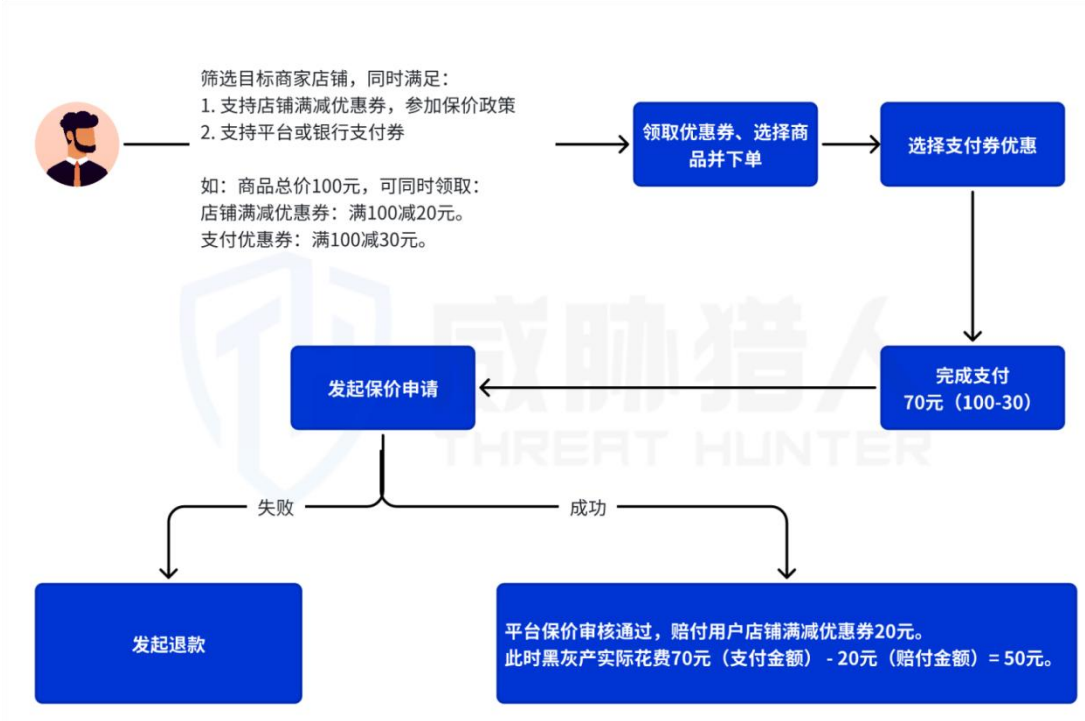
（3）欺诈角色边界逐渐模糊，越来越多的真人用户通过研究和利用平台业务的“正当”规则进行恶意牟利。

近几年，各平台层出不穷的多倍赔付、仅退款教程、价保退款攻略，更多反映了在黑灰产“引导”下，以平台真人用户为主的欺诈趋势。

案例：威胁猎人捕获了一起羊毛用户利用平台保价政策结合支付券识别漏洞，“0 撸”或低价购买平台商品，该类攻击短时间内对平台和开通价保的商家造成了大额的损失和退款。

羊毛党发现某平台某类商品可领取满减优惠券和支付券（合作银行或平台品类），但二者只能选择其一使用；羊毛党通过支付券购买了这款商品，然后利用商家的保价政策规则申请店铺满减优惠券保价金额（商家看不到用户使用了支付券，因为是不同平台），最终达到 0 撸或低价购入。

威胁猎人情报人员针对这类型漏洞攻击进行分析，发现羊毛党主要利用了两个方面的漏洞：首先，他们利用了保价政策中对店铺优惠券的补偿机制，该机制原本是为了在短时间内对用户发放补偿；其次，他们利用了保价政策无法识别已使用支付券优惠的漏洞。这使得黑产分子能够同时“享受”两种优惠券的优惠。这种行为在短时间内对平台和开通价保的商家造成了大额的损失和退款。



3.1.4 黑产交易市场更加活跃，月均售卖商品 101 万，涉及会员权益、教程工具、代下类服务

黑灰产业链能够持续不断地高效运作离不开上游资源交易和下游套利变现，上游黑产通过特定渠道采购账号、工具、手机号等攻击资源，下游黑产通过各种渠道（发卡网站和二手闲置交易平台等），将持有的上游攻击资源以及攻击所得的优惠券、现金券、会员权益、实体商品等进行变现。

自 2024 年 7 月正式上线黑灰产交易市场以来，累积捕获到黑灰产交易商品 610 万起，月均 101 万，大量活跃交易商品和丰富品类表明黑灰产攻击活动仍处上升期、持续运转。商品交易市场的流动，实则破坏了平台用户和玩家的平等权益，缩减、损害了业务方的预期收益。

基于 7 月份以来捕获的黑灰产交易商品数据，交易热度 TOP 的商品类别分别为：会员权益类、教程工具类和代下单服务类型，分别占交易商品总量的 22.16%、17.63%和 13.94%。

各商品大类下存在多个细分丰富商品，如会员权益类包含合作平台联合权益的会员转卖、等级 vip 权益；优惠券类包含平台红包、优惠券、折扣券转卖；教程工具类则是包含了一体机、绕过人脸验证、改定位、抢购、抢单等自动化、批量化作弊工具、搬砖项目教程等；代下单服务类型包含了收取使用费，使用业务方折扣账号、会员权益、补贴名额进行代下单和抢单等；代理服务类型与代注册、资质绕过相关，其中有大量商品触及违规。

教程工具类商品：网约车子母机，受众为资质未通过审核、欲多账号接单扩大收益的作弊司机群体。

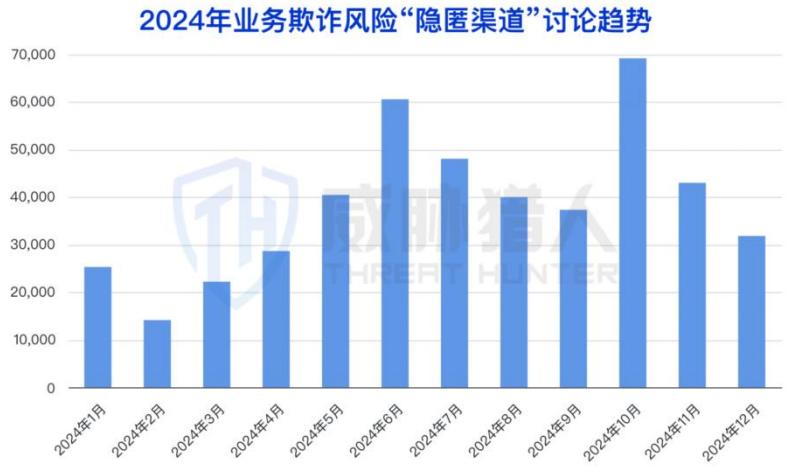
代理服务商品：违规绕过服务，如利用信息差和内部渠道等手段，为申请资质不合规的商家店铺、司机等，直接入驻平台运营。

代下单服务商品：各类低价卡券代下和自助下单商品，通过代下服务和上游搭建的自助对接下单系统，黑产将回收的券出售套利，羊毛党低于原价获取商品。

3.1.5 业务欺诈攻击黑产逐渐向更隐秘的渠道转移，监控难度进一步加大

威胁猎人关注到，相比过去主要在普通社交平台发布，现在更多业务欺诈黑产逐渐转向更隐秘的渠道，如在 Telegram 等匿名群聊渠道上建立大量与业务欺诈相关的讨论频道。

2024 年，威胁猎人监测到围绕业务欺诈风险的讨论量在匿名渠道上达到了 46 万起，且每月呈现增长趋势。



对匿名渠道内中活跃的频道发布信息进一步了解，信息涉及攻击业务方活动的活动脚本、羊毛讨论、恶意赔付教程、抢单工具等相关，下半年比上半年增加 91.43%。

涉及案例包含但不限于打假项目、活动自动薅取、出行行业抢单工具交易频道：

3.2 金融贷款欺诈场景

威胁猎人研究发现，金融贷款欺诈已经形成了一条分工明确、利益瓜分的成熟产业链。以“职业背债”为例，其上游操作方、中间黑产、下游中介以及背债人等角色各司其职，通过严密的协作机制组织骗贷活动。这种黑产的存在不仅破坏了金融市场的正常运行，给金融机构造成巨大的损失，还会对社会的稳定和经济的健康发展构成严重威胁。

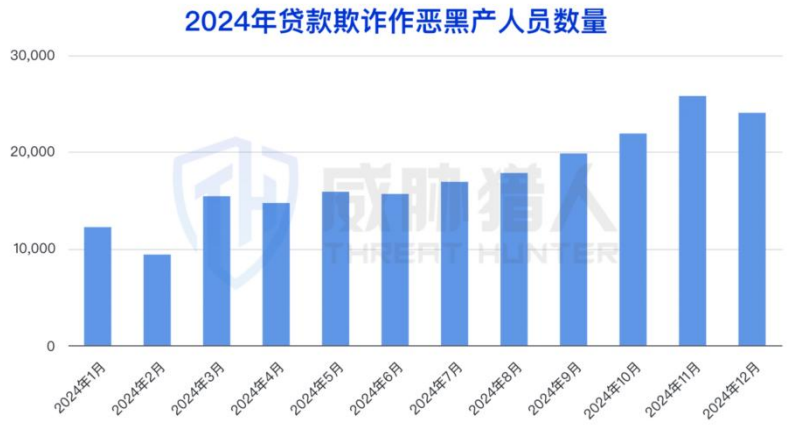
3.2.1 2024 年贷款欺诈风险依旧严峻，欺诈热度持续上涨

2024 年，威胁猎人共捕获贷款欺诈攻击情报 414 万条，监控活跃的作恶社交群组 34697 个，作恶黑产 11.5 万名；不管是欺诈情报热度，还是作恶群组数、作恶黑产数（包括恶意贷款中介），均呈逐渐上升趋势。

（1）2024 年捕获恶意贷款欺诈情报 414 万条，每月持续上涨

（2）2024 年监控活跃的作恶社交群组 34697 个，下半年比上半年增长 30%。

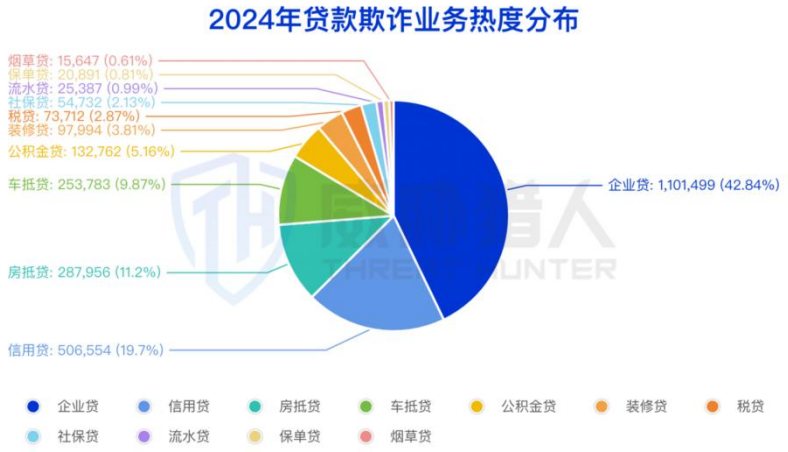
（3）2024 年捕获贷款欺诈作恶黑产 11.5 万名，下半年作恶黑产数比上半年增长 51%。



（4）2024 年贷款欺诈恶意中介 4.3 万名，下半年恶意贷款中介数比上半年增长 50%

3.2.2 2024 年贷款欺诈产品类型热度 TOP3：企业贷、信用贷、房抵贷

从贷款产品类型来看，2024 年信贷欺诈热度 TOP5 的贷款产品类型分别是：**企业贷、信用贷、房抵贷、车抵贷、和公积金贷。**



3.2.3 2024 年贷款欺诈地区热度 TOP3：广东、重庆、山东

从地域分布情况来看，2024 年信贷欺诈地区热度排在 TOP5 的地区是：广东、重庆、山东、浙江、四川。

3.2.4 职业背债：“卖征信换钱”现象加剧，黑产瞄准高信用、高资质客户

随着社会经济大环境的不断变化、金融消费文化的转变，越来越多消费者开始崇尚“卖征信换钱”，“背债”热度持续上涨。

（1）2024 年“背债”热度持续上升，下半年相关情报数量比上半年增长 56%

2024 年，威胁猎人捕获“背债”相关攻击情报呈上升趋势，背债热度上升，并在 9 月达到峰值，下半年比上半年增长 56%。

（2）2024 年背债地区热度 TOP3 省份：广东、四川、重庆

威胁猎人情报数据显示，2024 年“背债”相关的贷款欺诈，活跃热度 TOP3 的省份（含直辖市）是广东、四川、重庆。

（3）2024 年背债地区热度 TOP3 城市：重庆、深圳、长沙

威胁猎人情报数据显示，2024 年“背债”相关的贷款欺诈，活跃热度 TOP3 的城市（含直辖市）是重庆、深圳、长沙。

（4）黑产更倾向于选择征信条件好、资质好、外貌条件好的客户

威胁猎人研究发现，黑产在选择背债人选的时候，逐渐更偏向于选择征信条件好、资质好、外貌条件好的客户。很多金融机构现有的反欺诈模型、评分卡等很难识别这类优质的高风险客户，自动化审批通过的背债人占比也越来越高。

2024 年黑产对背债人属性的选择性变化主要体现为以下情况：

属性	2024年新变化	变化前	变化后
属地性	属地匹配要求高	本地户籍目标客户少，以全国户籍为主。	优先选择本地户籍（当地户籍或省内户籍人员），全国户籍为辅。
年龄	年龄呈现年轻化	以中老年为主，年龄区间在40-60岁，年龄偏大。	以青年、中年为主，年龄区间在25-45岁更受欢迎。
资质	个体资质条件好	三无人员，无资质要求	偏向自带资质条件的客户，最好名下有房或有车或自身为企业主的群体。
形象	注重个体形象气质	对形象外貌无要求，活人即可	外貌、气质与精神形象成为新标准

以下是背债黑产招募的一些广告信息：

房+信。十天左右房子下来。半年出300-500。一个月左右出30+50一年出500-1000客户资质不同,出款额度也不同 年龄25-45,客户形象各方面没问题可以放宽,纯白,小白,近期不能有申请记录,半年不能有单位更新 房子下来可以配非标企业,根据客户合中介选择 ★45岁以上客户额度同比降低。房子时间20天左右★ ★跑分。案底。形象差的不要★	1.湖南籍长沙签房/信贷/企业贷:25-47岁;可只合作签房/也可房信企一条龙,房包一年月供,有返; 2.全国户籍25-46岁纯白做全国资产包,返100万起。25-55岁有房贷或信用卡的做广州信贷20-50万。 3.长沙有房,快贷10-15万/装修贷:20-30万; 4.湖南省内有执照/有流水的,可以做长沙市内商铺/别墅/房子配资融资。	一手别墅,全国,纯白、单签、双签 28-44岁、落地费!可跟单,费用全包! 四川、重庆、贵州房、信、企 年龄25-48岁、省内客户为主, 外地优质客户也可,可单签、 形象好，能说会写 会背! 三包,催单、急单不收	山东房企,山东周边户籍，返佣5-8w,信贷当月出40-60, 企业800-1000,小白,小花(查询半年不超6,总共不超10，不能有单月集中查询，负债10w以内), 年龄25-45,单身或者离异

3.2.5 融车欺诈：车贷欺诈热度持续上涨，“买车套现”日益猖狂

近年来，汽车金融市场持续扩大，汽车贷款欺诈也日益猖狂。威胁猎人调研发现，不法黑产打着“融车”、“0 首付购车”、“买车套现”的旗号，召集一些无法通过正常贷款融资但有资金需求的人群，如征信为白户、花户、黑户等，通过身份包装后进行“假购车、真套现”的合同诈骗、贷款诈骗。

（1）2024 年融车相关攻击情报呈上升趋势，下半年融车风险舆情比上半年增长 62%。

（2）2024 年融车欺诈情报热度 TOP3 城市：深圳、重庆、保定

（3）融车欺诈手法和表现方式

威胁猎人研究发现，黑产通过召集一些自身无贷款资质但有资金需求的人群，在黑产链的组织、垫资、包装及客户配合下，一人可以办理多笔车贷、一辆汽车也可以办理多家金融机构贷款。

欺诈手法	表现方式	具体表现
材料包装	身份包装	**分为虚假包装和真实包装** **虚假包装：**填写虚假的工作单位、虚假的社保公积金、个税APP包装工作身份等。 **真实包装：**真实购房、真实过户企业、真实缴纳社保公积金、定时转账到客户工资卡上作为工资等。
	收入流水包装	公积金、个税、银行、支付宝等虚假APP银行流水、收入流水。
	车险、发票包装	通过虚开发票，操作超贷；购买高价车车险，贷款购买高价车，实则购买低价车套现。
贷款方式	一人多贷、一车多贷	一人办理多辆汽车贷款、同一辆车在多家金融机构申请贷款。
借名贷款	顶名车、代购车	黑产通过忽悠或诈骗客户有偿购车贷款。如顶名车、顶大车、买车包活等。

汽车贷款欺诈更多详情可查看：【黑产大数据】汽车贷款欺诈产业链解构

3.2.6 非标贷款：材料包装借贷欺诈盛行

威胁猎人研究发现，有些人因资质不符、缺乏条件等问题无法正常申请贷款，会通过虚假工作信息、虚假流水等“假数据”来达到借贷目的。

（1）2024 年材料包装欺诈热度呈上升趋势，下半年热度比上半年增加 148%

（2）材料包装欺诈类型和方式

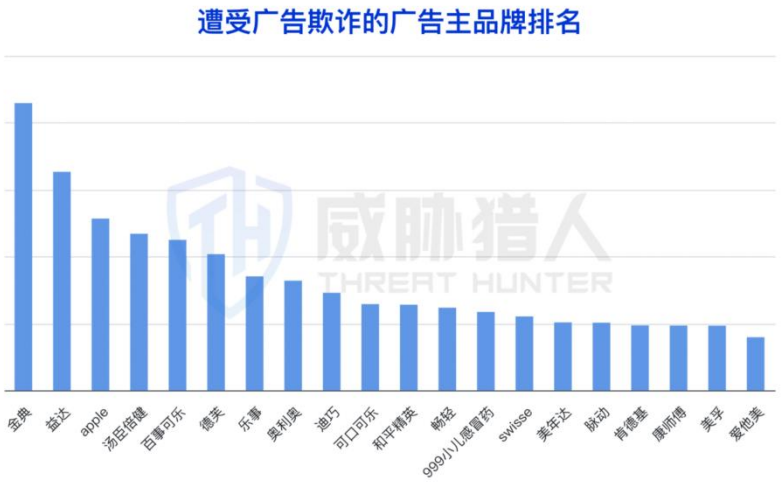
包装类型	包装方式	适用范围
公积金包装	虚假公积金APP	在消费贷、工薪贷等个人信贷贷款场景中，一些黑产利用虚假公积金APP打造虚假公积金数据、虚构劳动关系真实补缴公积金等方式给一些有资金需求又想赚快钱但本身无贷款资质的人群操作个人信贷骗贷业务。 通过黑产的一系列包装，帮助客户通过线上、线下申请多笔个人大额信贷产品，
	公积金补缴	
流水包装	纸质版/PDF版流水	虚假流水可能被黑产使用于任何需要核验个人、企业收入水平来评估还款能力的贷款产品中。如房贷、车贷、企业贷等涉及面签或线上补资质材料环节为黑产重点攻击场景。 黑产通过提供定制虚假的个人、企业流水资料，为贷款客户通过贷款审批及获取更高的贷款额度。
	山寨APP流水	
	银行官方APP虚假流水	

3.3 品牌广告欺诈场景

3.3.1 遭受欺诈的品牌广告主中，食品饮料类成为遭受广告欺诈占比最大的广告主

威胁猎人基于广告暗刷流量监测捕获到大量广告欺诈数据，涉及到多个行业，涉及到食品饮料、电子消费品等多个行业，食品饮料行业依旧是遭受欺诈占比最大的广告主。

遭到广告欺诈的广告主品牌排名如下：



3.3.2 从欺诈广告形式来看，100%播完欺诈广告占比达到 70.02%

从捕获数据中的欺诈广告形式来看，欺诈广告中以 15 秒的视频广告为主，这类广告占捕获欺诈广告总量的 99%以上。

从欺诈广告的播放情况来看，设备暗刷伪造并上报的广告中，大部分都是完整播放完毕的，100%播完的占比达到 70.02%，这一数据明显不符合正常用户的行为，现实情况下有耐心将广告看完的用户并不多。

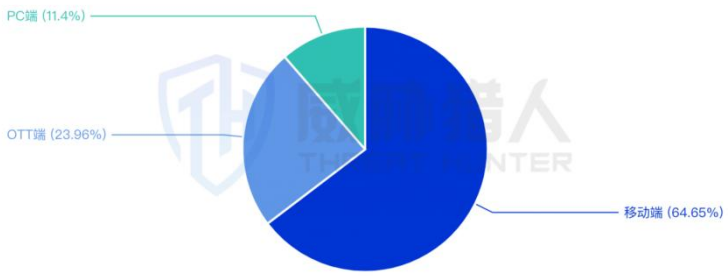
视频广告包括开始播放、播放中、完成播放等阶段，不同阶段都会进行广告追踪，并将流量上报至广告监测平台，实际上这些广告并未播放，仅仅是通过设备暗刷伪造了虚假的广告播放情况，并将虚假追踪情况上报。

3.3.3 品牌广告伪造的终端以移动端为主

在广告欺诈刷量的作弊链路中，上报的作弊广告流量往往会包含动态变化的伪造设备参数信息，模拟真实的设备信息及其展现广告的数据情况，以欺骗广告主。

威胁猎人针对伪造的广告播放数据进行分析发现，伪造并上报的虚假广告数据里，覆盖了三大类终端：移动端、OTT 端、PC 端。

广告伪造的终端情况分布



进一步分析发现，广告伪造的移动端中包含了手机及平板，其中以手机为主，覆盖多个手机品牌。

广告伪造设备信息的手机品牌分布

广告伪造的 OTT 终端中，包含了智能电视、电视盒子、智慧屏、智能音箱（带屏）、唱歌机、投影仪等，覆盖多个 OTT 终端品牌。

广告伪造设备信息的智能终端品牌分布

3.4 API 攻击场景

数字化与线上化趋势下，API 接口作为应用连接、数据传输的重要通道，近年来大规模增长。API 应用的增速与其安全发展的不平衡，使其成为恶意攻击的首选目标，围绕 API 安全的攻防较量愈演愈烈。

威胁猎人情报数据显示，2024 年遭受攻击的 API 数量超过了 250 万，涉及音视频、软件应用、汽车、电商、政务等多个行业。

3.4.1 2024 年平均每月遭受攻击的 API 数量超 21 万

威胁猎人情报数据显示，2024 年全年平均每月遭受攻击的 API 数量超过 21 万。

3.4.2 2024 年 API 攻击行业分布主要分布在音视频、政务机构、互联网软件应用

从 2024 年 API 攻击的行业分布数据来看，音视频行业受攻击热度最高。黑产利用音视频平台有安全缺陷的 API 非法爬取内容、用户信息等数据，通过贩卖音视频内容或用户信息获取高额利益，如非法分发、转售、侵犯版权，以及利用用户信息进行钓鱼攻击、诈骗等。

3.4.3 2024 年值得关注典型 API 攻击典型事件

（1）营销欺诈：某互联网平台登录 API 存在安全隐患，企业营销产品被薅羊毛

2024 年 9 月，威胁猎人风险情报平台监测到攻击者对国内某互联网平台发起批量登陆攻击，使用历史版本的登录 API 接口获取用户凭证，再访问“当前版本应用”利用积分免费兑换商品业务，给企业带来损失。

从威胁猎人蜜罐捕获的攻击流量发现，从 2024 年 9 月至 11 月，攻击者使用代理 IP，对该历史版本的登录 API 发起攻击超 13 万次，超 10W 左右的账号使用积分兑换商品。

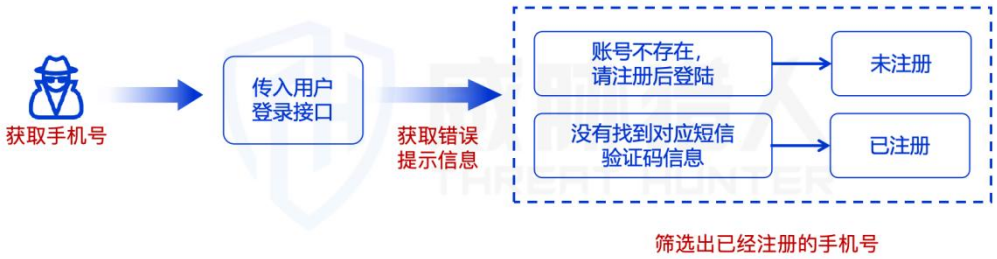
如下图所示，该登录 API 接口中账号密码参数并未进行加密，均为明文传输，且缺失简单的人机验证方式，导致成为了黑产发起批量登录攻击的主要对象。

（2）数据爬取：某银行线上业务遭受黑灰产扫号攻击，大量用户信息被泄露

2024 年 6 月，威胁猎人风险情报平台监测到攻击者对国内某银行发起扫号攻击。经过流量分析与复现，发现该银行资产接口存在“错误提示不合理漏洞”，黑产可大量验证手机号信息是否为平台注册用户，导致有效账号暴露，用户隐私泄露，威胁系统安全。

从威胁猎人蜜罐捕获的攻击流量发现，在 2024 年 6 月，攻击者在一周内，对该银行资产接口发起攻击超 24 万次，导致大量有效账号暴露。

如下图所示，黑产对请求体进行构造，使用不同的手机号，而其他鉴权参数信息特征保持不变，如验证码 id、操作记录变量等，如果手机号码为无效账号，回显“账号不存在，请注册后登陆”，如果手机号码为有效账号，平台回显“没有找到对应短信验证码信息”，黑产可通过回显来判断手机号是否为有效账号。



（3）黄牛抢号：医院线上挂号业务被黄牛抢号，医疗资源被抢占

2024 年 10 月，威胁猎人风险情报平台监测到攻击者对某大型医院进行批量注册，注册后访问医生挂号信息并进行抢号，抢占医疗资源。

通过对威胁猎人蜜罐捕获的流量进行分析，发现攻击者使用大量的黑卡进行批量注册，并伪装为正常病人，后续使用注册的账号进行登录，登录后开始不断访问医生挂号信息并进行预约抢号。如下图所示，由于挂号接口没有限制访问频率，攻击者可以不断的获取医生挂号信息并在第一时间进行抢号。

3.5 钓鱼仿冒场景

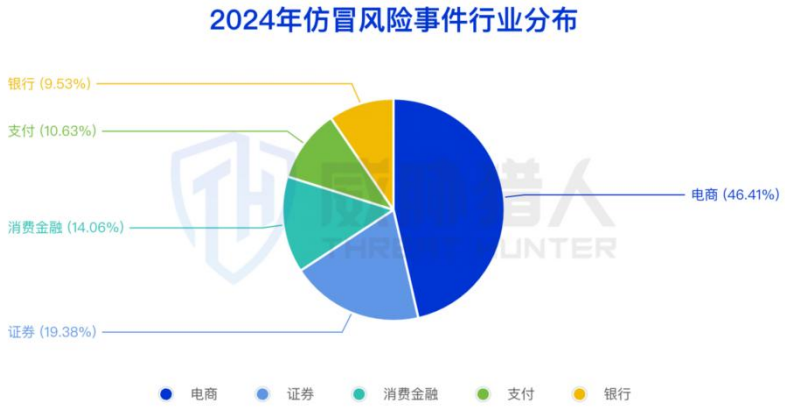
3.5.1 2024 年全年年监测钓鱼仿冒风险事件超 4 万，波及数百家企业

2024 年，威胁猎人共监测到钓鱼仿冒风险事件 44640 例，涉及 671 家企业，较 2023 年监测总量增长 150%，整体呈现持续增长趋势。

相较去年，威胁猎人今年进一步加强对仿冒社媒的监控力度，新增了多个主流平台，从渠道多样性、监测深度和覆盖面等角度全面提升监控能力，为企业提供更广泛的风险防护支持。

3.5.2 电商平台沦为钓鱼仿冒重灾区，事件量占比 46.41%

从 2024 年钓鱼仿冒事件的行业分布数据来看，钓鱼仿冒行业占比 TOP3 的行业为电商、证券行业和消费金融行业，其中电商行业成为钓鱼仿冒最为严重的行业，电商行业仿冒相关的风险案例占总量的 46.41%。



3.5.3 “海外商城盘”诈骗频发，“仿冒电商平台”是主要推手

随着跨境贸易的火热，海外电商平台为吸引新手卖家推出低门槛政策，导致大量缺乏经验的卖家涌入，成为骗子的目标。

“海外商城盘”就是其中一种以“开网店创业”为幌子的骗局，诈骗者冒用知名海外电商平台身份，以“零成本开店”和“高收益分销”吸引受害者注册仿冒电商平台进行诈骗，这种行为不仅给商家带来直接经济损失，还严重损害电商平台品牌资产；破坏了平台的商家准入机制，影响品牌公信力。

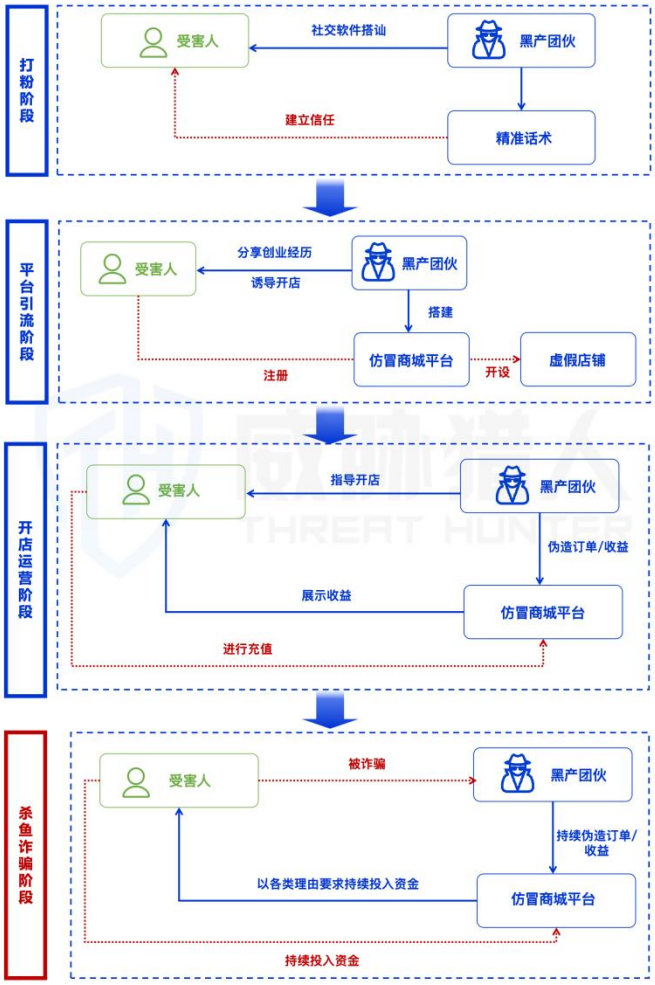
“海外商城盘”主要流程及角色分工如下：

打粉获客阶段：骗子通过交友软件等途径接触目标人群，与受害者建立信任。

仿冒平台引流阶段：骗子通过分享网店创业经验、用“零成本开店”和“高收益分销”为诱饵，让受害者注册仿冒电商平台。

诱导开店运营阶段：在受害者注册后，诈骗者引导开设店铺并通过虚拟订单和伪造盈利截图，营造生意兴隆的假象，诱导受害者不断充值垫资发货，逐步加大资金投入。

杀鱼诈骗阶段：当受害者投入大量资金后，诈骗者以延迟物流、冻结账户等为借口，进一步要求缴纳违约金或保证金，直到受害者资金被完全掏空。整个骗局伪装成合法创业，利用受害者对快速赚钱的渴望逐步完成诈骗闭环。



3.6 数据泄露场景

3.6.1 2024 年监测数据泄露事件 37575 起，涉及金融、电商、快递等行业 2598 家企业

威胁猎人数据泄露风险监测平台数据显示，2024 年 1 月至 12 月全网监测了 3.03 亿条关于数据泄露的情报，基于威胁猎人真实性验证引擎以及 DRRC 专业人工分析验证出有效的数据泄露事件共计 37575 起，涉及金融、电商、快递等行业 2598 家企业。

3.6.2 银行业数据泄露风险连续两年排行第一，本地生活首次进入前十

从行业分布来看，2024 年 1 月至 12 月数据泄露事件中涉及 88 个行业，前五行业分别是银行、电商、消费金融、保险以及快递。其中银行行业数据泄露事件数量高达 6333 起，连续两年为数据泄露事件数最多的行业。

此外，今年本地生活行业数据泄露事件行业排名相比 2023 年有所上升，从之前的 Top14 上升至 Top10。数据显示，2024 年本地生活行业共发现 700 多起数据泄露事件，较 2023 年大幅上涨 7.22 倍。

进一步分析发现，本地生活数据泄露大幅上涨的原因是新型泄露类型“强登”导致。

强登：指通过技术手段强制登录用户账号，获取用户账号中的隐私信息。

本地生活：主要指提供外卖、餐饮、电影票、买菜等与生活息息相关的服务平台。

3.6.3 新型数据泄露类型“强登”出现，涉及电商、外卖、快递等行业头部平台

威胁猎人在 2024 年发现了一种新的查档类型——“强登”，泄露信息主要涉及用户的网购订单、外卖配送订单、出行打车订单、快递订单信息等，涵盖了电商、快递、本地生活服务（主要是外卖行业）和出行服务等多个行业的头部平台。

自 2024 年 6 月起，通过“强登”获取数据的方式开始出现，到 12 月底已累计超过 6600 起。最初主要集中在电商头部平台，随后逐渐蔓延至外卖和快递等多个平台。

强登：指黑灰产通过多种复杂手法强行登录用户的平台账号，获取账号下的具体订单等敏感信息，再把这些信息提供给下游数据购买者，在中游数据售卖时售卖广告会标注【强登】。

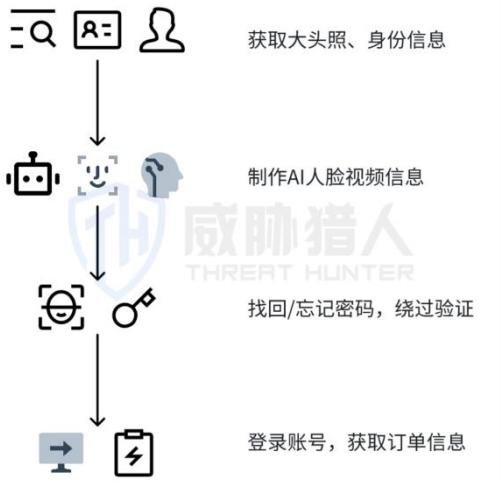
那么，“强登”数据是怎么来的呢?

威胁猎人情报人员对“强登”进一步挖掘和分析，发现上游团伙针对“强登”的主要作案手法如下:

信息获取: 首先，攻击者通过手机号在其他渠道（如查档或社工库等）获取用户的身份证号和证件照等信息。

绕过验证: 接着，利用获取到的证件照生成 AI 视频或模拟人脸，以此绕过平台的视频验证环节。

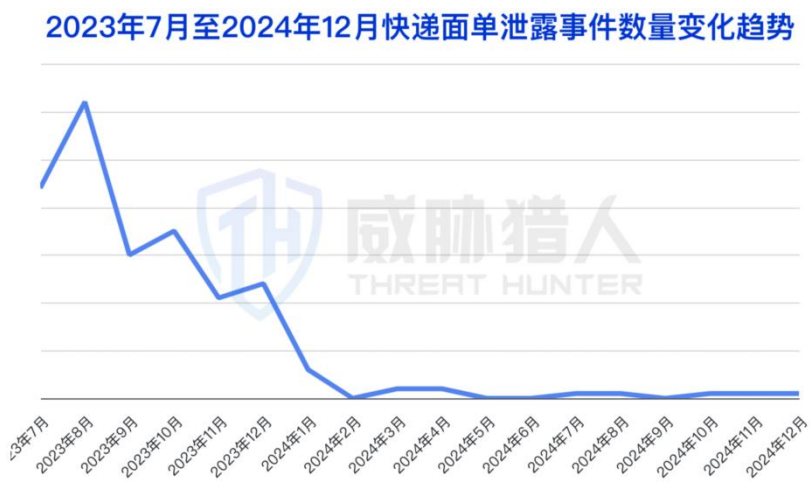
强行登录: 最后，通过平台的忘记密码或找回密码等接口，绕过平台的校验机制，强行登录用户的账号，从而获取账号中的订单内容等敏感信息。



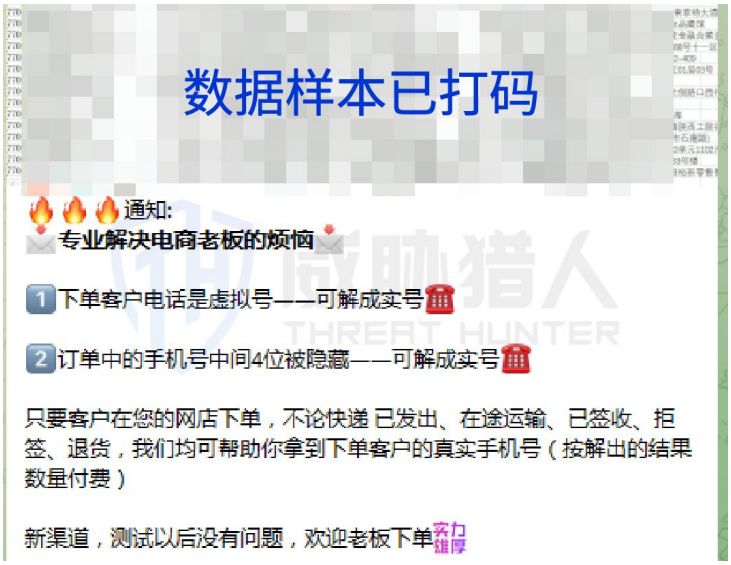
上游团伙通过“强登”方式获取到电商、外卖、快递、出行服务等行业订单信息后，再由中游团伙在各种匿名群聊、社交媒体等发布售卖广告，吸引更多下游需求人群。

3.6.4 物流行业“解密”服务兴起，近一年相关数据泄露事件逐渐增多

近年来，“隐私面单”技术不断发展，通过隐藏用户真实手机号来保护个人信息安全。过去一年，在物流行业监管加强和企业的共同努力下，隐私面单的推广有效减少了快递面单泄露事件，整体治理效果明显（见下图）。但道高一尺魔高一丈，2024 年黑产推出了新的查档服务——“解密”来破解隐私面单，最近一年，“解密”相关数据泄露事件逐渐增多。



订单解密主要是通过“快递单号+虚拟号码（或前三后四打码的手机号）”进行解密，获取完整手机号。



3.6.5 “IOS”字段相关风险事件下半年共发现 496 起，较上半年下降 59.90%

威胁猎人研究发现，从 2023 年下半年开始至 2024 年第一季度，泄露的数据字段中，“IOS”字段增多。从数贩卖黑产团伙与下游数据购买者的聊天记录来看，下游数据购买者对于数据的复购

要求中多次提及“IOS”设备数据的筛选要求。

0		订单号	姓名	身份证号	手机号	出生日期	年份	性别	保障到期	投保日期	公司分部	设备信息
9	某险创建订单	34	34 石	211	195	10/27/81	1981	女	2/2/24	2/3/23 0	省分公司	iOS
9	某险创建订单	90	60 潘	232	360	9/25/71	1971	女	4/25/24	4/26/23 (	江省分公	iOS
9	某险创建订单	11	32 胡	230	458	5/3/71	1971	女	7/25/24	7/26/23 (	江省分公	iOS
9	某险创建订单	65	66 农	210	097	8/20/80	1980	女	4/24/24	4/25/23 (	省分公司	iOS
9	某险创建订单	60	41 王	220	008	7/5/75	1975	女	10/4/24	10/5/23 (	省分公司	iOS
9	某险创建订单	81	14 邢	210	332	9/24/70	1970	女	4/16/24	4/17/2	省分公司	iOS
9	某险创建订单	25	35 朱	239	543	10/25/79	1979	女	2/21/24	2/22/2	江省分公	iOS
9	某险创建订单	12	05 王	230	578	10/3/67	1967	女	7/14/24	7/15/2	江省分公	iOS
9	某险创建订单	84	35 吕	220	707	7/26/75	1975	女	8/25/24	8/26/2	省分公司	iOS
9	某险创建订单	77	04 顾	210	135	2/16/73	1973	女	1/6/24	1/7/23	省分公司	iOS
9	某险创建订单	55	74 单	211	210	6/25/69	1969	女	7/5/24	7/6/23	省分公司	iOS
9	某险创建订单	31	17 杨	211	083	5/14/70	1970	女	12/11/24	12/12/	省分公司	iOS
9	某险创建订单	92	21 牛	210	235	11/14/73	1973	女	4/14/24	4/15/2	省分公司	iOS
9	某险创建订单	97	39 李	232	398	7/19/73	1973	女	6/12/24	6/13/23 (	省分公	iOS
9	某险创建订单	96	11 曲	220	511	8/16/79	1979	女	3/12/24	3/13/23 (	分公司	iOS
9	某险创建订单	80	28 姚	230	583	3/11/78	1978	女	7/1/24	7/2/23 0	省分公	iOS
9	某险创建订单	49	84 杜	230	334	10/1/69	1969	女	12/26/24	12/27/23	省分公	iOS
9	某险创建订单	84	44 李	220	111	2/1/76	1976	女	11/4/24	11/5/23 (	省分公司长	iOS

但从 4 月份开始，“IOS”字段相关的风险事件呈下降趋势，2024 年下半年相比上半年下降了 59.90%

威胁猎人情报人员针对下半年下降现象进一步分析原因，下半年“IOS”相关数据下降主要是因为苹果官方针对 Facetime 诈骗出台相关打击措施导致的。

2024 年 3 月，苹果官方升级 iOS 系统至 iOS17.4.1 版，推出对陌生 Facetime 号码来电拒接的功能，并在 5 月推送 IOS 17.5 版本，增强了 Facetime 通话功能。威胁猎人情报人员测试后确认，该功能已实现对陌生来电的拒接。

（黑产在匿名群聊中发布苹果官方关于 Facetime 陌生号码拒绝来电的通知）

3.7 电信网络诈骗场景

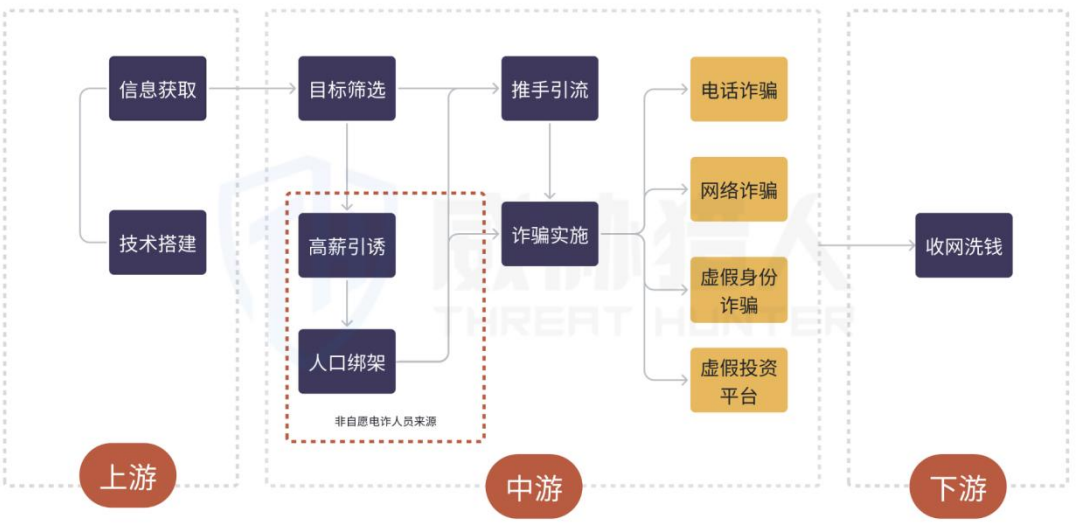
3.7.1 2024 年诈骗形势依旧严峻，活跃作恶群组超 10000 个

2024 年，威胁猎人风险情报平台共监测到电信网络诈骗相关情报 77 万条，活跃作恶社交群组 10032 个。

3.7.2 电诈团伙紧密协作，依托精密剧本布局多样诈骗陷阱

（1）电诈团伙的高效运作离不开团伙内部紧密分工合作

电信网络诈骗已形成了成熟的产业链条，电诈团伙内部有不同的角色和分工，成员之间紧密配合，共同开展诈骗活动：



信息获取：诈骗团伙通过各种非法渠道获取到各种人员资料，资料越详细，诈骗成功率越高。

技术搭建：诈骗团队伪造仿冒网站、开发仿冒软件、伪造交易记录等，用于后续诈骗使用。

目标筛选：筛选容易受骗的目标客群，如老年人、投资者、求职者等，并制定相应的诈骗策略（剧本）。

推手引流：“推手”指那些为诈骗活动提供帮助或支持的人员或团体，虽然不直接参与诈骗行为，但通过与受害者联系，将受害者引流至微信、QQ 等社交渠道供其他诈骗人员进行诈骗，即“推手引流”。

高薪引诱：发布高薪职位，承诺丰厚的报酬或表示能赚到巨额资金，诱使受害人对职位产生兴趣。

人口绑架：将受害人诱骗至目的地，并绑至电诈园区，强迫受害人从事诈骗工作。

（2）形形色色的骗局均离不开黑产进行设计的“剧本”

近期闹得沸沸扬扬的“王星事件”前期就是诈骗团伙在微信群发布名为颜十六选角导演的试戏通知，利用泰国著名娱乐公司的名义向王星发出试戏邀请，精心设计了一个为王星“量体裁衣”的诈骗剧本（可见前期诈骗团伙对王星的信息，特别是职业及工作经历掌握非常细致），以泰国拍戏的工作机会为诱饵，诱使王星前往泰国。

除了“王星事件”外，威胁猎人还监控到多种类型的剧本，分别利用不同人群的特定心理活动，精心制作匹配人物特性和心理的诈骗剧本，具体案例如下：

	人群画像	剧本	诈骗手法	利用心理	话术
案例1	45岁到65岁的老年人群体	完成任务可领取高额扶贫款	诱导受害者安装虚假的扶贫基金手机应用，以“登记“的方式获取到受害人的银行卡/身份证等信息，并诱导客户在该app里进行充值，或以包装流水的名义诱导受害者协助洗钱。	对社会福利、扶贫政策的不熟悉以及防范意识的薄弱	同志！您好，我是.大业.扶贫基金会的，给您通知一下，这边有您的扶贫.名额，可以领取您的扶贫金。大业扶贫基金领取的全程是不收费的，名额有限，请您尽快添加领取。1、这是政府下发的补助金，如果你不领取的话，那这边就认为你不需要补助了，以后国家政策也不会有您的名单了；2、扶贫办由国家资办，由北京推出发往各个小组，领取全程是不收取任何费用的，请您放心。
案例2	需要演唱会门票的人群	有大麦内部溢价票出售	诱导受害者在电诈团伙开发的虚假内部链接进行下单购票，骗取资金	利用了粉丝迫切求票的心理，以及对官方或内部渠道的信任感	要演唱会门票吗？溢价能接受吗？直接在大麦平台下单，我给你内部链接。这是大麦的内部溢价票，录入的还是你的信息，溢价是一起算进去的，跟你在大麦买票是一样的。
案例3	24到30岁的男性群体	人设是已婚少妇，喜欢情趣用品，约对方开房寻求刺激	诱导受害者开房并在电诈团伙开发的虚拟商城购买情趣用品，骗取资金	利用受害人急于与异性约会或寻求刺激的心理，以“同城免费约”等为诱饵	我是来寻找刺激的，我有家庭，前提是互不打扰双方家庭你开个房间，开好了把房间号和位置发给我，我再过去找你为了我们各自的安全，等下我买个测试纸，到时候测试一下看有没有病我不方便付，我老公经常会查我的消费记录，万一被查到了就不好了，要不然我早就付了

写在最后

近年来，互联网黑灰产通过不断提升攻击技术、挖掘隐蔽性更强的攻击资源等确保攻击的成功率，这使得企业在感知和防御上面临更大压力和滞后性。

对企业而言，应该认识到与外部黑产的对抗是动态、持续的，及时依托基于全网多渠道监测的黑灰产情报数据，从黑产攻击准备阶段就开始溯源追踪，知道攻击者正准备利用什么资源或工具，这些资源或工具有什么特征、攻击者会采用什么手段来攻击企业……先于攻击方达到被攻击方的防御前沿，让攻防对抗达到“敌方未攻我先控”的局面。这就是情报的价值所在，也是威胁猎人的价值所在。

说明：本报告所提供的数据信息系威胁猎人依据大样本数据抽样采集、小样本调研、外部情报数据采集、数据模型预测及其他研究方法估算、分析得出，由于统计分析领域中的任何数据来源和技术方法均存在局限性，依据上述方法所估算、分析得出的数据信息仅供参考。

威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

关注“威胁猎人”

公司官网：www.threathunter.cn

合作邮箱：Marketing@threathunter.cn