威胁猎人
THREAT HUNTER

2025
洞见未来
互联网反欺诈年鉴

黑产大数据

2025年中国数据泄露风险态势报告

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。

目录

前言

2025 年数据泄露持续高位运行，黑产在组织形态、攻击路径与数据交易方式上全面升级，高价值金融数据成为核心目标。基于对全年数据泄露事件的持续监测和分析，威胁猎人发布《2025 年数据泄露风险态势报告》，系统分析全年数据泄露趋势、场景变化及非法数据交易链路，综合体现 2025 年国内数据泄露风险态势全貌。

报告内容关键点总结：

1、数据泄露事件持续高位运行，银行行业数据泄露风险连续三年排行第一：

2025 年共监测到有效数据泄露事件 41,644 起，同比上升 10.83%。银行行业数据泄露风险连续三年位居榜首，泄露事件前 5 名的行业中，泛金融板块（银行、消费金融、支付、证券）占据四席，显示黑产攻击重心在于高变现价值的资金流数据。

2、黑产组织走向“联邦化”，资源互用，涉及多起勒索攻击事件：

2025 年黑产呈现明显的组织合体趋势，如 SLH 联盟（由 Scattered Spider、Lapsus$、ShinyHunters 组成）的出现。攻击手段正系统性地从传统漏洞利用转向语音钓鱼（Vishing）驱动的身份滥用以及恶意 OAuth 集成引发的供应链攻击。

3、非法交易市场展现极强韧性，头部论坛覆灭后流量迅速迁移：

尽管全球执法部门在 2025 年多次打击暗网头部论坛 BreachForums (BF)，但黑产流量并未消失，而是迅速向 D**s 等替代平台及匿名群聊迁移。非法数据交易市场具备极强的适应与自我修复能力。

4、高价值金融数据被精细化拆分，算法模型提升变现效率：

黑产交易的数据泄露事件中，金融类数据交易占比超过 50%，其中贷款类信息被高度精细化为“消金申请”、“银行扫码”、“租机料”等多种产品形态。同时黑产开始引入 AI 大数据识别与算法模型对原始数据进行清洗、质控和画像细分，以维持高价格和高转化率。

5、短信数据泄露风险新趋势，106 拓展码成为新型泄露入口。

106 拓展码数据泄露涉及多个行业，影响企业超 420 家，此外，黑产通过人为拼接、统一格式等手段规避企业的溯源取证。

01

2025 年

数据泄露风险概况

一、2025 年数据泄露风险概况

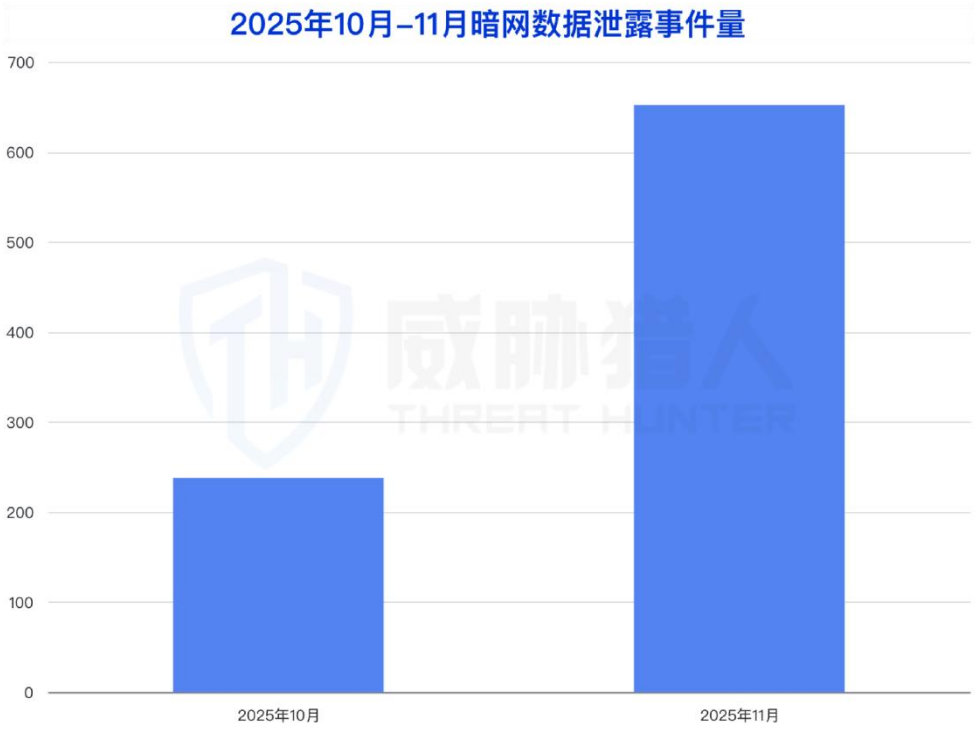
1.1 2025 年全年数据泄露事件共 41644 起，较 2024 年全年环比上升 10.83%

威胁猎人数据泄露风险监测平台数据显示，2025 年 1 月至 12 月全网监测了 7.67 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 41644 起，涉及金融、电商、快递等关键行业共 2120 家企业。

> 本报告中的年度数据未纳入部分海外及无明确企业主体的数据泄露事件，统计口径相较上半年有所收敛，相关指标变化主要由此产生。

如上图所示，2005 年数据泄露事件量级在 Q1、Q2、Q4 均有不同程度的波动，主要原因如下：

- 2025 年 2-3 月：威胁猎人监测到的非法数据交易团伙活跃度提升，团伙数量较 1 月合计上升 116.96%，推动数据泄露事件量上升。
- 2025 年 4 月：威胁猎人监测到数据泄露事件数量出现明显下降，威胁猎人发现，本次波动的主要原因主要源于 Telegram 平台在 2025 年 4 月发起的针对非法团伙的“封群行动”，导致大量非法数据交易群聊被封禁；数据泄露事件量短暂回落。
- 2025 年 11 月：：受电商购物节集中促销影响，头部暗网论坛中出现大量与电商行业相关的泄露数据；11 月暗网渠道相关事件量较 10 月增长 173.95%，成为推升 11 月数据泄露事件数量的重要因素。



1.2 银行行业数据泄露风险连续三年排行第一，软件应用行业首次登上前 10

1.2.1 金融行业风险"断层式"领先

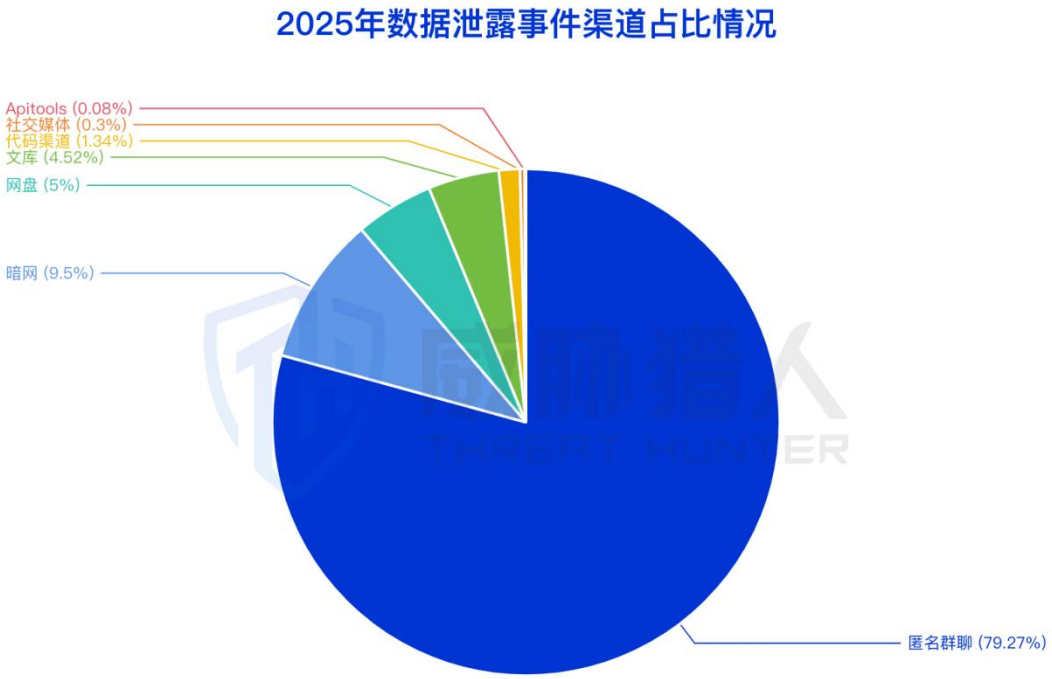
2025 年数据泄露重灾区进一步向资金密集型行业集中。银行业 数据泄露事件稳居榜首，对比 2024 年，消费金融行业则反超电商行业，跃升至第二位。同时，支付与证券行业排名显著前移，分别进入 Top 4 与 Top 5。“泛金融”板块在前五高风险行业中占据四席，表明黑产攻击重心已高度聚焦于具备高变现价值的信贷与资金流相关数据。

1.2.2 本地生活“强登”情报大幅下降，软件应用取代本地生活成为新靶点

据威胁猎人监测，2024 年本地生活行业中较为活跃的“强登”查档类数据泄露事件，在 2025 年出现明显回落，相关事件量同比下降 61.38%；上游非法数据获取方的攻击重点开始发生转移，更加聚焦于具备动态价值的移动端用户行为数据，如应用内交互行为、位置及轨迹信息等。

1.3 数据泄露的渠道概况

根据威胁猎人 2025 年监测平台数据统计，匿名群聊与暗网仍是数据泄露的主要渠道，两者合计占比高达 88.77%。整个非法数据交易市场呈现出高度集中的态势。



ApiTools：是指代 API 工具站/接口文档站/在线调试等平台

02

2025 年

数据泄露风险概况

二、2025 年非法数据交易场景变化趋势

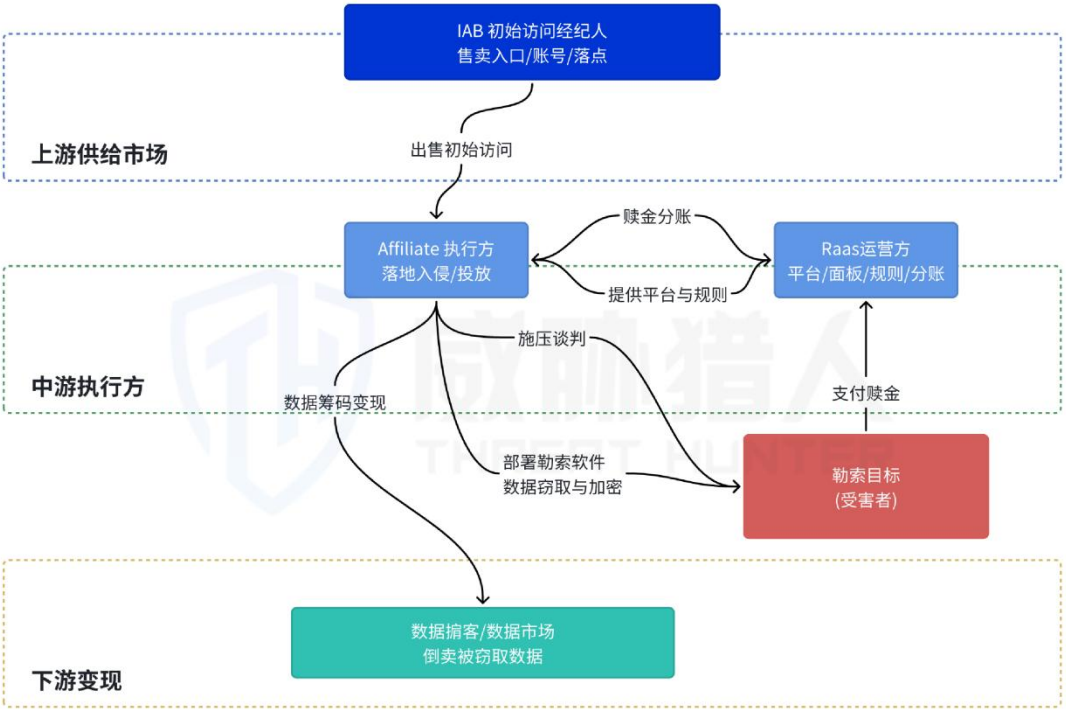
2.1 勒索团伙正走向联邦化趋势

2.1.1 从"各自为战"到"组织合体"：Scattered Lapsu$ Hunters 的出现

过去几年，数据泄露上游链条更多呈现"角色分工、按需协作"的形态：从入侵到数据窃取勒索，不同环节通常由不同团伙或个人完成，交易与协作主要通过暗网论坛与中介撮合完成（IAB、RaaS 运营方、Affiliate、数据掮客各自为战）。

- **IAB（Initial Access Broker，初始访问经纪人）：** IAB 主要负责获取并倒卖进入目标系统或网络环境的初始访问权限；包括账号凭证、VPN / RDP / SSO 会话，以及已落地的内部访问点，为后续攻击活动提供起始入口。
- **RaaS 运营方（Ransomware-as-a-Service operator）：** RaaS 运营方则是以平台化方式提供勒索软件工具、攻击基础设施和分成机制，招募并管理代理（Affiliate）实施入侵、加密和勒索行为，充当攻击能力的组织与调度中枢。
- **Affiliate（Raas 代理/执行方）：** Affiliate 是 RaaS 生态中负责"落地执行"的角色，通常获取或购买初始访问后进入受害者环境，完成渗透扩展、数据窃取/外传与加密投放，并按 RaaS 运营方的规则与其分成收益。
- **数据掮客（Data Broker）：** 数据掮客则是倒卖数据的角色；交易对象包括数据库导出、内部文档、客户或员工信息、邮箱内容及各类访问 Token 等，为诈骗、勒索或转卖变现提供数据基础。

其基本勒索协作运作链路如下：



这一格局在 2025 年出现了明显变化，勒索团伙开始走向联邦化趋势。

2025 年 8 月 8 日，一个名为"Scattered Lapsu$ Hunters – The Com HQ SCATTERED SP1D3R HUNTERS"的 Telegram 频道上线，正式宣告三个知名网络犯罪组织的合作。

该联盟由以下三大团伙合体而成：

- Scattered Spider
- Lapsus$
- ShinyHunters

这是一个以经济利益为动机、以社会工程与身份滥用为核心的网络犯罪团伙，其运作模式为 Federated 联邦模式；被研究界视为网络犯罪进入“联邦化”的重要信号。

联邦式（Federated）网络犯罪模式：指多个相对独立的犯罪团体不必统一指挥，而以共同品牌对外行动；按需共享/复用部分资源（如泄露渠道、社工剧本、基础设施与施压流程），以协作形式扩大影响与变现。

2.1.2 合体后攻击策略的变化

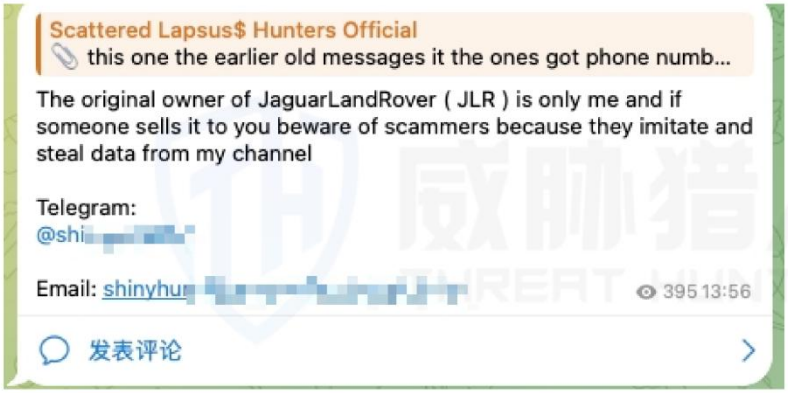
SLH 于 2025 年 8 月初正式合体后，仅 4 个多月时间，已公开宣称攻击超过 300 家企业，窃取了数以亿计的数据资产，涉及多家重量级目标，包括 Salesforce、CrowdStrike、Red Hat 等。

其合体后最显著的变化在于攻击策略的变化：社会工程与供应链攻击，正在系统性取代传统漏洞攻击。

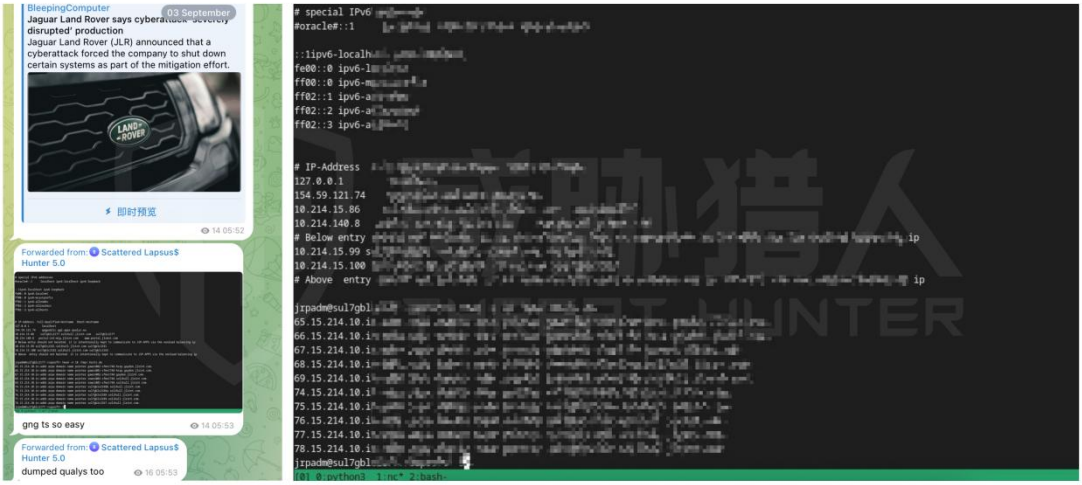
1. 身份与权限滥用：语音钓鱼驱动的高权限账户利用

- **捷豹路虎（JLR）勒索事件（2025 年 8 月–9 月）**

SLH 通过利用语音钓鱼冒充内部员工获取帮助台人员支持（重置或授予权限）的诈骗手段，入侵了高权限管理员帐户，并利用这些帐户访问和部署勒索软件，攻击捷豹业务的各个方面，从 CAD 和工程软件到支付跟踪，再到客户汽车交付。导致 JLR 全球 IT 网络被迫下线、多地工厂停产数周，被媒体称为"英国史上影响最严重的网络攻击之一"。随后 Telegram 上其勒索团伙在频道中嘲讽捷豹路虎在宣布印度塔塔汽车的 IT 安全漏洞后，股价开始出现小幅下跌。随后又公布了更多的数据样例信息以及项目文档。



该事件呈现的是典型的加密勒索模式：通过关闭 IT 系统 → 停摆生产 → 对核心业务形成直接、可量化打击。



2. 授权与信任滥用：语音钓鱼驱动恶意 Oauth 集成供应链攻击

OAuth 是一种“授权机制”，让你在不交出账号密码的情况下，允许第三方应用按约定权限访问你的数据。

Salesforce 和 Salesloft 勒索事件（2025 年 10 月）

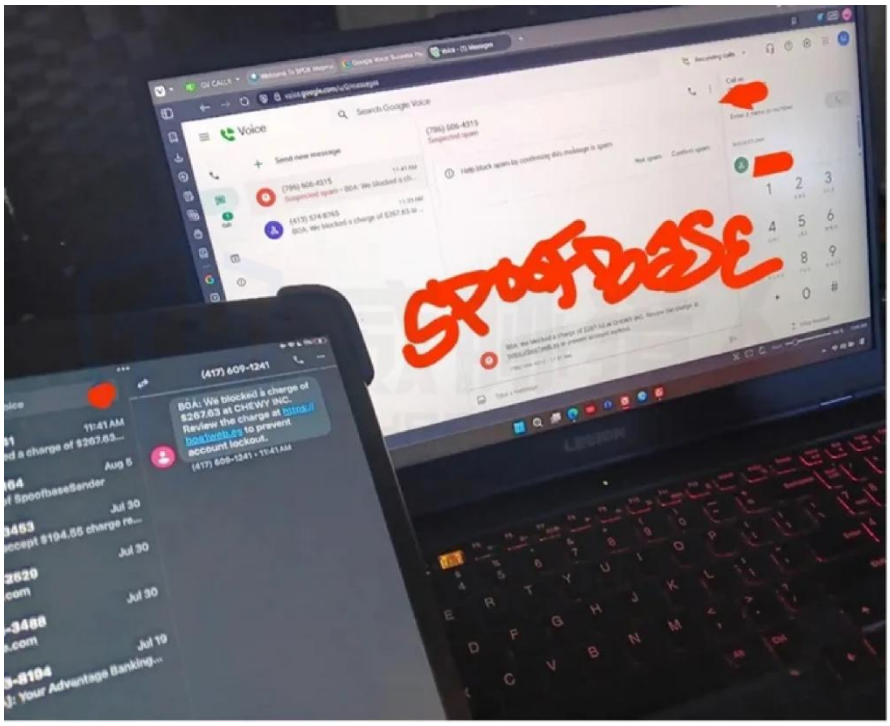
SLH 针对 Salesforce 客户的大规模攻击中，据攻击者称：

- 约 760 个 Salesforce 租户遭入侵
- 15 亿条记录被窃取

此次攻击可分为两类行动方式：

一类是直接针对 Salesforce 客户的语音钓鱼攻击。攻击者通过电话冒充官方支持或运维人员，诱导企业用户将所谓的“数据加载器”应用接入其 Salesforce 租户。该应用表面上是正常的数据管理工具，实则为攻击者控制的恶意 OAuth 应用。一旦用户完成授权，攻击者即可在合法 API 权限范围内，持续、大规模地导出客户数据。

另一类则体现出明显的供应链攻击特征。攻击者首先通过钓鱼手段入侵 Salesloft 一名开发者的 GitHub 账号，进而渗透其 AWS 环境并窃取访问令牌。由于 Salesloft 的官方集成（如 Drift）被广泛部署于 Salesforce 与 Google Workspace 等环境中，攻击者得以利用这些 OAuth 令牌，以“合法集成”的身份访问大量下游客户系统，并同步窃取数据。随后，攻击路径进一步横向扩散至 Gainsight，额外影响数百个 Salesforce 实例。



(图为频道中一位成员分享的屏幕截图，

描绘了一名操作员运行自动语音钓鱼工具，滥用 Google Voice 来扩大社会工程攻击的规模。)

2.2 暗网头部论坛的覆灭与黑产流量的迁移

2025 年，全球执法部门针对头部暗网论坛 BreachForums (BF) 展开了多轮次、多维度的打击。这一系列行动既重创了该平台，亦引发了黑产团伙的大规模迁徙。

2.2.1 针对 BF 论坛的"执法打击"时间线：

- 平台关停（4 月）：2025 年 4 月 15 日，BF 论坛突遭关停。根据威胁猎人监测数据，该平台活跃非法交易团伙数从 4 月约 166 个迅速暴跌，至 5 月归零 。
- 司法判决（9 月）：9 月 16 日，BF 创始人被美国司法部改判为 3 年监禁，从司法层面确立了打击成果。
- 全面查封（10 月）：10 月 9-10 日，美国执法部门联合法国方面正式接管 BF 明网域名，其 Tor 站点也随即离线。
- 运营方声明（10 月中旬）：勒索团伙 ShinyHunters 在 Telegram 发布 PGP 签名消息，承认 BF 后端服务器被扣押且数据库备份被破坏，无奈宣布“论坛时代结束 ，后续出现的新论坛应视为蜜罐” 。

（ShinyHunters 在 Telegram 发布 PGP 签名消息）

2.2.2 BF 论坛的倒下并未导致非法交易消亡，黑产转移至新平台持续作恶

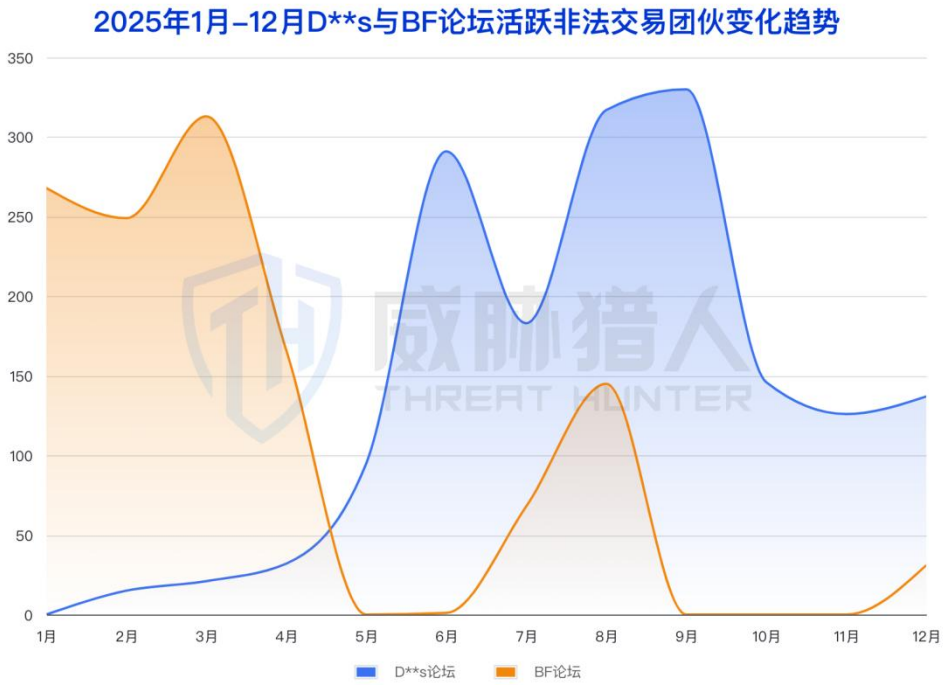
据威胁猎人监测趋势图显示：随着 BF 平台 自 4 月起整体活跃度快速下滑，并于 5 月接近归零，原本集中于 BF 平台 的黑产流量与交易需求并未消失，而是迅速向多个替代暗网论坛迁移。

- 以 D**s 平台为代表，其活跃度自 5 月起出现明显抬升，6 月进入高增长区间，并在 8–9 月达到全年峰值，显示出对黑产流量与交易需求的快速承接能力。尽管 10 月后平台整体活跃度有所回落，但其运行水平仍显著高于年初阶段，表明相关作恶需求已在替代平台中完成沉淀，并逐步形成新的交易“底盘”。

而从 BF 本身的恢复情况来看，威胁猎人针对 BF 非法团伙的持续监测数据显示：

9–11 月期间 BF 长期处于归零状态，未出现有效恢复迹象。直至 11 月 18 日，监测到一个与 BF 高度相似的新域名完成注册。经 GridinSoft 网站信誉解析，该域名被标记为低信任度，并伴随黑名单风险信号。结合 BF 历史上曾多次公开提示“警惕克隆站与蜜罐风险”的情况，威胁猎人判断，该新域名存在较高的钓鱼、诈骗或蜜罐站点风险，不具备稳定交易平台的可信特征。

进入 12 月后，监测到疑似 BF 克隆站的零星活动迹象，进一步反映出部分参与者仍在尝试恢复或复用“BF 平台”作为交易入口。但受"蜜罐/钓鱼"疑虑影响，其用户回流更可能是小规模测试或低频参与观望阶段。



综合 2025 年全年数据，黑灰产市场展现出较强生态韧性：当 BF 等头部平台被持续打击后，用户与交易需求并未消失，而是快速迁移至 D**s 等存量/新兴替代论坛，并与更分散的渠道（如匿名群聊）共同维持运转。

BF 的案例印证了黑灰产市场的核心规律：当主要交易平台被打击时，用户和需求会迅速迁移至现有或新兴替代品。数据交易市场具备极强的适应能力，即使头部平台被摧毁，黑产从业者仍能依托其他渠道维持业务运转。

03

2025 年数据泄露交易市场研究新趋势

三、2025 年数据泄露交易市场研究新趋势

3.1 金融类、定制化采集类以及社媒类数据交易高度活跃，金融类交易数据占比超 50%

在非法数据交易生态中，公群这类群组在黑产链条中充当着"担保方"的角色，作为黑产交易的核心枢纽，这些群组沉淀了海量的交易履约记录，客观反映了地下市场对数据的真实需求与资金流向。

2025 年 1 月至 12 月期间，威胁猎人情报运营团队持续对 Telegram 平台上的数据交易公群进行监测，累计覆盖 1,209 个活跃数据交易群组，共捕获近 3.6 万条数据交易相关情报。监测范围覆盖贷款、网购、股票、物流、电商、社交工具等多个行业。

从成交数据类型及其占比来看，2025 年公群中的数据交易类型主要集中于五大类：金融类数据、定制化采集数据、社媒数据、物流数据以及电商数据。

1. 金融类用户数据凭借其高变现价值，依然是黑灰产市场的"硬通货"。贷款类用户信息的需求最为旺盛，涵盖消金网贷、银行贷款、企业贷及贷款超市等多个细分领域，持续占据市场主导地位。

2. 定制化数据采集：需求端呈现出"由泛转精"的趋势。黑产从业者不再依赖通用的存量库源，而是针对特定目标（如特定公众号、APP 及具体的 URL 路径）发布定制化爬取与清洗需求，以获取更高时效性和精准度的数据。

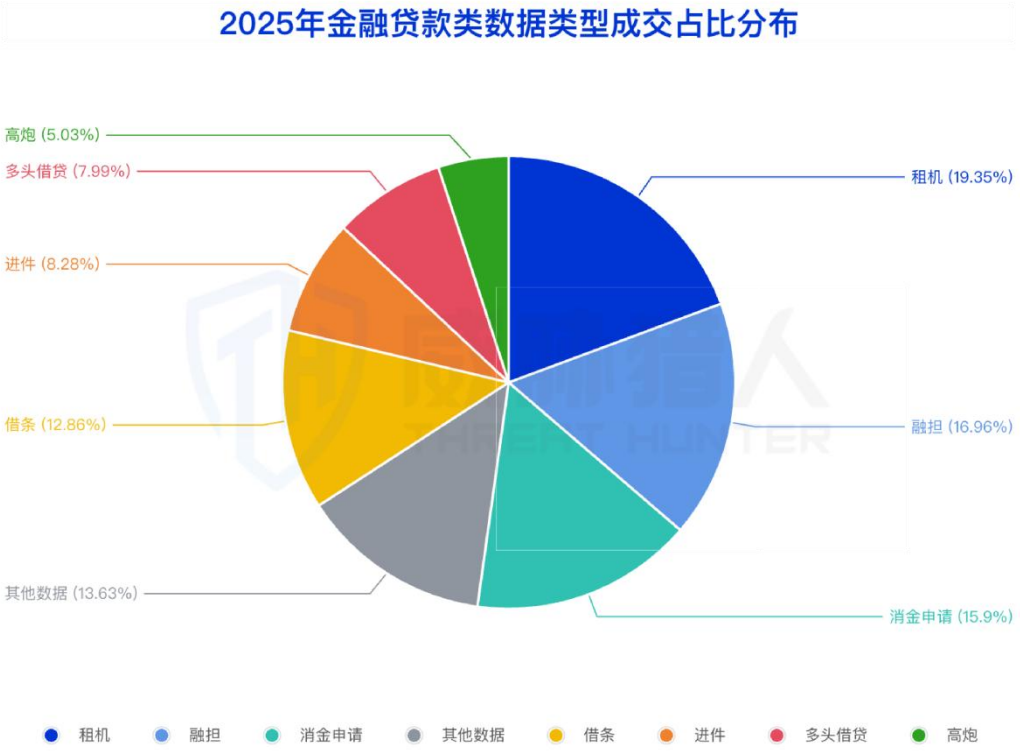
3. 社交/社媒数据：采集目标高度集中于国内主流社交软件及短视频内容生态。其中，直播间实时互动数据与公众号粉丝画像成为重点交易对象，反映出黑产对私域流量与即时转化的高关注度。

4. 物流数据：交易集中于"礼品单"类物流信息以及高净值女性消费群体的精准物流数据。

5. 电商数据：国内的电商数据则主要由"黑五类"敏感商品（减肥、增高、医疗等）受众数据及主流电商平台的购物行为数据构成。

其中，金融类交易数据占比超 50%，结合 2024—2025 年公群数据交易热词图谱分析结果（高频关键词包括“贷款”“公积金”“保险”“租机”等）可以发现，金融贷款类数据已连续两年位居交易需求首位。基于上述监测结果，威胁猎人推测，贷款类相关数据泄露风险仍将是 2026 年金融企业面临的主要安全挑战之一。

进一步从交易结构层面分析可以看到，金融网贷类数据在黑产流通过程中已被高度精细化拆分，形成多种面向不同黑产环节的数据产品形态，如“租机”“融担”“消金申请”“借条”“进件”“多头借贷”等，以适配不同欺诈场景和作业链条的实际需求。



"租机"：指用户在租机平台进行分期租机的行为，涉及用户办理租机贷业务。"租机料"即租机平台办理分期业务的用户信息数据。

"融担"：指的是网贷平台的一个系列，主要为小型或微型网贷 APP，申请流程简单，通过率高。“融担料” 即小型网贷平台的用户信息数据。

"消金申请" ：是指消费金融贷款用户的在贷款页面的申请操作，“消金申请料” 即消费金融贷款申请的用户信息数据。

"借条"：是指高利贷或私人借贷类型，会与借款人签订 “借条” 或电子签，“借条料” 指私人借贷或高利贷所签订 “借条” 的用户信息数据 。

"进件"：一般出现在信贷流程里把资料准备好后提交到贷款公司或银行的系统里面，标志着贷款申请的正式开始。 “进件料” 即信贷流程中用户提交的贷款录入的信息。

"多头借贷"：是指借款人用同一套真实材料同时向多家银行或民间机构申请贷款，以填补资金缺口。此外，在信贷风控领域，“多头借贷” 也指一种专门侦测借款人 “多头借贷” 行为的风控机制，以及借款人多头借款的记录信息数据。

"高炮"：高利贷平台或机构，“高炮料”指在高利贷平台进行贷款的用户信息数据。

3.2 消金贷款用户信息泄露事件持续上涨，新型泄露方式多样化

威胁猎人监测显示，2025 年消费金融行业非法数据交易事件在时间分布上呈现出阶段性上升趋势。

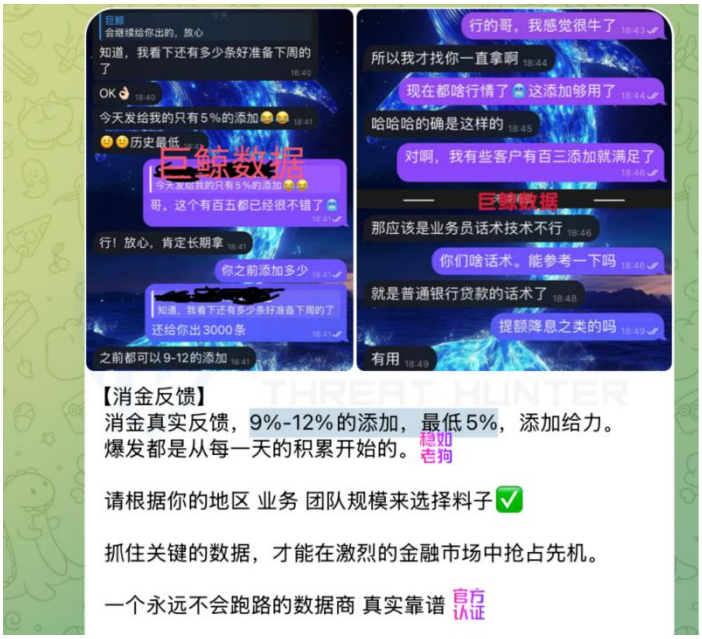
年初至上半年，相关事件数量整体处于较低水平并缓慢增长；进入下半年后，事件量明显抬升，并在 10—11 月 达到全年高点。

威胁猎人运营人员深入分析后发现消费金融非法数据交易事件上涨主要集中在几类新兴数据类型中。

在黑产频道中提及到“热销数据类型”名单中，“消金申请”“银行扫码”“多头贷款”等数据类型频繁出现。尤其是“消金申请”类数据；

以某黑产频道每周更新的热销榜单为例，该类数据产品自 2025 年 8 月至 2025 年 12 月期间持续位列热销 Top，显示其已在非法数据交易市场中形成稳定且活跃的交易需求。同时，从下游作恶场景中的使用反馈也从侧面反映出该类数据在真实性与可用性方面具有较高价值。

（某黑产团伙频道每周更新的数据类型热销榜单中，“消金申请”数据长期高居第一）

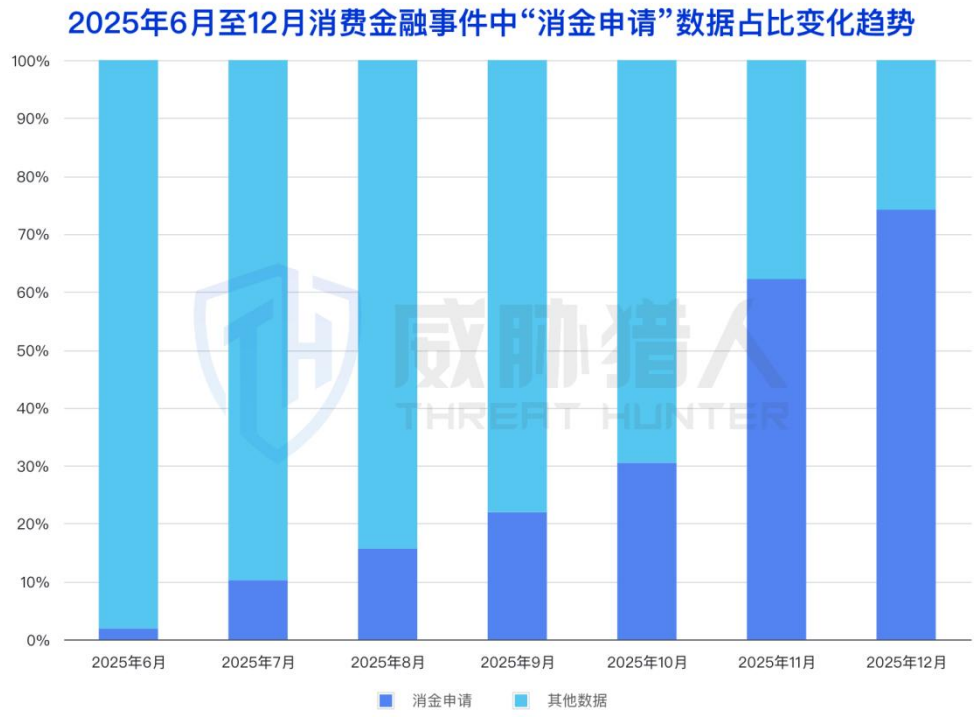


（下游作恶效果反馈，侧面反映了数据的真实性）

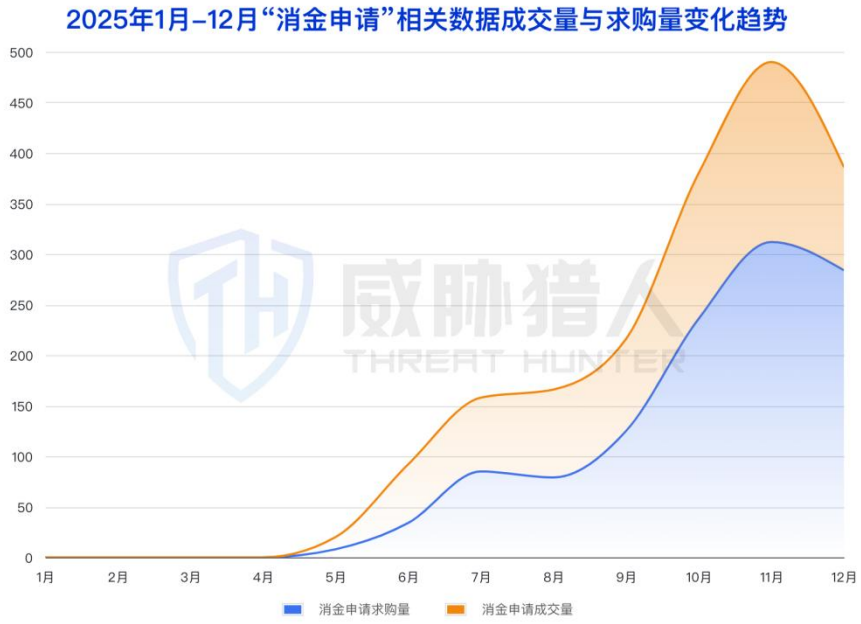
3.2.1 “消金申请”风险趋势与产业生态解析

3.2.1.1 消金申请数据泄露事件持续上涨，12 月事件量超 600 起，占当月贷款类非法数据交易的 70%。

威胁猎人监测发现，“消金申请”类数据最早于 2025 年 5 月底在部分非法数据交易渠道中出现，黑产通过约两个月的试探性流通，并于 2025 年 7 月底进入规模化传播阶段，被多方数据交易中介集中推广，至 2025 年 12 月，达到峰值，占当月贷款类非法数据交易的 70%。



同时从成交与需求变化来看，“消金申请”类数据的成交量与求购量走势高度一致，并在下半年同步呈现爆发式增长。



据威胁猎人观察，泄露的“消金申请”数据，其泄露的数据样例格式字段主要为：

用户手机号、平台名称、姓名、地区以及申请贷款成功的状态信息

其中姓名信息并非样本都具备的信息内容，威胁猎人进一步跟进了解到，部分样本中出现的姓名信息并非来源于原始泄露数据，而是黑产通过数据清洗、拼接或补充加工等方式人为添加，用以提升数据“可用性”与交易价值。

（左图为消金申请数据格式，右图为黑产反馈姓名字段为清洗添加的）

3.2.1.2 “消金申请”产品数据不断迭代，涉及国内绝大多数消金、贷款平台

威胁猎人运营人员针对“消金申请”进行了深入分析发现，该款产品类数据主要分为四个阶段，分别是测试阶段（5 月-6 月）、正式上线（7 月-8 月）、精细化运营（9 月-10 月）、AI 模型提升阶段（11 月），以下是具体的产品发展时间线情况。

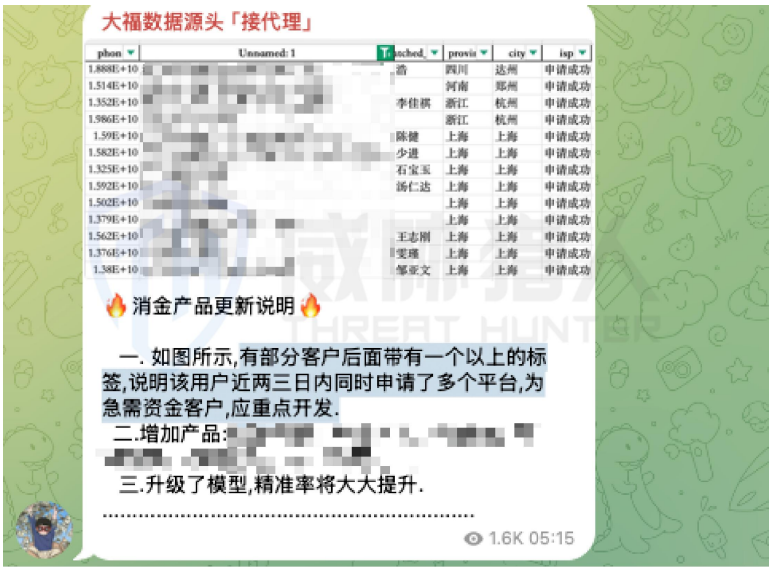
（消金申请产品发展时间线）

- **测试阶段：（5 月底 - 6 月）**

最早于 2025 年 5 月底首次有黑产提出明确的“消金申请”产品，其数据类型涉及部分消金平台以及银行贷款平台，数据时效性为隔夜（T+1），不支持指定平台，但可支持筛选用户所在地区，仅涉及 24 家持牌消金机构以及银行贷款产品。

- **正式上线：（7 月-8 月）**

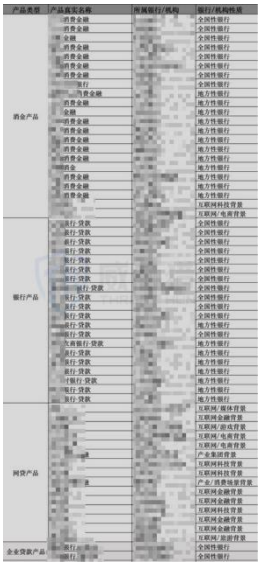
于 7 月初开始新增企业贷类型数据，不再局限于 C 端贷款需求用户，补充了 B 端或小微企业主的信息数据；同时梳理出部分用户在短时间内在多个贷款平台申请的行为特征，标记为急需资金客户，供下游购买者进行精准作恶，涉及消金/贷款平台达 27 家。



（图为黑产正式上线消金产品后，补充了多平台标签特征以及模型优化）

- **精细化运营：（9 月-10 月）**

针对持牌消金机构、银行系贷款、网贷平台、企业贷等不同类型平台进行划分拆解，以便满足下游不同贷款中介（资方）的作恶用户画像需求；同时数据类型共涉及消金/贷款平台达 40 家，支持可筛选具体平台。



（图为黑产精细化整理的平台清单）

- 数据中介黑产利用算法模型对原数据进行清洗，提高数据价值（11 月）

11 月初，非法数据交易黑产中介反馈“消金申请”数据交易量达顶峰，导致服务器内存极限，并针对性进行优化清理；涉及消金贷款、银行产品、网贷产品、企业贷款产品高达 60 家平台。在 11 月底，引入了 AI 大数据识别，从单纯的数据售卖转向“数据清洗+质量控制”，试图通过剔除劣质的用户数据来维持数据的高价格和高转化率。

（黑产不断优化升级消金申请模型）

下游作恶：黑产获取数据后会针对性进行贷后营销作恶

威胁猎人监测发现，黑产在获取“消金申请”类数据后，主要将其用于针对性较强的贷后营销类作恶行为。该类作恶通常围绕“已提交贷款申请”的用户展开，通过冒充官方或合作方身份，实施误导性引流与产品推广。

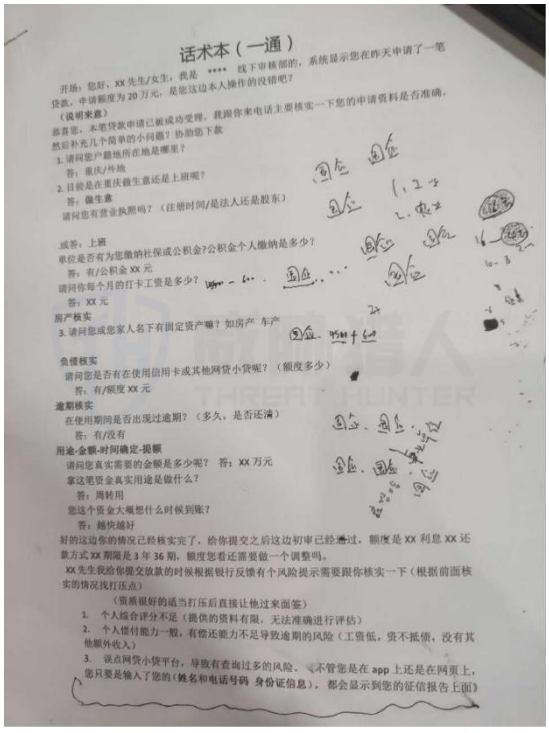
以下是威胁猎人监测到的两个案例：

案例 1：

从威胁猎人监测到某数据交易中介发布的“消金售卖测试话术”来看，该话术主要是伪装成与目标消金平台存在合作关系的客户经理，以电话方式联系已提交贷款申请的用户，声称用户的贷款或相关业务已转由其负责，进而引导用户更换贷款产品或接受其他贷款业务推广。

案例 2:

从威胁猎人从某贷款电销团伙获取到话术本内容来看，该类话术主要通过冒充消金贷款平台线下审核部门（或回访部门）工作人员的身份，与用户进行贷款资质确认等沟通，在取得用户信任后，引导其前往线下门店，推广其他贷款产品。


话术本（一通）

开场：您好，XX 先生/女生，我是 **** 线下审核部的，系统显示您在昨天申请了一笔贷款，申请额度为 20 万元，是您这边本人操作的没错吧？

（说明来意）

恭喜您，本笔贷款申请已被成功受理，我跟你来电话主要核实一下您的申请资料是否准确，然后补充几个简单的小问题？协助您下款

1. 请问您户籍地所在地是哪里？

答：重庆/外地

2. 目前是在重庆做生意还是上班呢？

答：做生意

请问您有营业执照吗？（注册时间/是法人还是股东）

或答：上班

单位是否有为您缴纳社保或公积金？公积金个人缴纳是多少？

答：有/公积金 XX 元

请问你每个月的打卡工资是多少？

答：XX 元

房产核实

3. 请问您或您家人名下有固定资产嘛？如房产 车产

负债核实

请问您是否有在使用信用卡或其他网贷小贷呢？（额度多少）

答：有/额度 XX 元

逾期核实

在使用期间是否出现过逾期？（多久，是否还清）

答：有/没有

用途-金额-时间确定-提额

请问您真实需要的金额是多少呢？ 答：XX 万元

拿这笔资金真实用途是做什么？

答：周转用

您这个资金大概想什么时候到账？

答：越快越好

好的这边你的情况已经核实完了，给你提交之后这边初审已经通过，额度是 XX 利息 XX 还款方式 XX 期限是 3 年 36 期，额度您看还需要做一个调整吗。

XX 先生我给你提交放款的时候根据银行反馈有个风险提示需要跟你核实一下（根据前面核实的情况找打压点）

（资质很好的适当打压后直接让他过来面签）

1. 个人综合评分不足（提供的资料有限，无法准确进行评估）
2. 个人偿付能力一般，有偿还能力不足导致逾期的风险（工资低，资不抵债，没有其他额外收入）
3. 该点网贷小贷平台，导致有查询过多的风险，不管您是在 app 上还是在网页上，您只要是输入了您的（姓名和电话号码 身份证信息），都会显示到您的征信报告上面）

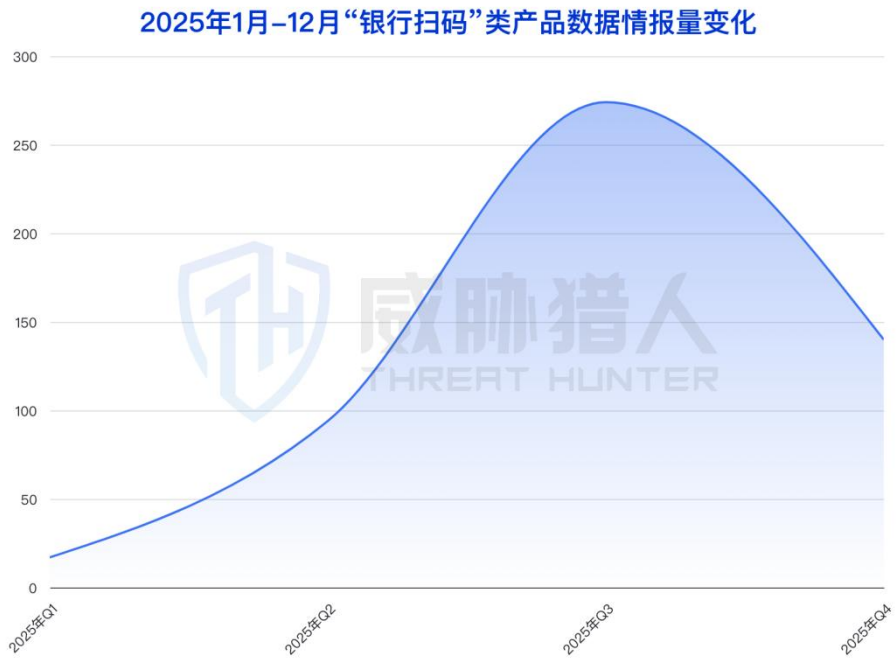
3.3 银行“扫码申请”贷款信息泄露事件持续上涨，第三方金融科技公司营销工具成核心风险点

3.3.1 银行“扫码申请”贷款信息泄露事件持续上涨，至 2025 年 Q3 达到最高峰

2025 年上半年，威胁猎人监测发现，捕获到“银行扫码申请”类型事件的大幅上涨（较比 2024 年下半年增幅 404.55%），并在 2025 年 Q3 引来了该类型事件情报的峰值，共发现 274 起银行“扫码申请”类型数据泄露事件。

进入 2025 年第四季度后，银行“扫码申请”类事件数量出现回落。主要下降原因是受新生热销产品“消金申请”的影响，下游作恶团伙更多转入购买“消金申请”类数据，导致“银行扫码”类事件有所下降。

银行扫码申请：是指用户通过扫描银行客户经理提供的贷款活动二维码，申请办理贷款业务的信息数据。



威胁猎人运营人员深入分析发现，黑产所称的“扫码申请隔夜”数据，其主要集中在银行“贷款”业务上。主要包含贷款用户的手机号、城市地区以及申请贷款审批结果等信息；同时，根据黑产提供的银行贷款平台筛选上来看，涉及共超过 80 家银行贷款业务，基本上以地方性银行或商业银行为主。

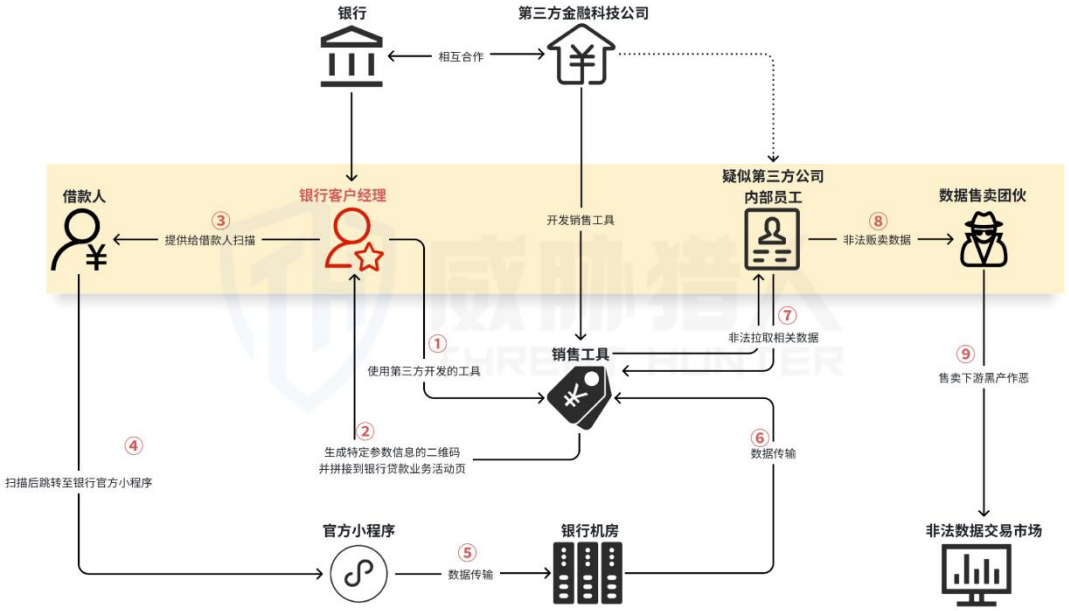
手机号	贷款平台	province	city	姓名
1.815E+10		安徽	合肥	
1.816E+10		安徽	合肥	
1.776E+10		安徽	合肥	
1.776E+10		安徽	合肥	
1.309E+10		安徽	合肥	
1.308E+10		安徽	合肥	
1.586E+10		安徽	合肥	汪
1.788E+10		安徽	合肥	
1.331E+10		安徽	合肥	许
1.396E+10		安徽	合肥	
1.526E+10		安徽	合肥	董
1.866E+10		安徽	合肥	张
1.361E+10		安徽	合肥	王
1.538E+10		安徽	合肥	仇
1.334E+10		安徽	合肥	王
1.387E+10		安徽	合肥	彭
1.596E+10		安徽	合肥	陈
1.591E+10		安徽	合肥	

（左图为泄露的数据格式，右图为黑产正式推出“扫码隔夜申请”数据产品）

3.3.2 第三方金融科技公司营销工具成核心风险点，关联超 80 家银行机构

威胁猎人对泄露数据中涉及的银行二维码进行溯源分析发现，相关线索均指向同一家知名金融科技服务商所开发的“XX 营销助手”平台。进一步结合 2025 年 6 月在非法数据交易渠道中流传的银行贷款平台名单进行交叉验证，可确认本次事件的潜在影响范围超过 80 家银行机构。

*如您想要了解您所在的银行机构是否在名单内，请联系威胁猎人。



（银行贷款申请信息泄露流程图）

相关业务流程操作情况如下：

银行贷款业务通常通过客户经理提供的专属活动二维码办理（该二维码中携带客户经理相关信息），用户扫码后跳转至银行官方小程序，并在对应贷款业务页面完成申请操作。

进一步分析发现，上述由客户经理提供的贷款业务二维码，并非直接由银行系统生成，而是通过第三方金融科技公司开发的营销与销售工具进行制作和分发（由于该工具页面较为敏感，此处不做具体展示）。

威胁猎人针对黑产发布的信息进行跟进以及分析后发现，在此类型事件开始宣传时，黑产声称，数据是来源于“内鬼”，即内部员工泄露的。结合上文中涉及到超过 80 家银行机构，80 家银行机构内部员工泄露的概率极低，初步推断为第三方金融科技公司内部员工。

为验证这一判断，威胁猎人在对该第三方金融科技公司的业务模式进行分析后发现，该公司不仅为银行提供应用系统软件开发服务，同时还配套提供智能风控策略支持。相关风控策略通常基于贷款用户的资质差异进行配置，用于辅助银行客户经理开展客户筛选与后续跟进。在实际运行过程中，当用户在银行官方小程序中提交贷款申请后，相关用户信息会同步至上述销售工具平台，用于客户经理的业绩统计与客户管理。

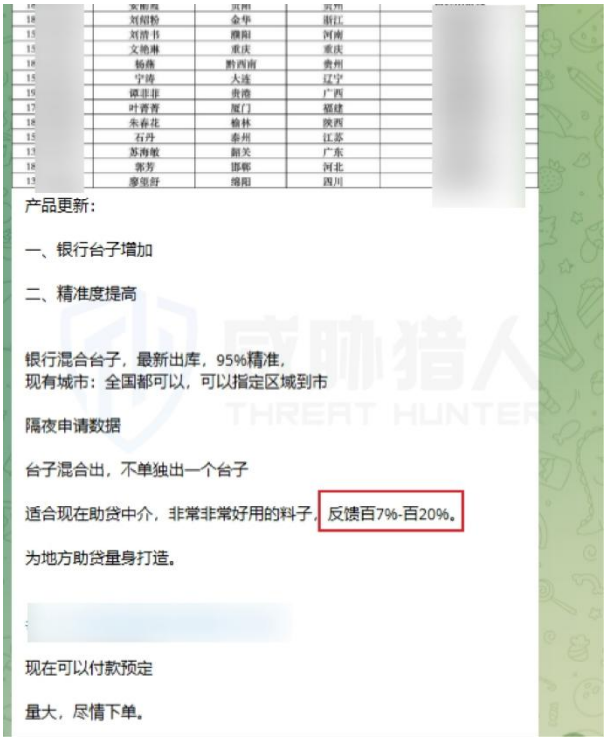
尽管该机制在业务效率层面具备一定合理性，但在数据跨系统同步与多机构复用的背景下，也客观上扩大了用户数据的流转链路与暴露范围，从而增加了数据被滥用或泄露的潜在风险。

隔夜申请平台推荐

平台名称	是否需要公积金	其他材料/备注	推荐级别	每日出量（三网）不固定 预计出量 一线及高配二线	二线	三线及以下
	部分产品需公积金	本地户籍优先	SSS	200左右-300	100-200	40-100
	否	需银行流水或工资证明	SSS	200左右-300	100-200	40-100
	部分产品需公积金	需公积金或个税证明	sss	250-400	200	100
	部分产品需公积金	需社保/工作证明	SSS	150	100	50
	需公积金或社保	限南京地区，需本地社保/公积金	SSS	60-100	60	40
	部分产品需公积金	可能需要社保/公积金辅助证明	SS	200-400	100-250	70-150
	部分产品需公积金	需工作证明或社保记录	SS	150	100	50
	否（部分抵押贷可能需）	可能需抵押或担保	SS	80	50	30
	需公积金或社保	限武汉地区申请	SS	200	150	80-120
	否	需工资流水或纳税证明	SS	150	100	60-100
	需公积金或社保	限温州地区申请	SS	100-200	100	60
	否	需提供收入证明	SS	50	30	20
	否	需营业执照、经营流水	S	500+	400+	400+
	否	部分产品需本地社保	S	150	100	60
	需要	征信上体现公积金信息且缴纳满6个月或历史记录缴纳大于60个月	s	200	150	50
	否	线上授权查询征信	S	300+	200+	150+
	否	纯线上申请，利率较高	S	100	80	50
	否	仅限信用卡分期业务	S	100	80	50
	否	线上授权查询征信	S	80	50	30
	否	需提供工作证明	S	50	30	20
	否	需绑定 银行卡	S	200	150	30
	否	需绑定 账户，利率较高	S	150	80	30
	否		s	400+	400+	300+
	否		s	200+	150+	100+
	否	线上申请，需人脸识别	A	150-200	100-150	100+
	否	需提供银行流水	A	150-200	100	80
	否	需授权查询征信	A	100	80	30
	否（抵押贷可能需）	可能需房产/车辆抵押	A	80	50	20
	否	线上申请，需人脸识别	A	100	70	30

（黑产发布的用户在不同银行贷款平台申请所需材料信息，以及不同平台不同城市地区数据量差异）

同时从黑产侧反馈来看，此类信息数据泄露到非法数据交易市场后，主要用于助贷公司进行精准营销。根据黑产在营销后的效果反馈上来看，效果是非常好，成功率最高可达 20%，也在侧面证明了此类数据的真实性。



3.3.3 数据类型范围持续增加，黑产采用 AI 模型对原始数据进行画像细分

据威胁猎人对该类型非法数据交易类型的持续跟踪发现，进入 2025 年下半年后，该类数据交易呈现出两个显著变化趋势：

一是数据类型覆盖范围持续扩大，二是黑产开始引入算法模型对原始数据进行精细化画像拆解，以提升数据的可用性与变现效率。

1）数据类型范围持续扩大：

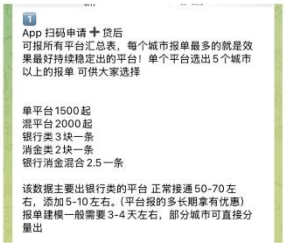
2025 年 7 月新增贷后用户数据，不再局限于原本的扫码申请用户；

2025 年 11 月新增信用卡申请数据，不再局限于普通扫码申请贷款用户；

支持多个大型银行，不再局限于原本的地方性银行或商业银行；

2）用户画像维度持续细化：

引入模型识别优化，对用户画像进行深入分析，可根据下游作恶黑产需求进行定制化筛选；如用户性别、年龄、设备类型、扫码后停留时间等细化标签信息内容。



3.4 短信数据泄露风险新趋势，106 拓展码成为新型泄露入口

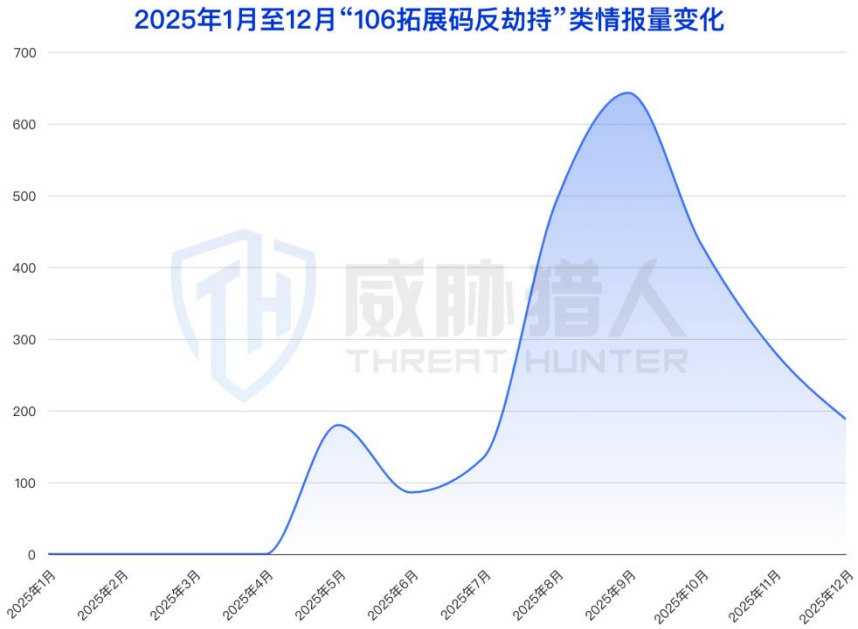
3.4.1 106 拓展码数据泄露涉及多个行业，影响企业超 420 家

近年来，随着短信“logo 认证”的推行，越来越多企业短信在用户手机上会显示品牌名称与标识，极大提升了用户识别度。但亦成为黑产识别特定平台用户的关键锚点。

2025 年 5 月，一种新型用户短信泄露风险开始在黑产圈悄然兴起——“106 拓展码反劫持”。并在今年 9 月达到顶峰，整体风险情报超 2400 条，涉及企业平台超过 420 家，覆盖金融（消金、银行、证券）、电商、出行、生活服务等多个行业。

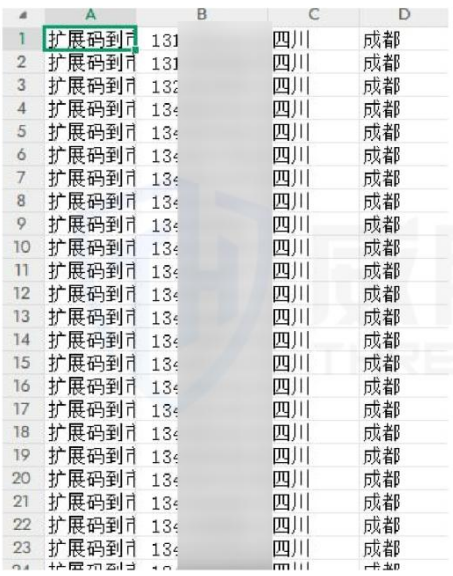
106 拓展码：指的是企业通过通信服务商的短信通道向用户发送通知所使用的号码，一般以 106 开头，其后的拓展数字则代表具体的通道商和服务应用。

106 拓展码反劫持：是威胁猎人发现的一种新型的短信数据窃取手法，黑产从 106 短信号码中提取出拓展码，反向查询收到此类短信的用户信息（如手机号、城市和平台名称），进而打包售卖或用于精准作恶。这类行为滥用了通信服务商的短信合规机制，已构成严重的数据安全风险。



以下是威胁猎人捕获到的数据样例：

*如需确认贵司用户数据是否在名单内，请与威胁猎人联系

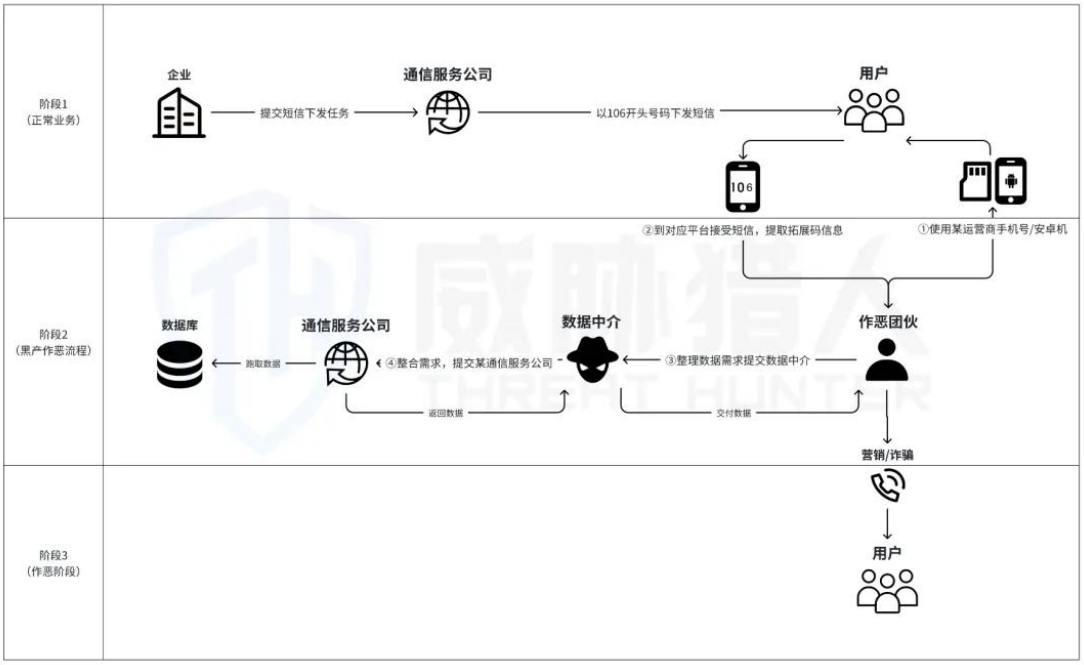


	A	B	C	D
1	扩展码到市	131	四川	成都
2	扩展码到市	131	四川	成都
3	扩展码到市	132	四川	成都
4	扩展码到市	13	四川	成都
5	扩展码到市	13	四川	成都
6	扩展码到市	13	四川	成都
7	扩展码到市	13	四川	成都
8	扩展码到市	13	四川	成都
9	扩展码到市	13	四川	成都
10	扩展码到市	13	四川	成都
11	扩展码到市	13	四川	成都
12	扩展码到市	13	四川	成都
13	扩展码到市	13	四川	成都
14	扩展码到市	13	四川	成都
15	扩展码到市	13	四川	成都
16	扩展码到市	13	四川	成都
17	扩展码到市	13	四川	成都
18	扩展码到市	13	四川	成都
19	扩展码到市	13	四川	成都
20	扩展码到市	13	四川	成都
21	扩展码到市	13	四川	成都
22	扩展码到市	13	四川	成都
23	扩展码到市	13	四川	成都

（左图为泄露的数据格式，右图为黑产正式推出“拓展码”短信数据产品）

黑产交易链条全景：从通信服务公司到黑市

威胁猎人针对泄露数据的手法进行调研分析，还原了“106 拓展码反劫持”的完整黑产交易路径：

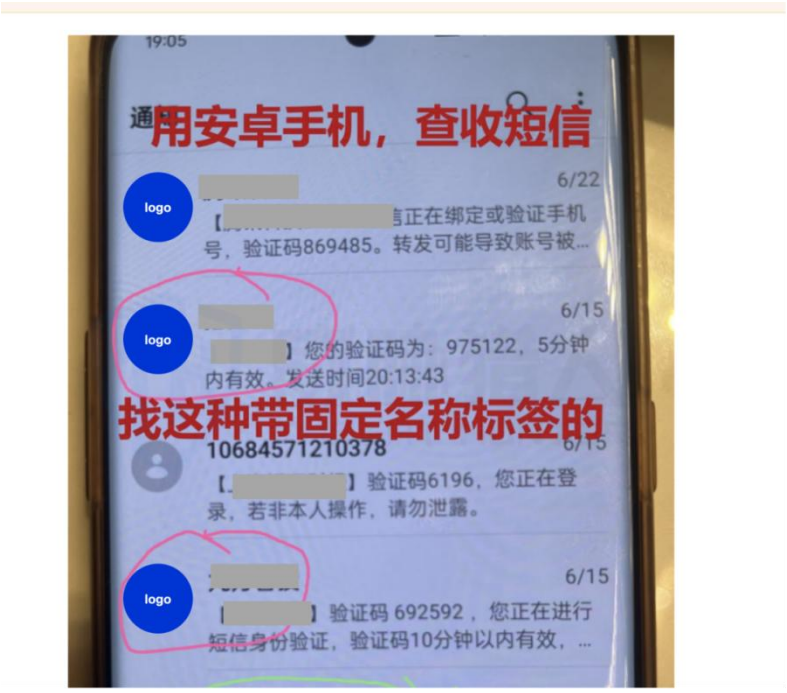


上游资源商：根据下游数据需求生成查询任务，最终提供用户手机号、地区和平台等信息。上游资源商将查询到的数据提供给数据中介，数据中介再交付给下游作恶团伙，整个过程从提单到资源商、到跑数据和交付数据，一般只需要三天。

中游数据中介：整合下游作恶团伙的数据需求，提交给上游资源商；

下游作恶团伙：如助贷团伙，通过特定运营商手机卡注册目标平台账号，获取绑定短信内容及 106 拓展码信息，基于拓展码信息整理数据需求（如省、城市等），然后交付给中游的数据中介；

值得关注的是，下游作恶团伙提取的数据必须是携带短信 logo 认证的 106 拓展码，如未通过短信 logo 认证的 106 拓展码则无法匹配出用户信息。



影响范围：

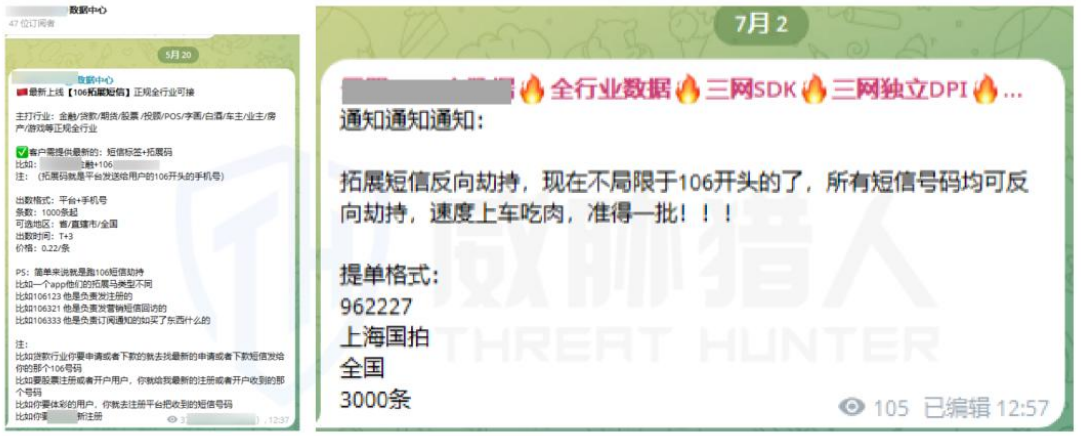
1. 短信类型维度：平台账号注册、验证码、贷款申请、逾期提醒、还款短信、下款短信等多种类型

2. 行业维度：金融（消金、银行、证券）、电商、出行、生活服务等多个行业

3. 城市维度：成都、杭州、重庆、苏州、武汉、西安、南京、长沙、天津、郑州、东莞、无锡、宁波、青岛、合肥、北京、上海、广州、深圳、福州、南宁、济南、福州、佛山、昆明、沈阳、哈尔滨、南昌、南通、贵阳、兰州、太原、长春、日照、宁波、温州

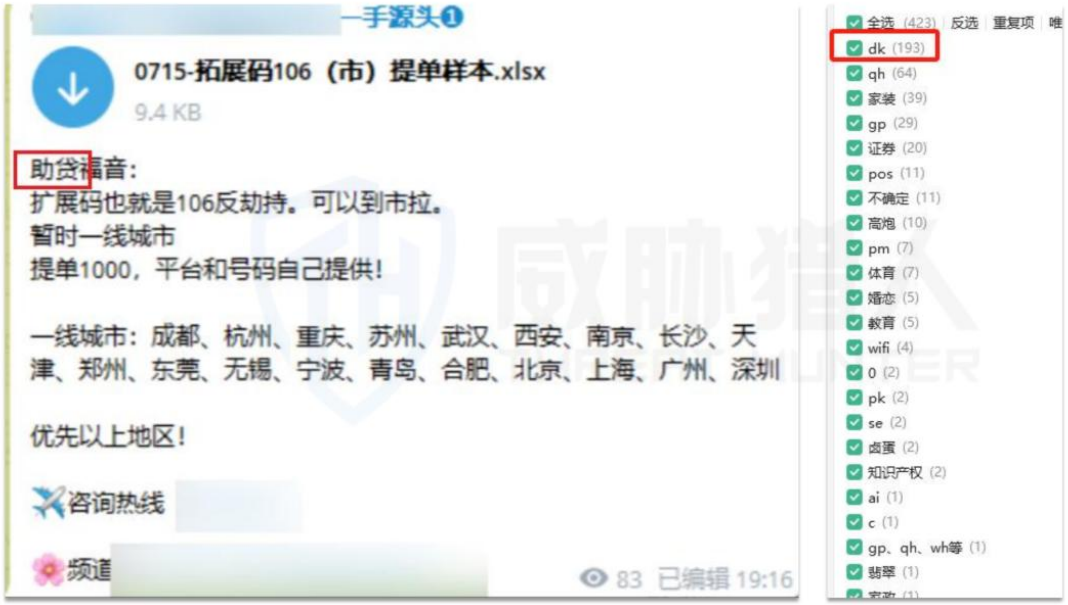
4. 时间维度：最早于 2025 年 5 月 13 日开始测试；5 月 16 日正式在非法数据交易市场推广，涉及 350 家企业，影响 19 个城市；7 月 2 日起，不局限于 106 开头的号码，支持 95 或 96 开头的号码下发的短信用户；8 月 6 日影响规模扩大到 420 家企业，影响全国 36 个城市的用户。

（时间线）



（左图为黑产推广该数据类型宣传，右图为 7 月 2 日黑产表示不局限于 106 开头的数据）

在非法数据交易市场上，数据中介黑产明确表示这类产品数据可以用于助贷营销作恶；同时，结合黑产提供的平台行业归属划分来看，有接近一半平台为贷款业务平台（消金、银行行业）。



（左图为黑产为助贷团伙推广，右图为黑产提供的平台类型划分）

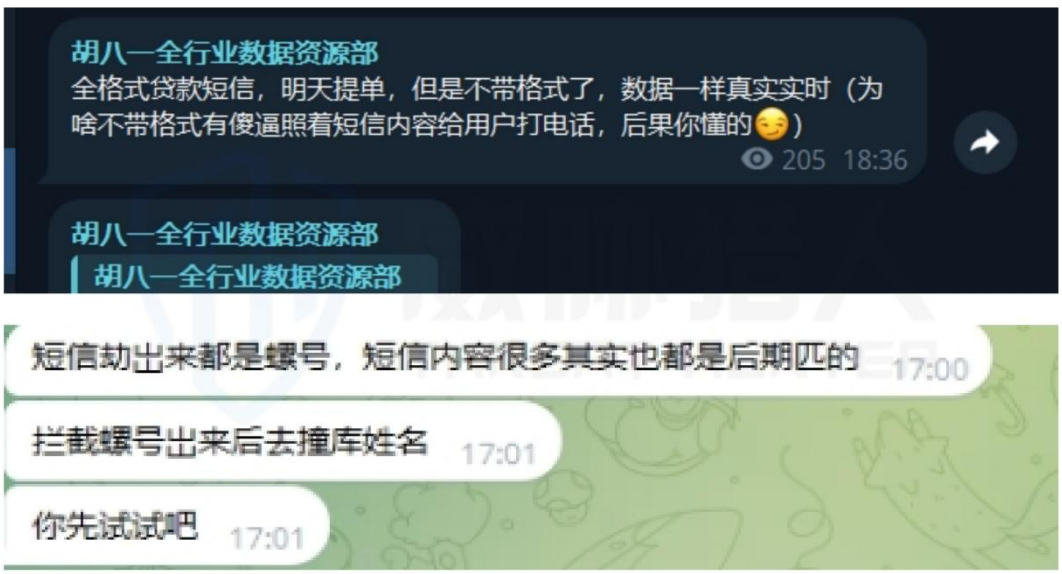
3.4.2 短信泄露溯源对抗持续升级，黑产通过修改数据原始格式提升企业取证难度

2025 年 11 月，威胁猎人监测发现，非法数据交易市场中陆续出现多家不同金融机构的用户短信信息同时泄露。相关泄露样本中，短信内容高度一致，普遍呈现为“您于 xxx 成功还款，详情请登录 xxx APP 查看”等通用表述。

然而，在实际业务中，不同金融机构通常不会采用完全一致的短信模板，多家机构同时采用完全一致的短信内容并不符合正常业务逻辑，存在明显异常。

威胁猎人对相关样本进行了进一步分析与跟进后发现，部分黑产在交易过程中明确说明，此类短信数据并非原始下发内容，而是通过人工拼接、统一格式重新生成。其常见表述为“您于 xxx 时间段的还款已成功！”，并在不同平台（即黑产所称的“混合台子”）中展示完全一致的短信内容。

该操作的主要目的，在于削弱短信模板特征，规避监管部门及企业基于内容模板的溯源与取证分析。



（黑产针对短信格式问题进行的解释）

威胁猎人建议：

上述情况表明，短信数据泄露风险正在呈现出去模板化、去平台特征化的发展趋势，单纯依赖短信内容或模板特征进行识别与溯源，已难以有效覆盖当前风险形态。部分非法数据交易行为通过统一重构短信内容、弱化平台差异，刻意规避基于文本模板的识别机制，显著提升了企业在取证与定位阶段的难度。

在此背景下，企业在处置短信泄露相关风险时，不宜仅以短信内容是否匹配自身模板作为判断依据，而应将核验重点前移至用户与业务关系本身，重点关注涉事手机号是否为平台注册用户、是否存在真实业务交互记录，以及其行为轨迹是否与正常业务流程相匹配。通过从“内容特征”向“关系与行为特征”转变，才能更准确地识别真实泄露风险，避免误判或遗漏关键风险信号。

04

威胁猎人数据泄露风险情报服务

四、威胁猎人数据泄露风险情报服务

2025 年全年数据泄露风险进入了“高位常态化”的深水区。纵观全年，黑灰产业链条已进化出极高的成熟度与组织韧性，其特有的“自我修复机制”使得单一维度的平台打击难以触及根本，导致风险事件量持续居高不下，泄露活动在打压下依然保持高度活跃。同时，黑产针对泄露来源持续升级对抗，修改原数据信息等方式，为企业/监管单位溯源追踪增加层层阻力。

面对如此严峻的形式，企业需要全面提升对风险的识别及应对能力，了解风险事件的细节，包括对风险真实性进行验证，及时进行溯源、处置下架并跟进潜在风险，增强数据泄露风险监测及预警的及时性等。

对此，威胁猎人提供针对性解决方案：

威胁猎人数据泄露风险监测服务，通过对全网多渠道情报的实时监测及深度挖掘，并基于风险真实性验证引擎及人工数据验证，7×24 小时实时预警数据泄露风险，联动应急处理机制，最大限度降低危害及损失。

1、全网情报监测及挖掘：覆盖暗网、匿名群聊、网盘文库、代码托管平台等各渠道，从不同维度持续提升渠道覆盖的全面性，包括新渠道的持续发现和更新、深层情报源（Deep Source）的专项挖掘、多语种的渠道覆盖。

2、数据泄露风险精准预警：针对监测到的黑产交易数据，通过风险真实性验证引擎+人工数据验证服务，提供综合的可信度评估结果，帮助企业精准感知风险、及时处置风险：

① **风险真实性验证引擎：**基于“信源置信度要素、三要素匹配度要素、历史重合度要素”3 个要素对风险真实性进行验证；

② **人工数据验证服务：**通过二次验证、主动验证等方式进一步帮助企业精准感知风险。

3、「7×24」应急响应：成立 DRRC 风险应急响应中心，对企业相关风险情报进行全天候监测、审核和预警，提供「7×24」样例获取、情报挖掘、协助溯源、处置下架等服务，同时提供月度数据泄露风险监测报告，以及典型风险事件分析结果。

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

扫码关注
获取行业最新反欺诈报告

服务热线：400-809-3699
官方网址：www.threathunter.cn
联系邮箱：marketing@threathunter.cn
总部地址：广东省深圳市南山区粤海街道科技园社区科苑路15号科兴科学园B2栋1705