威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

2026年上半年
数据泄露风险态势报告

出品方：威胁猎人

THREAT HUNTER

以客户为中心 | 正直 | 求真

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。

继《2026 年上半年互联网黑灰产研究报告》发布后，威胁猎人进一步将观察视角聚焦于企业数据安全场景，发布《2026 年上半年数据泄露风险态势报告》。

这是威胁猎人连续多年发布的互联网黑灰产行业研究报告，也是威胁猎人面向行业固定推出的年度趋势观察成果。作为专注于黑灰产情报与业务反欺诈的安全厂商，威胁猎人已在黑灰产情报领域深耕 10 年，依托长期积累的风险数据、真实攻击样本与企业治理实践，持续追踪黑产资源、攻击手法与产业链变化，持续为企业判断风险趋势、制定治理策略提供参考。

目录

前言

数据泄露已不再是孤立的安全事件，而是一条具备稳定供给、明确分工与持续交易的地下产业链。围绕个人信息与企业数据，从获取、加工、定价到分销，地下渠道已形成相对成熟的运转机制，并随外部治理环境与下游需求变化不断调整形态。

本报告基于威胁猎人对地下数据交易渠道的长期观察，覆盖 2026 年上半年的公开交易动态，呈现被交易数据的规模、流通渠道、受影响行业与主要品类及其结构性变化，供不同行业的企业研判自身外部暴露面参照。

报告内容关键点总结：

2026 年上半年，地下数据交易市场呈现供给高位化、渠道隐蔽化、借贷数据来源供应链化、借贷数据常态化流通、查询能力商品化五个特征。匿名群聊仍是主要交易场景，暗网占比明显上升；泛金融仍是数据泄露最集中的板块，电商、社交工具、软件应用等领域同样处于高位，制造业与零售业重大风险事件增量突出；借贷数据持续贯穿泄露、转卖与下游利用链路，金融查档则进一步表现出按人、按次提供查询结果的商品化特征。

- 地下数据交易仍处高位，2026 年上半年事件量较 2025 年下半年上升约 7.0%，被交易数据供给仍维持高位。
- 暗网在流通渠道中的占比明显上升，由约 10.6% 升至约 20.9%，在公开平台治理、匿名群聊风控、勒索披露常态化等多重因素影响下，高危数据和公开施压信息更倾向于向暗网侧集中。
- 泛金融仍是数据泄露最集中的板块；制造业与零售业重大风险事件增量突出，泄露风险正向更多行业扩散。

- 第三方供应链是数据泄露的重要来源；在借贷数据等高度依赖外部服务的业务中，供应链相关风险更加集中。内部人员直接外泄占比不高，其中相当部分仅为卖家声称。

- 借贷相关数据是 2026 年上半年最活跃、产业化程度最高、下游变现链条最完整的品类。相关数据外流后可能被反复转卖，并被用于外呼诈骗、假催收、精准营销和查档补全，风险并不会随着泄露源头被切断而结束。

- 针对个人的非法查档已形成独立稳定的地下交易赛道，其中金融类查询占比居首。借贷数据中的手机号、身份证号和银行卡号等线索，可被进一步补充名下卡、余额、流水、征信和支付交易等信息，由单次业务记录扩展为个人金融画像。

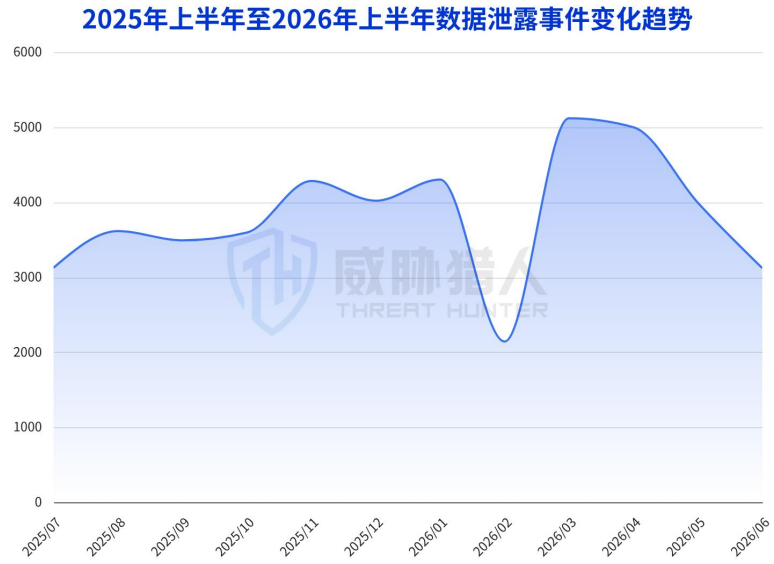
01

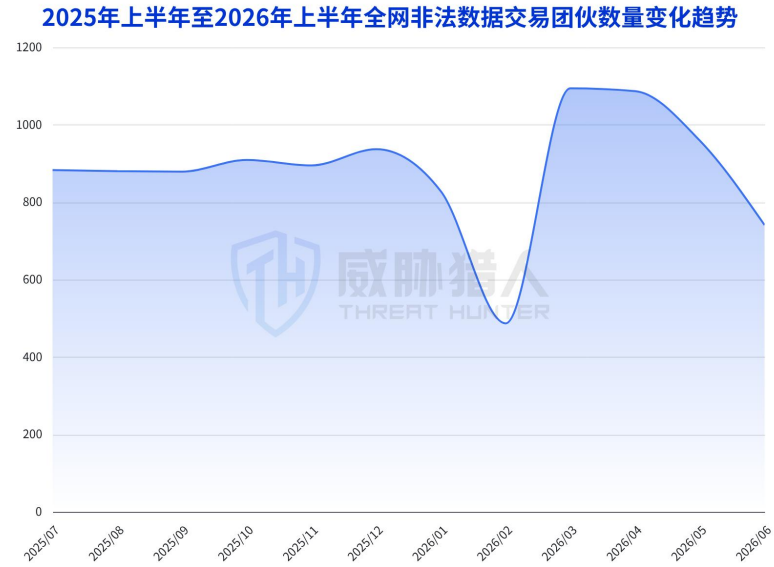
2026 年上半年
数据泄露风险概况

一、2026 年上半年数据泄露风险概况

1.1 2026 年上半年数据泄露事件共 23,645 起，涉及 3,426 家企业，月均较 2025 年下半年上升约 7.0%

据威胁猎人数据泄露监测平台统计，经真实性验证引擎与 DRRC 人工分析双重验证，2026 年 1—6 月确认有效的数据泄露事件共计 23,645 起，涉及银行、消费金融、电商、社交工具等重点行业共 3,426 家企业；事件量按月均计较 2025 年下半年上升约 7.0%。



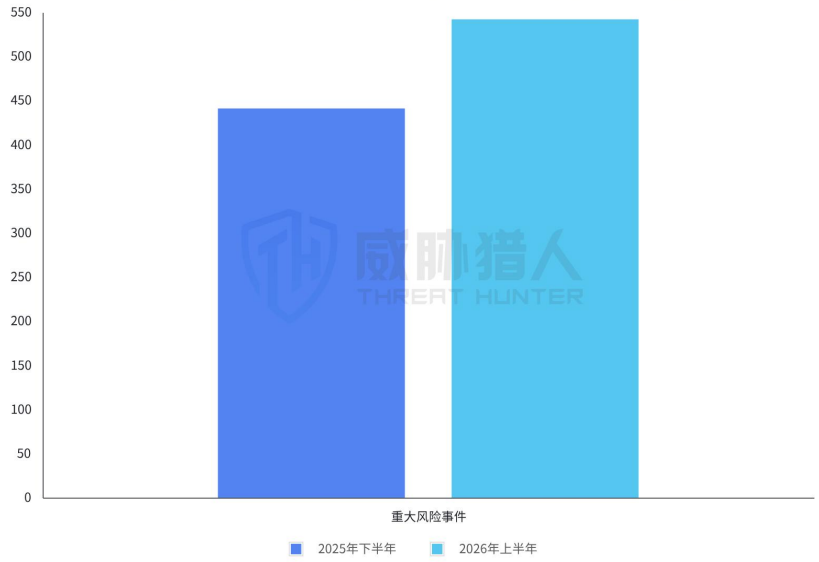


1.2 重大风险事件增长 22.90%，暗网披露高度集中，制造业与零售业增量突出

据威胁猎人统计，2026 年上半年，共监测到涉及数据量级较大或可能危害公共安全的“重大风险事件”542 起，较 2025 年下半年的 441 起增加 101 起，增幅为 22.90%。

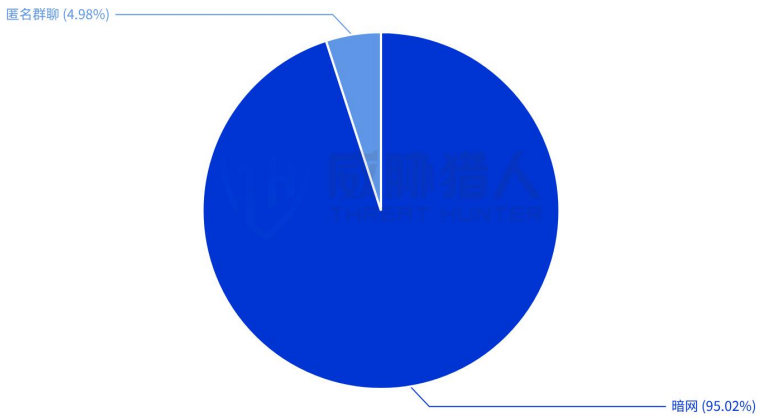
重大风险事件：数据量级较大、字段敏感度高、涉及核心业务数据、被勒索/黑客组织公开披露，或可能造成较高合规、声誉及公共安全影响。

2025年下半年与2026年上半年重大风险事件量对比情况

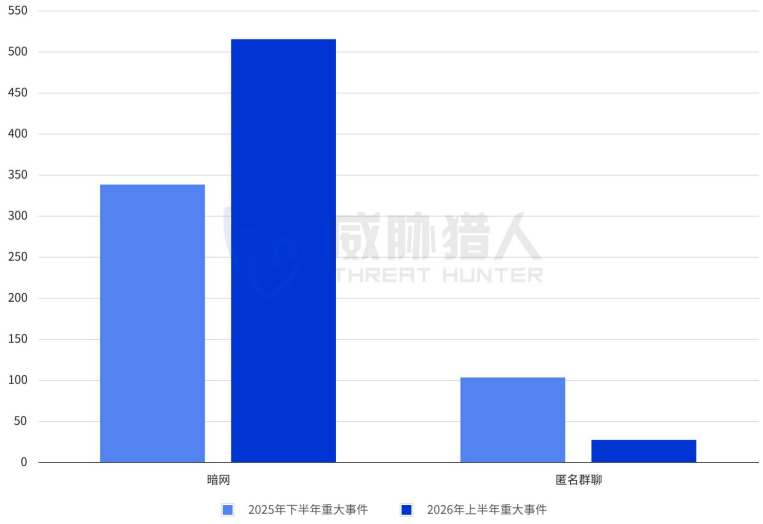


暗网重大风险事件占比由约 76.4%升至 95.0%，上升约 18.6 个百分点；重大风险事件的公开披露明显向暗网集中。

2026年上半年重大风险事件渠道分布占比情况

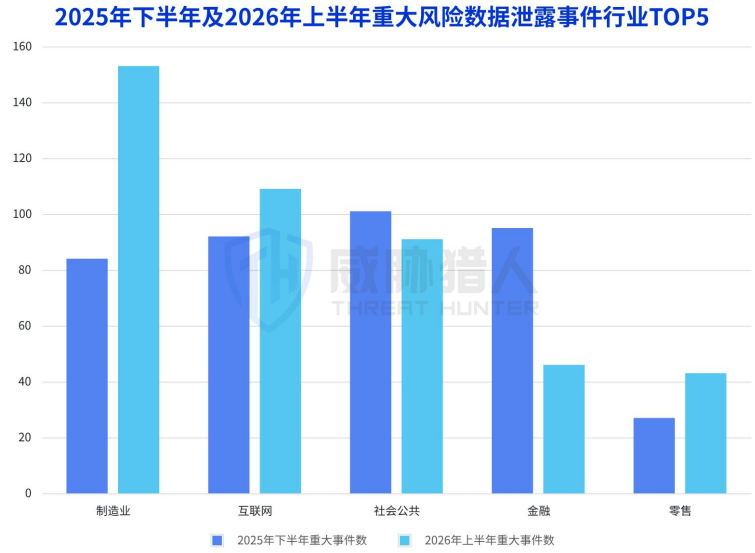


2025年下半年与2026年上半年重大风险事件渠道分布对比情况

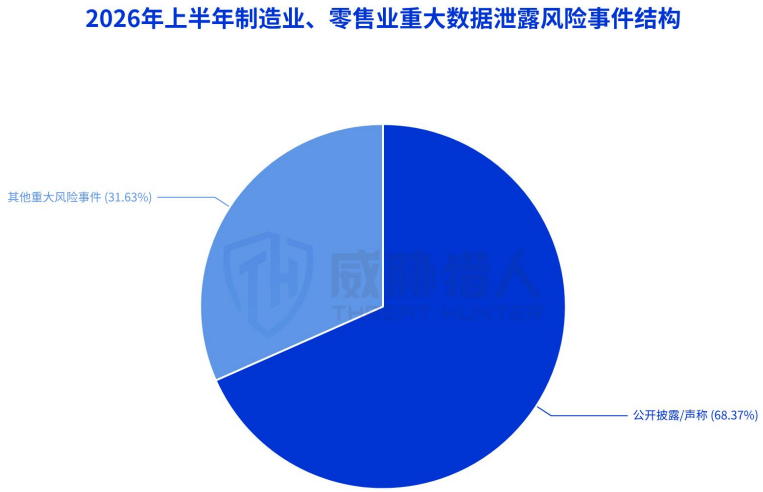


从行业维度来看，2026 年上半年重大风险事件主要集中于制造业、互联网、社会公共、金融和零售业。其中，制造业重大风险事件数量较 2025 年下半年增长 82.14%，为 TOP5 行业中增幅最大的行业；零售业紧随其后，增幅为 59.26%。相比之下，社会公共和金融行业重大风险事件数量较 2025 年下半年有所下降。整体来看，新增风险事件更多集中于制造业和零售业，呈现向实体生产与消费流通环节扩散的特征。

> 制造业事件主要涉及汽车、消费电子、机械器材和电子元件制造。

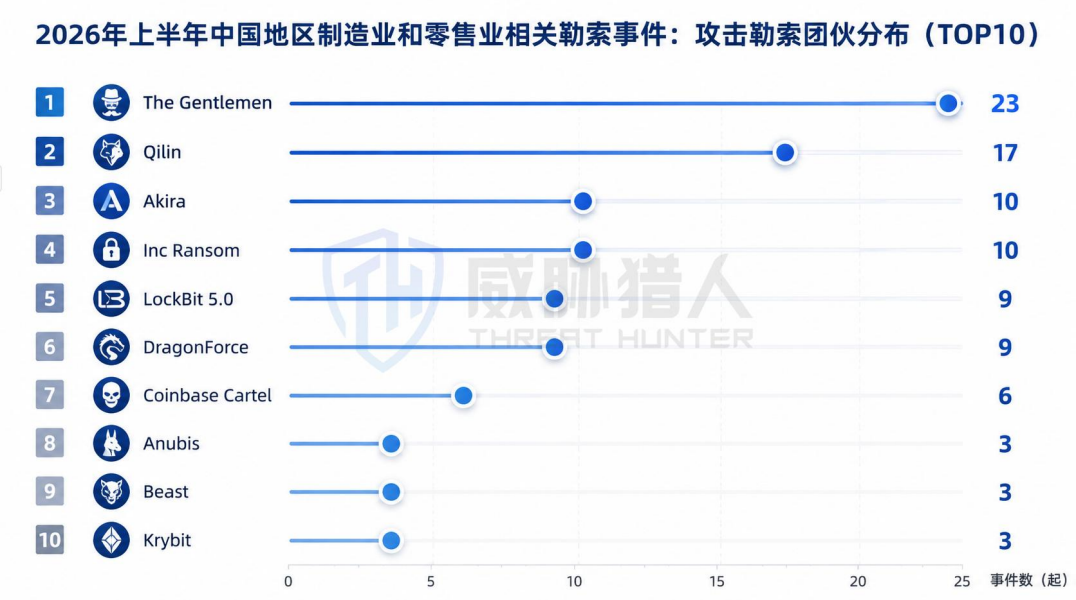


针对 2026 年上半年重大风险事件涨幅较大的制造业以及零售业进一步分析，共计 196 起风险事件，其中有 134 起为勒索/黑客组织披露事件，占比达 68.37%，共涉及 37 个组织。



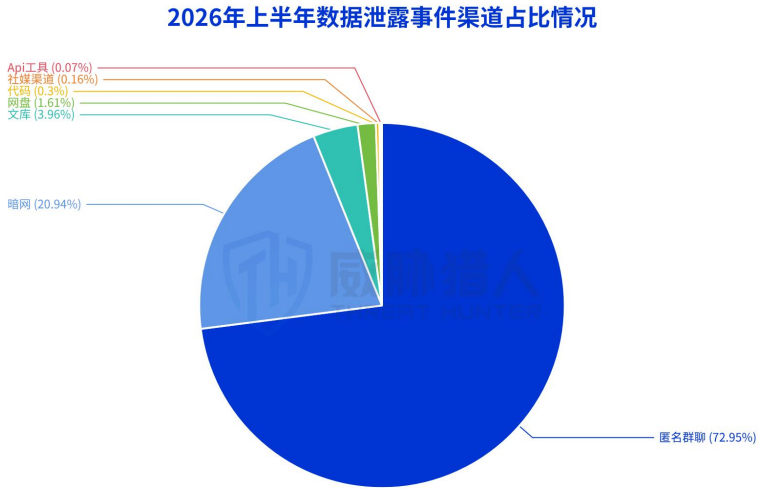
这 134 起为勒索/黑客组织披露事件中，活跃度居前的五个勒索团伙为 The Gentlemen（23 起）、Qilin（17 起）、Akira（10 起）、Inc Ransom（10 起）、LockBit 5.0（9 起）。前五个组织合计涉及 69 起事件，占上述 134 起事件的 51.5%。呈现一定的头部集中，同时仍有较多长尾团伙参与。

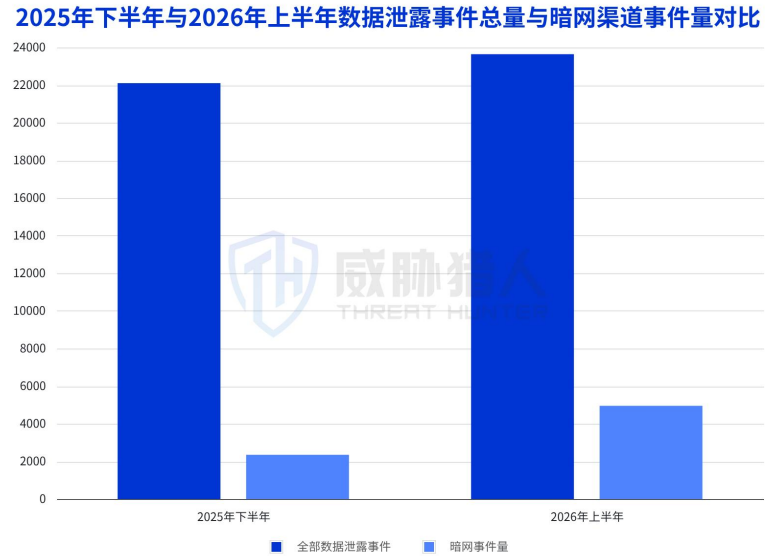
以上仅统计 2026 年上半年中国地区制造业和零售业相关事件，不代表全球勒索团伙活跃度排名。



1.3 数据泄露仍以匿名群聊和暗网为主，暗网事件量增长 110.5%

据威胁猎人 2026 年上半年监测平台数据统计，匿名群聊与暗网仍是主要泄露渠道，两者合计占比 93.9%。其中暗网渠道事件量由 2025 年下半年的 2,353 起增至 4,952 起，涨幅约 110.45%。



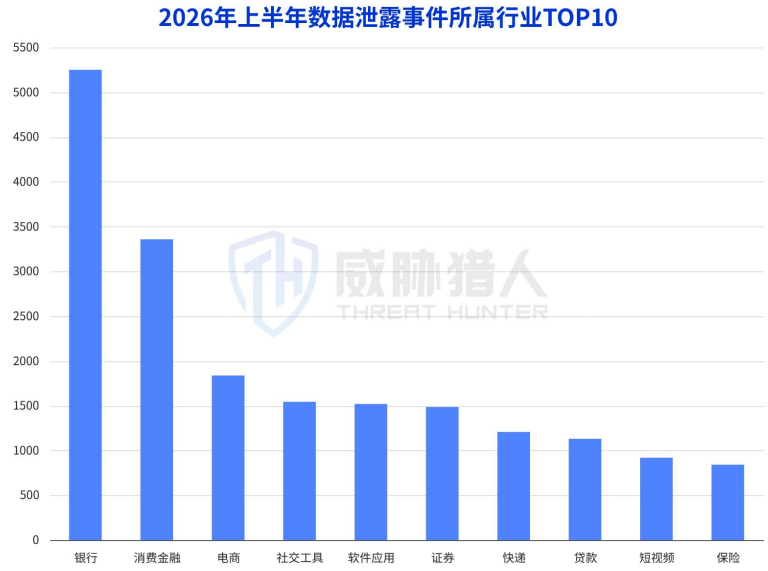


匿名群聊仍承担大量交易撮合，但高危事件和公开施压信息正更多迁移至暗网，企业监测和处置需要覆盖论坛、泄露站、聚合站和勒索发布页等多类暗网场景。

1.4 泛金融泄露总量持续高位，新增泄露进一步向借贷数据、支付、资产管理等“离钱更近”的数据集中

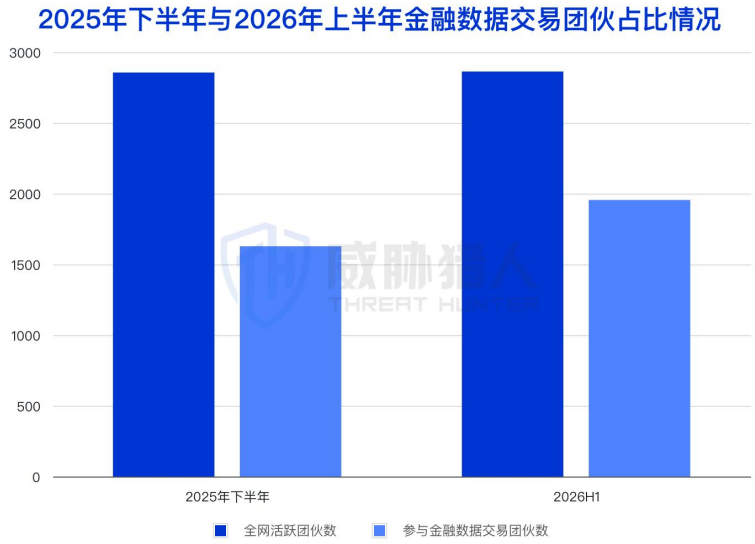
2026 年上半年，泛金融板块的数据泄露事件仍处于较高水平。其中，银行、消费金融、证券、支付等相关领域合计监测到约 1.25 万起数据泄露事件，占全网数据泄露事件总量的五成以上，仍是数据泄露交易最为集中的板块之一。

从细分行业来看，银行业数据泄露事件数量最多，消费金融行业次之。



从交易参与者变化来看，地下市场对金融数据的关注度进一步上升。2026 年上半年，在全网活跃团伙总量整体保持稳定的情况下，参与金融数据交易的团伙数量有所增加，占活跃团伙总数的比例由 57.0%提升至 68.3%。

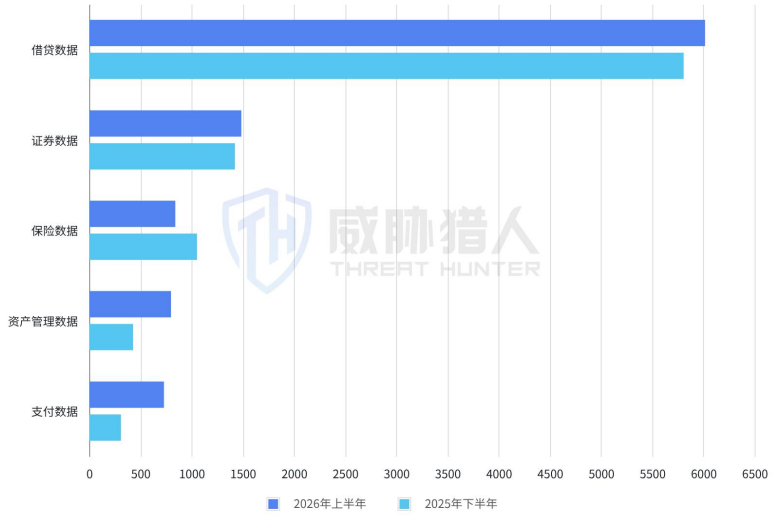
这说明，越来越多的地下交易团伙将金融数据作为重点交易对象，金融数据的市场吸引力仍在增强。



从泛金融行业事件中的细分数据类型来看，2026 年上半年金融数据泄露呈现分化趋势。借贷数据仍占绝对多数，较 2025 年下半年继续增长；资产管理和支付数据增长较为明显，证券数据整体保持稳定，保险数据则有所回落。

总体来看，新增泄露仍在向借贷、支付、资产管理等“离钱更近”的数据集中。其中，借贷数据体量最大，较 2025 年下半年继续增长，第二部分将重点分析其泄露链路、来源及下游利用方式。

2025年下半年至2026年上半年金融行业各细化数据类型事件量变化情况



02

借贷数据泄露整体链路与成因分析

二、借贷数据泄露整体链路与成因分析

综合 2026 年上半年数据泄露总体态势可以看到，当前地下数据交易主要呈现两类典型风险形态：

以勒索/黑客组织和暗网披露为代表的整库、高危数据事件，主要影响制造业、零售业和互联网等行业。

以金融客户及业务数据为代表的常态化交易，数据持续进入地下渠道并被用于诈骗、营销、催收和二次倒卖。

泛金融领域涉及支付交易、资产管理、证券投资、保险保单和借贷等多种数据类型。其中，借贷数据事件量最大，覆盖业务环节最多，下游变现链条也最为完整，因此第二部分选取借贷数据作为典型样本，分析其泄露链路、来源及持续利用方式。

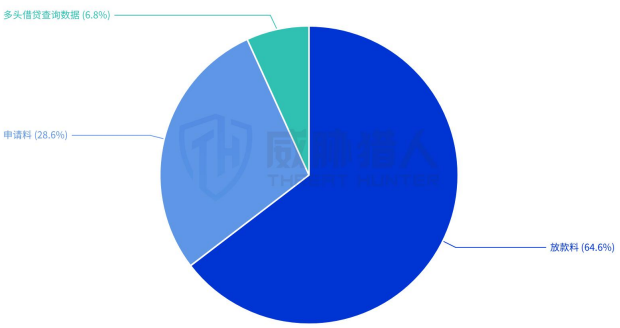
2.1 借贷数据为地下市场最活跃的高价值品类

借贷数据是 2026 年上半年泛金融地下数据交易中的第一大细分品类，相关事件约 6,000 起，产业化程度最高，变现链条也最为完整。历史数据持续被反复转卖，新增泄露数据不断进入市场，同时叠加下游催收、诈骗等需求，使借贷数据长期保持常态化流通。

从数据构成来看，放款料占据绝对主体，约占六成半；其次为申请料，约占三成；其余主要为贷前环节的多头借贷、风控查询等数据。

借贷数据泄露事件：覆盖银行、消费金融、网络小贷、助贷、风控、催收等多类主体。

2026年1月至2026年6月信贷数据品类构成



2.2 借贷数据泄露贯穿业务全生命周期

借贷数据风险并非集中在某一个系统或某一次数据库失守，而是与借贷业务链路高度重合。用户从产生借款意向，到完成申请、审批、放款，再到还款和贷后催收，通常需要经过获客平台、注册页面、风控查询、授信审批、支付结算、短信通知、催收外包等多个环节。

从地下市场中的交易数据看，借贷相关信息的泄露与利用大致贯穿以下四个阶段。

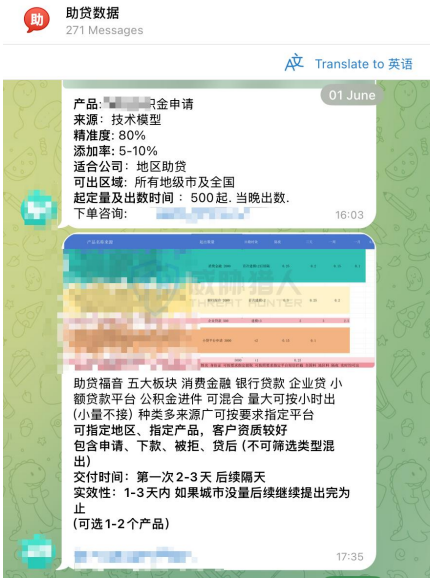
（1）获客与注册：运营商流量和 SDK/埋点数据形成实时意向名单。用户尚未提交申请，仅浏览借贷产品或进入落地页时，访问行为就可能被网络层采集或被嵌入式组件记录，形成“近期访问过某借贷产品”的名单。这类数据准确性不一定高，但覆盖面广、时效快，常被用于电话推销和精准营销。

（2）贷前审批：多头借贷和风控查询数据价值更高。该类数据记录用户发起申请后的查询动作，可能包含最大逾期金额、最长逾期天数、当前及历史放贷机构数等字段。它原本用于风控识别，一旦外泄，就会反向成为筛选多头负债、急需周转人群的工具；部分此类事件的字段特征和交易描述，显示其来源可能涉及上游风控、征信和数据服务供应链，而不一定直接来自放贷机构自身。

（3）贷中与放款：申请料、放款料是交易主体。网贷、助贷、融资担保、租机、借条等场景会沉淀大量申请和放款名单，字段可直接支撑外呼、诈骗、二次营销和转卖。中小平台安全能力不均衡、外部系统接入较多，可能是相关数据持续泄露的原因之一。

（4）贷后：催收逾期数据和短信通道数据带来长尾危害。逾期和催收名单指向还款压力较高的人群，容易被假催收、二次催收和冒充客服利用。短信通道风险需要区分两类：一类是运营商侧群

发短信签名通道产出的号码线索；另一类是短信通道商被攻破或劫持后产生的短信明文内容，后者可能跨多运营商、多平台，影响面更大。

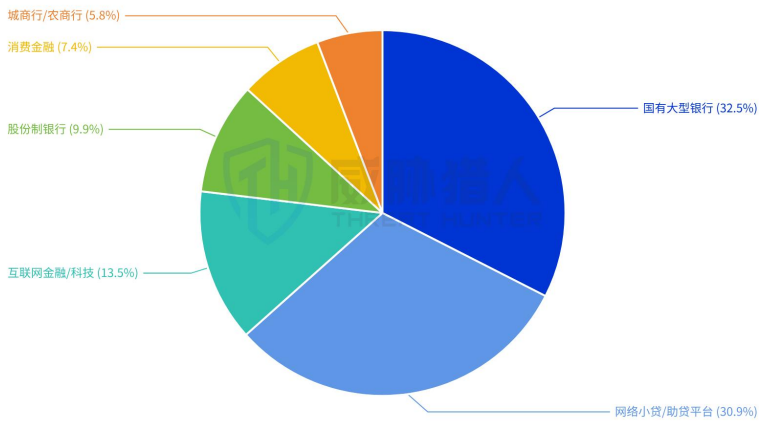


涉及机构：大型银行与网贷/助贷平台共同处在高暴露面

从能够明确判断涉及机构的借贷数据泄露事件看，国有大型银行和网络小贷、助贷平台占比几乎并列居前，分别约为 32.5%和 30.9%；互联网金融与科技类机构约占 13.5%，股份制银行约占 9.9%，消费金融机构约占 7.4%，城商行和农商行约占 5.8%。

这一结构表明，借贷数据风险并非只发生在规模较小或安全能力较弱的平台。大型持牌机构虽然通常具备较完善的内部安全体系，但其业务仍需要接入助贷、风控、征信、短信和催收等外部服务，相关数据仍可能在外部服务链路中发生泄露。

2026年1月至2026年6月信贷泄露涉及机构类型构成

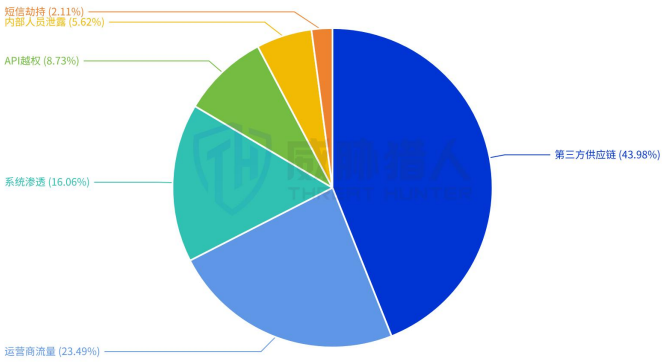


2.3 借贷数据泄露来源以第三方供应链为主

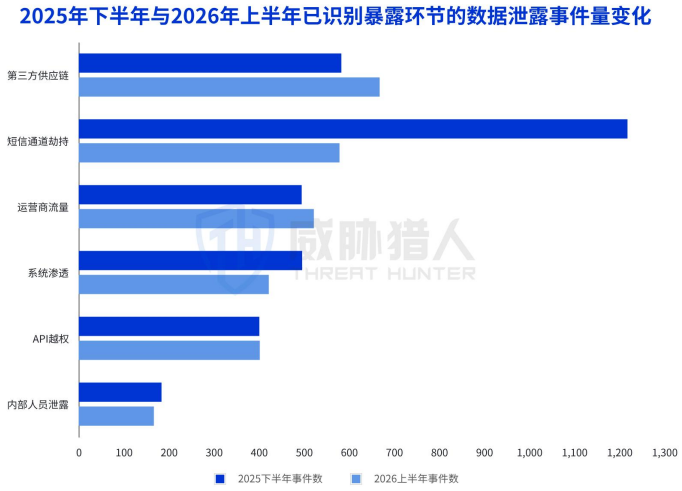
根据威胁猎人对借贷数据泄露事件来源的分析推断，2026 年上半年，在能够判断来源的相关事件中，第三方供应链相关事件约占 44%，运营商通道约占 23%，系统渗透约占 16%，API 越权约占 9%，内部人员外泄约占 6%，短信通道相关风险约占 2%。

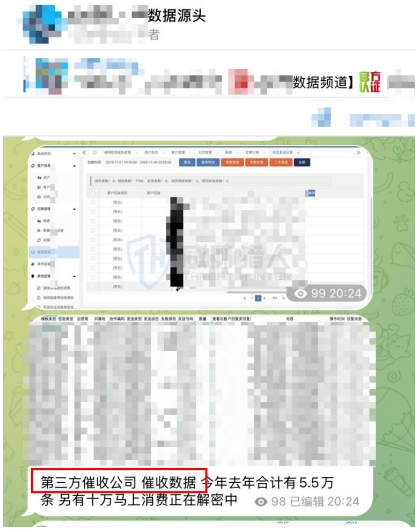
从可归因样本来看，第三方供应链泄露占最大比例，借贷数据的风险已经明显从单一机构内部向外部服务链条扩散，第三方风控、征信、助贷、短信和催收等环节已经成为泄露溯源和风险治理的重点。

2026年1月至2026年6月借贷数据泄露来源分布情况



从泄露来源来看，2026 年上半年，与第三方供应链相关事件数量进一步上升，短信通道劫持类事件则出现明显回落。值得注意的是，短信通道劫持类事件量虽然下降，但其业务危害和扩散能力仍不容忽视，仍需重点监测。短信通道一旦管理不到位，仍可能被用于假催收、诈骗短信、钓鱼链接投放和用户精准触达。

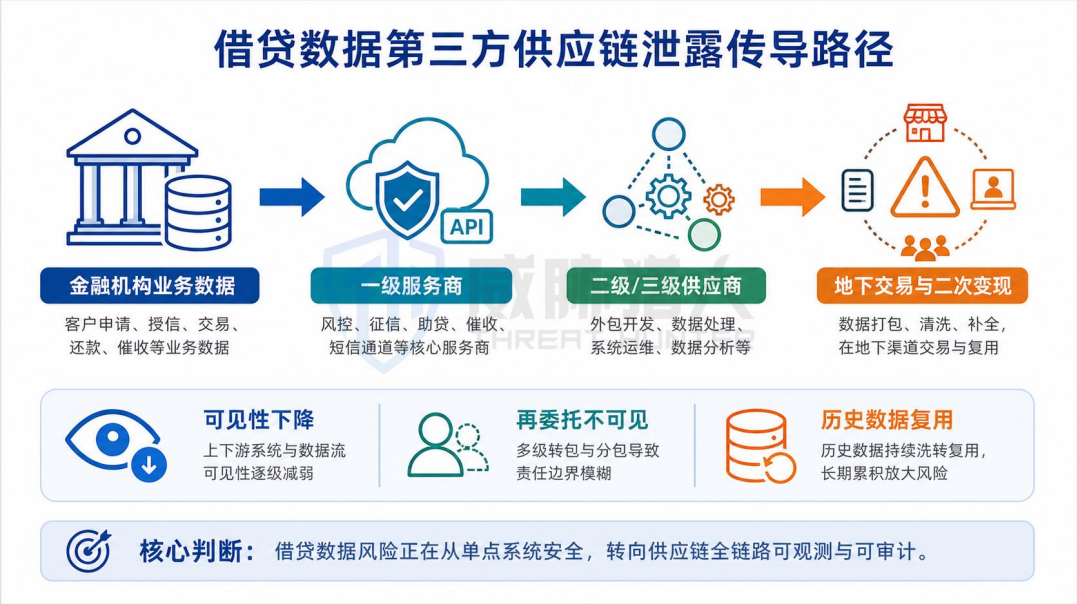




2.4 企业应将第三方供应链纳入借贷数据泄露重点治理范围

借贷业务依赖风控、征信、助贷、短信和催收等多个外部服务节点。数据进入第三方处理链路后，机构对数据流向、再委托关系、接口调用和历史留存情况的可见性随之下降。部分数据还可能继续流向二级、三级供应商，最终在原机构难以直接审计的供应链末端发生泄露。

此外，多家金融机构可能共同使用同一服务商。一旦某个外部节点失守，可能同时影响多家企业。这意味着，机构内部系统没有发现入侵，并不代表相关数据未在外部链路中泄露，借贷数据治理需要从保护自有系统进一步延伸至第三方供应链管理。



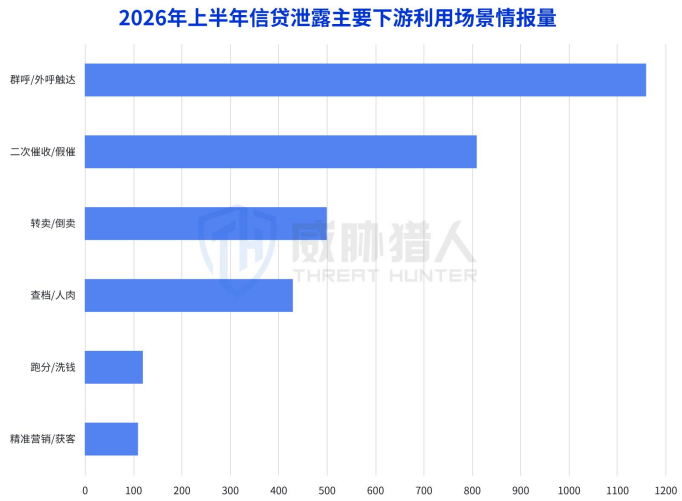
这类风险之所以难以管控，主要在于供应商链路不透明、内部系统未必出现明显告警、风险发现往往滞后。企业可能先从地下渠道、用户投诉或泄露样本中发现问题，而不是从自身系统中发现直接入侵痕迹。

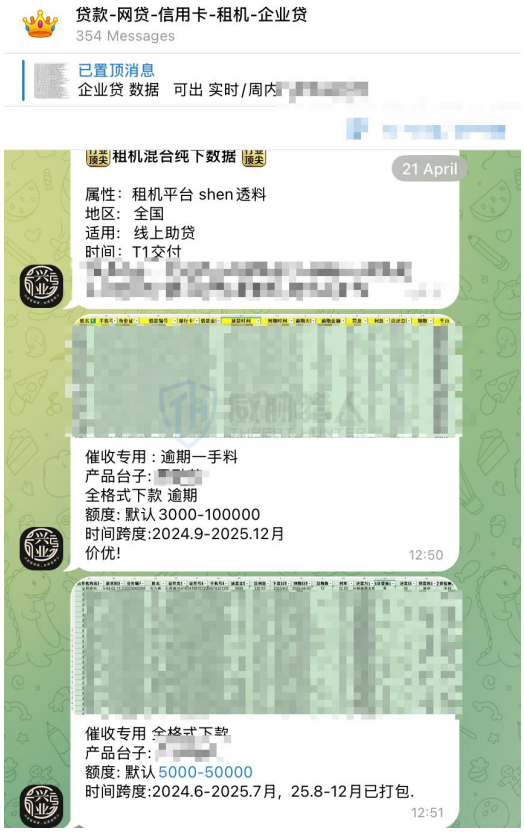
因此，借贷机构的治理重点应从保护自有系统，扩展到供应链管理和外部风险监测。企业需要加强关键服务商准入与持续评估，明确再委托和数据留存要求，监测接口异常调用和批量提取行为，同时持续关注地下渠道中的品牌、产品、字段和样本信息，及时开展真实性验证和事件溯源。

但上述措施主要用于减少新增泄露和供应链失控风险，无法消除已经流入地下市场的数据存量。已经外流的数据仍可能被长期保存、反复交易，并在不同下游场景中持续产生危害。

2.5 数据外流后的持续利用：外呼诈骗、假催收与信息补全并行

借贷数据进入地下市场后，通常不会只沿单一链路流通。同一批数据可能被反复转卖，并被用于外呼诈骗、假催收、精准营销及个人信息补全。其中，外呼诈骗和假催收最容易对用户造成直接损失；查档等信息补全服务则会进一步扩大原始泄露数据的深度和危害程度。





（1）实时外呼诈骗

刚提交申请、仍在等待审批或放款的用户名单，可能被迅速导入自动外呼系统。诈骗团伙赶在正规平台前联系用户，冒充平台客服或贷款审核人员，以“账户异常”“额度冻结”“缴纳手续费”等理由诱导转账。由于诈骗行为与用户真实申贷时间高度重合，相关话术更容易取得用户信任。

（2）二次催收与假催收

催收、逾期和放款数据外流后，黑产可以利用贷款机构、借款金额、放款时间、逾期情况和绑定卡号等信息冒充催收方，通过虚假催款短信、电话施压或高仿还款页面诱导用户转账。

如 2026 年 3 月，北京金融监管局发布防范“贷款催收”短信诈骗的消费者风险提示，公开报道中提到的典型手法包括假冒正规金融机构发送催收短信、引导点击高仿网站、以“逾期罚息翻倍”“纳入失信名单”等话术逼迫转账，以及以“核实身份”“确认还款意愿”为由套取敏感信息。

国家金融监督管理总局 北京监管局

无障碍浏览 | 繁 |

请输入您要搜索的内容...

机构概况 | 新闻资讯 | 政务信息 | 在线服务 | 互动交流 | 统计数据

当前位置： 首页 > 新闻资讯 > 监管动态

发布时间：2026-03-13 来源：北京监管局 文章类型：原创 打印 微博 微信 更多

消费者风险提示：防范“贷款催收”短信诈骗

当前，一些不法分子冒充正规金融机构发送虚假“贷款催收”短信，侵害金融消费者的财产安全。**北京金融监管局提示广大金融消费者：提高警惕，核实债务真伪，不轻信、不盲转，避免因慌生乱。**

陷阱一：假冒网站骗盗刷。不法分子诱导消费者点击短信链接，登录高仿网站“还款”，窃取银行卡号、密码及验证码。随后利用窃取的信息盗刷资金，导致消费者钱财两空且债务未消。

陷阱二：虚假催收逼转账。不法分子冒充贷款机构催收人员，以“逾期罚息翻倍”“纳入失信名单”“上门催收”“影响子女升学”“将被起诉”等话术恐吓消费者，谎称需立即转账还款才能减免罚息、撤销逾期记录，诱导消费者向其提供的私人账户转账，转账后失联，消费者逾期问题并未解决。

陷阱三：虚假协商骗信任。不法分子声称代表银行进行“债务重组”或“停息挂账”协商，骗取消费者信任后，索要高额“手续费”“咨询费”或“材料费”，并承诺办理成功后再收费，待费用到手后，对方随即失联。

陷阱四：恶意套取骗信息。短信以“核实身份”“确认还款意愿”为由，诱导消费者回复身份证号、家庭住址、工作单位等敏感信息，或拨打短信中的假冒客服电话。不法分子获取这些信息后，不仅用于精准诈骗，还可能将其倒卖，导致消费者面临更多的骚扰电话和潜在风险，个人隐私毫无保障。

面对虚假“贷款催收”短信，北京金融监管局提醒广大消费者：核渠道、拒链接，源头把关防忽悠，查征信、稳心态，严护隐私保安全。

一是核实渠道要“正”。收到催收短信后，切勿直接点击链接或拨打短信中的电话。应通过金融机构官方客服电话、官方APP或线下网点主动联系，核实债务真实情况及催收人员身份。

二是资金往来要“清”。坚持“三不”原则：不向个人账户转账、不扫描不明二维码、不透露短信验证码。所有还款操作务必在官方APP内完成，或转入合同约定的对公账户，并保留好还款凭证。

三是个人信息要“护”。不随意点击陌生短信链接，防止手机植入木马病毒或被引导至钓鱼网站。定期检查个人征信报告，了解自身负债情况，避免因信息不对称而被骗子钻空子。

（3）反复转卖与跨场景复用

借贷数据的风险并不会随着泄露源头被切断而结束。数据一旦流入地下市场，便可能被复制、清洗、重新分类和包装，并在不同团伙与渠道之间反复转卖。即使企业已经完成漏洞修复、账号处置或供应商整改，已经外流的数据仍可能继续用于外呼诈骗、假催收、精准营销和其他下游场景。

贷后阶段若集中出现能够准确说出贷款机构、借款金额、放款时间、逾期情况或绑定卡号等信息的异常客诉，应关注历史泄露数据被重新利用的可能性。此类异常不一定意味着企业近期再次发生泄露，也可能源于此前外流数据在地下市场中持续流通和二次变现。

典型案例：

威胁猎人监测到某贷款平台在 2025 年末收到大量用户投诉，用户称遭遇“假催收”骚扰。平台核查后发现，相关数据与数月前已经发现并阻断的一起泄露事件有关。虽然源头早已完成整改，但数据仍在地下市场被反复转卖，并被继续用于催收诈骗和二次变现。地下市场中，包含逾期时间、借款金额和联系方式的所谓“一手逾期数据”长期存在交易需求。

这一案例说明，数据泄露事件不能只以“泄露源头是否切断”作为处置结束的标准。企业在评估影响时，还需要将外流数据后续被交易和利用的周期纳入考量。贷后阶段集中出现“能够准确报出贷款信息”的假催收客诉，本身就是一条值得回溯排查的泄露信号。

除反复转卖和直接利用外，借贷数据中的手机号、身份证号、银行卡号等字段还可以成为进一步查询个人信息的入口，使原始数据在查档过程中得到补全和扩展。

（4）查档补全与金融画像扩展

借贷数据中的手机号、身份证号、银行卡号等字段，可以成为进一步查档的查询入口。黑产可能据此补充名下银行卡、账户余额、银行流水、征信及支付交易等信息，进而判断个人的账户持有情况、资产状况、资金活动和偿付能力。原本仅反映单次借贷行为的数据，由此被扩展为更完整的个人金融画像，并被用于提高诈骗话术可信度、实施假催收或继续转卖。

查档正是“线索核验—字段补全—画像扩展—再次变现”链条中的关键环节。它并非与借贷数据相互割裂的另一类风险，而是泄露数据在下游被进一步开发利用的重要方式。第三部分将在此基础上，进一步分析非法查档的市场结构，并重点讨论银行与支付机构相关查询权限被滥用所带来的数据安全与监管风险。

03

非法查档交易：金融信息查询能力的地下商品化

三、非法查档交易：金融信息查询能力的地下商品化

查档，是地下市场按人查询个人信息的交易方式。买家提供手机号、身份证号或银行卡号等线索，卖家按次返回金融、户籍、通信、出行等信息。不同来源的数据还可被交叉拼接，逐步还原个人身份、资产和活动轨迹。据威胁猎人监测，近一年相关事件约 2,800 起，已形成稳定交易市场。下文将重点分析金融类查档，并以银行账户、余额和流水等高风险查询项目为例。

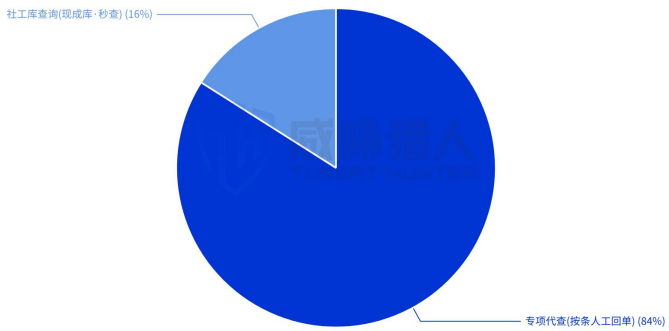
近一两年，非法获取、买卖公民个人信息的案件屡被公开披露，国家对侵犯公民个人信息犯罪的打击持续推进。但据威胁猎人监测，查档黑产并未消失：司法公安类核查在查档事件中的占比，由 2025 年下半年的 5.3%升至 2026 年上半年的 12.5%。需求端持续存在，供给又依托分散在各行业的内部权限与数据接口、难以一次性根除——这是它打而不绝的根源。

3.1 查档市场结构：专项代查占主导，金融类查询占比居首

3.1.1 交易方式：专项代查与社工库分工明确

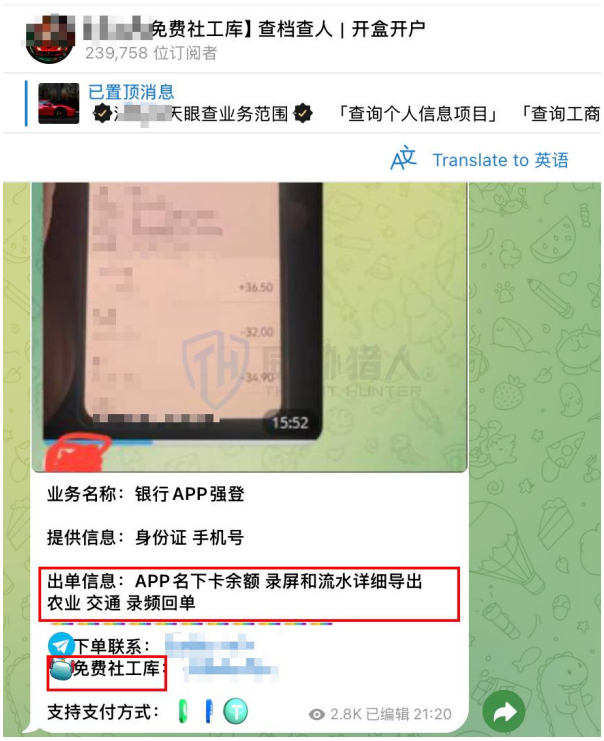
从交易形态看，查档主要分为专项代查和社工库查询两类。专项代查约占 84%，社工库查询约占 16%。

查档业态构成：专项代查 vs 社工库查询（2025年7月至2026年6月）



专项代查在地下市场中也被称为“人工回单”，通常由卖家按照买家提供的查询线索，定向返回相关信息。相关广告常以“内部直调”“人工回单”“实时查询”等话术宣传，其背后可能涉及人员权限滥用、系统账号被借用、外部服务接口失控或其他非法获取渠道。

社工库查询则主要依托历史泄露数据集和自动化机器人进行检索，通常以“免费、秒出、自助”等方式吸引用户。部分团伙先利用社工库提供低价或免费的基础信息，再将时效性更强、字段更深的金融、通信和户籍专项代查作为付费项目。

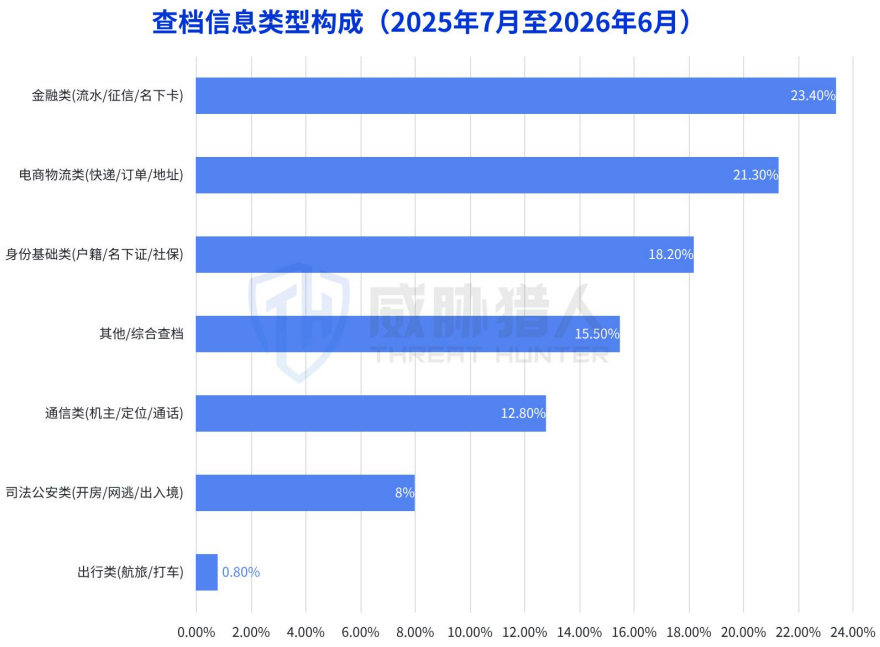


> 左图为：专项代查广告，以“人工回单”“银行 APP 强登”等话术提供按人查询服务。
>
> 右图为：社工库机器人，以免费或低价自动检索作为引流入口。

3.1.2 查询内容：金融类占比最高，查档覆盖多个行业

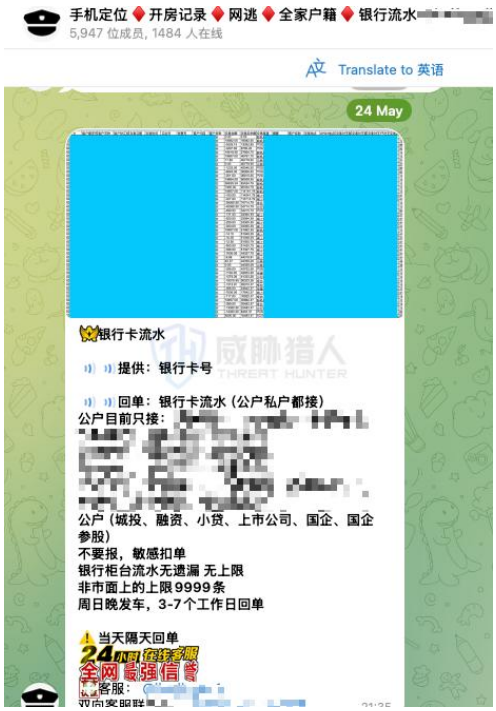
从查询内容看，金融类、寄递电商物流类和身份户籍类处于高位。其中，金融类约占 23.4%，在各类查档标的中居首；寄递电商物流类约占 21.3%，身份户籍类约占 18.2%。

金融类查询主要涉及名下银行卡、账户余额、银行流水、开户信息、征信及支付交易等内容。这些字段不仅能够核验个人身份，还可以反映账户持有情况、资产状况、资金活动和偿付能力，容易被用于精准诈骗、假催收、债务施压、敲诈勒索及二次转卖。



3.2 银行信息查询商品化：单项查询被拆分为不同价位的服务

银行账户、账户余额、银行流水、开户信息和对公账户等，是金融类查档中的高风险内容。地下市场常以“柜台”“开卡专线”“内部直调”等话术，将相关查询包装为按次收费的服务。



与历史数据包售卖不同，这类交易的核心并非一次性出售固定数据，而是将按人查询信息的能力持续对外收费。买家可以从手机号、身份证号或银行卡号等线索出发，继续补充账户关系、资金活动和资产信息。

从地下广告和交易话术看，不同查询项目通常按照字段深度、查询时效、覆盖机构和时间跨度分层定价。名下卡和账户余额等项目多用于快速定位；银行流水通常按照可回溯时间计价；对公账户及跨机构、跨领域的组合查询价格更高。

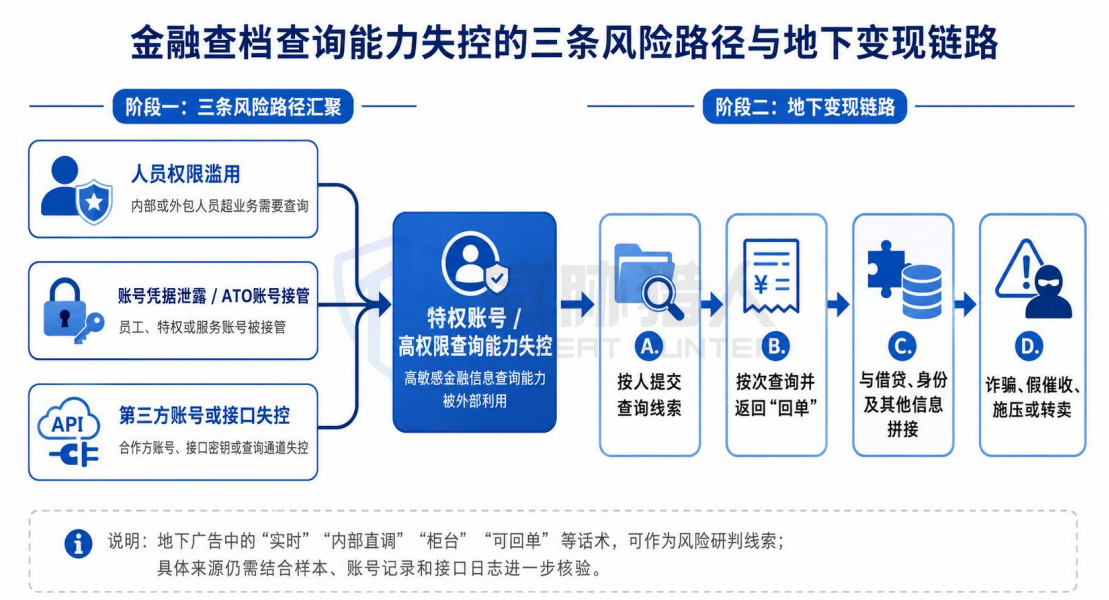
地下市场银行流水查询公开报价样本：

查询内容	可回溯范围	公开报价样本
银行流水	近1个月	110 USDT
银行流水	近3个月	170 USDT
银行流水	近6个月	220 USDT
银行流水	近12个月	260 USDT
银行流水	近36个月	415 USDT

3.3 金融查档的核心风险：查询能力被持续对外出售

金融查档与普通历史数据包倒卖的主要区别，在于卖家声称可以按人、按次持续返回查询结果。这种能力的形成路径并不单一：既可能是具备合法权限的人员违规查询，也可能是员工账号、特权账号或服务账号因凭据泄露、会话被窃取等原因遭到接管，还可能涉及外包账号、合作方账号或查询接口失控。

地下广告中的“实时”“内部直调”“柜台”“可回单”等话术，反映黑产试图将原本用于正常业务的查询权限转化为持续收费的地下服务。对于具备客户信息查询、结果导出或接口调用权限的账号，一旦发生权限滥用或账号接管，风险可能从单个账号失陷，进一步扩展为持续查询和批量外售数据的能力。



威胁猎人 ATO 监测关注外部泄露的账号、密码及相关身份标识，并结合员工邮箱、手机号、UID、登录行为和高价值账号标签进行二次匹配，用于识别具备真实接管可能的账号风险。若命中账号同时具备客户信息查询、数据导出或接口调用权限，其危害可能由单一账号失陷进一步扩大为高权限查询能力被滥用。

3.4 数据安全责任进一步落实至业务、技术和运维责任人员

地下金融查档反映的是查询权限和敏感信息可能被外部利用的风险，近期数据安全处罚案例进一步表明，银行与支付机构的数据安全责任不仅由机构承担，也进一步落实至相关业务、技术和运维责任人员。

需要说明的是，以下处罚案例并不一定直接对应非法查档事件，但其涉及的数据安全管理、权限控制、第三方风险及责任人员问责，与金融查档暴露出的治理问题具有较强关联。

银行机构数据安全“双罚”案例

2026 年 2 月，北京某银行因违反数据安全管理相关规定被罚款 100 万元，零售金融及运行维护相关责任人员分别被罚款 14 万元。该案例表明，数据安全责任不仅由机构承担，还会进一步落实到业务部门和科技运维岗位。

2026 年以来，银行业已出现多起涉及数据安全和个人信息保护的监管处罚案例，部分罚单直接涉及第三方合作数据安全风险管控、权限管理和数据治理机制不足等问题。

支付机构数据安全责任人员处罚案例

某支付机构因账户管理、清算管理、数据安全管理等违规被处罚，相关技术责任人员亦因对数据安全违规负有责任受到处罚。该案例表明，支付机构的数据安全责任同样可能穿透至技术和系统管理岗位。

综合来看，非法查档正由单项信息查询向多字段拼接和个人金融画像扩展，尤其是银行卡、账户余额、流水、征信及支付交易等金融信息，兼具敏感度高、可直接变现和危害持续的特点；相关处罚案例也表明，金融数据安全责任已由机构层面进一步延伸至相关业务、技术和运维责任人员。

结语

本报告由威胁猎人反欺诈情报研究团队基于长期监测数据、真实风险样本与行业治理实践编写。2026 年上半年，地下数据交易市场持续处于高位，暗网在数据流通渠道中的占比明显提升，第三方供应链成为借贷数据泄露的重要来源，金融相关数据仍是地下交易中的重点品类。

借贷数据外流后的风险已不止于一次泄露，而是可能被反复转卖，并通过查档补充账户、资产和交易信息，逐步形成个人金融画像；金融查档中按人、按次返回结果的交易方式，也反映黑产正由出售静态数据包向出售查询能力延伸，背后可能涉及特权权限滥用、账号接管或接口失控。相关监管案例同时表明，金融数据安全责任正由机构层面进一步延伸至相关业务、技术和运维责任人员。

希望本报告能够帮助安全、风控及业务从业者更准确地理解企业数据泄露风险变化，识别不同行业的主要风险结构与形成路径，并为企业制定更具针对性的数据安全保护和外部风险治理策略提供参考。

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