威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

2025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。

前言

在数字化浪潮持续推进的 2025 年上半年，数据作为企业核心资产，其安全问题愈发受到各方关注。数据泄露事件数量持续高位运行，攻击方式与交易链条也愈发复杂隐蔽，已成为威胁企业合规经营与业务增长的重大风险点。

威胁猎人《2025 年上半年数据泄露风险态势报告》聚焦当前数据泄露风险的变化趋势，从事件规模、行业分布、交易渠道到典型案例，系统剖析数据黑产产业链条的最新动向，全面展现 2025 年上半年国内数据泄露风险态势全貌。

报告内容关键点总结：

1. **数据泄露事件数量维持高位，短期波动后快速回升**

2025 年上半年共监测到 57,092 起有效数据泄露事件，较 2024 年下半年增长 1.54%。其中，4 月受 Telegram“封群行动”影响，事件量短暂下降近 30%，但 6 月因黑产团伙重组活跃，事件量快速反弹。

2. **高价值行业成为重点攻击目标，跨境电商泄露增长显著**

电商、消费金融、银行三大行业仍为重灾区，TOP3 行业事件总量为其余 TOP10 行业的 1.32 倍。电商行业中，跨境电商事件量环比增长超 10 倍，呈现明显国际化趋势。

3. **暗网泄露事件增长 35.2%，中文论坛活跃度大幅提升**

暗网渠道共监测到 18,106 起泄露事件，环比增长 35.2%。“长安**城”“D***Chinese”等中文暗网论坛用户快速增长，新注册用户贡献事件占比超过一半，泄露数据以境外平台信息为主。

4. “好旺担保”倒下，“土豆担保”迅速补位，担保平台替代性强

Telegram 头部担保平台“好旺担保”于 5 月被重点打击后业务瘫痪，但 6 月“土豆担保”等新平台快速填补空缺，反映黑产市场供需两端高度活跃，交易链条具备强“自愈能力”。

5. BF 关停后多平台接棒，黑产交易迁移性显著

BF 在停运前贡献了暗网 14.5%的泄露事件。平台关停后，核心用户快速迁移至 X*S、D**s 等替代平台，数据交易行为持续延续，显示出黑产用户强适应性与迁移效率。

6. 信贷风控数据“多头借贷”类泄露事件激增，构建完整产业链

以“多头借贷”为代表的信贷风控类数据泄露事件半年内增长 6 倍，形成覆盖数据窃取、平台搭建、精准诈骗的完整黑产生态。多个风控系统平台如“扶摇”“鑫辰”等已被黑产用作数据中转站。

7. 银行“扫码申请”类型数据泄露上涨超 4 倍，关联第三方营销工具

“扫码申请”类贷款信息泄露事件上半年达 111 起，关联超 80 家银行。风险核心源自某金融科技营销平台，涉及银行客户经理业务系统，疑因内鬼或系统漏洞导致高意向客户数据流入黑市。

目录

01

2025 年上半年
数据泄露风险概况

一、2025 年上半年数据泄露风险概况

1.1 2025 年上半年数据泄露事件共 57092 起，较 2024 年下半年上升 1.54%

据威胁猎人数据泄露风险监测平台数据显示，2025 年 1 月至 6 月期间，全网共监测到 1.8 亿条情报线索。经真实性验证引擎与 DRRC 人工分析，其中确认为有效的数据泄露事件共计 57,092 起。

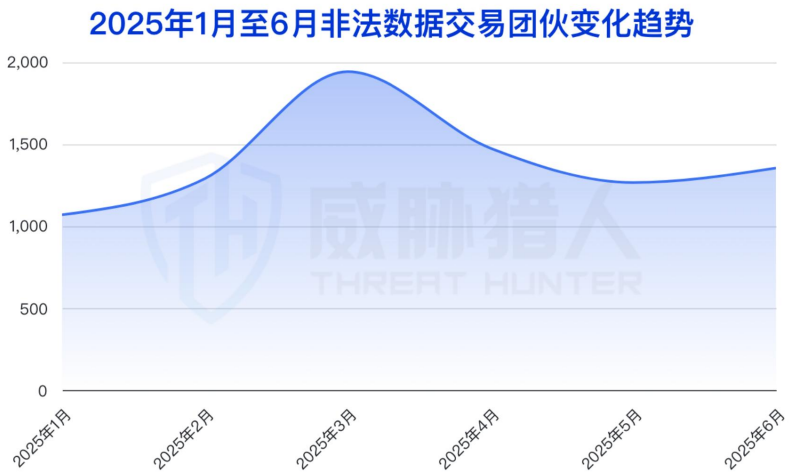
威胁猎人观察发现，2025 年 1 月至 3 月，数据泄露事件量呈现逐渐上升态势。然而，4 月份事件量较 3 月骤降 29.93%，减少了 3,882 起。5 月达到最低点，仅为 7,609 起，随后在 6 月开始回升。

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（详见本报告 2.1 章节）。从数据泄露源头进一步分析了解发现：

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，共计 9,085 起，环比 3 月（12,967 起）下降 29.93%。与之对应，活跃的非法数据交易团伙数量也从 1,943 个下降至 1,477 个，降幅为 23.98%。

同时，在 3 月份活跃的非法数据交易团伙中，有 33.71%的非法交易团伙在 4 月遭遇封禁。

受此影响，数据泄露事件数量出现明显下降。



然而，由于 Telegram 平台的封禁难以彻底，且非法团伙具备极强的“再生能力”，大量新群或替代群在短时间内重新活跃，推动了 2025 年 6 月数据泄露事件数量重新回升。

1.2 2025 年上半年 Top3 行业数据泄露事件量为其余 Top10 行业的 1.32 倍，攻击团伙更偏好高净值、高活跃度数据目标事件

从行业分布来看，2025 年上半年全网数据泄露事件共涉及 76 个行业，TOP3 行业是电商、消费金融、银行。

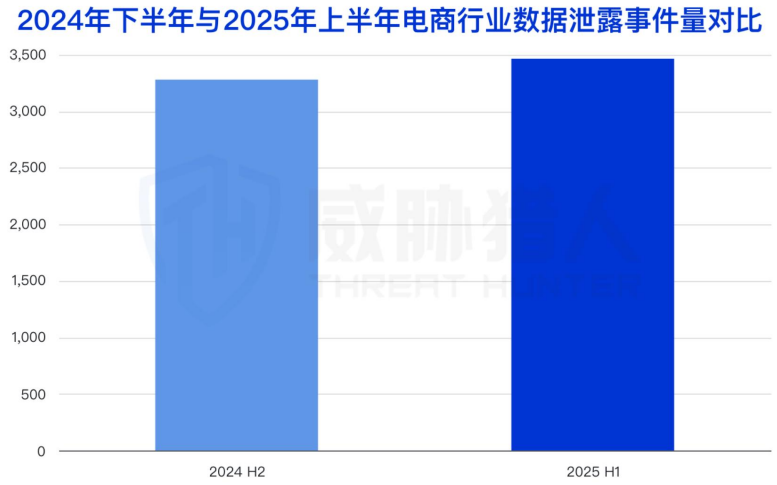
其中，以电商、金融为代表的高敏感度、高变现率行业，仍然是数据泄露的重灾区。

2025 年上半年 TOP10 行业排名变化情况如下：

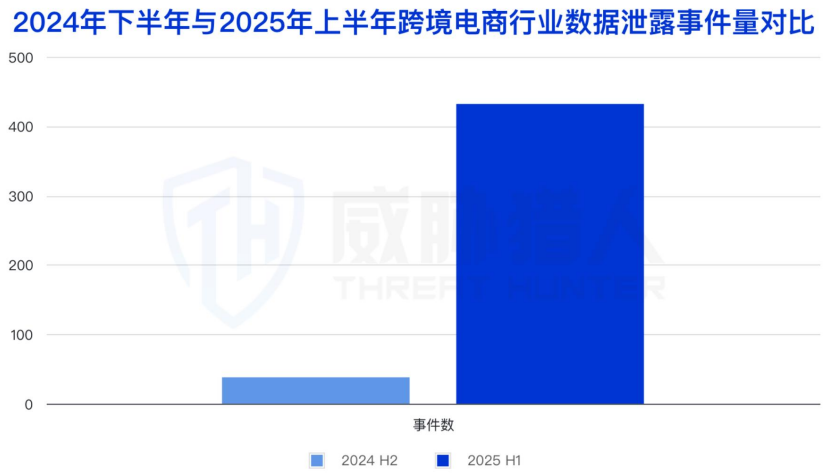
行业	2024年下半年排名	2025年上半年排名	排名变化
电商	3	1	↑2
消费金融	1	2	↓1
银行	2	3	↓1
快递	4	4	-
证券	5	5	-
社交软件	11	6	↑5
软件应用	10	7	↑3
保险	8	8	-
在线票务	6	9	↑3
汽车品牌	7	10	↓3

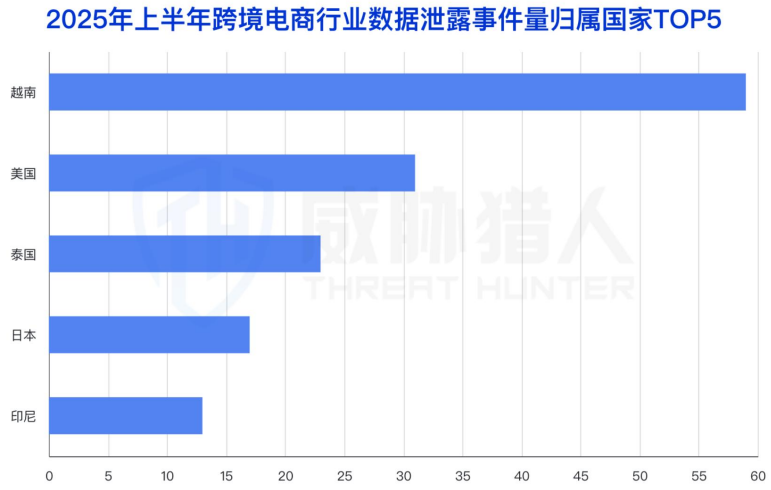
1.3 电商行业成为数据泄露事件数量 Top1 行业，事件量达 3,465 起，跨境电商泄露事件环比增长超 10 倍

威胁猎人数据泄露风险监测平台数据显示，2025 年上半年电商行业共发生 3,465 起数据泄露事件，较 2024 年下半年增加 184 起，增长 5.60%。



其中，跨境电商领域的数据泄露事件尤为突出，事件量较 2024 年下半年增加 394 起，涨幅超过 10 倍。泄露事件涉及全球多个国家和地区，主要集中在东南亚一带，TOP3 国家为越南、美国和泰国。





1.3.1 典型案例分析：多家跨境电商购物用户信息泄露，原因为第三方物流安全防护缺陷

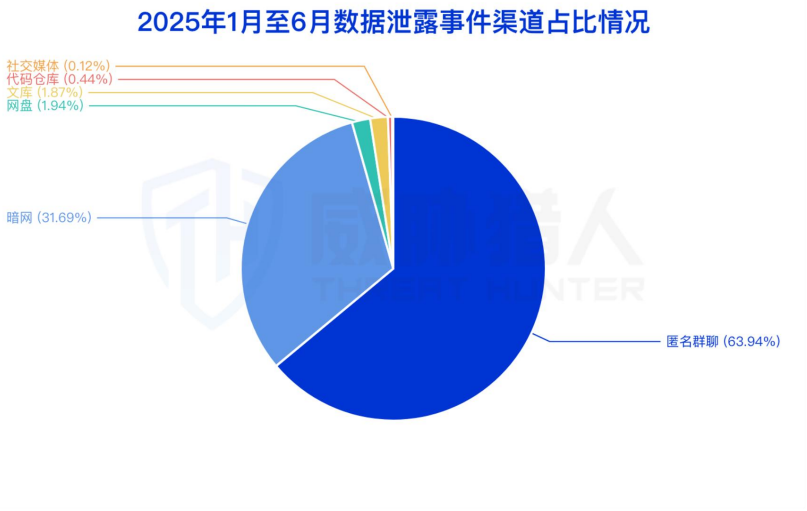
威胁猎人近期监测发现，暗网上有黑产团伙正在出售某跨境电商平台的用户网购信息数据。该发布者提供了部分数据样本，并声称数据覆盖东南亚、北美等多个国家和地区。

威胁猎人研究人员通过分析泄露数据中的“快递标签”“商品标签”等字段，推断该数据疑似来源于同一家国际快递物流公司。结合此前在暗网中文论坛监测到的该公司相关泄露事件，进一步确认应为该企业系统存在安全防护缺陷，被外部黑产团伙利用该漏洞实施攻击并获取了相关用户信息。

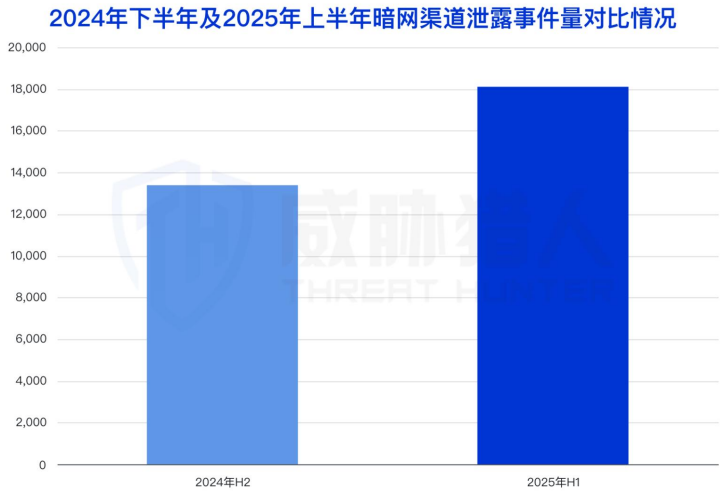
国家	订单号	交易号	订单状态	客户	ID	发货时间	仓库	创建时间	物流	快递号	商品名称	图片路径	价格	同步ERP	同步时间	快递标签	电话
新加坡	JOAS29	QW347	发货成功	香港xxx	Alexand	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	JIOA30	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS29	QW347	发货成功	香港xxx	Oscar	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	DAJOD3	https://c	382.4	同步成功	#######	https://t	237482
新加坡	JOAS29	QW347	发货成功	香港xxx	Elijah	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	QOU1J3	https://c	382.4	同步成功	#######	https://t	237482
新加坡	JOAS29	QW347	发货成功	香港xxx	Cedric	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	AU249	https://c	382.4	同步成功	#######	https://t	237482
新加坡	JOAS29	QW347	发货成功	香港xxx	Emma	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	HDAOO	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS29	QW347	发货成功	香港xxx	Charlott	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	QOU1J3	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS74	QW347	发货成功	香港xxx	Sophia	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	QOU1J3	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS74	QW347	发货成功	香港xxx	Eleanor	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	QOU1J3	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS74	QW347	发货成功	香港xxx	Taylor	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	HDAOO	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS74	QW347	发货成功	香港xxx	Quinn	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	HDAOO	https://c	382.4	同步成功	#######	https://t	237482
新加坡	JOAS74	QW347	发货成功	香港xxx	Alex	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	HDAOO	https://c	382.4	同步成功	#######	https://t	34720
新加坡	JOAS74	QW347	发货成功	香港xxx	Morgan	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	DAJOD3	https://c	382.4	同步成功	#######	https://t	34720
新加坡	JOAS74	QW347	发货成功	香港xxx	Casey	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	DAJOD3	https://c	39	同步成功	#######	https://t	34720
新加坡	JOAS74	QW347	发货成功	香港xxx	Camero	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	DAJOD3	https://c	39	同步成功	#######	https://t	34720

1.4 2025 年上半年暗网数据泄露活跃度持续攀升，事件量环比上升 35.2%

威胁猎人统计数据显示，2025 年上半年， 匿名群聊与暗网仍是数据泄露的主要渠道。



值得关注的是，暗网渠道共计发生 18,106 起数据泄露事件。与 2024 年下半年监测到的 13,389 起相比，事件总量增长了 35.2%。



1.4.1 中文暗网论坛活跃激增，泄露事件主要指向境外用户数据

威胁猎人进一步分析发现，“长安**城”论坛是暗网渠道中数据泄露事件量增长最多的平台。2025年上半年其贡献的数据泄露事件较 2024 年下半年增长 81.7%，1,493 起。与此同时，另一中文论坛“中**坛(D***Chinese)”的事件量也从 2024 年的 272 起增长至 560 起，涨幅超过一倍，达到 105.9%。

这两个中文暗网论坛在 2025 年共有 271 名用户发布数据交易贴，其中新注册用户达 166 人，占比达 61.3%；这些新用户发布的内容共计涉及 1,961 起数据泄露事件，占两大论坛的整体事件数一半以上。

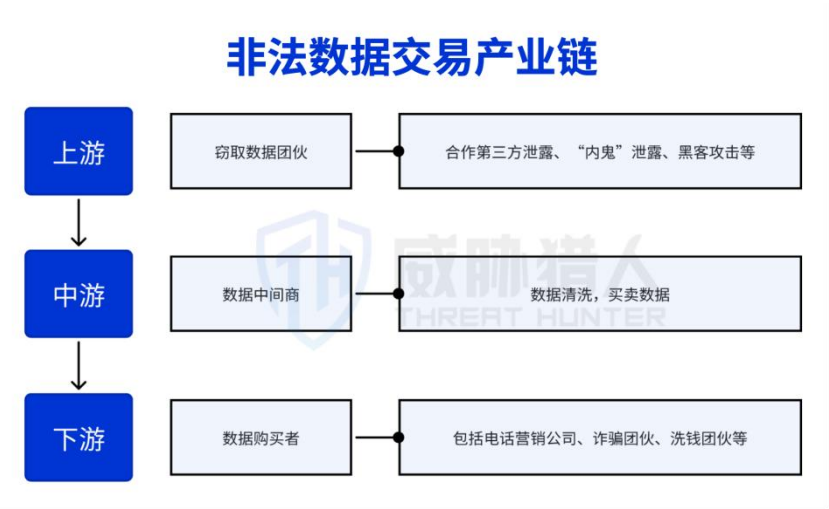
这些新增的数据泄露事件多数为境外平台或用户的数据信息泄露，其中“长安**城”单个平台就涉及来自全球超过 20 个国家和地区的用户数据。

02

2025 年上半年
数据交易市场动向分析

二、2025 年上半年数据交易市场动向分析

以下是非法数据交易产业链：

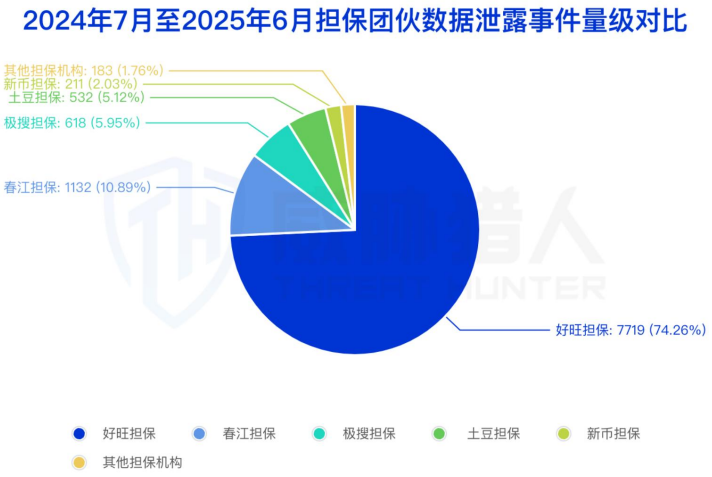


其中，中游的数据中间商活跃于暗网、黑产论坛、Telegram、Potato 等平台，负责对泄露数据进行清洗、分类、打包与撮合交易，是整个交易链条的关键枢纽。

尽管监管压力持续加大，但下游诈骗团伙、灰产电商等对高质量数据的需求始终旺盛，促使数据交易市场持续活跃。

2.1 头部担保团伙遭打击，新担保迅速补位

“好旺担保”（前身为“汇旺担保”）曾长期活跃于 Telegram 等匿名社交平台，凭借第三方信用中介服务，成为数据交易、诈骗、洗钱等黑产活动的核心担保平台，在 2025 年上半年以前处于市场主导地位。详情可查看：



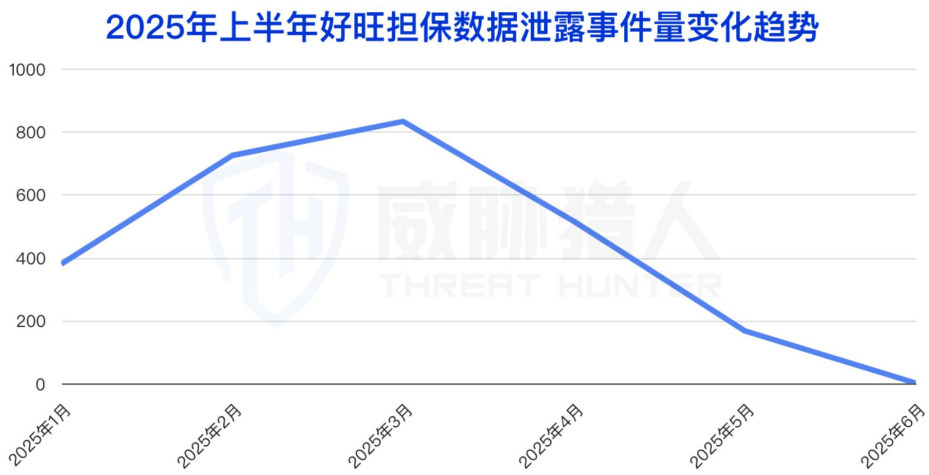
然而，在 2025 年 5 月，好旺担保遭遇重创：

- 5 月 1 日，美国金融犯罪执法网络（FinCEN）将其母公司 Huione 集团列为“首要洗钱关注”机构，切断其国际金融通道。随后 Telegram 官方于 5 月初集中封禁其交易群组及账号。

- 5 月 9 日，好旺官方发布公告称“交易员账号被大量注销”，至此，其运营体系全面崩溃，公群业务中断率达到 100%。

（好旺担保迁移全过程时间线）

威胁猎人监测发现，自“好旺担保”停运后，其相关数据泄露事件量从 3 月的 832 件直线下降，至 6 月基本归零。



但黑产市场的需求并未消失。“好旺担保”倒下后，以“土豆担保”为代表的等新平台迅速崛起。数据显示，土豆担保涉及的相关的数据泄露事件从 4 月的 12 起暴增至 6 月的 358 起，增幅接近 30 倍。

在非法数据交易市场中，数据供给端和需求端都高度活跃，形成了强烈的供需关系，也催生了完整的黑产交易链条。然而，由于交易本身存在高风险与高不确定性，买卖双方难以建立直接信任关系。

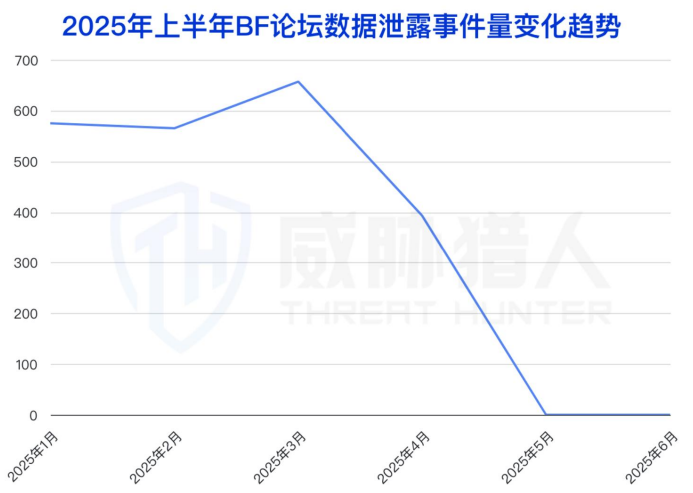
因此，黑产生态中逐渐出现了“担保平台”这一中介角色，中间商的存在不仅撮合交易，还承担着托管资金、仲裁纠纷的职能，是整个黑产交易能够持续运转的重要支点。正因如此，哪怕某个平台被打击清除，新的中间商也会迅速补位、变换马甲再次出现，只要交易存在，市场对这类“黑产服务商”的需求就不会消失，使得他们很难被彻底根除。

2.2 黑产平台可打击，交易需求难根除

2.2.1 头部论坛遭打击，供给量骤降；关停前贡献暗网渠道近 15%数据事件

尽管黑产平台面临持续高压打击，但数据交易的市场需求始终未见减弱。以头部暗网论坛 BF 为例，2025 年上半年，该平台依然是全球范围内最主要的数据泄露供给节点之一。

威胁猎人监测数据显示，2025 年 1 月至 6 月，暗网渠道共计贡献数据泄露事件 15,096 起，其中 BF 平台贡献 2,190 起，占暗网事件总量的 14.5%。尤其是在停运前的前三个月，BF 平台活跃度持续上升，2025 年 3 月更是达到月度峰值 657 起。



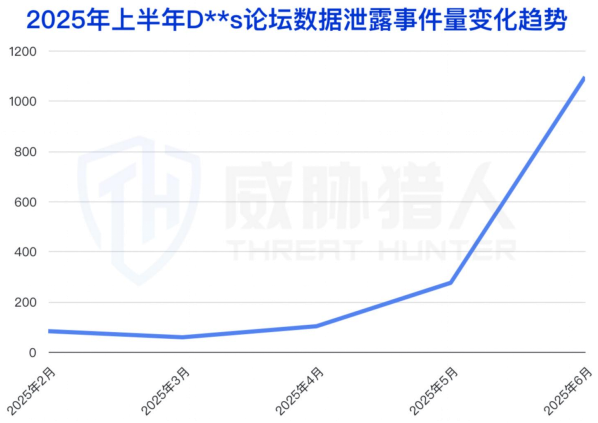
然而，随着 BF 于 4 月 15 日突遭关停，其相关数据泄露事件量迅速下滑，4 月仅监测到 393 起，环比下降 43.2%，5 月事件量归零；平台供给能力出现明显断崖式下跌。

2.2.2 BF 平台停运后，多个替代论坛快速接棒

尽管如此，BF 关停并未打击黑产的整体活跃度，而是迅速转移至其他暗网平台与私密通信工具。

以威胁猎人观察到的以下平台数据为例：

- D**s 论坛： 4 月事件量即突破 100 起，5 月飙升至 275 起（较 3 月增长 374%），6 月更暴涨至 1,095 起，较关停前增长近 20 倍；



- R**d 论坛： 虽在 4 月受 BF 影响短暂下滑，但 5–6 月强势反弹，6 月泄露事件量较 4 月增长 138%；

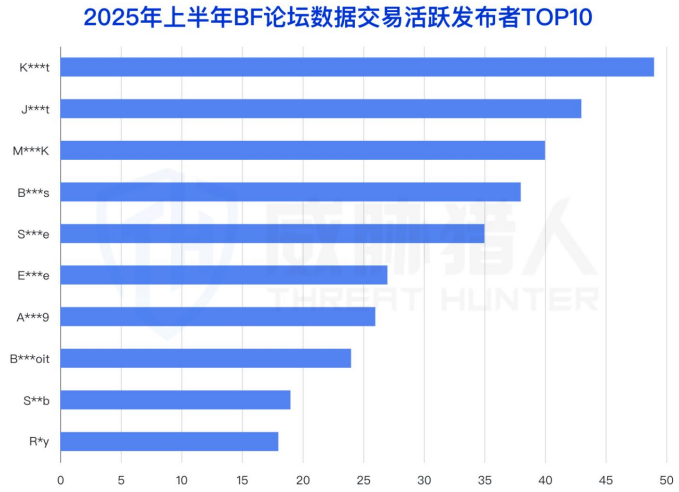
- X*S 论坛： 此前活跃度极低（1–3 月月均仅 13 起数据泄露事件），5–6 月激增至 48 起和 67 起，环比增长超 400%；

- E**t 论坛： 4 月事件量升至 70 起（较 3 月增长 169%），6 月达到 110 起，呈现稳步上升趋势。

上述数据表明，黑产生态具备强烈的“自我修复”能力，平台虽然被打击，但流量、资源与参与者很快在新平台重建，市场热度恢复迅速。

2.2.3 BF 平台核心用户快速迁移，黑产活动延续性强

威胁猎人追踪发现，BF 前十大核心发布者（贡献平台 14.6%的事件量）在平台关停后迅速转移至其他平台继续活跃。



以 BF 上半年最活跃用户 K*t 为例：**

“K***t”自 BF 停运后无缝转移至 XSS 论坛，继续发布境外用户数据、购物订单、CRM 系统信息等，数据类型丰富，覆盖多国多行业；

其发帖频率高、数据结构标准化，疑似具备较强的数据清洗与分发能力，是典型的“职业数据搬运者”，显示出对黑市交易平台极强的适应能力与迁移效率。

该趋势表明：黑产核心从业者具备极强的迁移性与复原力，只要数据交易需求存在，他们即可迅速重建交易渠道，保持黑产市场活跃。

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 年上半年数据泄露交易市场研究新趋势

三、2025 年上半年数据泄露交易市场研究新趋势

3.1 信贷风控审批场景下数据泄露风险态势与产业生态解析

3.1.1 公民多头借贷数据泄露事件较 2024 年下半年大幅上升，涨幅超 6 倍

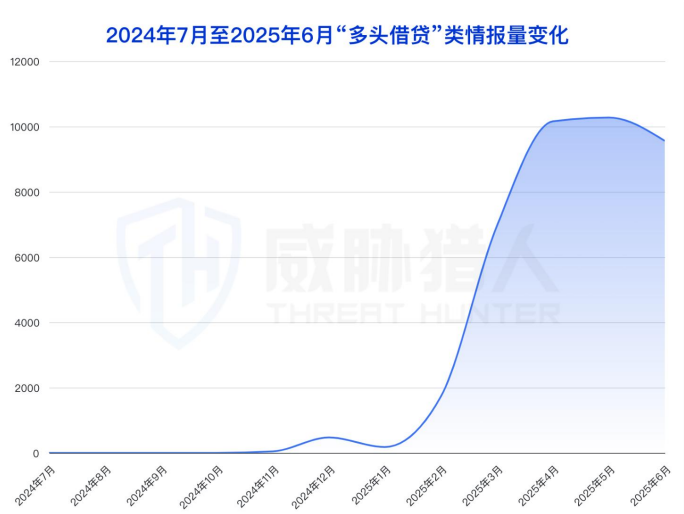
一类名为“多头借贷”的贷款信息数据泄露事件共计 117 起，相较于 2024 年下半年新增 101 起，涨幅高达 631.25%。

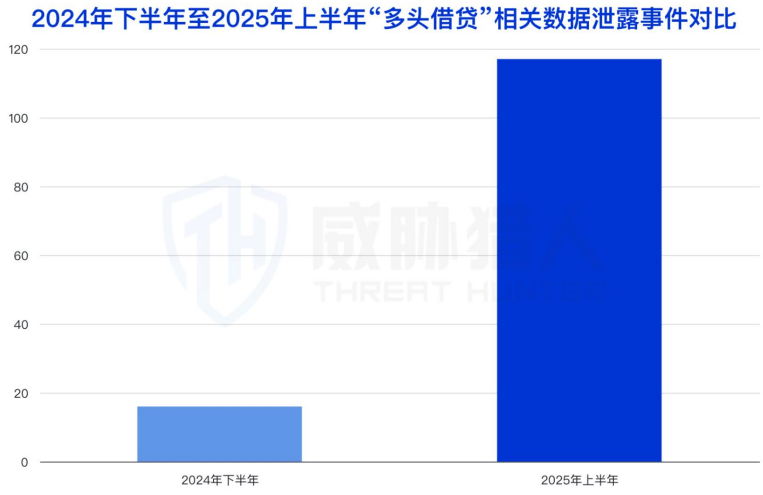
针对信贷“多头借贷”类风险情报的捕获数据显示，自 2024 年 11 月以来，此类数据泄露事件基本呈现持续上升的趋势。

多头借贷：是指一种专门侦测借款人“多头借贷”行为的风控机制，实际上是由第三方数据服务商与多家网贷公司共同建立的数据共享系统。当一个借款人向其中一家机构发起贷款申请时，这个"申请行为"本身会像一个信号一样，被系统捕捉到并记录下来。实际上就是指借款人多头借款的记录信息数据。

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；

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，排除历史虚假数据、确认有效的数据泄露事件；





通过深入分析，威胁猎人了解到黑产中所称的“多头借贷”数据，其核心内容主要涵盖贷款用户的还款履约情况及逾期记录。在当下信贷风控场景中，“多头借贷”数据扮演着关键角色，它能够反映借款人的“多头借贷”行为，即用户在不同平台申请或持有贷款的情况。这种数据被非法利用时，会对信贷机构的决策造成严重影响，可能导致风险评估失真，同时也会导致用户个人隐私信息泄露，遭遇精准营销或诈骗等情况。

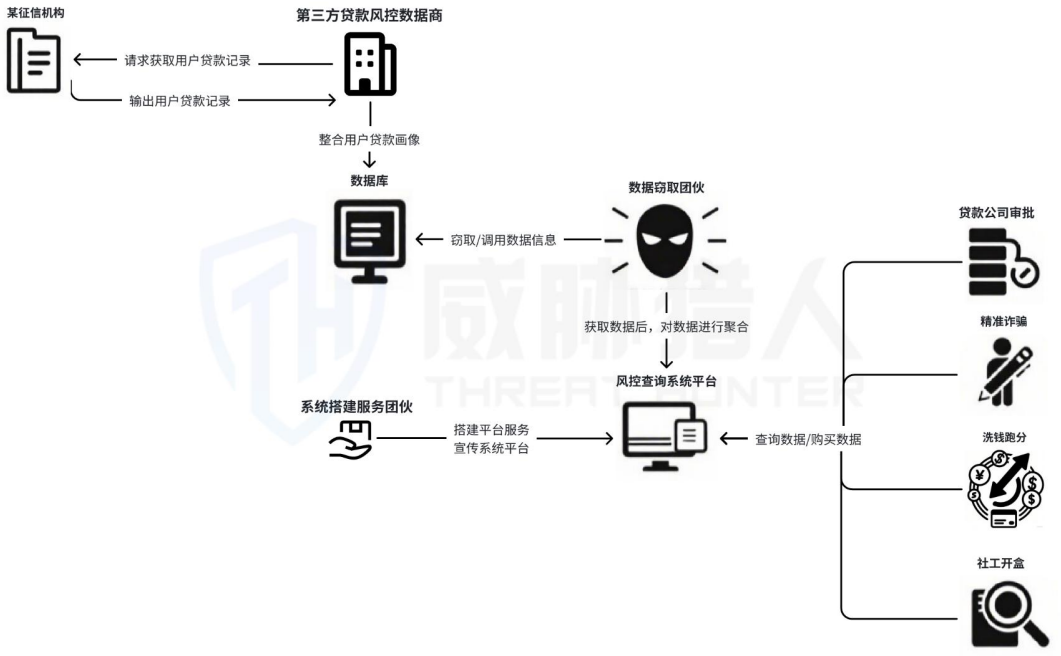
姓名	身份证	号码1	号码2	0：代表查无数据	最大履约金额	履约笔数	当前逾期机构数	睡眠机构数	当前履约机构	最近履约时间	异常还款机构	最大逾期金额	最长逾期天数	最近逾期时间
王			4	2	40	16	0	4	9	2025-01	0	NULL	NULL	NULL
韩			8	2	80	0 11	0	3	8	2025-02	0	NULL	NULL	NULL
刘			4	2	60	32	0	16	15	2025-02	0	NULL	NULL	NULL
王			1	2	10	00 14	0	6	8	2025-01	0	NULL	NULL	NULL
杨			0	2	40	22	0	4	14	2025-02	0	NULL	NULL	NULL
方			7	2	80	0 47	0	31	31	2025-02	0	NULL	NULL	NULL
高			2	2	80	0 21	0	9	14	2025-02	0	NULL	NULL	NULL
戴			8	2	10	00 43	0	8	15	2025-01	0	NULL	NULL	NULL
谷			6	2	10	00 160	0	27	59	2025-02	0	NULL	NULL	NULL
关			7	3	60	33	0	11	11	2025-01	0	NULL	NULL	NULL
桂			4	2	60	10	0	8	9	2025-02	0	NULL	NULL	NULL
龚			3	2	10	00 33	0	9	14	2025-02	0	NULL	NULL	NULL
龚			5	2	10	00 46	0	18	28	2025-02	0	NULL	NULL	NULL
龚			2	2	80	0 79	0	23	28	2025-02	0	NULL	NULL	NULL
龚			9	2	10	00 35	0	5	16	2025-02	0	NULL	NULL	NULL
龚			2	2	10	00 19	0	7	14	2025-02	0	NULL	NULL	NULL
韩			9	2	80	0 8	0	4	6	2025-01	0	NULL	NULL	NULL
韩			5	2	10	00 130	0	41	48	2025-02	0	NULL	NULL	NULL
蔡			2	2	10	00 30	0	17	20	2025-02	0	NULL	NULL	NULL
何			6	2	40	30	0	6	15	2025-02	0	NULL	NULL	NULL
何			8	2	40	7	0	0	6	2025-02	0	NULL	NULL	NULL

（威胁猎人捕获的泄露数据中包含用户履约信息）

3.1.2 以“借款记录信息”类数据为核心的信贷风控产业链已然形成

根据威胁猎人深入调查研究发现，一个以“借款记录信息”类数据为核心的地下信贷风控黑产产业链已然形成，其运作模式涵盖了数据窃取、平台搭建、数据售卖，以及下游的精准营销、诈骗等一系列非法活动。

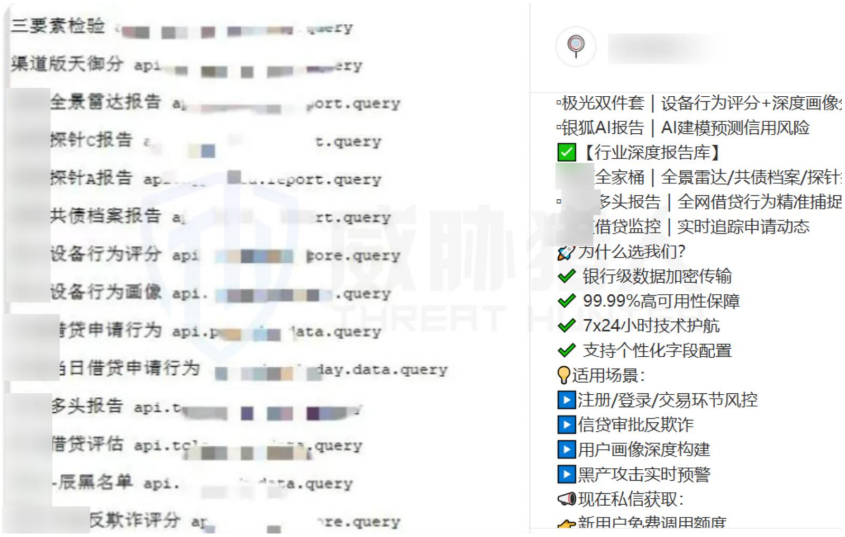
具体产业链情况如下所示：



1.上游：来源主要以征信机构、第三方持牌风控数据商为主

通过深入分析，威胁猎人了解到黑产中所称的“多头借贷”数据，其核心内容主要涵盖贷款用户的还款履约情况及逾期记录。在当下信贷风控场景中，“多头借贷”数据扮演着关键角色，它能够反映借款人的“多头借贷”行为，即用户在不同平台申请或持有贷款的情况。这种数据被非法利用时，会对信贷机构的决策造成严重影响，可能导致风险评估失真，同时也会导致用户个人隐私信息泄露，遭遇精准营销或诈骗等情况。

同时，威胁猎人针对黑产提供的风控数据查询系统进行深入分析，其中所有用户的授权书均涉及国内某征信机构。

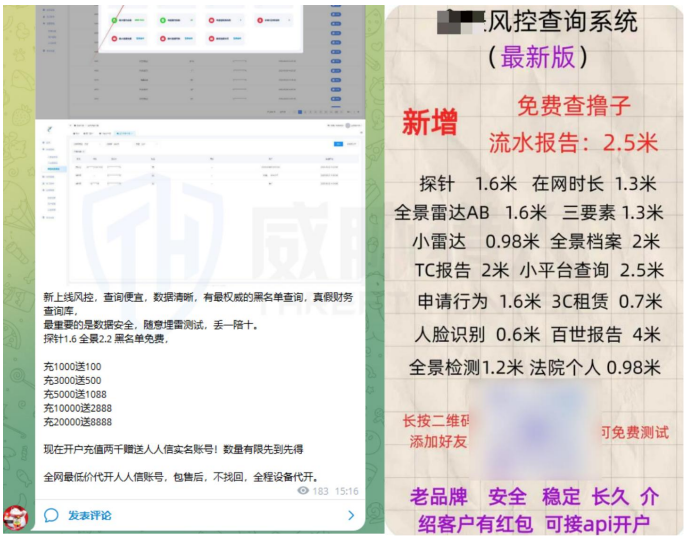


（某黑产发布的宣传广告信息，涉及某征信机构以及第三方风控数据商）

（与某黑产表示是某第三方持牌数据商公司）

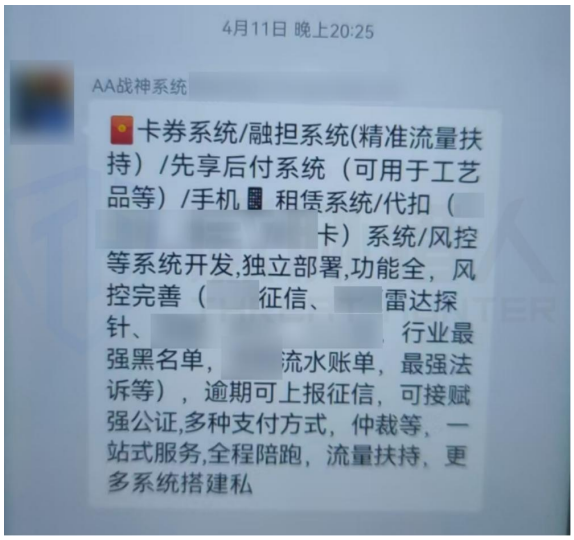
2.中游：催生多个风控数据查询服务平台以及平台搭建服务

威胁猎人观察到，受“多头借贷”类数据的影响，存在大量黑产出现宣传风控数据查询系统服务，或直接售卖贷款逾期用户信息数据。这些数据查询系统服务通常涵盖“多头借贷””、“三要素验证”等多种数据查询校验功能。威胁猎人所观察到的典型平台系统包括“扶*风控查询”、“亿*风控系统”、“鑫*风控查询系统”等。



（上图为黑产提供风控数据查询系统宣传）

同时，威胁猎人也注意到在微信等社交平台上，存在大量黑产宣传可协助中下游黑产团伙搭建相应的作恶平台，如“融担系统”、“租赁系统”、“风控系统”、“征信查询系统”、“借条查询系统”等多种类型。这些系统通常声称功能全面，风控完善，支持逾期上报征信、赋强公证等“一站式服务”，并提供“全程陪跑、流量扶持”。



（图为黑产团伙发布平台搭建服务宣传内容）

3.下游：助力精准营销、诈骗、洗钱等违法犯罪活动升级

据威胁猎人观察，下游接收并利用此类用户贷款资质信息记录的人群主要集中于以下几种类型：

1. **财务：**主要指中小型贷款平台的贷款审批人员，他们利用这些非法数据查询用户的资质情况，进行综合审批，或筛选出目标群体用户，从而进行精准营销；

2. **跑分人员：**主要为洗钱人员，在获取到数据后，通过获取用户信任后利用其银行卡进行非法资金流转，即所谓的“跑分”行为；

3. **诈骗人员：** 实施“杀鱼”（或称“鲨鱼”）行为，主要通过电信诈骗（包括贷款诈骗、冒充公检法等）对用户进行精准诈骗，利用非法获取的数据提高诈骗成功率。

4. **查档人员：**在数据交易查档场景中，有提供这种针对性查询开盒个人征信情况的业务，主要是通过提供用户姓名+身份证+手机号信息去调用上游数据查询，并返还对应的征信报告信息。

（左图为中游黑产表示数据适配于洗钱、诈骗等作恶行为，右图为查询输出个人征信报告）

附录：相关黑话词释义

威胁猎人针对“多头借贷”相关风险情报进行了深度调研与跟踪，以下是与“探针”相关的黑产常用黑话词汇释义

财务：又称“cw”，实际上是指高利贷/私人借贷平台人员。

融担：又称“融单”、“融蛋”、“RD”、融担指的是网贷平台的一个系列，该系列主要为诸多小型或微型的网贷 APP，这类平台申请流程简单，通过率高。因此“融担料”，实际上就是指小型网贷平台的用户信息数据。

借条：又称 JT，实际上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，而“借条料”，实际上就是指私人借贷或高利贷所签订“借条”的用户信息数据。

高炮：指高利贷平台或机构，高炮料则是指在高利贷平台进行贷款的用户信息数据。

租机：主要是指用户在租机平台进行分期租机的行为，这里面会涉及到用户办理租机贷业务，并且后续继续套现的行为。而租机料，实际上就是在租机平台办理分期业务的用户信息数据。

黄金：全称黄金商城，与租机套现的数据相似，实际上就是一些可以支持购买黄金并分期还款的平台，一般都是一些小型平台，黄金商城料则是在这些平台办理套现的用户信息数据。

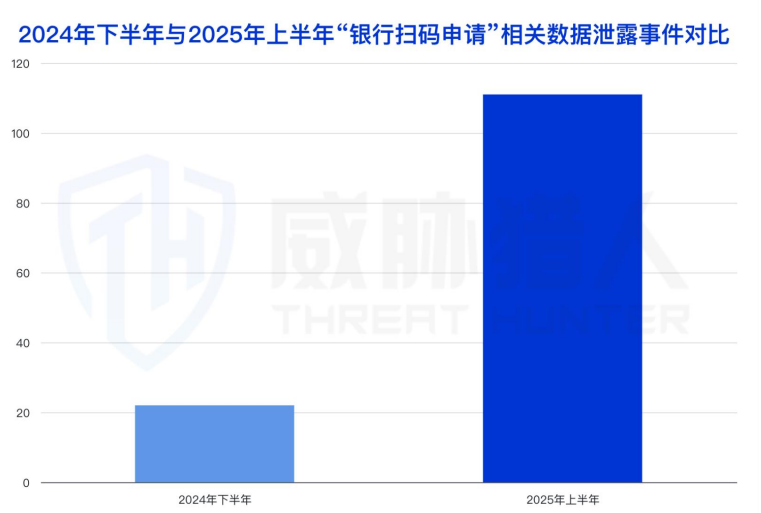
E 卡/卡券：与租机、黄金商城情况相似，即一些支持购买 E 卡或卡券红包等平台并允许分期还款的平台，一般都是一些小型平台，E 卡料则是在这些平台办理购买套现的用户信息数据。

3.2 银行“扫码申请”贷款信息泄露趋势与产业生态解析

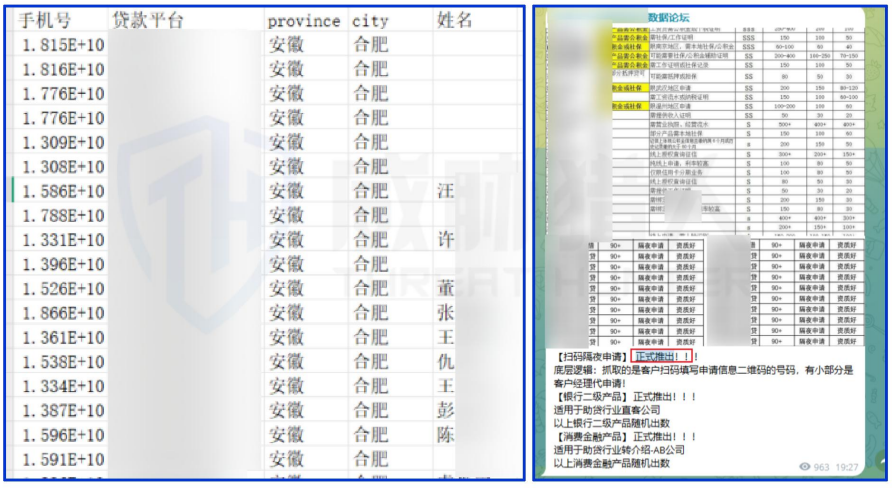
3.2.1 银行“扫码申请”贷款信息泄露事件较比 2024 年下半年大幅上升，涨幅超过 4 倍

威胁猎人持续监测发现，在 2025 年上半年所捕获的泄露数据中，还有另一类名为“银行扫码申请料”的贷款信息泄露事件，共计 111 起，相较于 2024 年下半年新增 89 起，涨幅高达 404.55%。

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。



通过深入分析，威胁猎人了解到黑产中所称的“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，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。

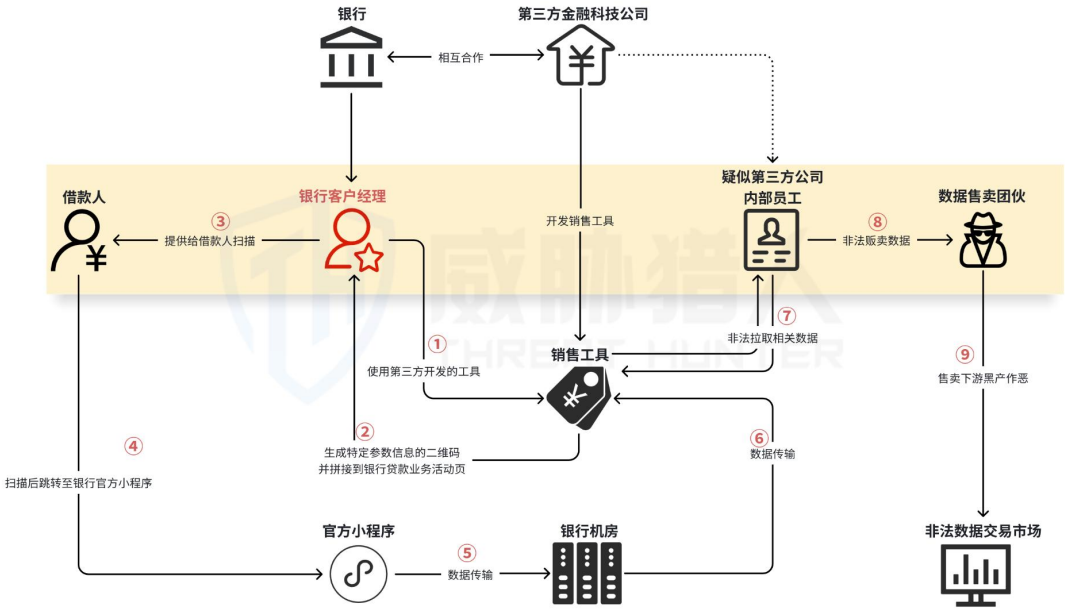


手机号	贷款平台	province	city	姓名
1.815E+10		安徽	合肥	
1.816E+10		安徽	合肥	
1.776E+10		安徽	合肥	
1.776E+10		安徽	合肥	
1.309E+10		安徽	合肥	
1.308E+10		安徽	合肥	
1.586E+10		安徽	合肥	汪
1.788E+10		安徽	合肥	
1.331E+10		安徽	合肥	许
1.396E+10		安徽	合肥	
1.526E+10		安徽	合肥	董
1.866E+10		安徽	合肥	张
1.361E+10		安徽	合肥	王
1.538E+10		安徽	合肥	仇
1.334E+10		安徽	合肥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

3.2.2 银行“扫码申请”贷款信息泄露：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

威胁猎人通过对泄露数据涉及到的银行二维码进行分析溯源，发现其均指向同一家知名金融科技服务商开发的“xx 营销助手”平台。结合黑产发布的银行贷款平台名单来看，可以确认影响范围超过 80 家银行机构。



（银行贷款申请信息泄露流程图）

基于该类相关事件涉及多家银行，根据威胁猎人针对具体细节进行深入还原发现：

1、用户在申请贷款的过程中，是通过扫描银行客户经理所提供的贷款业务活动二维码进行办理；

2、这一类银行贷款业务的二维码信息是携带客户经理信息，去跳转到银行官方的小程序上；

3、然后用户在银行官方小程序具体的贷款业务上操作提交贷款申请；

威胁猎人了解到客户经理所提供的贷款二维码信息，实际上是通过第三方金融科技公司开发的销售工具进行制作的。（基于该工具页面较为敏感，此处不做具体展示）

威胁猎人针对该第三方金融科技公司进行分析后发现，该公司不仅为银行提供应用系统软件开发，还提供智能风控策略。针对不同资质的贷款用户提供不同的风控策略，用于配合银行客户经理进行跟进。主要为银行提供业务数字化，推动银行贷款业务发展。用户在银行官方小程序提交地贷款申请后，银行会将用户相关信息同步至销售工具上，便于银行客户经理业绩统计以及跟进，与此同时也带来了数据泄露的风险。

隔夜申请平台推荐

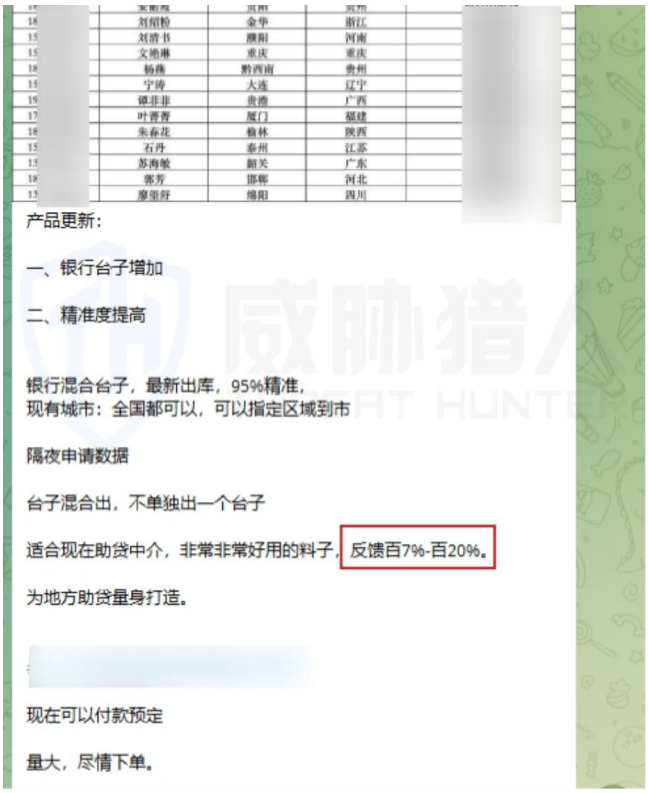
平台名称	是否需要公积金	其他材料/备注	推荐级别	每日出量（三网）不固定 预计出量		
				一线及高配二线	二线	三线及以下
	部分产品需公积金	本地户籍优先	SSS	200左右-300	100-200	40-100
	否	需银行流水或工资证明	SSS	200左右-300	100-200	40-100
	部分产品需公积金	需公积金或个税证明	sss	250-400	200	100
	部分产品需公积金	需社保/工作证明	SSS	150	100	50
	需公积金或社保	限南京地区，需本地社保/公积金	SSS	60-100	60	40
	部分产品需公积金	可能需要社保/公积金辅助证明	SS	200-400	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）

用户在银行官方小程序提交地贷款申请后，银行会将用户相关信息同步至销售工具上，便于银行客户经理业绩统计以及跟进，与此同时也带来了数据泄露的风险。

据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。

根据威胁猎人调研发现，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。同时，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。



风险与危害：

客户流失与营收损失： 高意向客户在申请次日即被竞争对手（助贷公司）联系，提供利率更低或审批更快的替代产品，直接导致银行潜在客户流失，损失可预期的利息收入和中间业务收入。

品牌声誉损害： 数据泄露严重打击了用户对银行数据安全能力的信任，尤其是在贷款这一核心业务上，将对银行品牌造成长期负面影响。”

监管合规风险： 此类事件已构成严重的个人金融信息泄露，违反了《个人信息保护法》等相关法规，银行作为数据处理者将面临高额罚款和监管问责的风险。

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

综上所述，2025 年上半年数据泄露风险态势依然严峻，整体事件量持续高位运行，产业链条高度成熟且具备强烈的“自我修复能力”；平台打击难以从根本遏制市场活跃度。

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。

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