威胁猎人
THREAT HUNTER

以 情 报 构 筑 数 字 化 安 全 基 石

2024 年
数据泄露风险态势报告

(2024 年 1 月 1 日至 2024 年 12 月 31 日)

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

在数字化时代浪潮中，数据已成为企业核心竞争力的关键要素。然而，数据泄露风险如同达摩克利斯之剑，高悬于各行业头顶。2024 年，数据泄露事件频发，波及众多企业，严重威胁用户隐私与企业利益。

威胁猎人《2024 年数据泄露风险态势报告》对 2024 年国内企业数据资产泄露风险概况、非法数据交易产业链等进行多维度分析，客观呈现 2024 年国内数据泄露风险态势全景。

报告内容关键点总结：

1.2024 年数据泄露风险态势依旧严峻，多个行业多家企业均存在数据泄露风险

2024 年全年监测到 37575 起有效数据泄露事件，涉及 2598 家企业，覆盖金融、电商、快递、汽车、本地生活等多个关键行业。

2.银行业再登数据泄露风险榜首，本地生活首次进入前十

2024 年银行业数据泄露事件数量高达 6333 起，连续两年位居榜首，金融行业数据安全管控迫在眉睫；本地生活行业数据泄露事件从 2023 年的 Top14 跃升至 Top10，2024 年共发现 700 多起事件，新型泄露类型“强登”是主要推手。

3.匿名群聊与暗网仍是主要泄露渠道，文库及网盘风险事件翻倍

2024 年数据泄露渠道仍以匿名群聊与暗网为主，二者总量占比 90.83%；文库及网盘渠道风险事件量翻倍增长，达 2714 起。

4.“私域群”、“担保”模式快速发展，非法数据交易更隐蔽且“规范化”

2024 年“私域群”、“担保”模式快速发展，在私域群中累计发现数据泄露风险事件 4193 起，黑产团伙数量突破 500 个，且超过一半的“私域群”由担保机构运作。

5.特权账号成攻击者利器，ATO 风险持续增长

2024 年 ATO 风险持续增长，仅一周超 470 万员工账号泄露，涉及社交、电商、金融、短视频等多个行业 21 万家企业。

6.新型数据泄露“强登”、“解密”兴起，涉及电商、外卖、快递等行业

2024 年，“查档”模式迅速发展，并出现“解密”与“强登”两种新型数据泄露方式。“强登”自 6 月起现身，先在电商巨头平台出现，后波及外卖、快递等多平台；“解密”则是黑产为破解隐私面单而生，近一年来，相关数据泄露事件呈上升趋势。

7.“IOS”字段相关风险事件下降，“扶贫”相关非法数据交易需求上涨

苹果官方针对 Facetime 诈骗的打击使得“IOS”字段风险事件下降，下半年较上半年下降 59.90%；同时，“扶贫”相关非法数据交易需求上涨。

目录

01

2024 年国内数据泄露风险概况

一、2024 年国内数据泄露风险概况

1.1 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。

威胁猎人发现，在 2024 年 2 月数据泄露事件量出现大幅下降（较 2024 年 1 月下降了 36%，共 898 起），在 11 月出现了较大幅度上升（较 2024 年 10 月上涨了 29.48%，共计 1096 起），从数据泄露源头进一步分析了解，主要原因如下：

2024 年 2 月，第三方泄露、短信通道泄露等不同原因所引发的数据泄露事件量均出现下降，可以看出 2024 年 2 月数据泄露事件大幅下降主要是受到春节期间黑产放假带来的交易为放缓的影响。

2024 年 11 月，非法数据交易团伙的活跃度有所增加，团伙数量相较于 10 月新增了 156 个非法数据交易团伙，这一增长导致了 11 月全网数据泄露事件数量明显上升。

1.2 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。

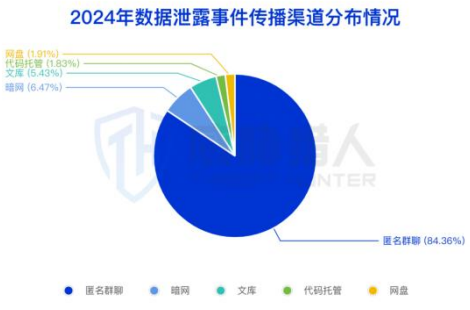
强登：指通过技术手段强制登录用户账号，获取用户账号中的隐私信息。

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。

注：关于“强登”的进一步信息请查看 2.2 章节。

1.3 匿名群聊与暗网仍是数据泄露的主要渠道，文库及网盘渠道事件翻倍增长

威胁猎人统计数据显示，2024 年数据泄露的主要渠道仍然是匿名群聊和暗网，占比高达 90.83%。值得关注的是，2024 年文库及网盘渠道泄露的风险事件量有 2714 起，占全渠道事件量的 7.34%，相比去年有了大幅提升。



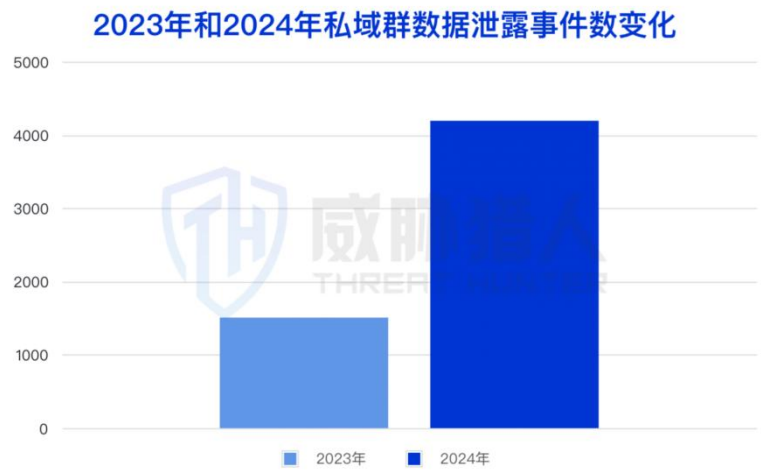
值得一提的事，自 2024 年 6 月起，威胁猎人数据泄露风险监测平台引入了大语言模型技术，利用大模型的智能筛选与海量数据分析能力，再结合威胁猎人 DRRC 专业团队的校验和判断，极大提升了来自文库及网盘渠道的风险文件审核效率和风险事件检出能力。

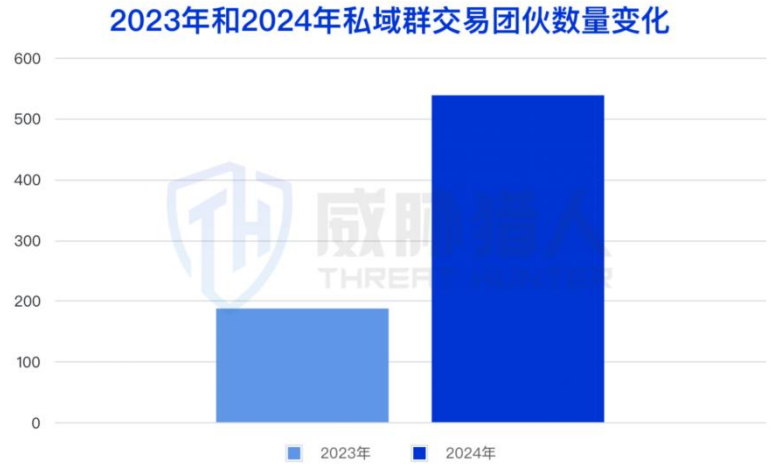
1.4 “私域群”、“担保”模式快速发展，非法数据交易更加隐蔽和规范化

随着非法数据交易的规模化和复杂化趋势加剧，愈来愈多的黑产团伙倾向于选择私域环境进行交易，使得交易更加隐蔽化、组织化和规范化。

威胁猎人数据统计，2024 年在 Telegram “私域群”中，累计发现数据泄露风险事件 4193 起，较 2023 年增长了 2.70 倍，“私域群”中的黑产团伙数量突破 500 个，是 2023 年的 2.88 倍。

私域群：需通过邀请链接/管理员同意后才能进入的群组，一般外部人员无法监测或进入该群聊，群组有管理员定期清洗群成员名单，一定程度上过滤了广告、机器人、二道贩子、中介等可信度较低的人员，群组内容质量更接近真实数据泄露源头。





威胁猎人情报人员针对“私域群”内的数据泄露事件和黑产团伙进一步分析发现：

1）黑产团伙在“私域群”中通过加密消息、暗号和私密聊天等方式与买家进行交流联络，使黑产非法交易更加难以被监管机构察觉。

2）超过一半的“私域群”由担保机构运作。

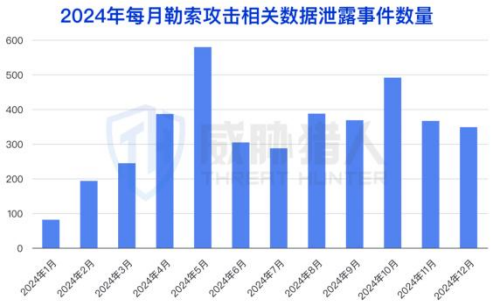
担保机构：在非法数据交易中扮演“中间人”的角色，负责验证交易双方的资质、监督交易过程并确保交易的顺利完成。这种模式提高了交易双方的信任度、非法数据交易流程更加“规范”，一定程度上保障了非法数据交易的顺利进行。

威胁猎人对担保团伙进一步分析，在当前众多担保团伙中，前三大担保团伙分别是“好旺担保”（原汇旺担保）、“新币担保”和“春江担保”。其中，“好旺担保”在担保团伙中占据主导地位，由其担保的非法数据交易事件量占比高达 94.34%，可谓“一家独大”。

值得关注的是，为规避监管打击，“原汇旺担保”在 2024 年 10 月 19 日正式改名为“好旺担保”。

1.5 勒索攻击导致的数据泄露事件共 4034 起，涉及制造业、金融、房地产等行业

2024 年，威胁猎人捕获到由勒索攻击导致的数据泄露事件共 4034 起，涉及全球多个行业，排名前三的行业是制造业、金融、房地产。



1.6 特权账号成攻击者利器，ATO 风险持续增长

注：鉴于特权账号泄露事件的特殊性，威胁猎人捕获相关情报后，将直接与合作客户沟通处理，故此类事件未纳入本次报告的总数据泄露事件统计。

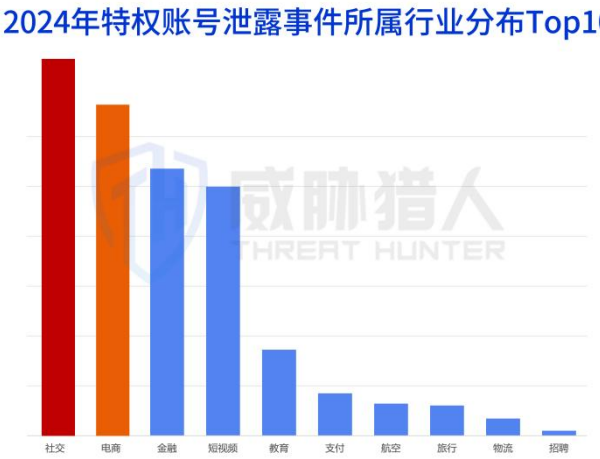
特权账号（Privileged Account）：指具有特殊权限的账号，通常拥有对系统、网络或数据的高级访问权限，如企业员工账号。特权账号存在权限大、分布散、数量多等特点，分布在业务系统、应用程序、数据库、网络设备等各类应用系统中，一旦账号被接管（账号接管 Account Takeover，ATO），可能导致敏感数据资源泄露、业务中断等后果。

对黑产团伙而言，与其穿透层层防护窃取数据，不如直接窃取账号，通过内网横向移动，利用特权账号的管控手段缺失攻破授权账号，最终利用特权账号权限对系统进行恶意破坏。

近年来，因账号权限管控不当或失窃导致的风险事件正在逐年上涨，IBM X-Force 最新发布的《2024 年威胁情报指数报告》中表示，攻击者使用被盗凭据访问有效账户的情况比去年增加了 71%，占 X-Force 在 2023 年应对的所有风险事件的 30%，与网络钓鱼并列成为头号感染媒介。

1.6.1 仅一周超 470 万员工账号泄露，涉及社交、电商等行业 21 万家企业

威胁猎人 ATO 情报服务持续对企业账号泄露风险进行监测，仅一周时间就监测到被泄露的企业员工账号数量超 470 万，涉及社交、电商、金融、短视频等行业近 21 万家企业。



注：统计图数据统计周期为 2024 年 2 月至 12 月。

1.6.2 Salesforce、HubSpot、Zoom 等第三方办公协同工具是账号泄露的高风险区

威胁猎人情报人员对已泄露的企业账号信息进一步分析发现，泄露的账号有大量外部软件账号，其 Salesforce 平台(客户关系管理 CRM)数量最多,其次是 HubSpot 平台(客户关系管理 CRM)、Zoom（视频会议软件）。

这些平台均存在大量敏感账号数据，包括但不限于用户身份信息、企业机密、客户信息、财务信息以及通信内容等，一旦这些数据的安全防线被突破，账号被恶意接管，将给企业和用户带来一系列严重问题。

2024年泄露特权账号的企业外部软件类型分布

注：统计图数据统计周期为 2024 年 2 月至 12 月。

1.6.3 企业内部系统普遍面临账号泄露风险，以企业邮箱、招聘系统、统一登录系统等为主

除了企业外部软件账号信息，企业内部系统，如企业邮箱、招聘、统一登录、文档系统等都出现了不同程度的账号泄露情况。这些系统涉及企业内部通信、业务流程等，承载着大量敏感数据和关键信息，一旦某个员工的账号被恶意接管，如同为企业的大门开了一道缝隙，让攻击者有机会窥探、窃取甚至篡改这些敏感数据，进而给企业带来损失。

2024年泄露特权账号的企业内部系统类型分布

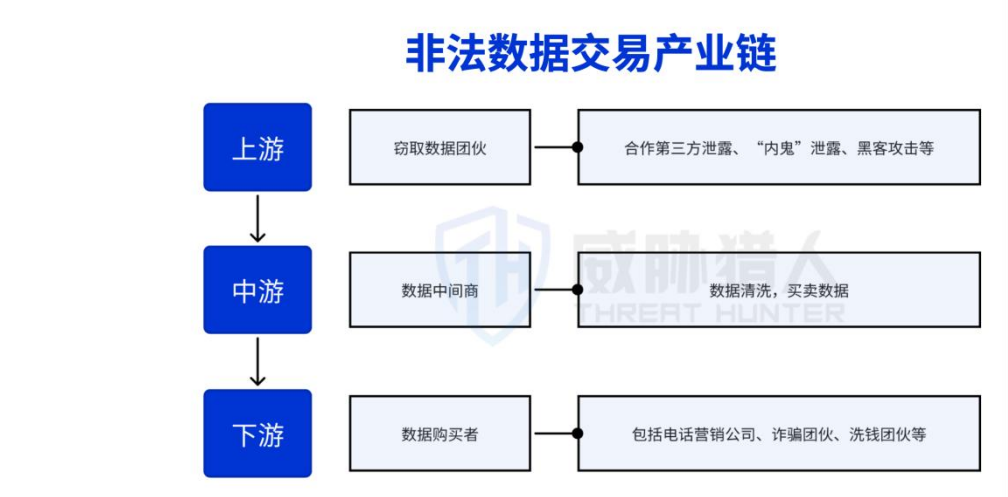
注：统计图数据统计周期为 2024 年 2 月至 12 月。

02

2024 年非法数据交易产业链分析

二、2024 年非法数据交易产业链分析

互联网黑色产业链发展至今，围绕数据资产泄露和倒卖的非法数据交易产业发展已相当成熟，基于不同角色分工、定位演化出了上、中、下游：



上游：数据窃取团伙

包括公司内鬼、黑客、运营商、运营商第三方代理、短信通道服务商等。这些人专门负责从各公司的内部和外部寻找获取数据的渠道并窃取数据。在数据越来越值钱的当下，巨大的利益和极低的犯罪成本驱动着上游的数据窃取者甘愿铤而走险。

中游：数据中间商

大部分活跃在暗网、黑产论坛、Telegram、Potato 等平台。这些人在不同的平台上发布帖子销售数据，并负责对数据进行分类和清洗，以满足客户的各种需求。

下游：数据购买者

包括电话营销公司、诈骗团伙等。购买数据的人通常会用于精准营销和诈骗。数据在使用后可能会被二次出售或与其他非法团体交换。近年来，对精细化数据的需求日益增长，例如针对保险客户、理赔用户、高净值人群的数据。这些数据被用于更精准的营销和诈骗活动，其成功率远高于传统方法。下游的需求变化促使上游和中游的非法人员采用各种技术手段收集用户数据，并根据需求对数据进行分类整理后出售。

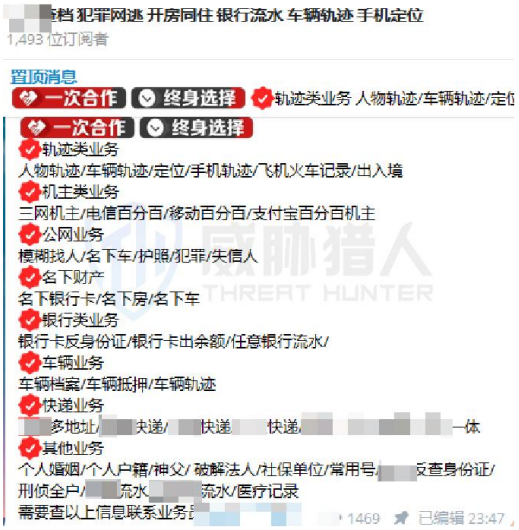
威胁猎人研究发现，2024 年非法数据交易产业链在上、中、下游均出现了一些新的变化：

2.1 2024 年“查档”类型泄露事件快速上涨，涉及电商、外卖、社交、快递等行业数据

近年来，威胁猎人陆续关注到非法数据交易产业链中游频繁出现的“查档”数据泄露情况，例如通过一个手机号，就可以查询这个手机号相关的所有身份信息，如地址、银行卡号、名下资产等等。

查档：指黑产团伙可提供指定人员的资料档案，如通过一个手机号，可以查询这个手机号相关的身份信息，如地址、银行卡号、名下资产等。查档服务包含查询类服务、解密服务、强登类服务等。

常见的查档服务有：轨迹类（人物轨迹、车辆轨迹）、名下财产（名下卡、名下车、名下房）、网购订单、快递业务（快递地址、物流信息）、个人信息（婚姻、户籍、社保）等。



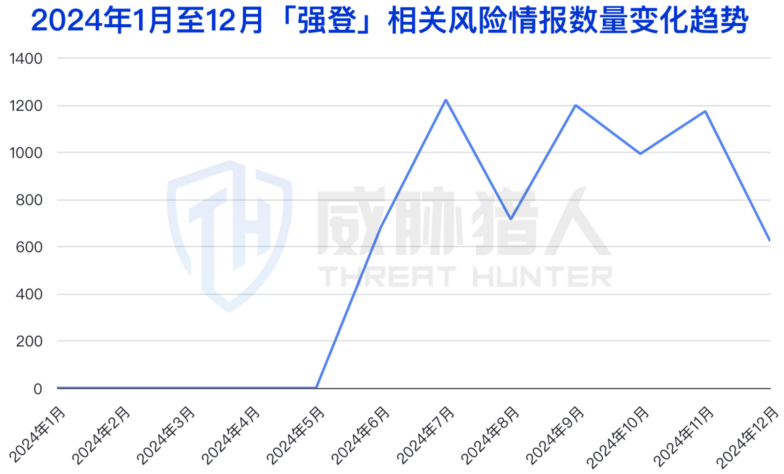
威胁猎人情报数据显示，2024 年“查档”相关的数据泄露趋势上涨，全年超过 3200 起风险事件，泄露信息涉及电商购物信息、外卖配送信息、社交账号、快递信息、银行流水等。

2.2 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】。



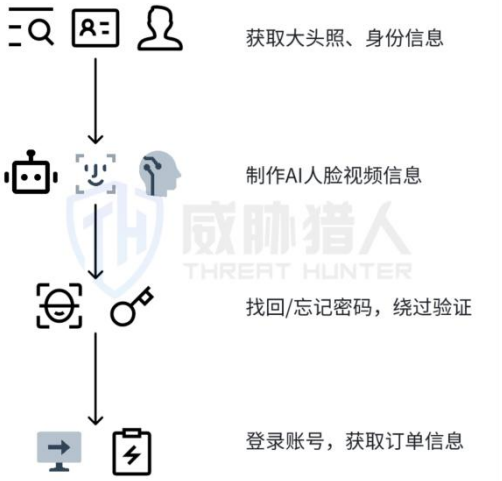
那么，“强登”数据是怎么来的呢?

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:

1、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。

2、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。

3、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。



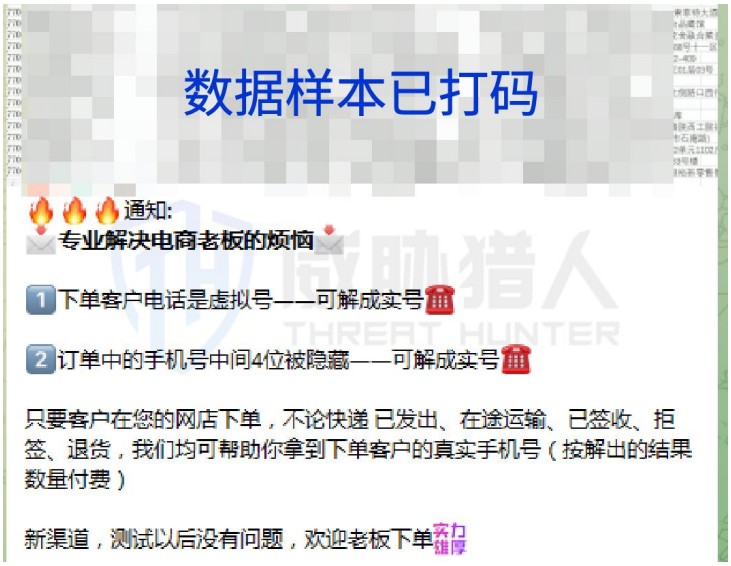
上游团伙通过“强登”方式获取到电商、外卖、快递、出行服务等行业订单信息后，再由中游团伙在各种匿名群聊、社交媒体等发布售卖广告，吸引更多下游需求人群。

2.3 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

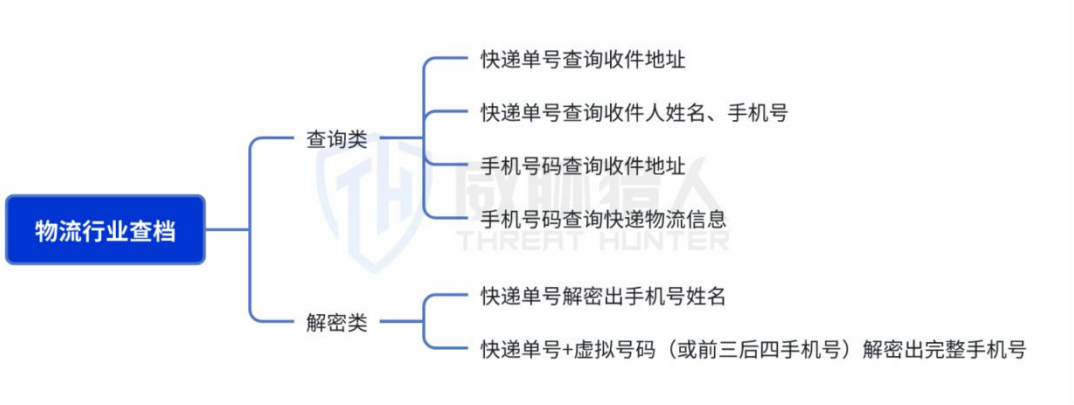
近年来，“隐私面单”技术不断发展，通过隐藏用户真实手机号来保护个人信息安全。过去一年，在物流行业监管加强和企业的共同努力下，隐私面单的推广有效减少了快递面单泄露事件，整体

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。



【拓展资料】物流行业查档主要分为查询类和解密类：



威胁猎人关注到，解密类服务价格远低于查询类服务价格，通过对每月捕获到的查询类和服务类事件涉及价格的中位数进行统计：

1、查询类服务价格中位数在 75-435 元之间，其中通过手机号码查询收件地址等信息的价格更高，主要受服务复杂度和风险影响。

2、解密类服务价格中位数仅 4 元左右，最高 7.5 元，最低 2 元。解密服务属于分布式查询，主要面向电商商家群体。

2.4 贷款类、网购类、股票类、招聘类等数据下游需求旺盛

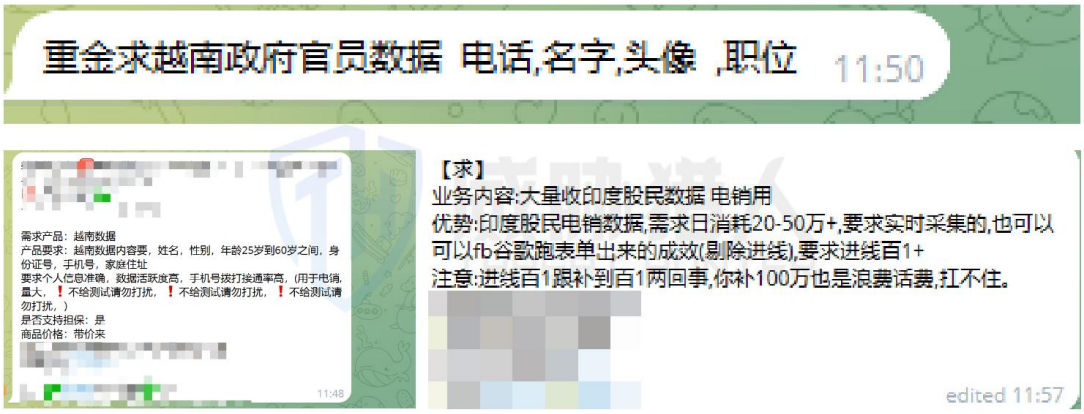
在 2024 年 1 月至 12 月期间，威胁猎人在各类黑产渠道捕获了近千条精准求购数据信息，涉及贷款类、网购类、股票类、招聘类、快递类等数据。其中，贷款类用户信息需求最为旺盛，包括消金网贷、银行贷款、企业贷、贷款超市等多个细分品类下的用户信息。

求购数据：指下游电信诈骗或营销团伙在黑产渠道中发布他们对特定类型数据的购买需求信息。

威胁猎人针对求购数据信息及求购人员进一步分析：

从求购数据类型来看，主要包括三大类，金融类数据、物流快递数据和招聘求职数据。金融类数据主要针对境外股民和虚拟货币投资者；物流快递数据则重点针对大型快递公司的订单信息，存在内部人员参与倒卖的可能；招聘求职数据主要涉及主流招聘平台，黑产一般用于电话营销、诈骗。

从求购数据指向地区来看，印度和越南重灾区。求购印度地区的数据主要涉及股票证券等金融类数据需求；求购越南地区的数据类型则较为多样，包括政府官员、在外越侨、宝妈学生等群体信息。



03

2024 年非法数据交易市场研究

三、2024 年非法数据交易市场研究

3.1 “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	保险创建订单	34	34 石	211	195	10/27/81	1981	女	2/2/24	2/3/23 0	省分公司	支公	iOS
9	保险创建订单	90	60 潘	232	360	9/25/71	1971	女	4/25/24	4/26/23 (	江省分公	心支	iOS
9	保险创建订单	11	32 胡	230	158	5/3/71	1971	女	7/25/24	7/26/23 (	江省分公	心支	iOS
9	保险创建订单	65	66 衣	210	097	8/20/80	1980	女	4/24/24	4/25/23 (	省分公司	支公	iOS
9	保险创建订单	60	41 王	220	008	7/5/75	1975	女	10/4/24	10/5/23 (	省分公司	支公	iOS
9	保险创建订单	81	14 邢	210	332	9/24/70	1970	女	4/16/24	4/17/2	省分公司	支公	iOS
9	保险创建订单	25	35 朱	239	543	10/25/79	1979	女	2/21/24	2/22/2	江省分公	心支	iOS
9	保险创建订单	12	05 王	230	578	10/3/67	1967	女	7/14/24	7/15/2	江省分公	心支	iOS
9	保险创建订单	84	35 吕	220	707	7/26/75	1975	女	8/25/24	8/26/2	省分公司	公	iOS
9	保险创建订单	77	04 顾	210	135	2/16/73	1973	女	1/6/24	1/7/23	省分公司	公	iOS
9	保险创建订单	55	74 单	211	210	6/25/69	1969	女	7/5/24	7/6/23	省分公司	公	iOS
9	保险创建订单	31	17 杨	211	083	5/14/70	1970	女	12/11/24	12/12/	省分公司	公	iOS
9	保险创建订单	92	21 牛	210	235	11/14/73	1973	女	4/14/24	4/15/2	省分公司	公	iOS
9	保险创建订单	97	39 李	232	398	7/19/73	1973	女	6/12/24	6/13/23 (	省分公	江	iOS
9	保险创建订单	96	11 曲	220	511	8/16/79	1979	女	3/12/24	3/13/23 (	分公司		iOS
9	保险创建订单	80	28 姚	230	583	3/11/78	1978	女	7/1/24	7/2/23 0	省分公司		iOS
9	保险创建订单	49	84 杜	230	334	10/1/69	1969	女	12/26/24	12/27/23	省分公		iOS
9	保险创建订单	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%

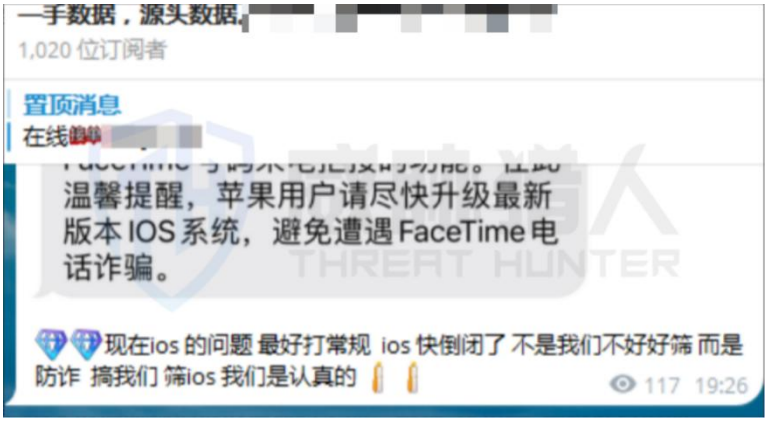
威胁猎人情报人员针对下半年下降现象进一步分析原因，下半年“IOS”相关数据下降主要是因为苹果官方针对 Facetime 诈骗出台相关打击措施导致的。

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）

威胁猎人在 5 月的舆情监控中发现，部分境外诈骗团伙，尤其是缅北地区，因 Facetime 更新而无法继续使用该方式进行诈骗，初步判断这是苹果官方针对此类违法行为的打击措施。

与此同时，威胁猎人关注到，非法数据交易市场上负责数据清洗和贩卖的黑产团伙建议诈骗团伙改用“常规”方式进行诈骗（即受用手机号码进行诈骗），以应对 Facetime 的打击行为。



3.2 “扶贫”相关数据风险情报数量显著上涨，求购“扶贫料”需求逐月增加

威胁猎人数据泄露风险监测平台情报数据显示，2024 年“扶贫”相关的非法数据交易情报数量显著上涨，尤其是第四季度。

扶贫料：在非法数据交易中和扶贫补贴对象相关的个人信息或数据，这些数据被黑产非法获取后，通常会转售给第三方，用于精准诈骗、洗钱等非法活动。

威胁猎人情报人员通过对非法数据交易产业链各环节深入研究发现，非法交易市场中兜售的“扶贫料”有来自资金盘 APP、手工打扶贫粉等。

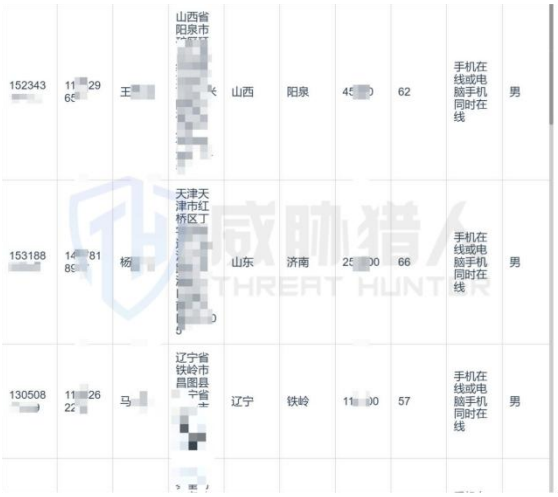
资金盘 APP：指黑产团伙通过对一些“投资项目”相关资金盘进行数据采集获取到“投资人”个人信息，这些投资人一般都会有银行卡，售卖给下游团伙实施骗卡跑分。

手工打扶贫粉：指黑产团伙通过人工方式在社交媒体等渠道大规模收集扶贫对象的个人信息。

数据清洗团伙和贩卖团伙则会对以上数据进行年龄、地区、活跃情况等筛选后，售卖给下游团伙进行精准诈骗、跑分洗钱、招募作为“背债人”实施贷款欺诈等。

案例：2024 年 10 月，威胁猎人曾捕获到一起“QQ 扶贫样本”相关数据泄露事件，泄露样本字段包括联系方式（手机号、QQ 号）、个人身份信息（姓名、性别、年龄）、详细地址（具体到

街道和住址）、经济信息（年收入 45,000 元）、行为属性（在线设备状态），以及“高活跃”等标签。



值得关注的是，除了中游团伙在交易市场售卖“扶贫料”，2024 年下半年下游团伙求购“扶贫料”的情报显著上涨，逐月增多，比例高于出售“扶贫料”的情报。

随着下游需求的不断增长，上游和中游团伙为了满足这一需求，势必会竭尽全力获取更多的“扶贫料”数据。这可能导致大量与“扶贫”相关的个人信息流入非法交易市场，这一现象值得相关机构及平台的高度关注。

3.3 牛市背后的隐藏风险：2024 年投资相关数据泄露风险趋势显著上涨

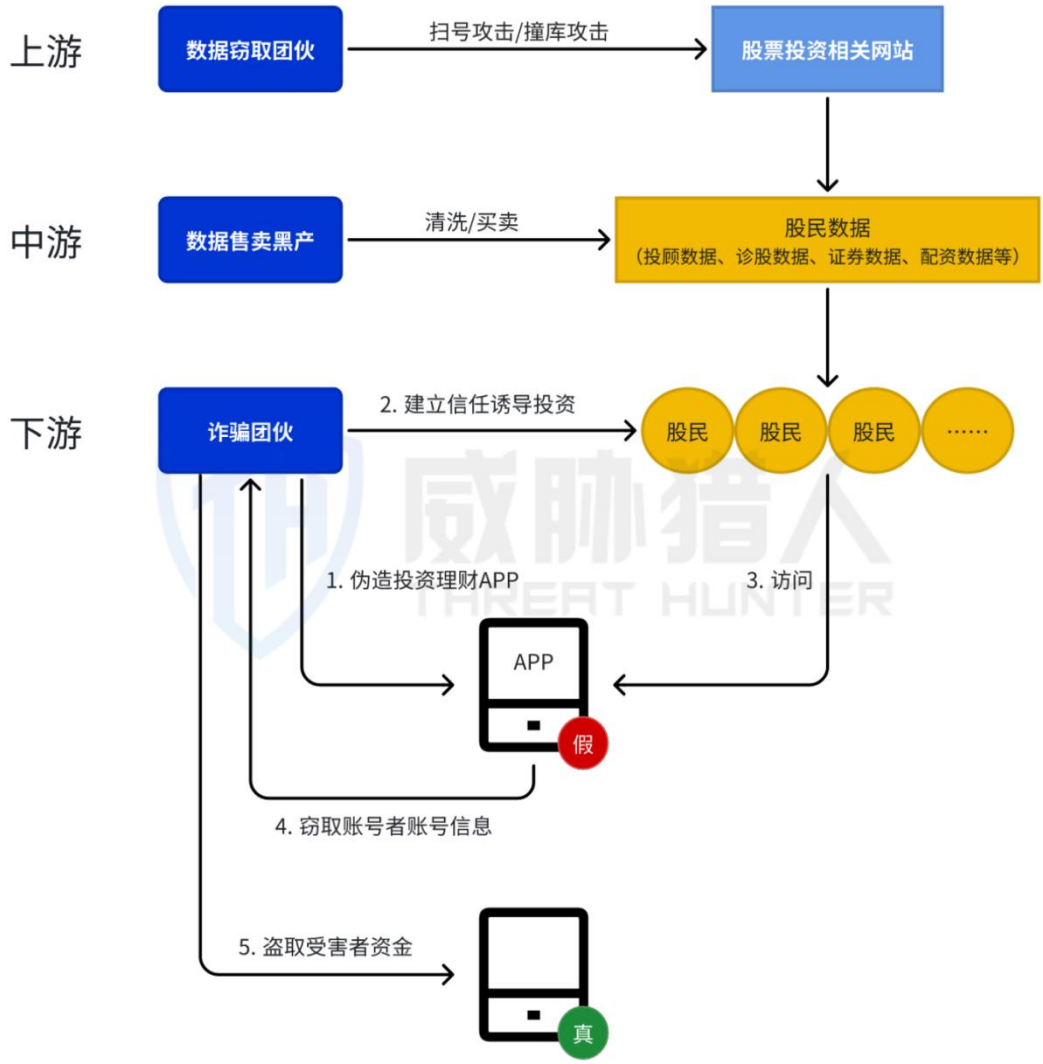
3.3.1 股民数据泄露及诈骗攻击

牛市期间，股市活动频繁，投资者参与度提高，股民数据风险暴露面也在增大，一旦投资平台或金融服务网站安全防护不足，股民数据泄露风险也可能随着股市的活跃而增加。

威胁猎人数据泄露风险监测平台数据显示，随着市场热度上升，非法数据交易市场中关于股民数据的风险情报量显著增长，尤其在下半年和年底的牛市高峰期。

威胁猎人对情报数据进一步分析发现，非法数据交易市场中主要涉及的股民数据有投顾数据、诊股数据、证券数据和配资数据，每条数据价格在 0.6 至 0.8 元之间。

股民数据泄露及诈骗攻击流程：



诈骗攻击流程部分解释：

1、诈骗团伙通过黑灰产渠道非法获取大量的股民个人资料和财务信息，包括姓名、联系方式、投资习惯等，同时伪造投资理财网站或 APP；

2、诈骗团伙添加受害者，诱导他们访问伪造网站或 APP；

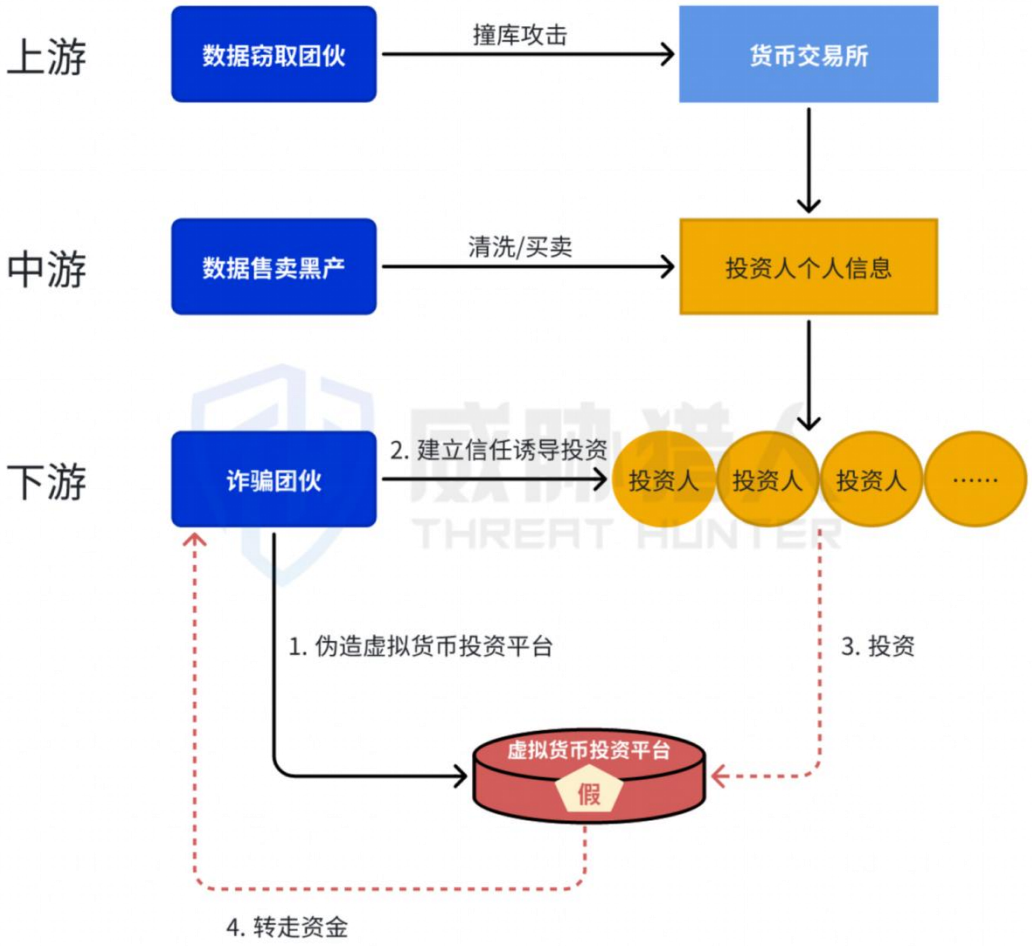
3、一旦投资者上当访问了伪冒网站或 APP，被诱骗提供个人账号信息；

4、诈骗团伙通过受害者提供的个人账号信息，到真实的理财平台登陆，窃取受害者资金。

3.3.2 加密货币投资数据泄露及诈骗攻击

同样，2024 年下半年的虚拟货币新一轮牛市，似乎也带来了关于加密货币相关的风险情报的上涨，从黑产团伙发布的广告来看，此波热度主要是因为知名加密货币交易所遭受撞库攻击。

加密货币数据泄露及诈骗攻击流程：



诈骗攻击流程部分解释：

1、诈骗团伙伪造虚拟货币投资平台，用于后续诈骗受害者（投资人）使用；

2、诈骗团伙通过社交媒体与受害者建立联系，并引导他们注册和使用虚拟货币投资平台，过程中诈骗者还会扮演"币圈大哥"等角色，进一步获取受害者的信任；

3、受害者把钱投进诈骗团伙伪造的平台中，过程中诈骗团伙会对平台后台操纵用户的投资结果，比如通过小额回报的方式吸引他们继续投资，实际上资金已经被诈骗团伙转走了；

4、一旦受害者意识到被骗，诈骗者会立即切断所有联系方式，如拉黑受害者，使其无法追回损失。

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，数据泄露风险在 2024 年呈现出前所未有的严峻态势，涉及众多行业和海量企业，给用户隐私和企业利益带来巨大威胁。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。

DRRC专业团队提供7*24小时应急响应服务

重庆、深圳两大DRRC专业团队，提供7*24，365天全方位应急响应服务

验证预警 | 下架处置 | 协助溯源 | 专项运营 | 月度报告 | .....

威胁猎人情报专家服务团队组织架构

威胁猎人建立完善的数据泄露风险情报服务管理体系，为企业提供7*24小时专业服务。

05

数据泄露相关名词解释

五、数据泄露相关名词解释

DRRC：数字风险应急响应中心，威胁猎人成立深圳、重庆两大 DRRC，汇集 30+安全运营专家，为企业提供 7×24 小时应急响应服务。

真实性验证引擎：通过不同文件类型的个人要素提取和比对，以及对图片 OCR 结果中的要素进行提取及验证，有效识别该图片内容中是否含有伪造数据/历史泄露数据。

数据泄露情报：威胁猎人通过 TG 群、暗网等渠道捕获到的“未授权个人或组织的敏感信息被公开交易或使用” 的情报信息，包含数据售卖广告、数据求购信息、无验证的虚假信息/历史数据/重复数据等等，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、虚假事件，确认真实有效的数据泄露事件。

历史数据事件：黑产将泄露过的真实信息进行整合并再次用于交易的事件，通常黑产会对数据进行精细化处理，补充数据字段完整性，从而提升数据价值及盈利空间。

虚假数据事件：黑产将伪造的虚假数据数据用于交易的事件。

私域群：需通过邀请链接/管理员同意后才能进入的群组，一般外部人员无法监测或进入该群聊。

担保机构：在非法数据交易中扮演“中间人”的角色，负责验证交易双方的资质、监督交易过程并确保交易的顺利完成。这种模式提高了交易双方的信任度、非法数据交易流程更加“规范”，一定程度上保障了非法数据交易的顺利进行。

查档：指黑产团伙可提供指定人员的资料档案，如通过一个手机号，可以查询这个手机号相关的身份信息，如地址、银行卡号、名下资产等。查档服务包含查询类服务、解密服务、强登类服务等。

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。

特权账号（Privileged Account）：指具有特殊权限的账号，通常拥有对系统、网络或数据的高级访问权限，如企业员工账号。

求购数据：指下游电信诈骗或营销团伙在黑产渠道中发布他们对特定类型数据的购买需求信息。

扶贫料：在非法数据交易中和扶贫补贴对象相关的个人信息或数据，这些数据被黑产非法获取后，通常会转售给第三方，用于精准诈骗、洗钱等非法活动。

资金盘 APP 数据采集：指黑产团伙通过对一些“投资项目”相关资金盘进行数据采集获取到“投资人”个人信息，这些投资人一般都会有银行卡，售卖给下游团伙实施骗卡跑分。

手工打扶贫粉：指黑产团伙通过人工方式在社交媒体等渠道大规模收集扶贫对象的个人信息。

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