威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

2024年上半年
数据泄露风险态势报告

出品方：威胁猎人

目录

Contents

前言

在快速崛起的数字经济时代，数据作为企业的核心资产及重要战略资源，在高速增长的同时，其背后的数据风险也在不断攀升，日渐复杂的数据泄露形势，已成为企业数字化发展赛道的严重阻碍。

威胁猎人**《2024 年上半年数据泄露风险态势报告》**对 2024 年上半年数据资产泄露风险概况、黑产数据交易市场等进行具体分析，结合典型行业案例，多维度呈现 2024 年上半年国内数据泄露的态势全景：

1、2024 年上半年全网监测并分析验证有效的**数据泄露事件 16011 起**，较 2023 年下半年**增长 59.58%**，共 9539 起；

2、2024 年上半年监测到 3.4 万个黑产团伙中，经分析验证涉及真实数据泄露事件的**黑产团伙共计 1973 个**，较 2023 年下半年增新增 984 个，增长近一倍。

3、从行业分布来看，2024 年上半年数据泄露事件涉及 85 个行业，数据泄露事件数量 Top5 行业分别为**银行、电商、消费金融、保险、快递**；

4、从区域、年龄、性别等维度来看，2024 年上半年数据泄露人群最多的区域分别是：**浙江、四川、广东**；35-54 岁占比最高达 62%；女性占比最高达 64%。

5、针对黑产数据交易市场研究发现，2024 年上半年利用 Facetime 诈骗活动增多，2024 年上半年泄露的数据中包含“**IOS”字段的相关风险事件高达 1237 起**，较 2023 年下半年增加 8 倍。

相关名词定义：

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

2、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；

3、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；

4、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；

5、公民个人信息：指公民个人身份信息，包括但不限于姓名、身份证号码、出生日期、手机号码、家庭住址、银行账户信息等；

6、历史个人信息：指此次数据泄露事件之前就已经泄露过的个人信息，很多历史个人信息被黑产收集整合成社工库；

7、暗网：指隐藏的网络，普通网民无法通过常规手段搜索访问，需要使用一些特定的软件、配置或者授权才能登录；

8、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。

9、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；

10、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。

01

2024 年上半年
数据泄露风险概况

一、2024 年上半年数据泄露风险概况

1.1 2024 年上半年数据泄露事件共计 16011 起，较 2023 年下半年增长 59.58%

据威胁猎人数据泄露风险监测平台数据显示，2024 年上半年（1-6 月）全网监测到的 1.1 亿条情报中，基于真实性验证引擎及 DRRC 人工分析验证有效的数据泄露事件共计 16011 起，较 2023 年下半年增长 59.58%，9539 起。

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 36%（898 起），进一步分析了解到，主要有以下两个方面所致：

（1）从数据泄露源头来看，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在 2024 年 2 月出现下降的情况，可以看出主要是受到春节期间黑产放假带来的交易行为放缓的影响。

2024 年上半年数据泄露的主要原因包括：

短信通道泄露：随着历年来短信收发业务的发展，短信通道商开始通过压低价格的方式来获取更高的订单，比如会以低于市场标准价格与短信下发方（甲方）达成交易，而其收益空间降低很多，因此内部会通过非法售卖短信信息数据的方式获取更多收益。

运营商通道：黑产通过运营商内鬼或违规代理等渠道，获取到指定网页的访问数据、指定应用的安装数据、指定短信的接收和发送数据等信息；

内鬼泄露：企业内部员工在利益的驱使下，采用资料导出、人工拍摄等方式，获取客户敏感信息后进行售卖；

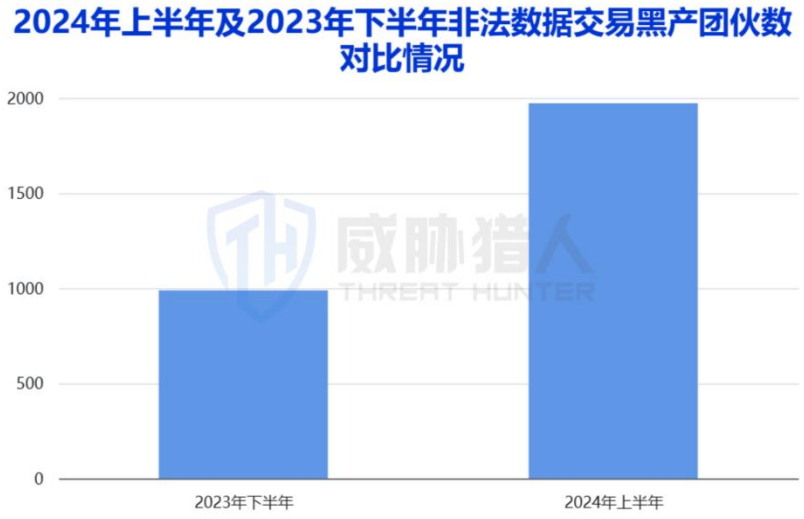
黑客攻击：外部黑客使用爬虫、扫描、渗透等方式攻击企业系统和网络资产，利用企业网络漏洞大规模窃取数据;

第三方泄露：和企业存在合作关系的第三方，具有访问企业某些敏感数据的权限，但由于管理不规范等问题，导致这些敏感数据通过第三方泄露到黑产手中;

（2）从贩卖数据（中间商）的黑产团伙数量来看，2024 年 2 月非法数据交易黑产团伙数量出现下降。

1.2 监测到非法数据交易黑产团伙 1973 个，较 2023 年下半年增长近一倍

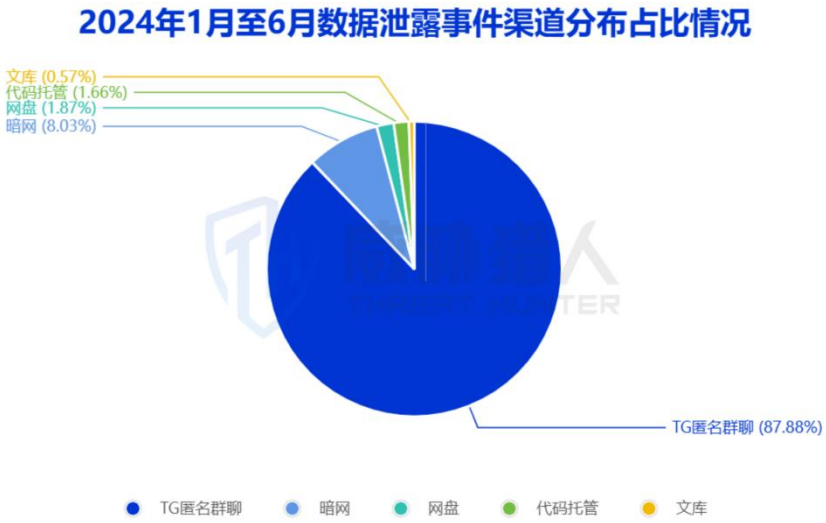
威胁猎人针对非法数据交易团伙进行深入分析，2024 年 1 月至 6 月监测到 3.4 万个黑产团伙中，经分析验证涉及真实数据泄露事件的黑产团伙共计 1973 个，较 2023 年下半年增新增 984 个，增长近一倍。



针对非法数据交易黑产团伙 Top10 研究发现，2024 年上半年各团伙关联的数据泄露风险事件总量均高于 2023 年下半年，可见非法数据交易团伙的整体活跃度不断上升、非法交易行为更加高频，同时新的大型黑产团伙的不断加入（如小富豪**、阿包**等），使得黑产通过 Telegaram 进行非法数据交易的形势更加严峻。

1.3 Telegram 及暗网依旧活跃，在数据泄露渠道中占比高达 95%

2024 年上半年威胁猎人监测到的数据泄露事件中，发生在 Telegram 及暗网的达 95%以上，其中 87%集中在 Telegram。



1.3.1 Telegram “私域群”捕获超 1400 起风险事件，较 2023 年下半年增长近 2 倍

自 2023 年起，大多数黑产团伙开始转向私域群进行交易，数据交易团伙也对自身的账号信息进行匿名隐藏。Telegram 渠道监测到风险事件最多的频道/群聊为私域群，2024 年上半年，威胁猎人在私域群累计发现超过 1400 起风险事件，较 2023 年下半年增长近 2 倍。

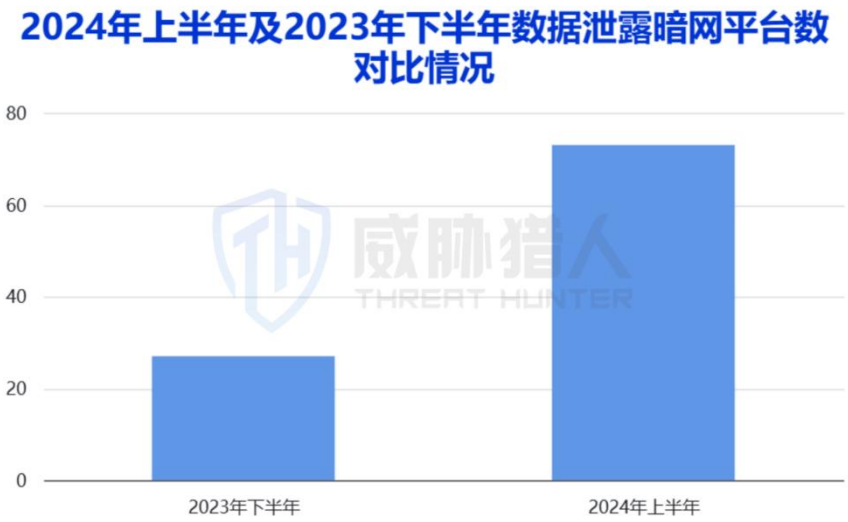
私域群：需通过邀请链接/管理员同意后才能进入的群组，一般外部人员无法监测或进入该群聊，群组有管理员定期清洗群成员名单，一定程度上过滤了广告、机器人、二道贩子、中介等可信度较低的人员，群组内容质量更接近真实数据泄露源头。

2024 年上半年 Telegram “私域群”数量快速增长，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。

1.3.2 2024 年上半年暗网平台数量较 2023 年下半年新增 46 个

暗网平台作为黑产非法数据交易的主流渠道之一，其平台数量的快速增长也侧面反映出暗网的活跃性持续提升，为黑产非法数据交易提供了更多新的隐蔽渠道。

2024 年上半年，威胁猎人在暗网渠道发现数据泄露事件累计 1229 起，共涉及 73 个网站（如 spyhackerz、crakingx 等），较 2023 年下半年新增 46 个网站。



威胁猎人基于数据泄露事件量最高的 Top10 暗网网站，共发现 994 起数据泄露事件，占捕获暗网数据泄露事件总量的 80%以上，主要集中在长安不夜城、breachforums 以及 cracked 这几大网站。

1.4 银行、电商、消费金融成为数据泄露事件数量 Top3 行业，银行事件数量 2961 起位列第一

从行业分布来看，2024 年上半年数据泄露事件涉及 85 个行业，1524 家企业，数据泄露事件数量 Top5 行业分别为银行、电商、消费金融、保险、快递。其中，银行行业数据泄露事件数量高达 2961 起，成为数据泄露事件数最多的行业。

2024 年上半年 TOP10 行业排名变化情况如下：

行业	2023年下半年排名	2024年上半年排名	排名变化
银行	2	1	↑1
电商	5	2	↑3
消费金融	1	3	↓2
保险	4	4	-
快递	3	5	↓2
在线票务	7	6	↑1
证券	8	7	↑1
汽车品牌	9	8	↑1
支付	6	9	↓3
本地生活	15	10	↑5

排名靠前的数据泄露行业中以金融、电商行业为主，金融行业的数据泄露事件主要体现在银行、消费金融、保险等企业的客户信息倒卖，通常被下游黑产团伙用于精准营销及诈骗，因涉及大量高价值用户数据，且靠近交易环节，成为了个人信息泄露的重灾区。

近年来线上购物发展更加火热，据 2024 年 3 月发布的《中国互联网络发展状况统计报告》显示，截至 2023 年 12 月，我国网络购物用户规模达 9.15 亿人，占网民整体的 83.8%。线上购物的持续稳定增长下，电商平台产生了海量购物订单及物流信息，这些购物订单及物流信息由于暴露面较大，成为了黑产团伙的重点目标，同样被用于营销或诈骗。

同时，在公安部近期公布的“十大高发电信网络诈骗类型”中，刷单返利、虚假网络投资理财、虚假购物服务、冒充电商物流客服、虚假征信等 10 种常见的电信网络诈骗类型发案占比近 88.4%。

其中刷单返利类诈骗是发案量最大和造成损失最多的诈骗类型，虚假网络投资理财类诈骗的个案损失金额最大，虚假购物服务类诈骗发案量明显上升，已位居第三位，而金融、电商类用户群体正是此类诈骗案件的受害群体。

1.5 2024 年上半年泄露数据量达千万级事件共 9 起，以公民三要素信息及网购数据为主

威胁猎人在 2024 年上半年监测到泄露数据量达千万级的事件共 9 起，其中最高泄露数据量达 12 亿，经过威胁猎人多次深入分析验证发现，该事件泄露数据主要由发布者整合拼接而成（基于此前发生的多起国内大型数据泄露事件），并非近期泄露数据。

泄露的数据信息中主要以公民个人信息三要素（姓名、手机号、身份证）为主，其次是网购电商数据，最后是金融数据（银行、借贷信息）。从泄露渠道来看，主要集中在 breachforums、长安不夜城、cc2crd 等知名暗网，以及 Telegram 匿名群聊。

02

2024 年上半年数据泄露字段及人群画像分析

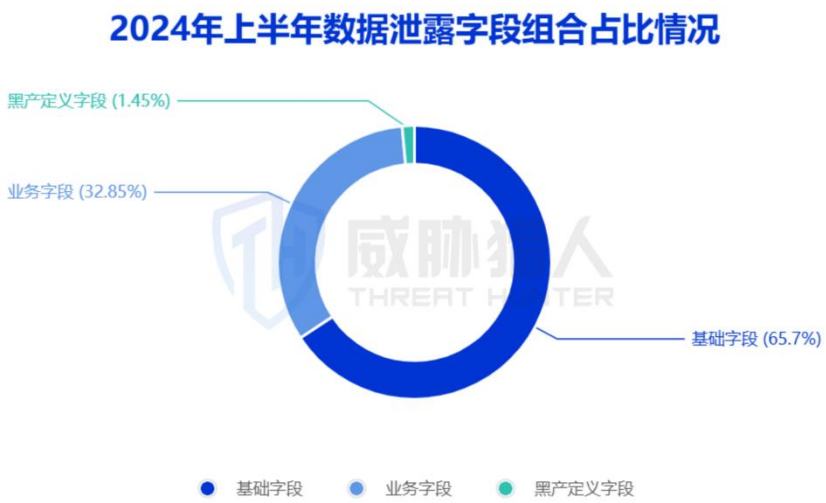
二、2024 年上半年数据泄露字段及人群画像分析

2.1 2024 年上半年数据泄露字段分析：基础字段占比 65.7%

威胁猎人针对泄露字段调研统计发现，数据泄露字段主要包含基础字段、业务字段、黑产定义字段等类型，基础字段占比最高，达 65.7%，基础字段中姓名、手机号、身份证号占比最高。

泄露数据价值与其所包含的具体字段密切相关，下游黑产可通过“全格式”数据字段构建完整的公民画像，进行定向性作恶，使整体作恶成功率及收益更高。

“全格式”数据是黑产描述数据所包含字段格式的专业通用型词汇，通常指包含身份证、姓名、手机号等基础字段信息，加上不同行业相关的业务字段信息，以保险行业为例，保险行业全格式信息通常包括身份证、姓名、手机号、投保金额、保险类型等。



基础字段：主要指个人基础信息，包括姓名、手机号、身份证号、银行卡号、地理位置、详细地址等；

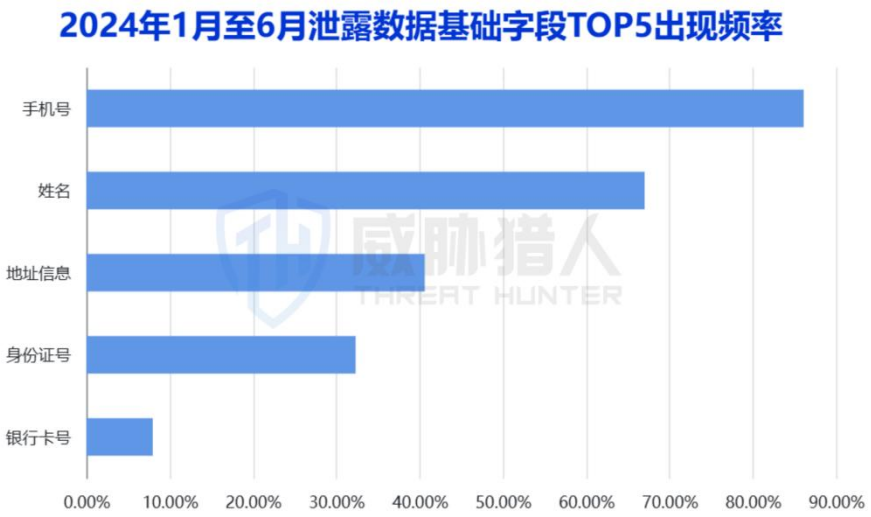
业务字段：主要指业务相关信息，包括平台名称、保险类型、品牌、快递单号、航空公司、航班号等；

黑产定义字段：主要指黑产团伙数据清洗后定义的字段，如：验证 ID、设备信息（IOS/安卓）、所属运营商等（验证 ID 主要是黑产对数据进行标记，防止被二次贩卖）；

2.1.1 泄露的基础字段中"手机号"出现频率最高达 86%

威胁猎人针对泄露字段调研统计发现，数据泄露字段主要包含基础字段、业务字段、黑产定义字段等类型，基础字段占比最高，达 65.7%，

手机号作为重要基础数据字段之一，是黑产作恶的不可或缺的数据资源，频繁被下游营销/诈骗团伙用于对相关手机号发送短信、电话营销等，进一步实施非法作恶行为。2024 年 1-6 月公民信息泄露事件超过 15000 起，其中泄露信息字段包含“手机号”的超过 86%。



威胁猎人安全运营人员调查了解到，部分上游黑产团伙因技术手段受限，仅能获取到“手机号”字段，黑产团伙会通过多种方法拼接个人信息、补齐数据字段信息，从而提高数据的价值。

2.1.2 泄露的业务字段中"银行"占比最高，其中“银行卡号”字段占比最高达57%

经统计分析，泄露的业务字段中"银行"行业占比最高，进一步分析发现，银行行业泄露的数据中出现频率最高的业务字段信息为“银行卡号”，在银行行业所有业务字段中出现占比达57.08%。

银行数据出现频率 TOP3 业务字段如下：

字段	出现频率
银行卡号	57.08%
交易金额	25.99%
交易时间	21.11%

2.1.3 黑产自定义字段中，2024 年 1 月首次出现“低频骚扰”、“验证 ID”字段

威胁猎人针对泄露的数据中进行分析发现，2024 年 1 月黑产自定义的字段中首次出现“低频骚扰”、“验证 ID”等字段，针对相关字段研究分析发现：

① 黑产通过对数据“低频过滤清洗”提升诈骗成功率，相关事件累计发现 52 起

威胁猎人发现自 2024 年 1 月起，泄露的数据字段开始高频出现“低频骚扰”字段内容，2024 年上半年共发现 52 起该类型的风险事件。

13	刘	3203	30	男	1970	徐州		DP2024218	2024/2/18 2:02 低频骚扰
13	贾	3307	52	女	1970	金华		DP2024280	2024/2/25 15:4 低频骚扰
15	邱	3326	20	女	1979	浙江		DP2024221	2024/1/22 18:0 低频骚扰
15	刘	3325	92	男	1960	丽水		DP2024260	2024/1/21 1:15 低频骚扰
13	徐	3210	21	男	1969	江苏		DP2024274	2024/1/10 20:5 低频骚扰
13	蒋	3210	52	男	1968	江苏		DP2024282	2024/2/20 7:22 低频骚扰
13	王	3301	1	女	1971	河南		DP2024218	2024/2/20 16:4 低频骚扰
18	楼	3301	22	女	1968	杭州		DP2024253	2024/1/7 17:49 低频骚扰
13	刘	3201	3	男	1973	江苏		DP2024247	2024/2/22 12:1 低频骚扰
13	庞	3210	32	男	1953	江苏		DP2024285	2024/1/17 10:5 低频骚扰
15	周	3209	52	男	1977	江苏		DP2024231	2024/1/4 8:57 低频骚扰
13	侯	3208	71	男	1968	连云港		DP2024215	2024/1/22 19:4 低频骚扰
13	陈	3307	91	女	1983	绍兴		DP2024299	2024/2/9 1:11 低频骚扰
13	赵	3309	00	女	1975	浙江		DP2024280	2024/2/15 19:0 低频骚扰
18	郭	3208	70	男	1976	天津		DP2024209	2024/1/4 16:18 低频骚扰
15	周	3307	51	女	1989	浙江		DP2024250	2024/2/28 9:27 低频骚扰

（低频数据样例形式）

威胁猎人与发布相关数据的黑产进一步沟通了解到，黑产将此类数据定义为低频骚扰数据，“低频过滤清洗”主要指数据售卖方在对数据筛选时，会对普通用户手机号的骚扰频率进行分析，从而过滤筛选出低骚扰率的用户手机号，即平时接收到骚扰电话的情况较少，对陌生电话的接听抗拒程度较低的用户手机号。

针对这类手机号，作恶团伙可以在进行营销推广或诈骗时，实现更高的用户接听率，可以更好地套取到用户的信任从而进行精准推广，极大提升诈骗成功率。

② 黑产通过“验证 ID”标识校验定位可信度更高的数据源，相关事件累计发现 37 起

2024 年 1 月，威胁猎人在泄露的数据字段中发现“验证 ID”字段高频出现，2024 年上半年共发现 37 起该类型的风险事件。

验证ID	姓名	手机号码	保险类型	公司	身份证号	地址	运营商
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	15[illegible]0	年金保险	[illegible]	3[illegible]0562	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	14[illegible]0	年金保险	[illegible]	3[illegible]3229	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]6	人寿保险	[illegible]	3[illegible]6522	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]0	健康保险	[illegible]	3[illegible]3540	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]2	人寿保险	[illegible]	3[illegible]1606	湖[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]6	年金保险	[illegible]	3[illegible]062X	广[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	15[illegible]7	人寿保险	[illegible]	3[illegible]3628	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]8	健康保险	[illegible]	3[illegible]7325	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	15[illegible]8	意外伤害保险	[illegible]寿	3[illegible]214X	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]3	健康保险	[illegible]	3[illegible]0222	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	18[illegible]9	人寿保险	[illegible]	3[illegible]3745	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]9	人寿保险	[illegible]寿	3[illegible]0429	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]8	人寿保险	[illegible]	3[illegible]0648	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	18[illegible]9	人寿保险	[illegible]寿	3[illegible]0529	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]3	人寿保险	[illegible]	3[illegible]5427	广[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	18[illegible]5	人寿保险	[illegible]	3[illegible]2023	广[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	18[illegible]0	人寿保险	[illegible]	3[illegible]7624	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	15[illegible]8	健康保险	[illegible]寿	3[illegible]5422	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	18[illegible]2	人寿保险	[illegible]	3[illegible]6823	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]3	人寿保险	[illegible]	3[illegible]1044	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	18[illegible]8	人寿保险	[illegible]	3[illegible]2146	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]7	人寿保险	[illegible]	3[illegible]0584	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]8	人寿保险	[illegible]	3[illegible]7424	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]2	人寿保险	[illegible]	3[illegible]2448	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	18[illegible]3	人寿保险	[illegible]	3[illegible]6843	广[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	15[illegible]5	人寿保险	[illegible]	3[illegible]1847	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	15[illegible]2	意外伤害保险	[illegible]	3[illegible]0041	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]4	人寿保险	[illegible]	3[illegible]0021	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	18[illegible]2	人寿保险	[illegible]	3[illegible]5946	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	15[illegible]5	人寿保险	[illegible]	3[illegible]2022	福[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]3	人寿保险	[illegible]	3[illegible]2224	浙[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	17[illegible]7	人寿保险	[illegible]	3[illegible]2627	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]5	人寿保险	[illegible]	3[illegible]482X	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	15[illegible]9	人寿保险	[illegible]	3[illegible]5420	江[illegible]	中[illegible]
u3y2mo9n-qy[illegible]agj7epk1x2	[illegible]	13[illegible]3	人寿保险	[illegible]	3[illegible]2121	江[illegible]	中[illegible]

(验证 ID 字段类数据)

深入调研发现，“验证 ID”实际上是非法数据交易黑产团伙为了验证数据是否真实，同时防止数据被中介二次贩卖而制作的标识，下游购买数据的团伙可通过其提供的数据验证系统校验数据是否真实。

非法数据交易市场中数据二次售卖、多次售卖的情况屡见不鲜。威胁猎人调研发现，平均同一份数据样例就有至少 2 个黑产团伙进行售卖，同一份数据样例最多被 433 个黑产团伙进行售卖。黑产交易市场新旧真假数据鱼龙混杂，ID 验证的方式在一定程度上帮助下游购买数据的黑产团伙有效寻找到可信度更高的数据。

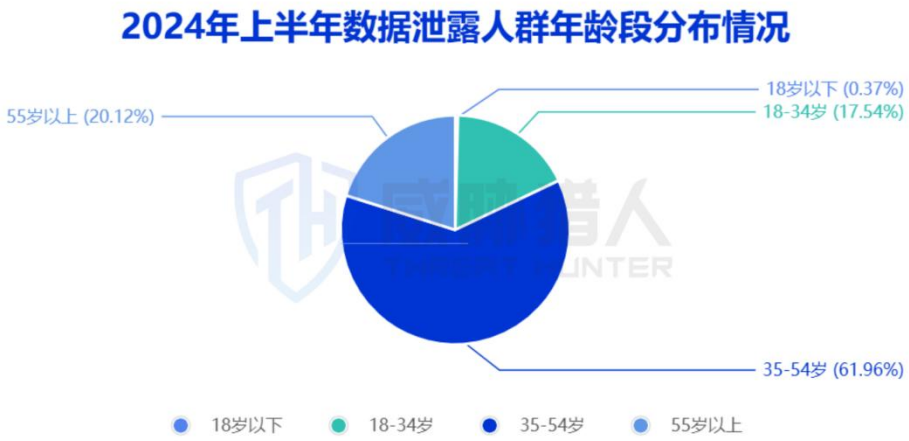
（验证 ID 字段黑产解释情况）

2.2 2024 年上半年数据泄露人群画像分析

2.2.1 2024 年数据泄露人群地区分布 TOP3：浙江、四川、广东

威胁猎人针对全行业数据泄露人群相关信息进行分析，从所在区域维度来看，数据泄露人群数量最多 TOP3 区域分别是：浙江、四川、广东。

2.2.2 2024 年数据泄露人群年龄段分布：35-54 岁占比达 62%



各年龄阶段分布定义（供参考）：

未成年人：18 岁以下

青年阶段：18-34 岁

中年阶段：35-54 岁

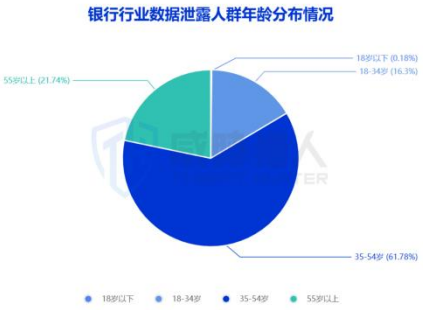
老年阶段：55 岁以上（退休年龄）

2.2.3 2024 年数据泄露人群性别分布：女性占比较大，达 64%

2.2.4 TOP3 行业（银行、电商、消费金融）人群画像分析

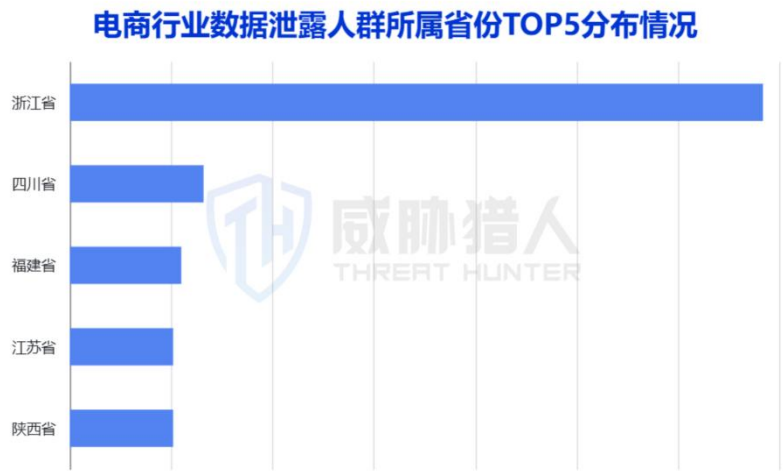
① 银行数据泄露人员画像

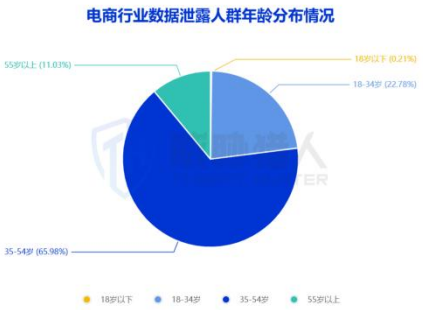
威胁猎人针对银行数据泄露人群相关信息进行分析，数据泄露人群最多的区域分别是：广东、四川、江苏、安徽、河南。泄露人群年龄主要在 35-54 岁，占数据泄露人群中 61.78%，女性占 66.42%。



② 电商数据泄露人员画像

威胁猎人针对电商数据泄露人群相关信息进行分析，数据泄露人群最多的区域分别是：浙江、四川、福建、江苏、陕西。泄露人群年龄主要在 35-54 岁，占电商数据泄露人群中 65.98%，女性占 68.25%。





③ 消费金融数据泄露人员画像

威胁猎人针对消费金融数据泄露人群相关信息进行分析，数据泄露人群最多的区域分别是：浙江、安徽、江西、四川、陕西。泄露人群年龄主要在 35-54 岁，占消费金融数据泄露人群中 57.71%，女性占 52.46%。

03

2024 年上半年黑产数据交易市场相关研究

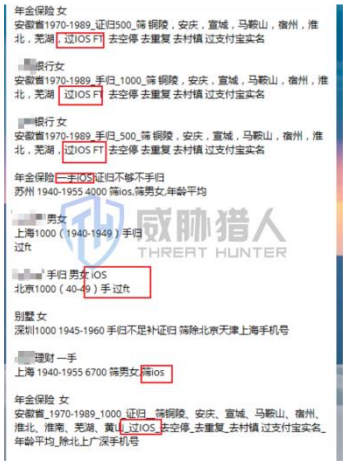
三、2024 年上半年黑产数据交易市场相关研究

3.1 2024 年上半年出现多起利用 Facetime 诈骗活动，“IOS”字段相关风险事件共 1237 起，较 2023 年下半年增长 8 倍

威胁猎人安全研究员发现 2024 年上半年泄露的数据中，“设备信息”字段信息出现频率逐渐增多，尤其是“IOS”类数据字段，从数贩卖黑产团伙与下游数据购买者的聊天记录来看，下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	2/3/23 0:辽宁省分公司辽阳中心支公	iOS
9	保险创建订单	90 60	潘	232	360	9/25/71	1971	女	4/25/24 2	4/26/23 (黑龙江省分公司绥化中心支公	iOS
9	保险创建订单	11 32	胡	230	458	5/3/71	1971	女	7/25/24 2	7/26/23 (黑龙江省分公司伊春中心支公	iOS
9	保险创建订单	65 66	衣	210	097	8/20/80	1980	女	4/24/24 2	4/25/23 (辽宁省分公司大连中心支公	iOS
9	保险创建订单	60 41	王	220	008	7/5/75	1975	女	10/4/24 2	10/5/23 (吉林省分公司吉林中心支公	iOS
9	保险创建订单	81 14	邢	210	332	9/24/70	1970	女	4/16/24 2	4/17/23 (辽宁省分公司抚顺中心支公	iOS
9	保险创建订单	25 35	朱	239	543	10/25/79	1979	女	2/21/24 2	2/22/23 (黑龙江省分公司富锦中心支公	iOS
9	保险创建订单	12 05	王	230	578	10/3/67	1967	女	7/14/24 2	7/15/23 (黑龙江省分公司鸡西中心支公	iOS
9	保险创建订单	84 35	吕	220	707	7/26/75	1975	女	8/25/24 2	8/26/23 (吉林省分公司长春中心支公	iOS
9	保险创建订单	77 04	顾	210	135	2/16/73	1973	女	1/6/24 2	1/7/23 0:辽宁省分公司抚顺中心支公	iOS
9	保险创建订单	55 74	单	211	210	6/25/69	1969	女	7/5/24 2	7/6/23 0:辽宁省分公司朝阳中心支公	iOS
9	保险创建订单	31 17	杨	211	083	5/14/70	1970	女	12/11/24	12/12/23 辽宁省分公司铁岭中心支公	iOS
9	保险创建订单	92 21	牛	210	235	11/14/73	1973	女	4/14/24 2	4/15/23 (辽宁省分公司抚顺中心支公	iOS
9	保险创建订单	97 39	李	232	398	7/19/73	1973	女	6/12/24 2	6/13/23 (黑龙江省分公司松花江中心	iOS
9	保险创建订单	96 11	曲	220	511	8/16/79	1979	女	3/12/24 2	3/13/23 (吉林省分公司四平中心支公	iOS
9	保险创建订单	80 28	姚	230	583	3/11/78	1978	女	7/1/24 2	7/2/23 0:黑龙江省分公司鸡西中心支公	iOS
9	保险创建订单	49 84	杜	230	334	10/1/69	1969	女	12/26/24	12/27/23 黑龙江省分公司齐齐哈尔中	iOS
9	保险创建订单	84 44	李	220	111	2/1/76	1976	女	11/4/24 2	11/5/23 (吉林省分公司长春中心支公	iOS

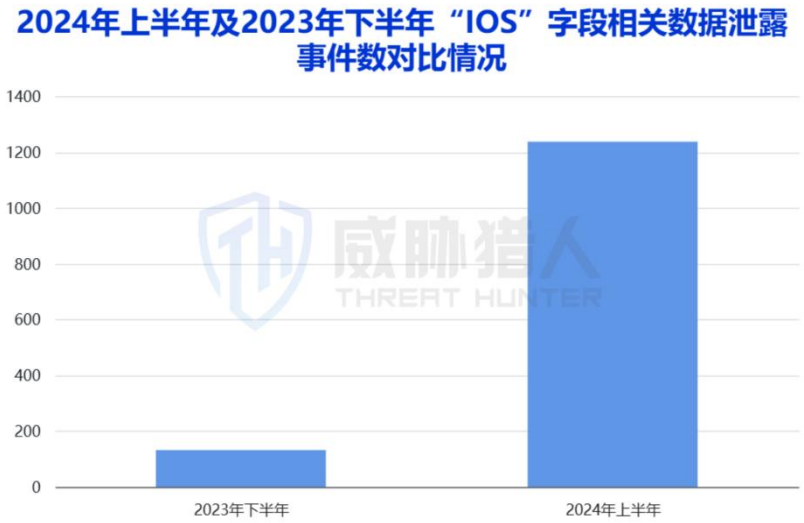
（威胁猎人捕获的泄露数据中包含设备信息）



（下游作恶团伙以及数据售卖方反馈需过 IOS、FT 等要求）

威胁猎人统计发现，2024 年上半年泄露的数据中包含“IOS”字段的相关风险事件高达 1237 起，较 2023 年下半年增加 8 倍。

随着国家公安机关对传统电话诈骗的打击加大、运营商监管加强，而 Facetime 日渐普及，不法分子开始盯上 Facetime 通话功能，试图通过这一功能实施诈骗活动。“IOS”类数据字段的大幅增加，以及黑产沟通验证，进一步佐证了利用 Facetime 进行诈骗的现状使得上游数据清洗产业链发展更加猖獗。



自 2024 年起，威胁猎人发现不少诈骗分子冒充“金融平台客服”、“国家征信中心工作人员”等身份，使用 FaceTime 功能向苹果手机用户发起通话，以“开通百万医疗保险需要关闭”、“有未结清的贷款需要处理”等为由进行诈骗，告知手机用户如不取消会被强制扣款，或个人征信受损，从而诱骗手机用户将相关款项转移至指定账户，给受害者带来巨额损失。

3.2 2024 年上半年数据泄露事件中，包含历史数据的事件占 30%

历史数据事件：威胁猎人通过与过往泄露数据的匹配验证，识别出黑产发布数据样本中包含旧数据的事件；

虚假数据事件：威胁猎人对数据样例中所包含的三要素进行匹配验证，识别黑产伪造的虚假数据的事件；

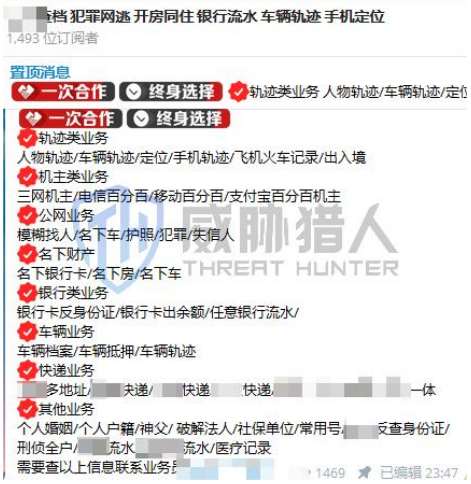
威胁猎人基于数据真实性验证引擎的优化，有效识别样本数据泄露事件中包含历史数据的事件数占比，经抽样分析发现 2024 年上半年黑产交易市场中 30.60%数据泄露事件包含历史数据，即 10 次非法数据交易就有 3 次是历史数据售卖，较 2023 年下半年上涨 15.93%。可见，数据交易市场中诸多黑产多次通过售卖历史数据、伪造数据、拼接数据等方式进行牟利的行为更为严峻。

3.3 2024 年上半年“查档”信息事件共 657 起，事件数呈现快速上升趋势

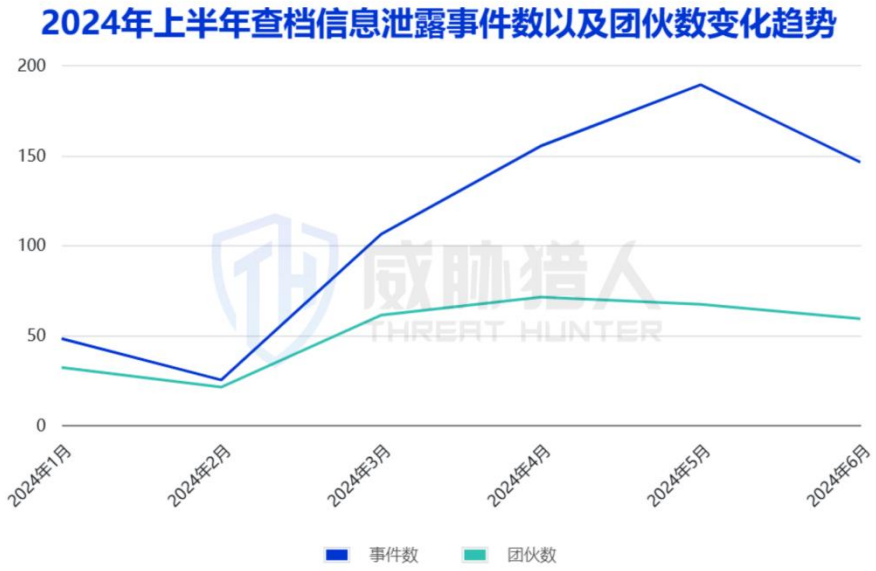
黑产在 Telegram 等渠道社工查档的事件屡见不鲜，例如通过一个手机号，就可以查询这个手机号相关的所有身份信息，如地址、银行卡号、名下资产等等。

查档：指提供对指定人员信息的资料档案进行调查或相关数据提取服务。

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）、快递业务（快递地址、物流信息）、个人信息（婚姻、户籍、社保）等。

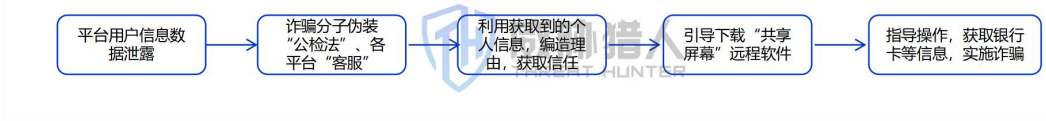


在 2024 年上半年发现的数据泄露事件中，威胁猎人累计发现 657 起“查档”信息泄露事件，占整体数据泄露事件的 4.10%。从每月变化趋势来看，查档类的相关风险事件数呈上升趋势，相关黑产团伙数量也不断增加。一定程度上反映出通过查档进行非法收益的形式更加普遍，背后收益更加可观。



3.4 利用“共享屏幕”诈骗的事件高发，2024 年上半年监测“共享屏幕”远程软件达 25 种

2024 年上半年，利用“共享屏幕”诈骗的事件频繁发生，诈骗分子通过一些非法渠道获取乘客个人信息、航班信息，冒充航空公司工作人员，通过短信或电话的方式通知航班延误或取消。通过一些特定的话术，以“退费”“理赔”等理由引导受害人下载具有屏幕共享功能的 App，再通过屏幕共享状态下获取的用户信息实施诈骗，具体流程如下：



举一个真实的案例：

李某接到陌生来电，冒充某航空公司的“客服”告知其航班需要改签同时会进行相关赔偿，要求李某点击某线上会议链接开启屏幕共享，由于对方能准确说出自己的航班信息，李某信以为真，按照其要求进行了屏幕共享的操作。

此时诈骗者利用该功能趁机获取李某个人信息，并以进行身份认证、解绑银行卡为由，要求李某提供自己的银行卡号、密码、手机验证码等信息，并进行人脸识别，最终李某银行卡里的 30000 元被对方全部转走。

进一步研究发现，利用“屏幕共享”的诈骗手法层出不穷，“共享屏幕”远程软件快速更新，据威胁猎人风险情报平台数据统计，仅在 2024 年上半年就发现了 25 种被黑产恶意利用的“共享屏幕”远程软件，如常见的“畅联云”、“Vymeet”等等。

04

结语

四、结语

从 2024 年上半年数据泄露风险现状来看，企业需要重点关注以下问题：

1、“数据泄露有效事件数”及“黑产交易团伙数量”持续上涨，数据泄露风险态势不容乐观

2024 年上半年（1-6 月）全网监测并验证有效的数据泄露事件共计 16011 起，较 2023 年下半年增长 59.58%；此外监测涉及数据交易的黑产团伙共计 1973 个，较 2023 年下半年增新增 984 个（增长近一倍），Telegram 非法数据交易团伙的整体活跃度不断上升。

2、银行、电商、消费金融等行业仍处数据泄露高位，银行数据泄露事件 2876 起位列第一

2024 年上半年数据泄露事件涉及 85 个行业，涉及企业 1489 家，数据泄露事件数量 Top5 行业分别为银行、电商、消费金融、保险、快递。其中，银行行业数据泄露事件数量高达 2876 起，成为数据泄露事件数最多的行业。

3、2024 年数据泄露人群地区分布 TOP3：浙江、四川、广东

从区域维度来看，2024 年上半年数据泄露人群最多的区域分别是：浙江、四川、广东；从年龄段维度来看，35-54 岁占比达 62%；从性别维度来看，女性占比达 64%。

针对以上情况，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，威胁猎人提出了针对性的解决方案：

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：**2023 年 10 月，在深圳、重庆建立两大应急响应中心，并在深圳、上海、重庆、北京等地建立售后服务中心，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”

深圳永安在线科技有限公司（品牌名：威胁猎人）

官方服务热线：400-809-3699

官方合作邮箱：marketing@threathunter.cn

官网地址：www.threathunter.cn