威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

2024年保险行业数据泄露风险半年度报告

出品方：威胁猎人

THREAT HUNTER

以客户为中心 | 正直 | 求真

目录

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，已成为各行各业数字化发展赛道的严重阻碍。

保险行业作为金融行业三大支柱产业之一，涉及大量高净值人群，数据转化效率高，变现能力强，是黑灰产重点攻击的对象。威胁猎人近期发布的《2024 年上半年数据泄露风险态势报告》数据显示，**保险行业 2024 年上半年发生数据泄露事件 2039 起，行业排名第四。**

一旦发生数据泄露，或数据泄露后不及时管控，导致数据被黑灰产进行大范围交易、作恶，严重损害平台客户的利益，保险等金融机构不仅会遭到客户投诉，同时也会面临监管部门的惩罚，损害其经济和品牌声誉。

威胁猎人长期致力于黑灰产业链及数据泄露风险的深入挖掘和研究，报告将与同业者一起探讨保险行业数据资产泄露的主要特点和发展

相关名词定义：

1、DRRC：威胁猎人在深圳、重庆成立 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，排除历史虚假信息、确认有效的数据泄露事件；

5、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；

6、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；

7、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；

8、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；

9、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；

10、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；

11、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。

12、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；

13、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；

14、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；

15、基础字段：主要指个人基础信息，包括个人信息（姓名、手机号、身份证号、出生日期、性别、年龄、邮箱、具体居住地、学历等）、财产信息（收入情况、车牌号、汽车品牌、号码种类、车价等）、家庭信息（婚姻情况、家庭关系等）、工作信息（企业单位、职业等）；

16、业务字段：主要指保险业务相关信息，包括投保类型（险种）、投保日期、保障期限、投保金额、保单号、保单形式、保单目的、投保责任、缴费形式、平台名称、订单编号、订单支付状态、订单支付金额、订单来源等；

17、黑产自定义字段：黑产为了提高黑产数据交易价值及效率，会对数据进行清洗后定义，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）。进行标记，防止被二次贩卖）。

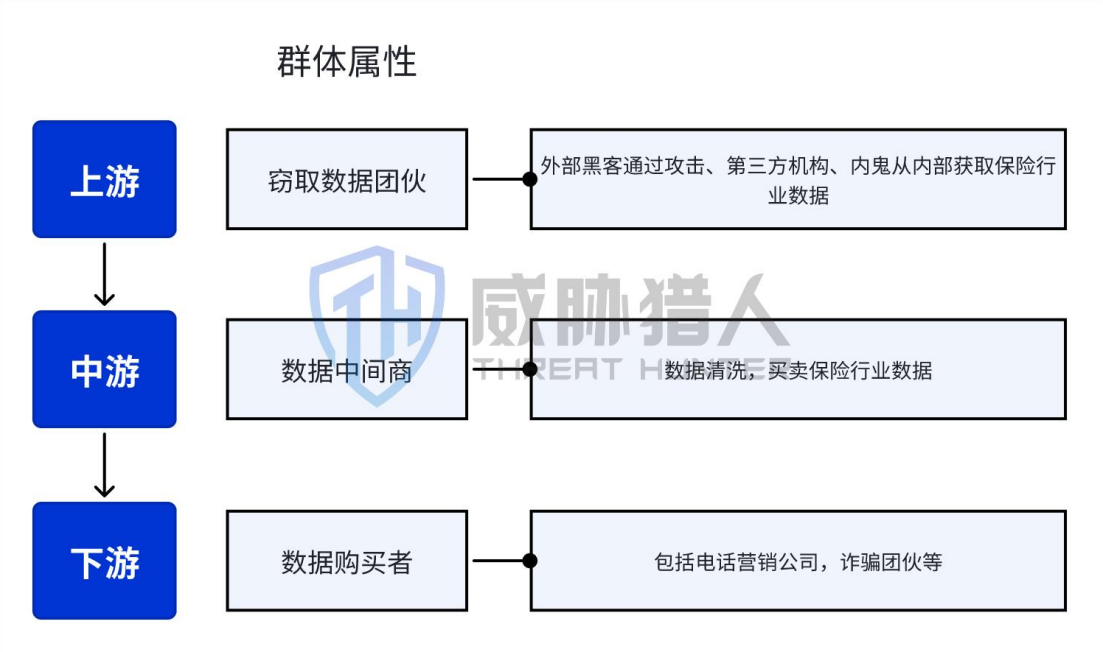
01

保险行业

数据泄露黑色产业链介绍

一、保险行业数据泄露黑色产业链介绍

威胁猎人针对保险行业数据泄露产业链进行深入研究，发现围绕数据资产泄漏和倒卖的产业链目前已经相当成熟，基于明确的分工和定位分为上、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。这些人专门负责从保险机构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。

注：下文将会对保险行业已被攻击平台、数据泄露渠道等进行分析，详情见第二章。

中游：数据中间商

大部分活跃在暗网、Telegram、黑产论坛、Potato 等平台，这些人在不同的平台上发布帖

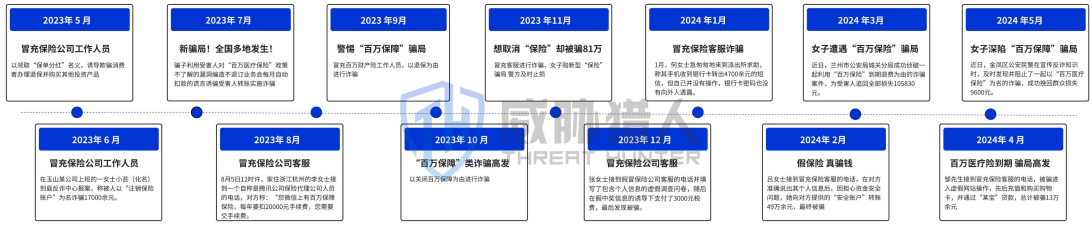
子销售数据，并负责对数据进行分类和清洗，以满足下游客户的各种需求。

注：下文将会对保险行业已泄露数据的地下交易渠道、数据字段等进行分析，详情见第二章。

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。比如，利用保险客户数据推销新的保险产品，或者利用理赔用户数据进行保险理赔诈骗等。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。

威胁猎人梳理了 2023 年 5 月至 2024 年 5 月发生和保险行业相关的涉诈事件，平均每月都有诈骗事件发生，**保险行业相关诈骗事件高频发生。**根据过往的保险行业相关的诈骗案例，可见，泄露出的个人信息是**保险行业诈骗**发生的主要基础要素：电诈团伙可利用泄露的个人信息和保险相关数据，量身定制剧本和话术，来实施虚假理赔、身份盗窃、保险欺诈等活动。



诈骗流程大体如下：

诈骗话术框架如下：

02

2024 上半年保险行业数据泄露风险概况

二、2024 上半年保险行业数据泄露风险概况

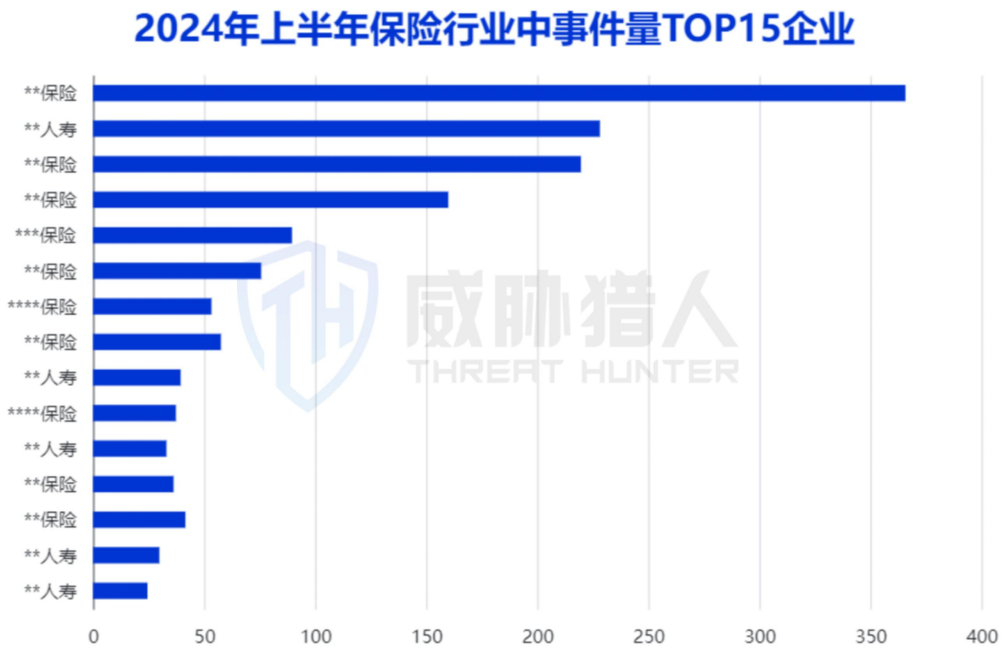
2.1 2024 上半年保险行业数据泄露事件共有 2039 起，涉及 80 家保险机构

2024 年上半年威胁猎人全网监测到的 1.1 亿条情报，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，涉及 85 个行业**，其中**保险行业排名第四，共有 2039 起**，平均每月约 340 起，**涉及 80 家保险机构。**

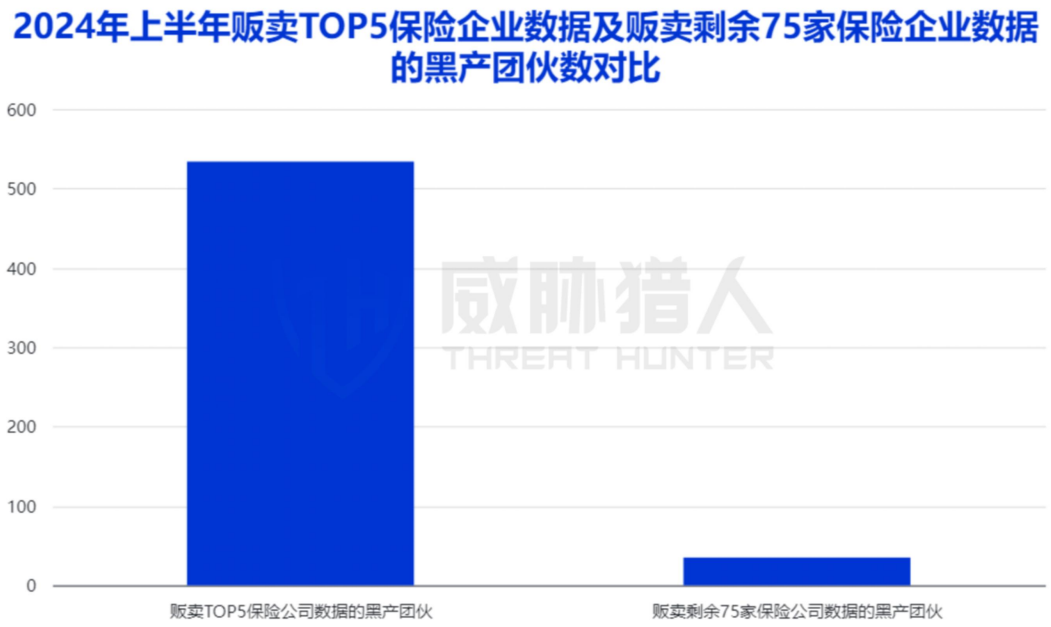
2.2 国内大型保险机构是黑产团伙的主要攻击对象，数据泄露事件占比超 50%

威胁猎人情报研究员对上半年存在数据泄露最多的 15 家保险机构进一步分析发现，这 15 家保险机构涉及的数据泄露事件占据了整个保险行业数据泄露总量的近 80%，其中 Top5

机构数据泄露事件占比超 50%。

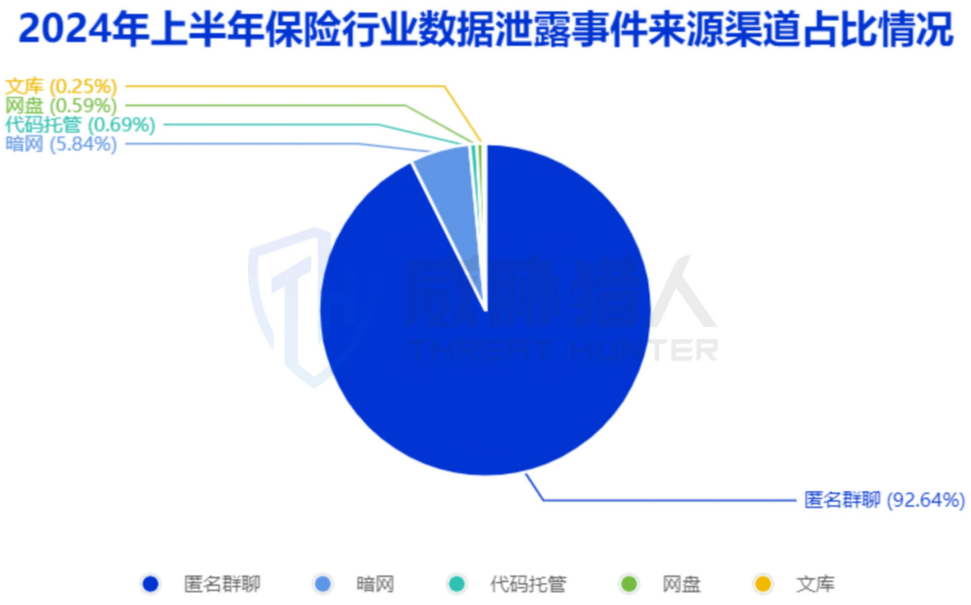


对 Top5 机构及黑产数据交易情况进一步分析，Top5 均是国内保险十大品牌的保险机构，机构规模大、平台用户群体多、用户数据量大；从黑产交易团伙来看，非法贩卖保险机构数据的黑产团伙共计有 569 个，其中贩卖 Top5 机构数据的黑产团伙数量共有 534 个，远超售卖其他机构数据的黑产团伙数量。由此可见，Top5 保险机构是黑产团伙主要的攻击目标。



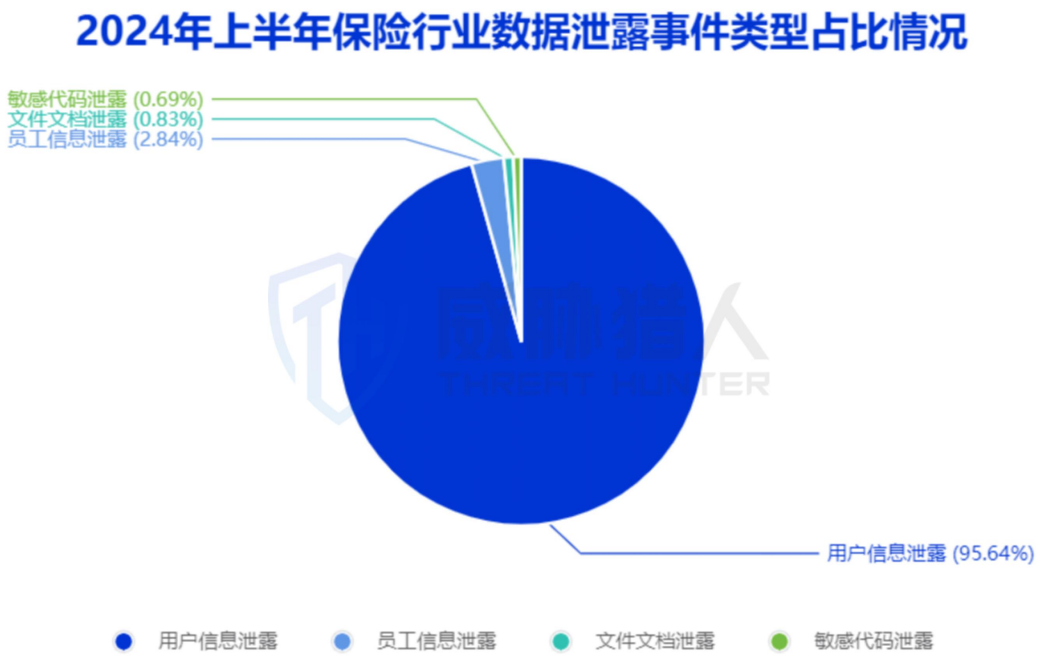
2.3 TG 和暗网渠道是非法数据交易的主要交易渠道，占比超过 98%

威胁猎人针对保险行业数据泄露的交易渠道进行分析发现，匿名群聊 Telegram 和暗网占比 98.47%，是黑产进行非法数据交易的主要渠道，与 2024 年上半年全行业非法数据交易渠道分布基本一致。



2.4 保险行业被泄露的数据类型主要是用户信息，占比超 95%

威胁猎人针对保险行业泄露的数据信息进行分析发现，泄露的数据中用户信息类占比高达 95.64%，为非法数据交易的主要类型。



用户信息：为平台用户个人信息，包含姓名、手机号、身份证号、保险相关信息、健康信息、财产信息等；

员工信息：为企业员工个人信息以及职业信息，包括员工姓名、手机号、身份证、职业岗位等信息；

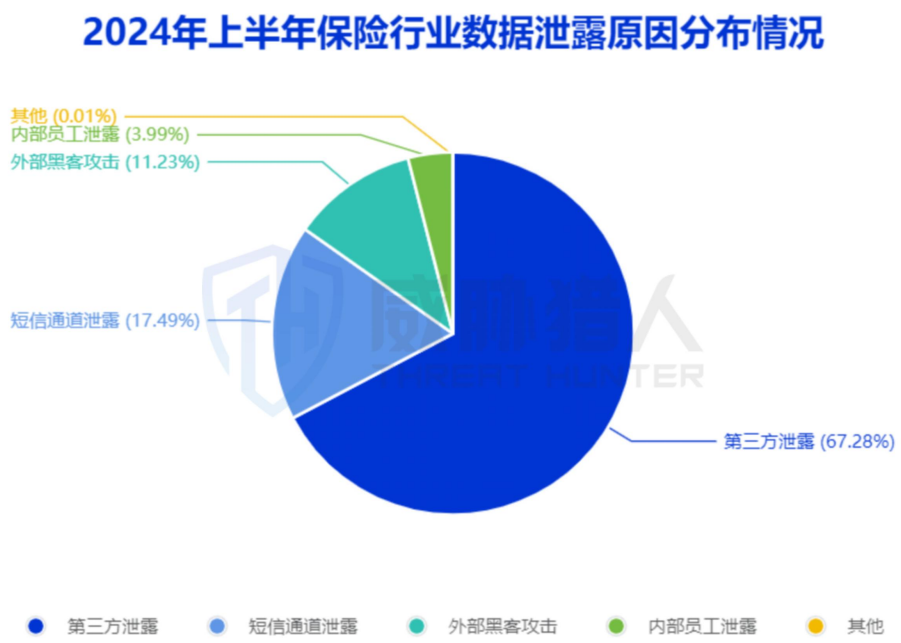
敏感文件：为企业内部敏感文件文档信息，包括企业内部机密文档、合同文件、产品图纸等信息；

敏感代码：为企业内部敏感代码信息，包括源码信息、API 接口密钥、环境配置、域名等信息。

注：为进一步了解被泄露的用户信息详情，威胁猎人针对泄露的数据字段进行了分析，详情见第三章。

2.5 保险行业被泄露数据主要来源于第三方泄露，其次是短信通道泄露

威胁猎人针对保险行业数据泄露的源头进行分析，第三方导致的数据泄露是主要原因，占比高达 67.28%，其次是短信通道泄露，占比 17.39%，外部黑客攻击占比 11.23%，内部员工泄露 3.99%。



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；

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。

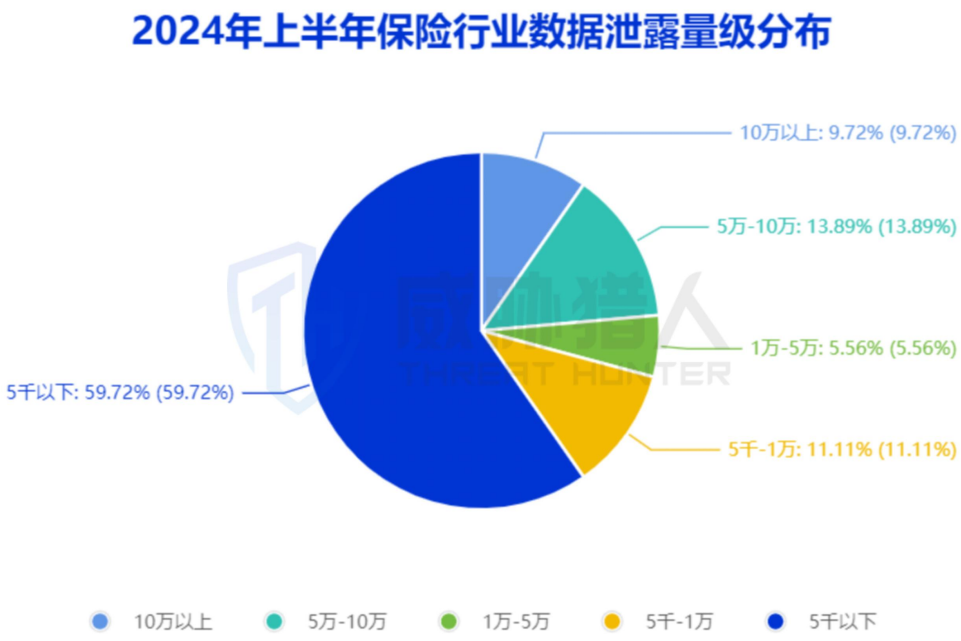
运营商通道：黑产通过运营商内鬼或违规代理等渠道，获取到指定网页的访问数据、指定应用的安装数据、指定短信的接收和发送数据等信息；

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。

2.6 单个事件泄露的数据量以小规模居多，5000 条以下占比将近 60%

2024 年上半年，威胁猎人捕获到的保险行业黑产数据交易量级以 5000 条以下小规模居多，占比 59.72%。



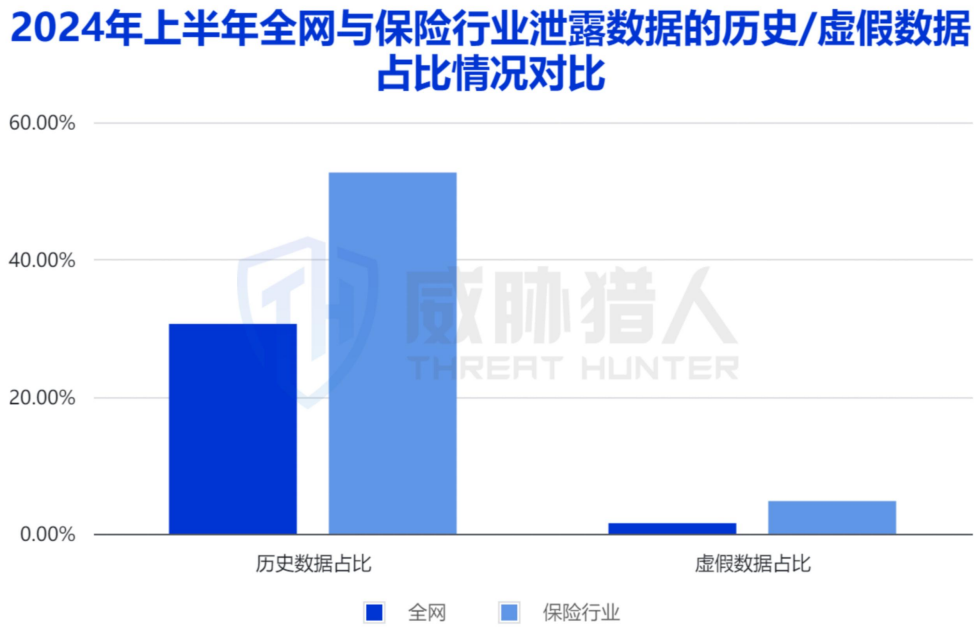
虽然整体以小规模数据交易为主，也存在不少单次泄露数据量级 10 万以上的，**其中最高可达 70 万条数据**，进一步分析，该事件为 2022 年某保险机构出现的重大数据泄露事件。

2.7 保险行业被黑产交易的数据中历史数据、虚假数据占比远超全网水平

威胁猎人针对保险行业被黑产交易的数据进行真实性验证分析发现，其虚假数据、历史数据占比远超全网整体水平：

从历史数据的维度上分析，泄露的保险数据中有 52.67%为历史泄露的数据，超过全网的历史数据占比 30.60%；

从数据的真实性维度上分析，泄露的保险数据中有 4.76%为虚假不匹配的信息数据，超过全网虚假数据占比 1.54%。



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。

威胁猎人真实性验证引擎会基于数据样例的历史重合度、三要素匹配度，以及信源置信度等维度对风险情报进行可信度评估和初步验证，帮助企业识别黑产发布的虚假数据、历史数据及无关数据，提高事件预警的准确性和可信度。

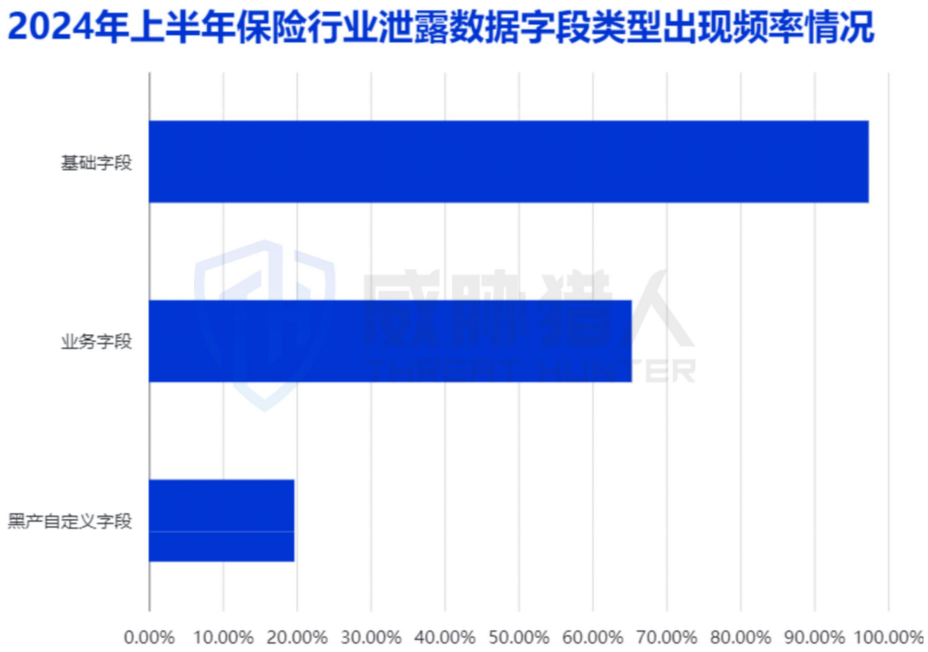
03

保险行业数据泄露字段及人群画像分析

三、保险行业数据泄露字段及人群画像分析

3.1 近 98%的数据包含个人基础信息，20%的数据包含黑产自定义标签

威胁猎人针对保险行业被泄露的数据字段统计分析发现，数据字段主要包含基础字段、业务字段和黑产定义字段等类型，**其中 97.40%的数据包含了基础字段，有 65.35%的数据包含了业务字段，值得关注的是，黑产自定义字段达到了 19.71%，黑产为了提高黑产数据交易价值及效率，会对数据进行清洗并自定义标签。**



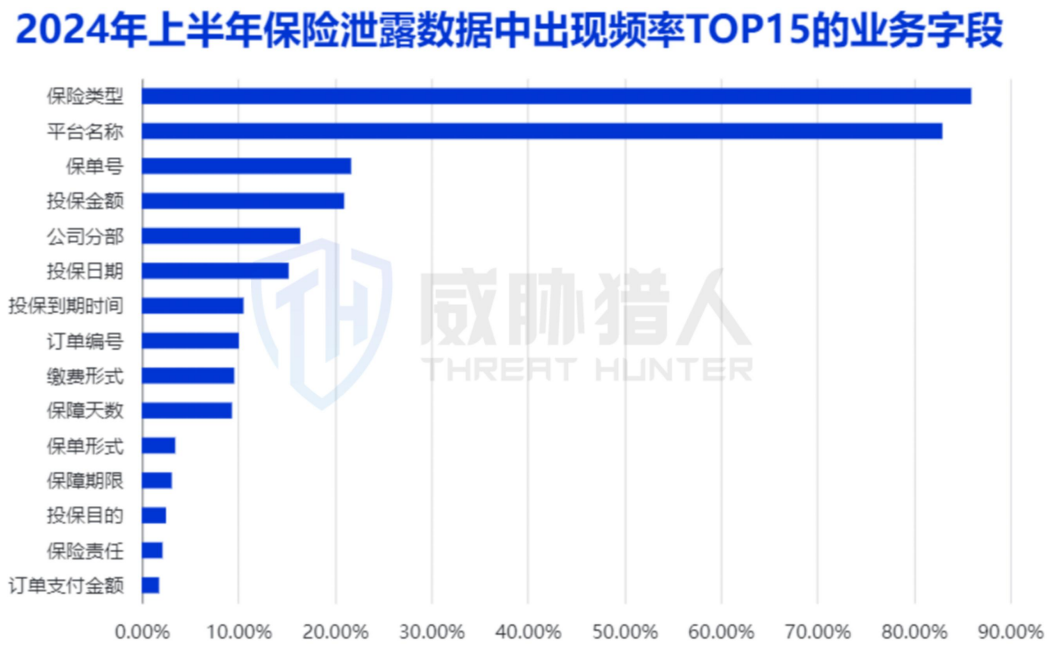
基础字段：主要指个人基础信息，包括个人信息（姓名、手机号、身份证号、出生日期、性别、年龄、邮箱、具体居住地、学历等）、财产信息（收入情况、车牌号、汽车品牌、号码种类、车价等）、家庭信息（婚姻情况、家庭关系等）、工作信息（企业单位、职业等）；

业务字段：主要指保险业务相关信息，包括投保类型（险种）、投保日期、保障期限、投保金额、保单号、保单形式、保单目的、投保责任、缴费形式、平台名称、订单编号、订单支付状态、订单支付金额、订单来源等；

黑产自定义字段：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）。

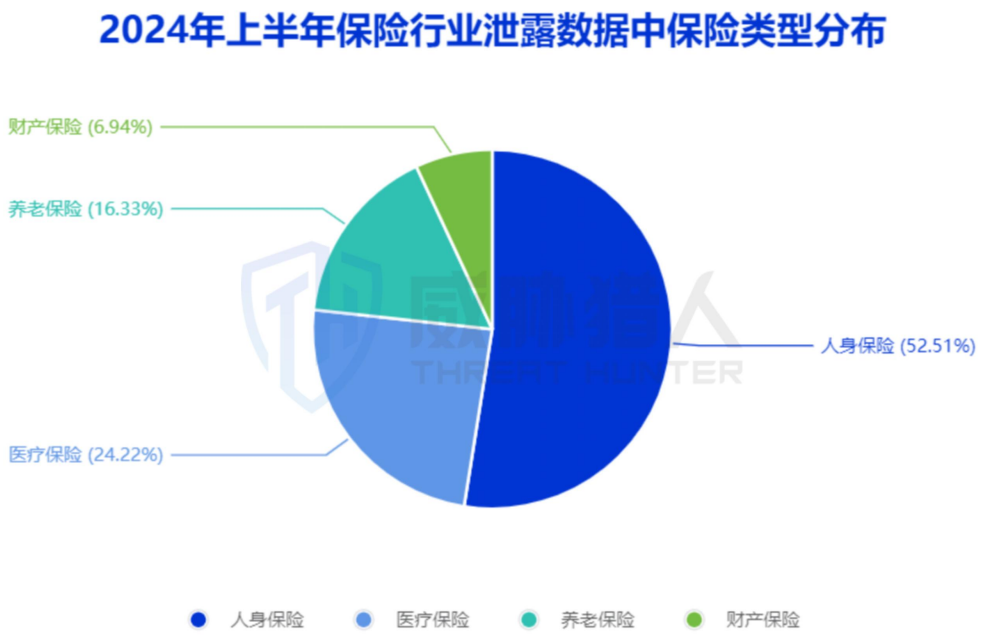
3.2 保险业务字段出现频率最高的是“保险类型”和“平台名称”

威胁猎人针对保险业务信息字段进行分析发现，“保险类型”、“平台名称”、“保单号”、“投保金额”等字段的出现频率较高，其中“保险类型”最高，高达 85.97%，其次是“平台名称”，高达 82.97%。这些数据指向性非常高，诈骗团伙一旦获取到这些数据，可精准地掌握到保险机构用户的投保情况并进行诈骗。



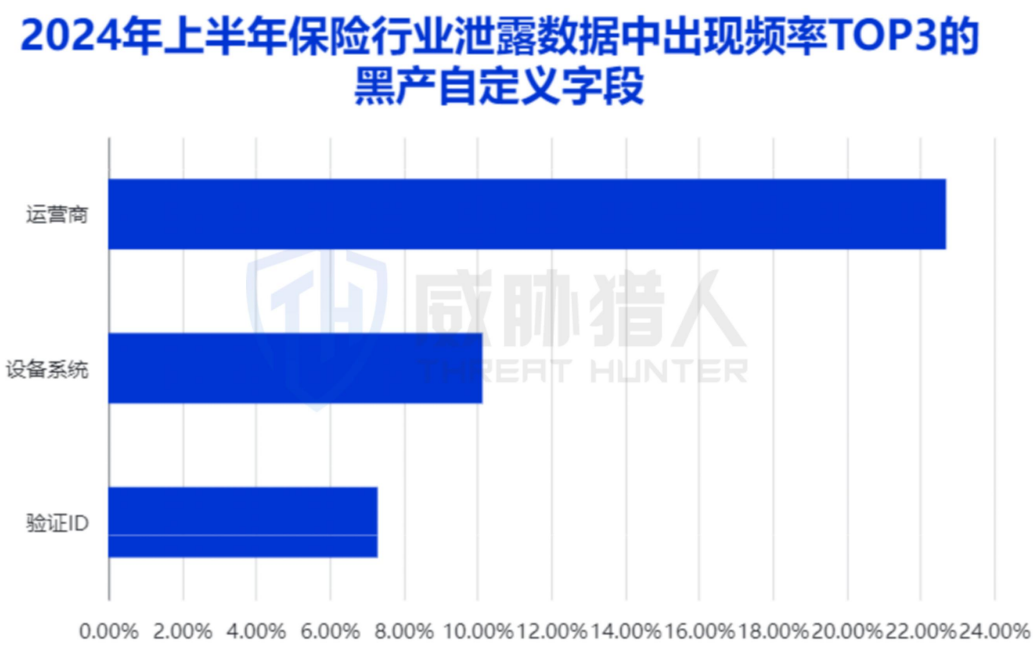
3.3 “保险类型”中“人身保险”占比最高，以“人寿保险”和“年金保险”居多

威胁猎人针对“保险类型”进行分析，被泄露的保险行业数据主要涉及“人身保险”、“医疗保险”、“养老保险”以及“财产保险”等产品，其中“人身保险”占比最高，达 52.51%。进一步分析发现，**“人身保险”产品中，“人寿保险”、“年金保险”居多。**



3.4 诈骗团伙通过“IOS”字段标签对保险平台用户进行精准诈骗

为了提高黑产数据交易价值及效率，黑产团伙会对数据进行清洗并自定义标签。2024 年上半年，被泄露的数据中出现大量黑产定义字段，**“运营商”、“设备系统”、“验证 ID”**等出现频率最高：



值得关注的是，“设备系统”中有大量标注“IOS”的数据，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。

在威胁猎人《2024 年上半年数据泄露风险态势报告》中有提到，诈骗分子正是通过筛选出“IOS”用户信息来通过 Facetime 功能进行诈骗，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。

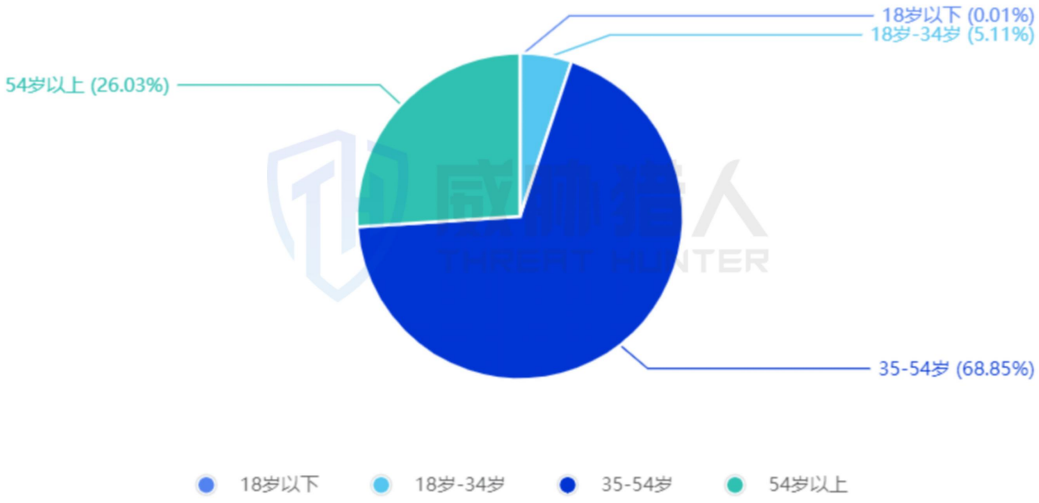
以一个真实事件为例：

3 月 19 日，受害人林先生接到陌生号码打来的 FaceTime 视频电话，对方称其在网络上购买了“百万医疗保险”，每个月缴费标准是 800 元，一年费用为 9600 元。如果没有办理取消手续的话，就要一直扣款。受害人林某信以为真，便按照对方要求办理解除手续，被引导通过支付宝向指定的支付宝账户发送口令红包，被骗 30 余万元。

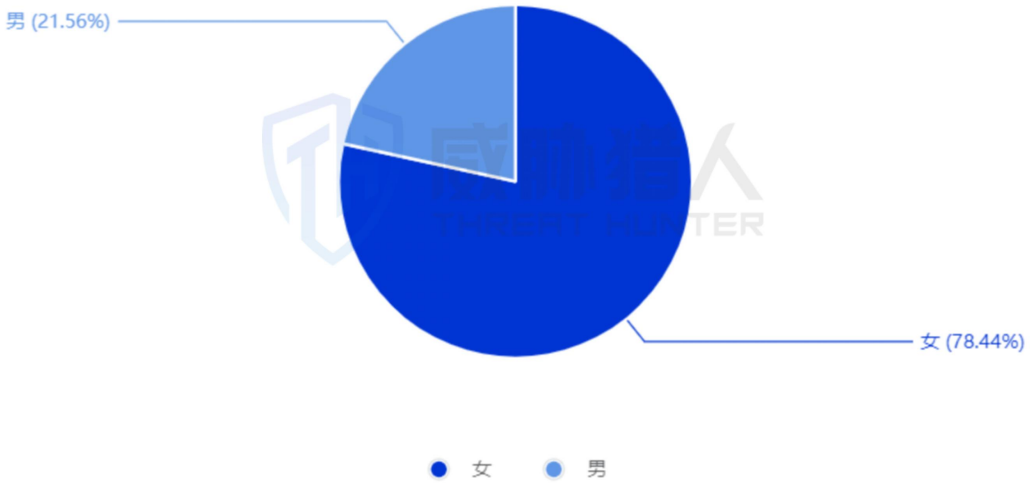
3.5 保险行业数据泄露用户群体主要集中在浙江、四川等地，以中年女性为主

威胁猎人通过对保险行业泄露数据的人群画像进行抽样分析，发现保险行业数据泄露的受害群体，在地区上主要集中在浙江、四川、江苏等地；在年龄分布上，35 岁至 54 岁之间的人群占比最多，达 68.85%；在性别分布上，女性占比 78.44%，远超于男性占比 21.56%。

2024年上半年保险行业数据泄露人群年龄段分布情况



2024年上半年保险行业数据泄露人群性别分布情况



04

保险行业
典型数据泄露事件分析

四、保险行业典型数据泄露事件分析

4.1 因第三方安全管控不足，导致大量保险行业敏感数据泄露

保险机构为了提升业务拓展效率和服务质量，往往会引入第三方合作代理，很多第三方合作代理是以“业务优先”的中小型企业，在安全建设上的投入相对较少，而且业务会涉及到大量客户的敏感数据，很容易成为黑产攻击的对象。

威胁猎人在匿名聊天平台渠道的监测情报分析发现，大量保险行业的敏感数据正在被交易，其中泄露的数据字段不仅包含用户的个人信息，且包含用户的投保具体信息（保险类型、投保金额、保险周期等），同时涉及到多家保险企业。

数据样例如下：

人身意外伤害方案	24	51.00	刘	身份证	男	310	2812	644075	刘	上海市	上海市	保险
人身意外伤害方案	48	129.70	刘	身份证	女	310	0946	555239	刘	上海市	上海市	保险
人身意外伤害方案	32	88.96	单	身份证	女	310	2826	67157	单	上海市	上海市	保险
人身意外伤害方案	32	633.44	卜	身份证	女	341	532X	9224	卜	上海市	上海市	保险
人身意外伤害方案	56	412.08	卫	身份证	女	310	1228	3821	卫	上海市	上海市	保险
门急诊医疗方案	20	554.52	印	身份证	女	310	2025	723	印	上海市	上海市	保险
人身意外伤害方案	8	2582.00	吕	身份证	女	141	0024	081	吕	上海市	上海市	保险
人身意外伤害方案	8	3229.30	吴	身份证	女	310	0029	10	吴	上海市	上海市	保险
人身意外伤害方案	8	1904.08	吴	身份证	男	310	7519	8	吴	上海市	上海市	保险
人身意外伤害方案	8	1000.00	吴	身份证	女	310	5105	0	吴	上海市	上海市	保险
人身意外伤害方案	32	1167.90	吴	身份证	女	310	1467		吴	上海市	上海市	保险
人身意外伤害方案	8	1970.00	吴	身份证	女	310	0464		吴	上海市	上海市	保险
人身意外伤害方案	48	1146.24	吴	身份证	男	310	4012		吴	上海市	上海市	保险
人身意外伤害方案	32	680.40	吴	身份证	女	310	5226		吴	上海市	上海市	保险
人身意外伤害方案	360	117.94	吴	身份证	女	310	042X		吴	上海市	上海市	保险
人身意外伤害方案	16	30.00	吴	身份证	女	310	3223		吴	上海市	上海市	保险
人身意外伤害方案	56	358.10	吴	身份证	女	310	0024		吴	上海市	上海市	保险
人身意外伤害方案	136	6.57	周	身份证	女	310	3264		周	上海市	上海市	保险
人身意外伤害方案	112	36.40	周	身份证	女	310	0569		周	上海市	上海市	保险
人身意外伤害方案	376	182.59	周	身份证	男	310	4655		周	上海市	上海市	保险
人身意外伤害方案	80	670.33	周	身份证	女	320	3424		周	上海市	上海市	保险
人身意外伤害方案	24	295.88	周	身份证	男	310	3459		周	上海市	上海市	保险
人身意外伤害方案	8	600.00	周	身份证	男	310	1216		周	上海市	上海市	保险
人身意外伤害方案	248	0.00	周	身份证	男	310	2417		周	上海市	上海市	保险
人身意外伤害方案	48	426.00	周	身份证	女	310	3041		周	上海市	上海市	保险
人身意外伤害方案	56	71.40	周	身份证	女	310	322X		周	上海市	上海市	保险
人身意外伤害方案	8	420.89	周	身份证	男	330	2715		周	上海市	上海市	保险
人身意外伤害方案	16	227.14	周	身份证	女	310	0665	1705	周	上海市	上海市	保险
人身意外伤害方案	8	1000.00	周	身份证	男	310	0032		周	上海市	上海市	保险
人身意外伤害方案	72	541.23	唐	身份证	女	310	1923		唐	上海市	上海市	保险

分析过程：

威胁猎人发现此类数据样例泄露的数据字段较为齐全，不仅包含个人信息，且包含保险信息，

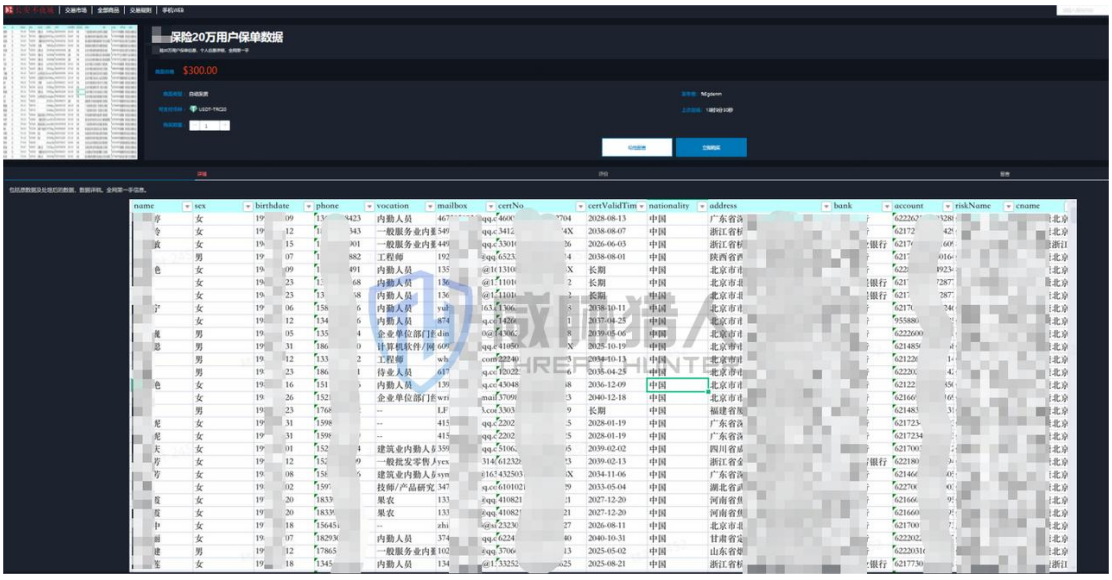
同时涉及多家保险机构，因此威胁猎人初步判断为该多家保险机构有关联合作的第三方所导致的泄露。

4.2 某保险机构 API 机构被黑客攻击，20 万用户保单信息泄露

随着各行业网络安全水位不断提高，黑客入侵并获取后台权限的难度越来越高，因此不少黑客将攻击对象瞄准为存在安全缺陷的 API 接口，通过数据遍历攻击等方式窃取数据。

威胁猎人在暗网平台渠道的监测情报分析发现，国内某保险机构 **20 万用户保单信息数据被黑产进行售卖，以 300 美元的价格进行出售**，泄露的数据样例中不仅包含用户姓名、手机号等基础信息，此外还有用户的工作岗位、家庭地址以及银行卡等信息。

数据样例如下：



分析过程如下：

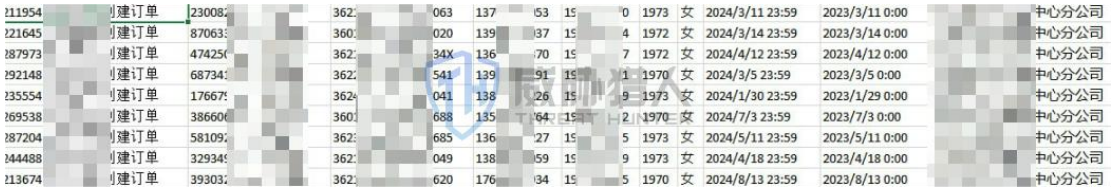
根据该暗网帖子提供的信息来看，对方售卖的保险数据仅涉及到国内某一保险机构，针对性较强；同时泄露的数据字段较为齐全，涉及多个敏感字段信息。因此结合以上两点，威胁猎

人初步判断疑似为外部黑客攻击该保险机构所导致的。

4.3 疑似保险机构“内鬼”非法获取用户数据获利

威胁猎人在匿名聊天平台渠道的监测情报分析发现，有黑产在售卖国内某保险机构用户信息数据，以下为提供的数据样例信息。

数据样例：



211954	创建订单	230082	362	063	137	53	15	0	1973	女	2024/3/11 23:59	2023/3/11 0:00		中心分公司
221645	创建订单	87063	360	020	139	37	15	4	1972	女	2024/3/14 23:59	2023/3/14 0:00		中心分公司
287973	创建订单	474256	362	34X	136	70	15	7	1972	女	2024/4/12 23:59	2023/4/12 0:00		中心分公司
292148	创建订单	68734	362	541	139	91	15	1	1970	女	2024/3/5 23:59	2023/3/5 0:00		中心分公司
235554	创建订单	17667	362	041	138	26	15	9	1973	女	2024/1/30 23:59	2023/1/29 0:00		中心分公司
269538	创建订单	38660	360	688	135	64	15	2	1970	女	2024/7/3 23:59	2023/7/3 0:00		中心分公司
287204	创建订单	58109	362	685	136	27	15	5	1973	女	2024/5/11 23:59	2023/5/11 0:00		中心分公司
244488	创建订单	32934	362	049	138	59	15	9	1973	女	2024/4/18 23:59	2023/4/18 0:00		中心分公司
213674	创建订单	39303	362	620	176	34	15	5	1970	女	2024/8/13 23:59	2023/8/13 0:00		中心分公司

分析过程：

威胁猎人分析到该数据样例中不仅包含用户的个人信息，同时还包含有企业内部关于保险机构的创建状态、保险机构分公司的情况。

因此，威胁猎人初步判断为疑似该保险机构内部员工采用内部渠道非法获取数据后售卖到数据交易市场。

4.4 疑似短信通道存在安全隐患导致保险机构数据泄露

威胁猎人在匿名聊天平台渠道的监测情报分析发现，有黑产在售卖保险机构用户短信信息数据，以下为提供的数据样例信息。

数据样例：

陈	135	1198	女	1984	广东	佛山	【 】保单生效通知：尊敬的	今日生
肖	180	6197	男	1975	湖南	长沙	【 】保单生效通知：尊敬的	今日生
王	135	2198	男	1983	陕西	宝鸡	【 】保单生效通知：尊敬的	今日生
钟	136	7198	男	1984	湖南	长沙	【 】保单生效通知：尊敬的	今日生
罗	138	1197	女	1976	湖南	岳阳	【 】保单生效通知：尊敬的	今日生
肖	153	1198	女	1983	湖南	长沙	【 】保单生效通知：尊敬的	日生效
黄	130	1198	女	1989	广东	深圳	【 】保单生效通知：尊敬的	日生效
刘	139	3197	女	1972	海南	海口	【 】保单生效通知：尊敬的	今日生
张	137	2198	女	1985	广东	东莞	【 】保单生效通知：尊敬的	今日生
钟	152	1198	女	1986	广东	东莞	【 】保单生效通知：尊敬的	今日生

分析过程：

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。

短信数据泄露源来自短信通道，短信通道一般为三方服务，其本身存在被渗透或信息泄露的风险，导致三方服务内的数据泄露。

威胁猎人根据泄露的数据样例分析到，泄露的数据中包含用户短信内容，而企业自身平台短信下发接口安全防护都比较完善，因此初步判断疑似泄露渠道为短信通道所导致泄露的。

05

结语

五、结语

2024 年上半年保险行业数据泄露事件不容乐观。从保险行业数据泄露风险状况来看，企业需要重点关注以下问题：

1、2024 年上半年保险行业数据泄露事件数 2039 起，涉及 80 家保险机构

2024 年上半年，全网数据泄露事件共计 16011 起，保险行业排名第 4，共有 2039 起，平均每月约 340 起，涉及 80 家保险机构。

2、大型保险机构是黑产团伙的主要攻击对象，数据泄露事件占比超 50%

2024 年上半年 Top5 均是国内保险十大品牌的保险机构，机构规模大、平台用户群体多、用户数据量大，贩卖 Top5 保险机构数据的黑产团伙 534 个（非法贩卖保险企业信息数据的黑产团伙共计 569 个）。

3、第三方泄露、短信通道泄露是保险机构数据泄露的主要原因

与前几年不同，随着保险机构对数据保护的日渐加强，重视内部系统的数据安全管理，传统的内鬼泄露、渗透拖库等导致的数据泄露逐渐减少，合作方数据访问管控不当、短信通道泄露等方式成为当前主流，2024 年保险行业数据泄露事件由第三方导致的占比高达 67.28%，由短信通道导致的数据泄露事件占比 17.39%。

4、“保险类型”中“人身保险”占比最高，以“人寿保险”和“年金保险”居多

2024 年上半年保险行业被泄露的数据中，涉及“人身保险”的数据占比最高，达 52.51%；进一步分析发现，“人身保险”产品中，“人寿保险”、“年金保险”居多。

5、保险行业被黑产交易的数据中虚假数据、历史数据占比远超全网水平

2024 年上半年泄露的保险数据中，有 52.67%为历史泄露的数据，超过全网的历史数据占比 30.60%；有 4.76%为虚假不匹配的信息数据，超过全网虚假数据占比 1.54%。

6、保险行业数据泄露用户群体主要集中在浙江、四川等地，且以中年女性为主

从区域维度来看，2024 年上半年保险行业数据泄露人群最多的区域分别是：浙江、四川等地；从年龄段维度来看，35-54 岁占比达 68.85%；从性别维度来看，女性占比达 78.44%。

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