威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

2022年数据资产泄露分析报告

出品方：威胁猎人

THREAT HUNTER

以客户为中心 | 正直 | 求真

目录

Contents

前言

大数据、互联网为企业带来无限发展生机的同时，也暗藏了巨大的数据安全隐患。伴随数字化转型深入发展，数据泄露事件的频率、规模和成本也较往年有所上升，对不少企业造成了持续、难以消弭的影响。

2022 年 2 月，国内主流招聘平台简历数据疑遭爬取，涉及 2.1 亿余条个人信息；

2022 年 7 月，国内某视频分享平台 2.2 亿余条用户 ID、手机号疑被出售;

2022 年 11 月，Meta 被罚 2.65 亿美元，起因是 Facebook 遭遇爬虫攻击致 5.33 亿用户数据泄露;

……

威胁猎人《**2022 年数据资产泄露分析报告**》基于过去 1 年捕获到的数据泄露事件，结合数据安全现状，多维度呈现 2022 年国内数据泄露的态势全景。

01

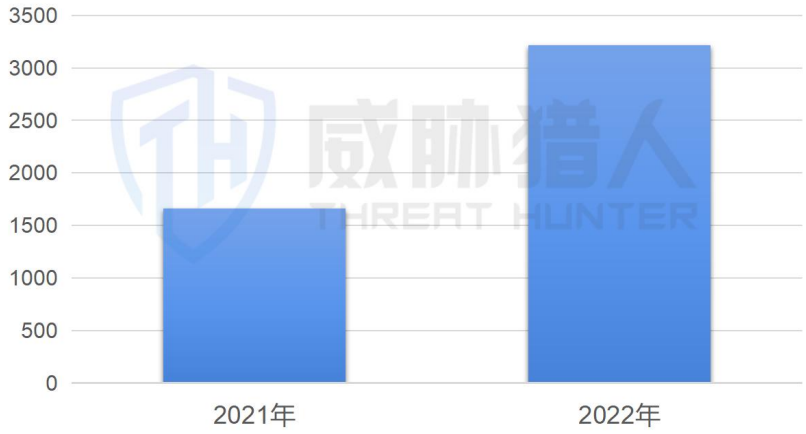
数据泄漏风险概况

一、2022 年 数据泄漏风险概况

1、2022 年累计捕获数据泄露事件超 3200 起，较 2021 年上升近一倍

威胁猎人情报平台在 2022 年发现并验证有效的数据泄露事件超过 3200 起，与 2021 年相比，上升了将近一倍，其中下半年数据泄漏事件的数量比上半年明显增多。

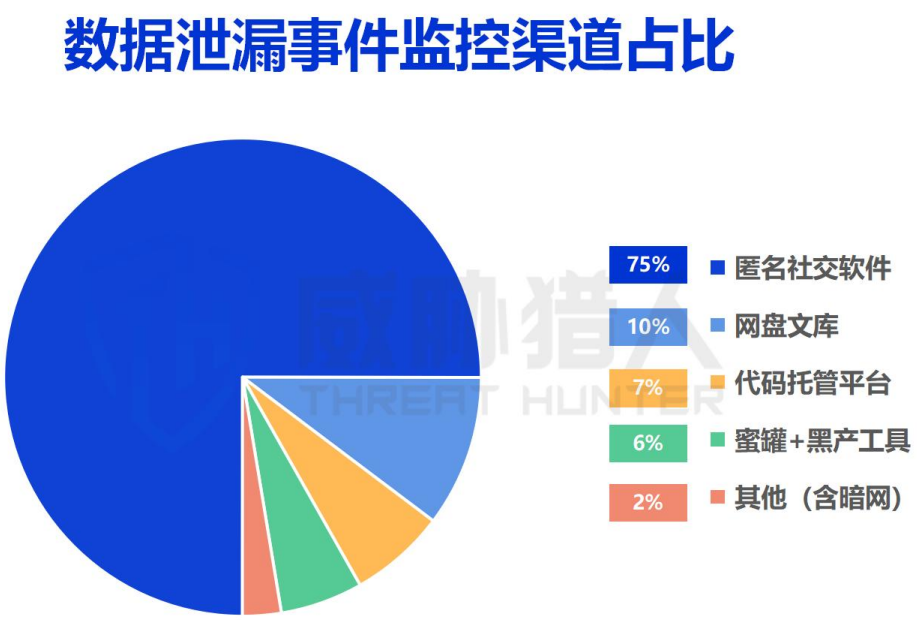
数据泄漏事件年度数量对比



数据泄漏事件月度数量趋势

2、数据泄露渠道来源广泛，匿名社交软件占比超 75%

如下是 2022 年威胁猎人情报研究员从各渠道发现的数据泄露事件占比，超过 75%的数据泄露事件通过匿名社交软件发现，匿名社交软件以 Telegram 为主。



2022 年，威胁猎人情报平台捕获数据泄漏事件的主要渠道如下：

匿名社交软件：以 Telegram（飞机）、Potato（土豆）、Batchat（蝙蝠）等为代表的匿名社交软件，被黑产用来作为数据交易的平台，是当前捕获数据泄露事件的主要渠道；

网盘文库：一些企业员工将网盘和文库作为文件存储和文档共享的工具，由于安全意识不足等原因，可能会误传一些包含敏感信息的文件或文档，且任何人都可以公开访问，最终导致数据泄露；

代码托管平台：一些开发人员会将编写的代码上传到 Github、Gitee 等代码托管平台，可能会暴露后台地址、账号、密码等敏感信息。

2017 年，丰田“T-Connect”应用程序源代码发布在 Github 遭受恶意利用，泄露了 30 万客户的电子邮件，直到 5 年后的 2022 年 10 月才发现并更改；

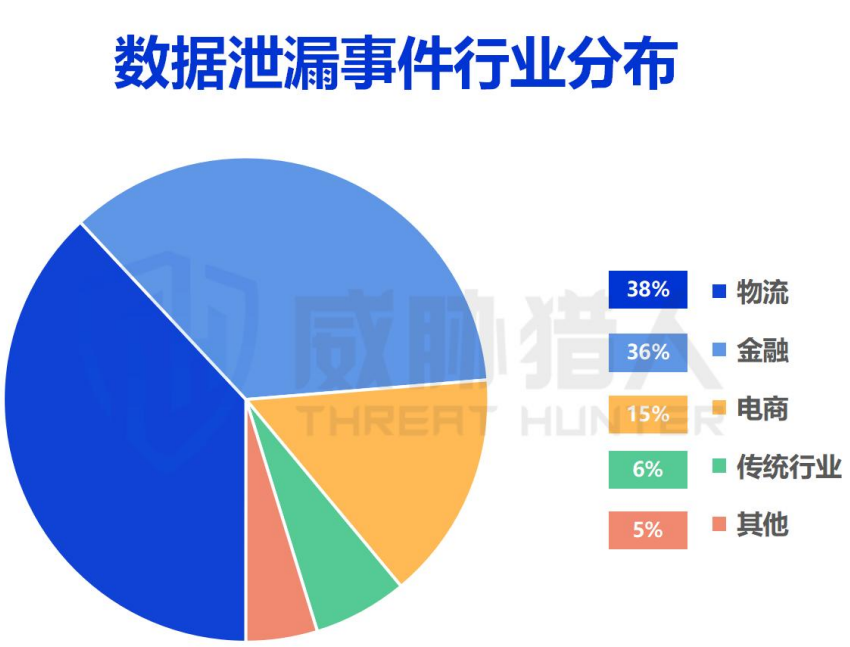
蜜罐+黑产工具：威胁猎人独有的蜜罐技术和黑产工具分析技术，实时捕获网络黑灰产的攻击流量，通过对这些攻击流量进行分析，可以发现大量窃取数据的攻击，成为发现数据泄露事件的重要渠道之一。

暗网：基于 Tor、I2P 等匿名通信技术构建的暗网网络，存在着各种地下交易市场和论坛，历史上不少的重大数据泄露事件都在暗网最先曝光；

此外，还包含以 Raid Forums、Breach Forums 等为代表的**黑产论坛、公共媒体**等渠道。

3、2022 年数据泄露行业分布中，金融、物流、电商行业占据前三

从行业分布来看，2022 年捕获的数据泄露事件中，占比较大的是金融行业、物流行业、电商行业。

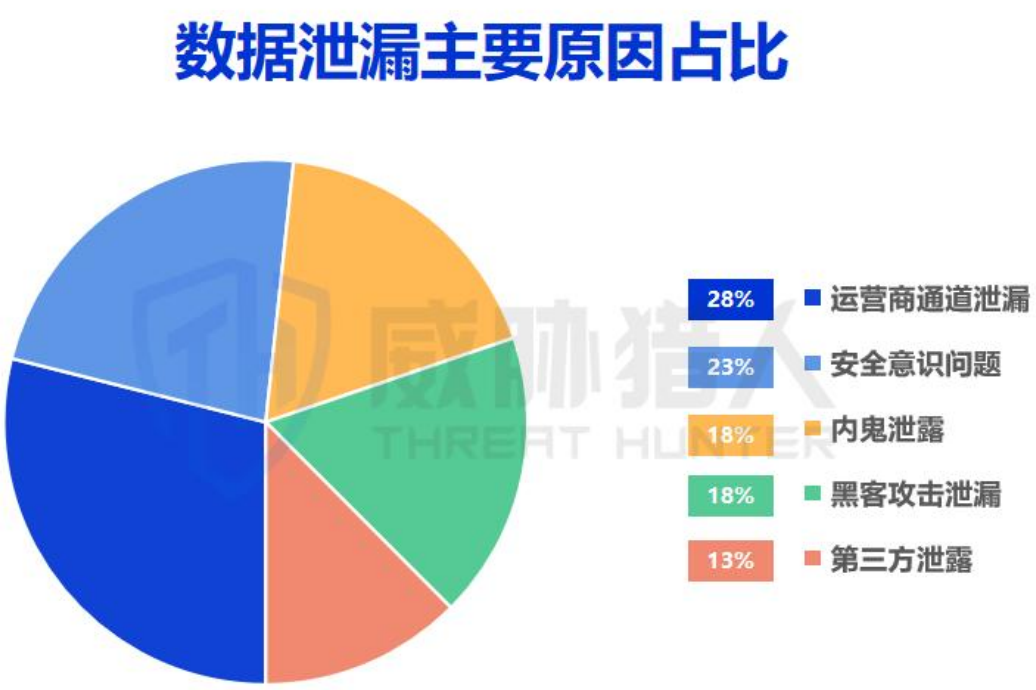


金融行业因涉及大量高价值用户数据，且靠近交易环节，成为了黑产攻击的主要对象。金融行业的数据泄露事件主要体现在**借贷、银行、证券、保险**等企业的客户信息倒卖，通常被下游黑产团伙用于精准营销及诈骗。

伴随线上购物的火热发展，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，逐渐成为了黑产团伙的重点目标，同样被用于营销或诈骗。

4、2022 年数据泄露主要原因中，运营商通道泄露占比第一

2022 年威胁猎人捕获的数据泄露事件中，部分事件可以通过溯源分析定位到泄露原因。经威胁猎人情报专家统计分析，2022 年数据泄露的主要原因及占比如下：



运营商通道：黑产通过违规代理或运营商内鬼等，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；

安全意识问题：企业内部员工在工作过程中，无意识间把公司内部的重要文件、文档、代码等，上传到网盘文库、代码托管平台等公网环境；

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：黑客使用爬虫、扫描、渗透等方式攻击企业的网络资产和系统，找出安全漏洞后大规模窃取数据；

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。

第三方泄露：和企业存在合作关系的第三方，具有访问企业部分敏感数据的权限，因数据权限管理不规范等问题，导致这些敏感数据通过第三方泄露到黑产手中。

02

地下黑产数据交易分析

二、2022 年地下黑市数据交易分析

1、Telegram 取代暗网交易市场，成为数据交易最主要的平台

曾经最大的中文暗网交易市场之一“茶马古道”在 2021 年底被警方捣毁，后续又发展出了“长安不夜城”、“自由国度”等暗网交易市场。

2022 年暗网交易市场发布的数据售卖信息不在少数，但经过分析和验证，暗网交易市场发布的数据中绝大多数都是历史泄露数据、虚假数据或渗水数据，新出现的真实泄露数据比重较少。

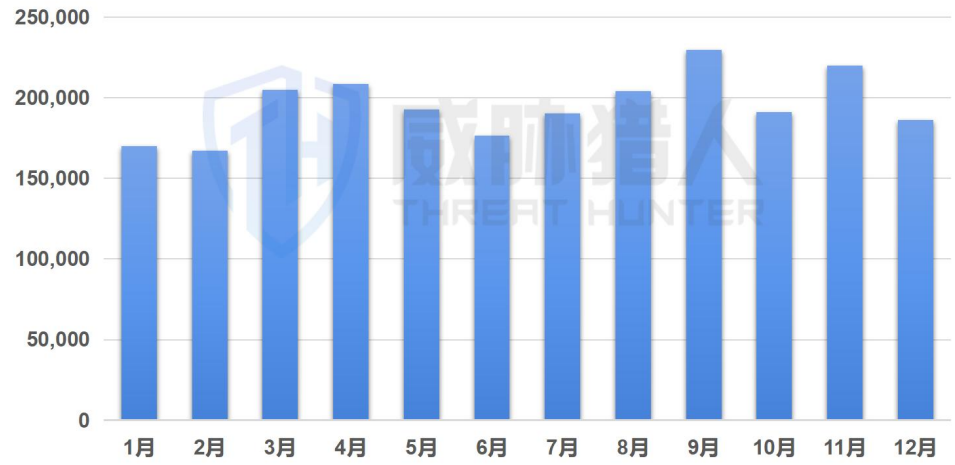
经研究分析，主要原因如下：

1、由于警方对暗网市场展开多轮打击，很多数据卖家不再将其视为首选平台；

2、由于部分暗网交易市场出现无法提现、管理员跑路等情况，大大降低了卖家对平台的信任。

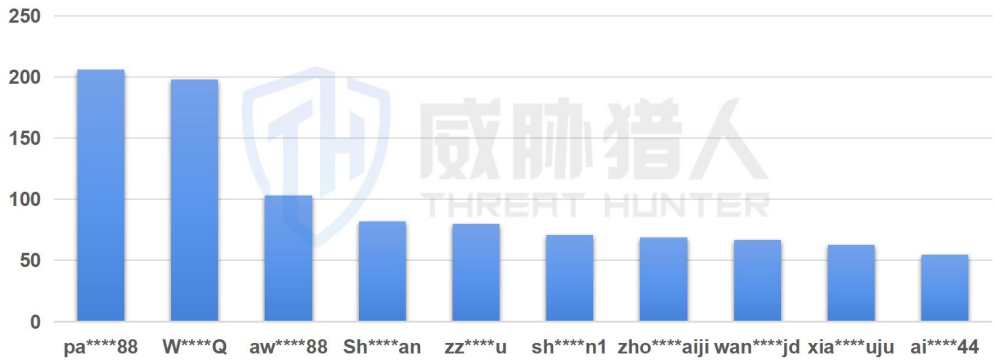
相较之下，匿名社交软件 Telegram 已逐渐取代暗网交易市场，成为黑产非法交易数据最主要的平台。2022 年，威胁猎人监控到 Telegram 上活跃的黑产人员超过 146 万，平均每个月活跃超过 19.5 万。

2022年每月Telegram活跃黑产人数



经研究调查发现，Telegram 上长期活跃的黑产团伙中，2022 年数据交易数量排名前十的黑产团伙，进行数据交易超过 50 起，排名前二的黑产团伙累计进行数据交易达到 200 起左右。

TG数据交易Top10黑产团伙泄漏事件数量



这些黑产团伙在 Telegram 上创建了多个群聊、频道以及机器人，一旦掌握新的数据就会在这些渠道发布售卖信息，吸引更多购买者。2 月 12 日，疑似 45 亿地址信息泄露事件引起了广泛关注，该团伙最早就是在其 Telegram 频道上发布的相关数据信息。

2、小规模的实时数据成为数据交易的主流

2022 年，威胁猎人情报平台捕获的地下黑市数据交易中，约有 71%的交易披露了售卖的数据量，其中交易数据量级在 1W 以下的“小规模的实时数据” 超过了 73%，成为数据交易的主流。

经威胁猎人研究分析，小规模数据交易成为主流的原因如下：

1、在部分数据泄露的渠道中，卖家一次性可以获取的数据往往较少，甚至需要买家提前预订；

2、这些数据虽量级不大，但基本都是实时或准实时的数据，有效性好，因此更易受到买家的“青睐”；

3、实时数据的单价往往比较高，一次性购买大量实时数据的花费过高。

相较而言，大规模数据交易由于量大、成本高，少有买家“吃得消”，且里面可能存在较多的历史数据，数据价值有限，因此大规模数据交易占比大大降低。

3、“历史数据+新数据”组合进行交易的事件频发

为提高精准营销或诈骗的效果，下游黑产团伙往往需要尽可能多地掌握受害者信息，因此卖家也会通过组合数据进行交易，其中最典型的就是“历史数据”组合“新数据”。

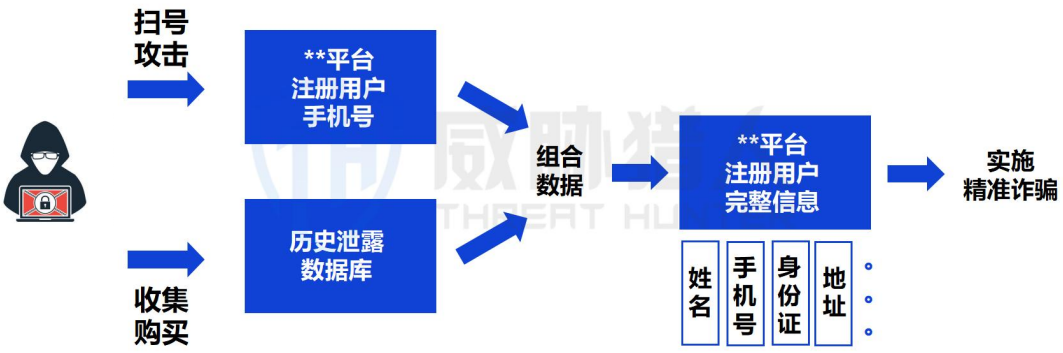
对于历史数据，很多数据卖家掌握了海量的历史泄露库，从历史数据中可以提取出大量的姓名、手机号、身份证、住址等个人敏感信息。

对于新数据，黑产团伙利用某些金融、电商等平台存在安全缺陷的 API 接口，通过批量扫号攻击的方式，筛选出该平台注册用户的手机号。

以手机号为关联，将历史数据和新数据进行组合，就可以得到一份全面的数据，包括某平台注册用户的手机号、姓名、身份证、住址等信息。

2022 年威胁猎人情报平台通过蜜罐技术捕获到了大量的扫号攻击，覆盖多个平台。在攻击者传入的手机号中，有不少手机号与历史泄露数据库中的手机号吻合。

“历史数据+新数据”组合进行交易流程



03

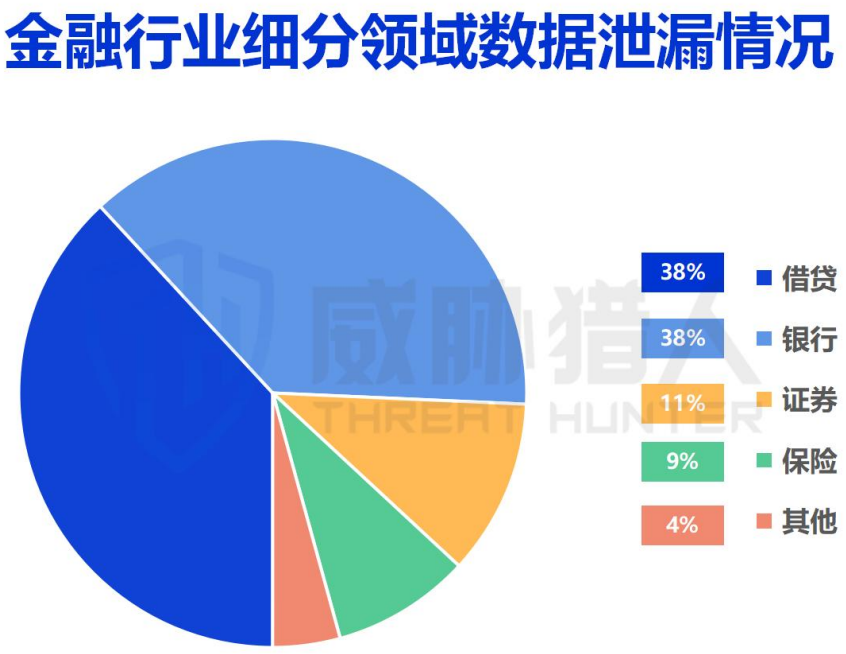
数据泄漏案例

三、2022 年值得关注的数据泄露案例

1、金融机构数据泄漏事件累计捕获超 1100 起，涉及企业超 300 家

金融机构在开展业务的过程中积累了海量的高价值数据，这些高价值数据一直都是黑产团伙眼中的“香馍馍”，在威胁猎人数据泄露监测情报中，金融机构的数据泄露事件往往排名前列。

2022 年，威胁猎人累计捕获到超过 1100 起金融机构相关的数据泄露事件，涉及的企业超过 300 家，覆盖银行、证券、保险、借贷等多个细分领域。

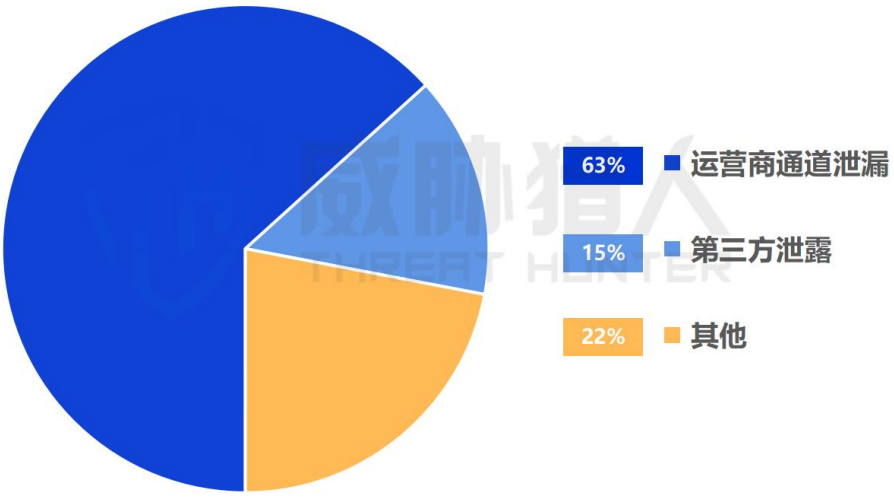


2022 年 11 月，威胁猎人情报平台监控到国内某银行泄露客户信息数据超过 8 万条，泄露的数据格式包含客户姓名、身份证号、出生日期、贷款情况、手机号、有无抵押以及婚姻状况、文化程度等敏感字段。

该类数据往往会被下游黑产团伙用于精准营销以及诈骗作恶，例如通过获取客户贷款信息，以短信、手机号等方式联系客户，进行相关贷款平台的精准营销，又或通过冒充某银行工作人员报出客户相关信息，诱导用户进行转账或其他违法操作。

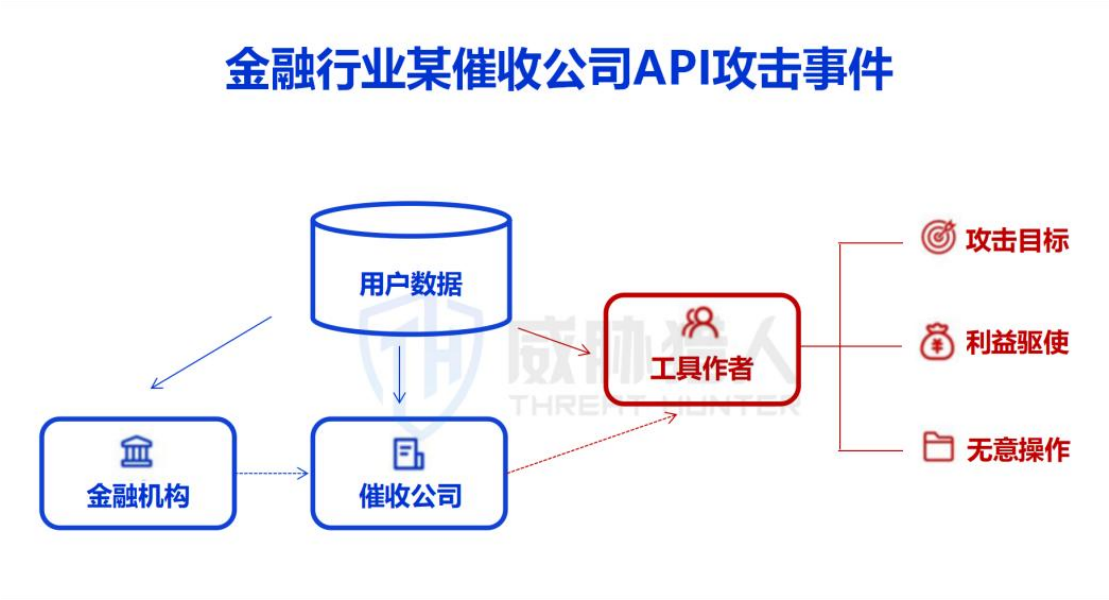
当前，金融机构在数据安全建设上已经较为成熟，但在数字化交互的推动及利益的驱使下，客户信息仍然通过**运营商通道、第三方工具/平台**等方式被黑产窃取，给“严监管、高标准”的金融行业带来了前所未有的风险与挑战。

金融机构数据泄漏主要原因占比



金融机构由运营商通道、第三方工具/平台引发数据泄露的事件屡屡发生。2022 年 7 月至 8 月，威胁猎人情报平台捕获到了多起国内借贷平台客户短信内容数据泄露，经研究发现，泄露原因主要是**运营商通道泄露**，泄露的数据格式主要包含用户手机号、短信内容、接收短信时间以及姓名等敏感字段。

2022 年，威胁猎人 Karma 情报平台监控到某**第三方催收公司**通过外部的工具作者开发自动化的“**催收辅助工具**”，涉及到多家金融机构。经研究分析发现，“催收辅助工具”可以绕过催收系统，通过**破解和伪造“拉取数据的 API 接口”请求**，获得用户数据的访问权限并批量下载客户数据（包括借款人名字、身份证、借款数量、住址等），不受系统访问权限和操作限制的影响，给金融机构带来了较大的数据泄露风险。



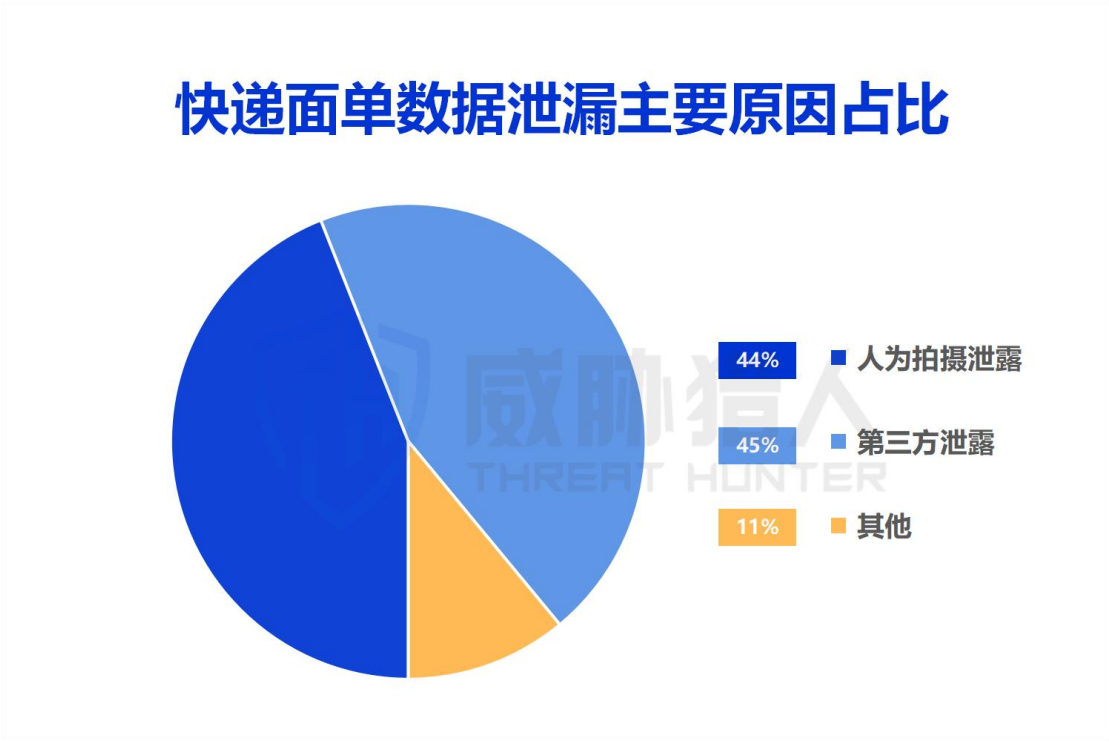
2、物流行业数据泄漏事件累计捕获超 1200 起，泄露量级最高超 100 万

2022 年威胁猎人累计捕获到超过 1200 起物流行业相关的数据泄露事件，涉及 40 家物流快递公司，泄露量级最高超过 100 万，平均每天有超过 1 万条的用户信息在地下黑市交易，价格基本保持在 3-4 元每条。其中主要是快递面单导致的泄露，泄露的信息包含寄收件人的姓名、手机号、商品信息、快递单号、时间等敏感字段。

经调查分析，快递面单泄露的主要原因包括：

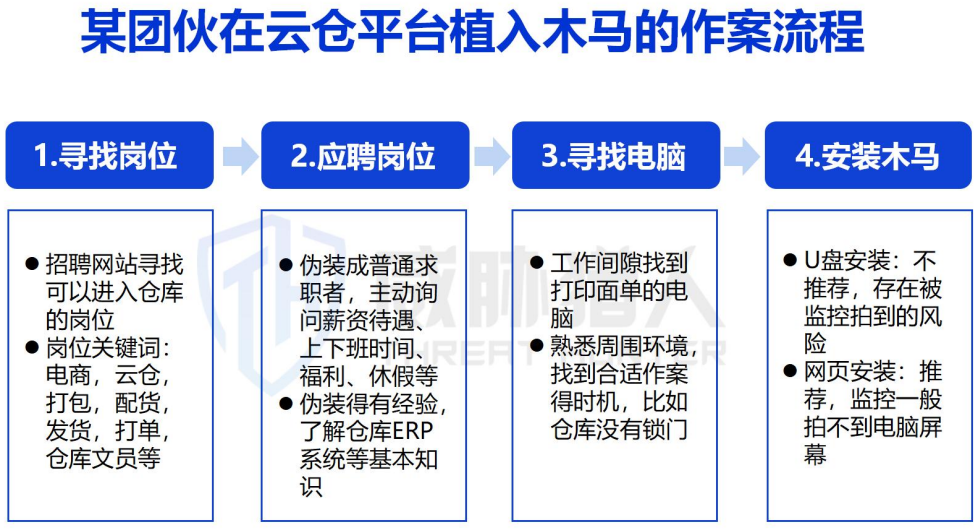
1. **人为拍摄泄露：**快递站点工作人员进行面单拍摄并出售给黑产；

2. **第三方渠道泄露：**企业使用的第三方渠道存储了大量快递数据，相关第三方平台对快递数据保管不当，或受黑产攻击导致数据泄露。



物流行业某云仓平台被植入木马、漏洞攻击：

2022 年，威胁猎人情报平台监控到多个有组织的黑产团伙，以云仓或者电商园区打印面单的电脑为目标展开作案。黑产团伙以应聘工作为由虚假入职国内某云仓，伺机在其使用的工作电脑或面单打印机电脑上**安装木马软件**，对用户敏感信息数据进行窃取，并在数据交易市场上以**单价 3 元**进行售卖。



3、电商行业数据泄露事件累计捕获近 500 起，涉及国内外知名品牌

近年来新电商和新零售发展如火如荼，众多用户通过商家自有电商、第三方电商、直播电商等方式进行购物，产生了海量购物信息，随之而来的数据泄露风险也逐渐增加。2022 年威胁猎人累计捕获到近 500 起与电商行业相关的数据泄露事件，涉及美妆、服装等国内外知名品牌。

2022 年 5 月份，威胁猎人监测到国内某大型美妆品牌的电商平台购物数据遭到泄露，泄露量级超过 15 万条，泄露的数据包含客户姓名、手机号、商品信息、下单时间、支付方式、收件地址等诸多敏感信息。

经分析，电商行业数据泄露的主要原因包括：

1、物流环节泄露；

2、店铺运营“内鬼”泄露；

3、第三方工具软件泄露。

如前文所提，金融和物流行业出现第三方渠道导致的数据泄露的事件不在少数，在电商行业，很多店铺商家为了提高运营效率，往往会使用第三方开发工具软件管理客户、订单、服务等，这些工具逐渐成为了黑产窃取数据的重要突破口。

以某店铺商家使用的第三方工具为例：

2022 年 3 月，威胁猎人情报平台捕获到一款店铺商家使用的第三方工具，该工具内置了一个后端接口，可以对已加密的购物数据进行解密，从而获取到明文的订单号、客户姓名、地

址、电话号码等信息。一旦该接口遭到黑产恶意攻击，所有使用该工具的商家，其订单信息将全部遭到泄露：

某店铺商家因第三方工具引发信息爬取：

2022 年 6 月，威胁猎人通过蜜罐技术捕获到了一起黑产盗取商家 Token 并爬取订单信息的攻击行为。

商家需授权第三方工具登录电商平台，而黑产团伙通过在第三方工具中植入后门，成功获取到了多个商家的登录 Token，并利用拿到的 Token 批量请求订单接口并爬取数据。为避免被发现，黑产利用了秒拨代理 IP 等黑产资源，不同商家使用不同的 IP。

4、传统行业数据泄露事件累计捕获超 200 起，涉及 24 家国内外知名汽车品牌

2022 年威胁猎人共监控到超过 200 起跟传统行业相关的数据泄露事件，值得关注的是，汽车行业的数据泄露事件共涉及 24 家国内外知名汽车品牌，泄露数据包含车辆品牌、识别代码、发动机号、客户姓名、手机号、车牌号等敏感信息。其中泄露量级最高超过 270 万条，黑产以平均单价 6.5 元在地下黑市进行交易。

由于传统行业数字化进展起步较晚，在数据安全建设中往往存在防守的薄弱环节，其中 API 接口存在安全缺陷是最为典型的薄弱环节，黑客利用未授权访问、敏感数据过度暴露等 API 安全缺陷，对 API 接口发起数据遍历攻击，批量窃取平台的用户数据或业务数据。

以国内某大型企业的 API 攻击事件为例：

2022 年 12 月，威胁猎人情报平台捕获到了一起极为严重的传统行业数据泄露事件。国内某大型企业的 API 接口存在敏感数据过度暴露的缺陷，黑产通过攻击该接口获取到了企业内部员工的姓名、身份证、手机号、住址、密码等敏感信息（如下图）。

```
"address": "兰溪市                                    ",
"empNo": "3101      ",
"idNo": "33078                    ",
"idtype": "身份证",
"email": null,
"ophone": "15          ",
"empName": "钱      ",
"officephone": "150          ",
"groupId": "0001G1          ",
"orgId": "0001G11000          ",
"psndocId": "0001G                    ",
"sex": "",
"photoUrl": null,
"password": "6aa1                                                    ",
"qq": null,
"wx": null,
"orgName": "                有限公司",
"deptName": "供应部业务一处",
"postName": "业务主管",
```


黑产获取到的密码并非明文密码，而是密码 md5，但只要密码复杂度不高，基本都可以通过彩虹表还原出原始的明文密码。攻击者可以利用泄露的手机号和密码，以员工的身份登录该企业的 OA 系统，入侵内部网络展开进一步攻击，给该企业带来难以预估的损失。

注：想了解更多与 API 安全相关的数据泄露案例，可点击查看《2022 年 API 安全研究报告》。

04

数据保护措施与建议

四、数据保护措施与建议

在日渐严峻的安全形势下，数据安全日益得到重视。2022 年，《数据出境安全评估办法》、《数据安全管理与保护指引》、《信息安全技术关键信息基础设施安全保护要求》等一系列数据安全的政策法规陆续发布，在数据安全、合规等方面提出了更明确的要求及实现路径，这也增加了企业安全合规的压力。

2022 年 7 月,《数据出境安全评估办法》审议通过，提出数据出境安全评估坚持**事前评估和持续监督相结合、风险自评估与安全评估相结合**等原则。

2022 年 12 月，《证券期货业数据安全管理与保护指引》发布，从数据安全管理基本原则、组织架构、制度、技术等方面提供指引，**规范行业机构数据安全管理和保护工作**，体现了数据安全对于证券期货业的重要性和紧迫性。

2022 年 10 月，《信息安全技术关键信息基础设施安全保护要求》发布，规定了关键信息基础设施运营者在**识别分析、安全防护、检测评估、监测预警、主动防御、事件处置**等方面的安全要求。

“网络攻击”高一尺，“数据保护”需再高一丈。面对越来越多的数据泄露风险，企业需要从多个维度保障企业及其用户的数据安全，**不仅要对内部数据资产状况了如指掌，更需要基于外部风险情报监测来及早感知及时防御。**

针对内部资产管理，威胁猎人安全专家建议企业在“业务优先”的基础上，基于情报对已上线的 API 及 API 上流动数据资产进行整体梳理，实现对所有 API 资产及流动敏感数据的可视，再进行持续的 API 缺陷评估及攻击威胁感知，实现 API 风险可控。

针对外部情报监测，企业可通过全网多渠道监测及时感知数据泄露风险，在事件发生之前进行预防和阻断，做到先于攻击者发现攻击面，利用对外部情报的监测更好地保护组织数字资产。

兼顾数据安全内外部视角，做到内部数据安全与外部威情报监测相结合，企业才能在数字化建设与创新发展的道路上走得既稳又快。

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

总部地址：深圳市南山区科华路3号讯美科技广场3号楼1609

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