威胁猎人 THREAT HUNTER

以情报构筑数字化安全基石

2026年上半年
企业品牌外部风险研究报告

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。

继《2026 年上半年互联网黑灰产研究报告》发布后，威胁猎人进一步将观察视角聚焦于企业品牌边界之外，正式发布《2026 年上半年企业品牌外部风险研究报告》。

这是威胁猎人连续多年发布的互联网黑灰产行业研究报告，也是威胁猎人面向行业固定推出的年度趋势观察成果。作为专注于黑灰产情报与业务反欺诈的安全厂商，威胁猎人已在黑灰产情报领域深耕 10 年，依托长期积累的风险数据、真实攻击样本与企业治理实践，持续追踪黑产资源、攻击手法与产业链变化，持续为企业判断风险趋势、制定治理策略提供参考。

目录

前言

2026 年上半年，企业品牌保护正在经历一次深层转变，从处置单一仿冒资产，转向保护企业与用户之间的可信连接。数据泄露、身份冒用、渠道截流与公开披露等风险，正在从不同位置共同影响品牌身份、官方渠道、客户关系与公共声誉。我们围绕品牌外部风险全景、风险形成机制、重点行业差异与典型案例四个板块，梳理五项核心判断。这五项判断共同呈现出一套相互关联的风险变化：品牌保护由此不再只是发现和下架仿冒资产，而是需要同时识别信息暴露、渠道滥用及其对用户信任的持续影响。

报告内容关键点总结：

- **品牌保护正在从处置单一仿冒资产，转向保护企业与用户之间的可信连接。**涉及品牌身份、官方渠道、客户关系和公共声誉四个方面；发生在企业边界之外的数据、渠道和内容风险，同样可能持续损害品牌信任。

- **数据泄露事件总量小幅增长，但重大风险上升更快，并进一步向暗网集中。** 2026 年上半年共确认数据泄露事件 23,645 起，较 2025 年下半年增长 6.98%；其中重大事件 542 起，增长 22.90%。暗网在重大事件中的占比由 76.64%升至 95.02%，已成为重大数据风险公开披露和传播的主要外部渠道。

- **搜索和仿冒网站是品牌渠道滥用最集中的入口，用户可能在找到官方服务前就被截流。** 上半年共记录钓鱼仿冒与品牌滥用事件 45,321 起，其中 SEO 污染占 45.73%，仿冒网站占 29.56%。搜索结果、内容平台、社交媒体、客服电话、应用及下载渠道正在形成多入口并行的风险网络。

- **真实业务信息与仿冒身份、非官方渠道结合，会显著增强欺诈的可信度。** 泄露的贷款、订单、退款或催收信息可以帮助风险主体还原用户业务背景，再通过虚假短信、客服、高仿页面或动态二维码完成触达，两者共同强化“官方”假象。

- **不同行业面临的外部风险结构明显不同，需要采用差异化的保护策略。** 金融与借贷同时承受客户数据暴露和身份冒用压力；电商风险主要集中在营销、交易和售后入口；制造业与零售业更易受到重大数据事件公开披露及业务连续性影响；游戏行业则以仿冒社交传播、私服、账号交易和商品侵权为主要风险形态。

01

品牌外部风险的两类核心风险面

一、品牌外部风险的两类核心风险面

企业外部风险并非只集中于某一个仿冒页面或某一次数据泄露事件。数据和身份可能在企业控制范围之外持续流通，用户触点也可能分散在搜索、内容、社交、下载和私域渠道之中。品牌保护面对的核心问题，正在从“是否存在假冒资产”扩展为“企业与用户之间的可信连接是否仍然可识别、可控制”。

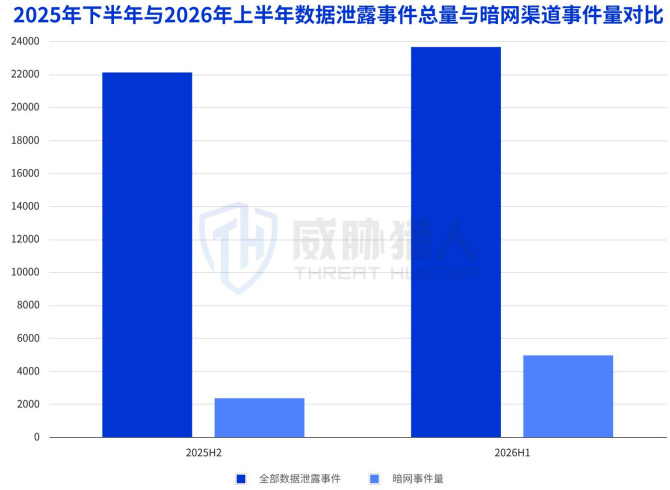
1.1 品牌保护围绕四类对象展开

保护对象	主要外部风险	典型影响
品牌身份	企业名称、产品名称、标识、域名、应用程序和官方账号被冒用	用户难以判断服务主体，企业授权关系和品牌秩序受损
官方渠道	搜索结果、网站、客服电话、下载入口、内容账号、活动页面和二维码被截流	用户在到达官方服务前进入虚假联系方式、非授权下载或欺诈页面
客户关系	贷款、支付、订单、会员、退款和催收等真实业务记录进入外部渠道	业务背景被还原，目标被筛选，冒充客服或催收的话术更具针对性
公共声誉	暗网披露、攻击声明、数据样本和侵权内容公开传播	客户质疑、合作伙伴审查、舆情压力和业务连续性风险上升

围绕上述四类保护对象，企业面临的外部风险可以概括为两类相对独立的风险面：数据、身份与权限暴露，以及品牌、渠道与流量滥用。二者既可独立发生，也可能相互叠加，共同影响客户关系、用户信任和品牌声誉。

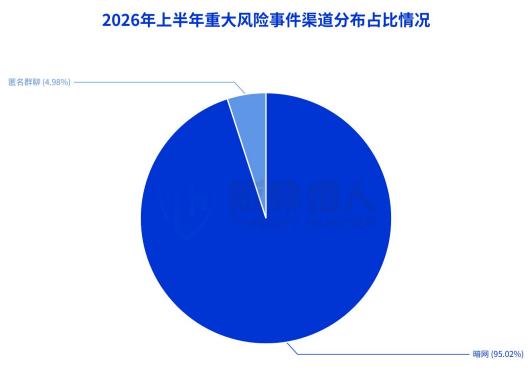
1.2 数据泄露事件总量小幅增长，重大风险向暗网集中

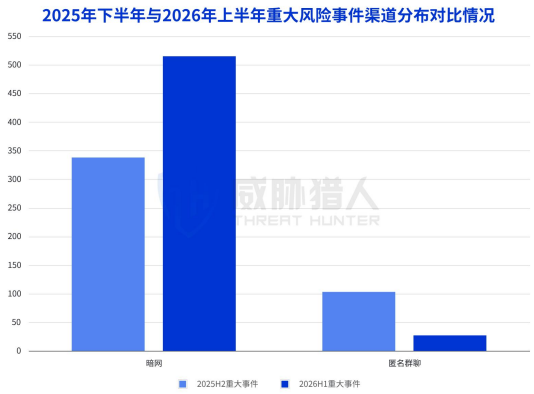
2026 年 1 月至 6 月，经验证确认的有效数据泄露事件共 23,645 起，较 2025 年下半年的 22,102 起增长 6.98%。其中，暗网渠道记录由 2,353 起增至 4,952 起，增幅明显高于整体事件增幅。



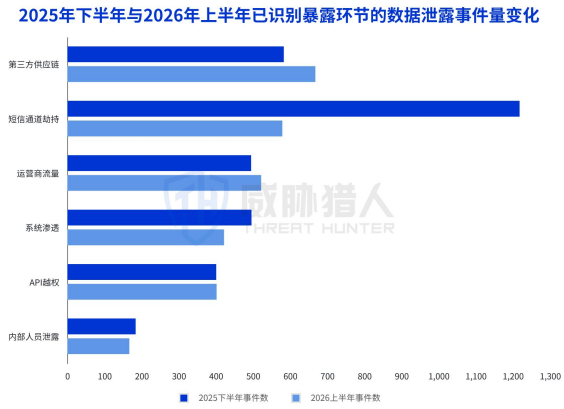
与总体事件量相比，重大数据泄露风险事件增长更为明显。2026 年上半年共确认重大数据泄露风险事件 542 起，较 2025 年下半年的 441 起增长 22.90%。本报告所称重大数据泄露风险事件，是指数据量级较大、字段敏感度较高、涉及核心业务信息、被公开披露，或可能造成较大合规、声誉及公共安全影响的事件。

其中暗网渠道在重大风险事件中的占比由 76.64%升至 95.02%，增加 18.38%。暗网已成为重大数据泄露风险公开披露和传播的主要外部渠道。





从已识别的风险来源看，泄露数据涉及第三方服务、短信通道、运营商流量、系统渗透、API 越权和内部权限等多个环节，反映出企业数据暴露面已从单一系统安全问题，延伸至供应链、通信链路和权限管理等多类外部及内部节点。



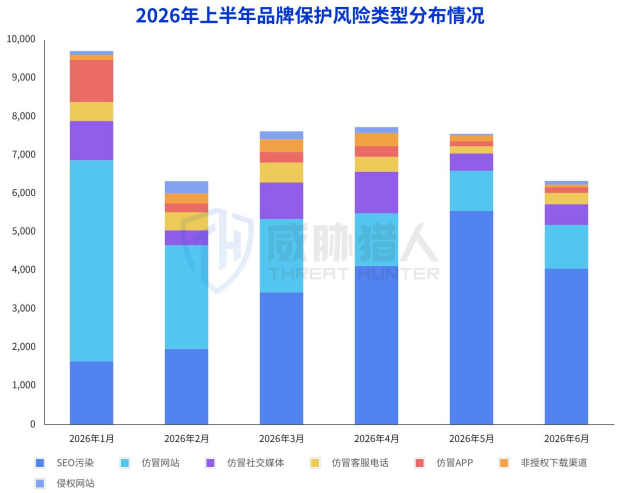
企业面临的风险已不再局限于“数据是否泄露”，还包括外部主体掌握了哪些业务数据、账号与访问权限，企业名称、数据样本和攻击声明是否被公开披露并持续扩散，以及这些信息是否持续影响客户、合作伙伴以及外部舆情压力。

1.3 品牌与渠道滥用：仿冒风险主要分布在多类用户主动搜索入口。

2026 年上半年，威胁猎人共监测到钓鱼仿冒与品牌滥用风险事件 45,321 起。相关风险出现在搜索结果、仿冒网站、社交媒体、客服电话、应用程序和下载渠道等多类用户主动搜索入口。

从风险类型分布看，SEO 污染记录 20,726 起，占比 45.73%；仿冒网站占比 29.56%。搜索结果和仿冒页面仍是品牌被滥用的重要位置：前者可能在用户寻找客服电话、账户异常处理、退款理赔、贷款办理或应用下载时截获需求，后者则可能承担信息收集、恶意下载、假客服联系或资金欺诈等承接作用。

2026 年上半年，SEO 污染、仿冒网站、仿冒社交媒体、仿冒客服电话、仿冒应用、非授权下载渠道和侵权网站等多类入口在半年内持续并行，品牌滥用并未集中于单一渠道。



其中，侵权网站指可能冒用品牌名称、代理商或合作伙伴身份，但未直接表现出账号窃取或资金欺诈意图；非授权下载渠道可能分发与官方版本一致的应用，却未经品牌方授权。两类事件的危害路径不同于直接钓鱼，但都会削弱企业对品牌身份、授权关系和下载渠道的控制。

1.4 信息暴露与身份冒用共同侵蚀品牌信任

用户对企业的信任，既来自企业名称、网站、账号和客服电话等身份标识，也来自对方能否准确说明与自身相关的业务信息。信息暴露可能为外部主体提供真实业务细节，身份冒用则提供接触用户的入口。两类风险虽然表现形式不同，但都会削弱用户识别真实企业身份、官方渠道和正常业务关系的能力。

品牌保护需要同时关注外部主体可能掌握的信息，以及企业身份可能被冒用的入口。只有将信息暴露与身份冒用并行观察，才能更完整地识别用户信任和官方渠道面临的风险。

02

品牌外部风险如何形成?

二、品牌外部风险如何形成?

第一章呈现了两类风险的规模和分布，本章进一步回答这些外部信号如何进入企业与用户之间的可信关系。风险形成于信息、身份、入口和公共传播等不同位置，并不遵循一条固定的攻击链。

2.1 业务信息如何成为黑产身份冒用条件

客户接到客服、催收、退款处理或账户异常处置相关通知时，判断对方是否可信的重要依据，往往是对方能否说出与自身业务经历相符的细节。机构名称、金额、时间、状态和联系方式等字段一旦进入外部渠道，黑产无需掌握完整档案，也可能通过字段组合还原一段足以支撑冒充的客户背景。

从风险形成过程看，最初暴露的可能只是分散字段；经过筛选、交叉比对和按业务阶段分类后，字段可以转化为对象画像和话术线索。而真正面向用户的风险发生在下一步：黑灰产借用企业身份，通过电话、短信、社交账号或仿冒页面接触用户，让真实业务细节成为错误信任的依据。

企业可以通过漏洞修复、账号处置和供应商整改，阻断新的数据暴露与滥用路径，但这些措施无法自动清除已经外流、复制和转存的数据。即使初始安全事件已经完成处置，相关数据仍可能被黑灰产反复利用。因此，客户关系风险往往不会随着安全事件结束而同步消失，而可能持续转化为身份冒用、精准诈骗、客户投诉和品牌信任受损等后续影响。

2.2 黑产通过仿冒信息抢占用户入口

当用户主动搜索客服电话、贷款办理、账户异常处理、退款理赔或应用下载等信息时，往往具有明确的业务需求。黑产通过在搜索结果、内容页面、社交账号和广告位中投放虚假信息，冒充企

业官方客服、业务渠道或合作机构，在用户进入官方网站或接触官方服务之前将其拦截。随后，黑产再利用二维码、跳转链接、中转页面或私域账号，将用户引导至仿冒网站、虚假客服或其他欺诈渠道。

截流入口本身未必是假页面。真实存在的内容平台、媒体页面或广告位也可能承载未经授权的品牌活动。因此，页面是否真实、发布主体是否获授权、跳转链路最终到达哪里，是三个需要分别判断的问题。第四章将以具体样本展示这一差异。

2.3 三类容易混淆的渠道风险

仿冒网站或应用、侵权网站和非授权下载渠道，都可能使用企业名称、商标、产品信息或应用素材，表面上具有较高相似性，但三类风险的识别依据和主要危害并不相同。

企业判断时需要重点观察三个方面：**相关主体是否伪造企业官方身份，网站或下载渠道是否获得品牌方授权，以及当前证据中是否已经出现账号窃取、恶意下载、虚假客服、诱导付款等直接欺诈行为。**

三类风险之间可能发生转化。例如，非授权下载页在后续替换安装包或增加虚假客服后，风险性质会发生变化；侵权网站如果开始收集凭据或诱导付款，也不再只是品牌信息被未经授权使用。分类的意义在于准确描述当前证据，而不是把所有非官方入口都写成同一种欺诈。

03

不同行业面临的外部风险结构存在明显不同

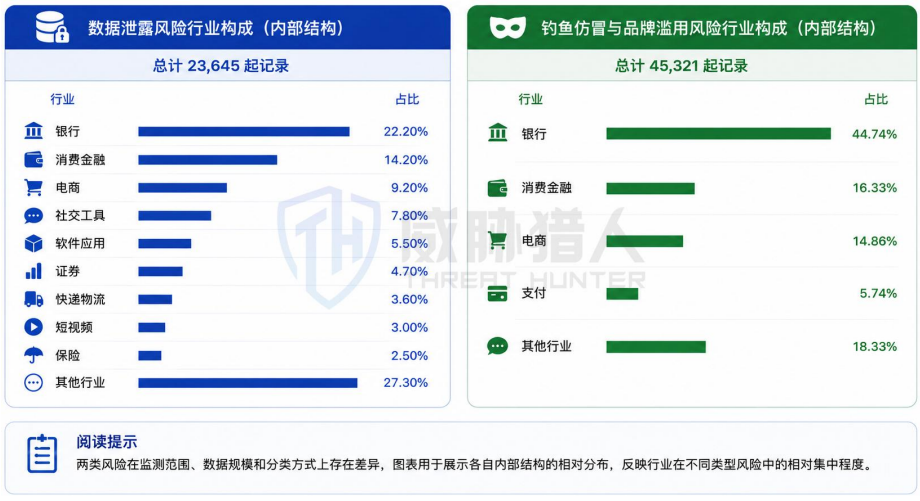
三、不同行业面临的外部风险结构存在明显不同

不同行业所依赖的业务关系、用户触点和外部平台存在差异，品牌外部风险的主要载体、传播路径和影响结果也各不相同。

3.1 金融行业在两类外部风险中均处于高位

2026 年上半年，金融相关行业在数据泄露风险和钓鱼仿冒风险中均处于较高位置。在 23,645 起数据泄露风险事件中，银行记录 5,251 起，占 22.2%；消费金融记录 3,359 起，占 14.2%。在 45,321 起钓鱼仿冒风险事件中，银行和消费金融分别占 44.74%和 16.33%，支付行业占 5.74%。

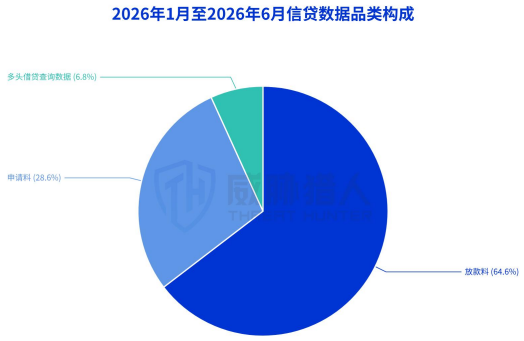
这一分布反映出，金融行业既面临客户和业务信息进入外部渠道的风险，也长期受到仿冒网站、虚假客服、搜索引流和非官方应用等身份冒用问题影响。除金融行业外，电商、社交工具、软件应用、证券、快递、短视频和保险等行业也呈现不同规模的外部暴露。



3.1.1 金融行业真实业务数据外流加剧身份冒用风险

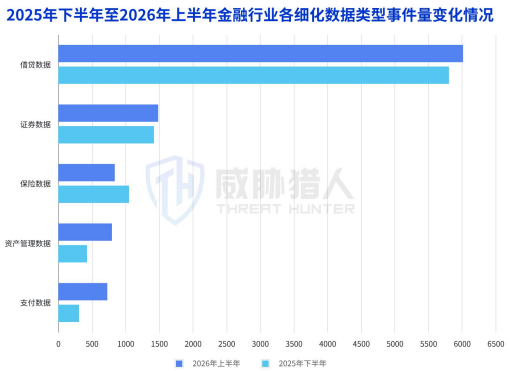
金融与借贷业务覆盖申请、审批、放款、支付、还款、催收和客户服务等多个环节，相关记录通常包含客户身份、业务状态、交易金额和联系方式等信息。一旦这些信息进入外部渠道，不仅可能造成个人信息和业务数据暴露，也可能被用于提高虚假客服、假催收和其他身份冒用行为的迷惑性。

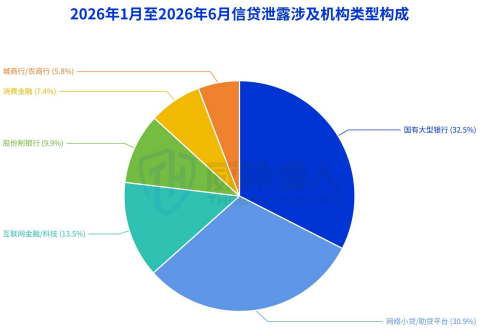
据威胁猎人分析，在2026年上半年泄露的借贷数据样本中，放款料约占64.6%，申请料约占28.6%，其余主要涉及多头借贷等贷前查询信息。相关记录覆盖贷前申请、审批放款及贷后管理等不同业务阶段，表明外部流通的数据已不仅限于基础联系方式，还可能反映客户与金融机构之间的真实业务关系。



威胁猎人监测发现，较 2025 年下半年，2026 年上半年借贷数据风险记录由 5,807 起增至 6,016 起；资产管理数据由 428 起增至 799 起；支付数据由 310 起增至 730 起,资产管理和支付数据的增幅较为突出。

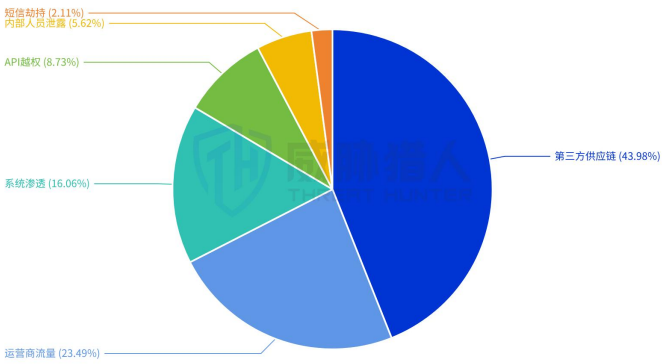
相关借贷数据涉及国有大型银行、股份制银行、城商行和农商行、消费金融公司、网络小贷及助贷平台、互联网金融和科技企业等多类机构，反映出风险并非集中于单一机构类型，而是分布于金融服务链条的不同参与方。





从已识别的暴露环节看，主要涉及第三方服务、运营商流量、系统渗透、接口权限、内部人员和短信通道等多个节点。金融数据可能从机构自身系统流出，也可能出现在外包服务、通信链路、接口调用和合作机构等业务连接环节。

2026年1月至2026年6月借贷数据泄露来源分布情况

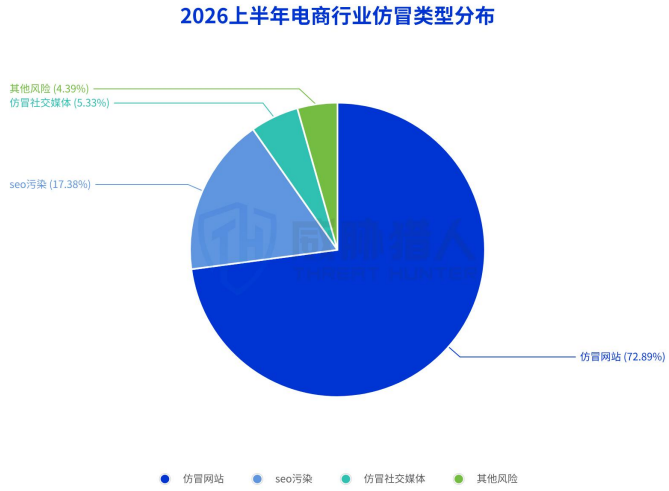


金融机构的品牌风险因此不仅表现为名称、网站或客服电话被冒用，也与客户业务信息是否脱离控制密切相关。当外部主体掌握贷款状态、交易金额、还款时间或服务记录时，冒充客服、催收或业务人员的内容更容易获得用户信任，并可能进一步引发信息泄露、资金损失、客户投诉和品牌声誉风险。

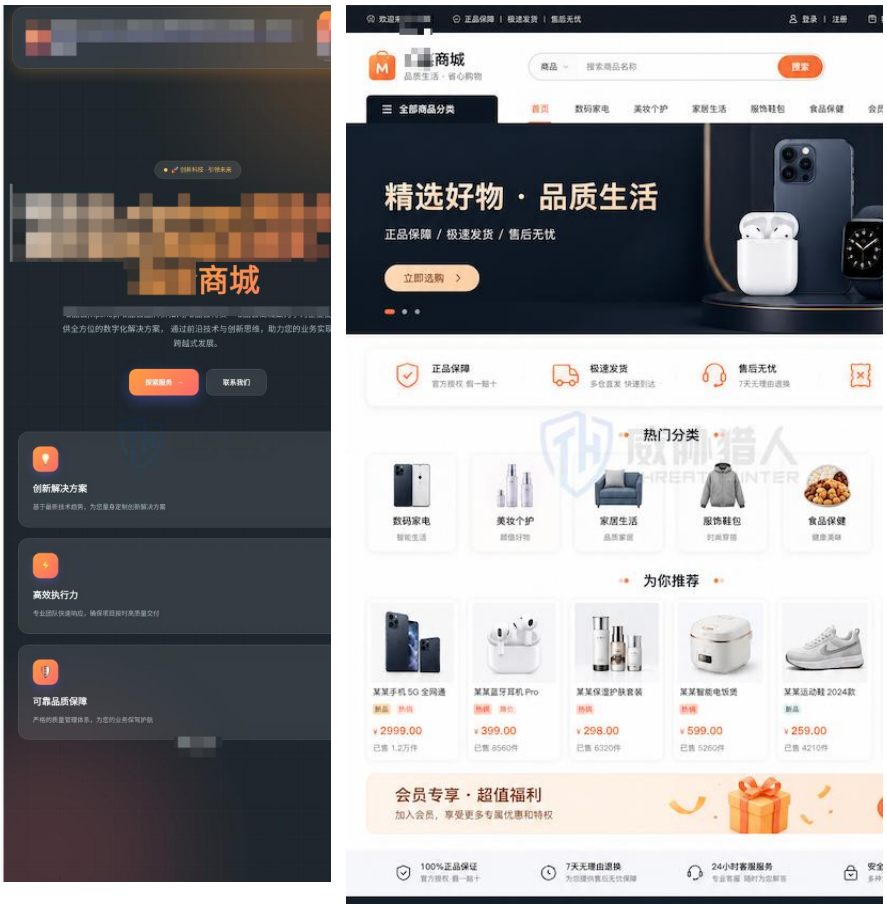
3.2 电商行业：面向消费者的渠道滥用风险

2026 年上半年，电商行业共发现钓鱼仿冒风险事件 6,736 起，是资金交易类行业之外风险最集中的场景。

从风险类型看，仿冒网站是电商行业最主要的风险类型，共 4,910 起，占比 72.89%；SEO 污染 1,171 起，占 17.38%；仿冒社交媒体 359 起，占 5.33%。其中，仿冒网站与 SEO 污染合计占比达到 90.27%，表明电商行业的钓鱼仿冒风险主要集中在“搜索引流”和“仿冒页面承接”两个环节。



相关风险通常围绕促销活动、订单异常、退款理赔、物流通知和平台客服等高频场景展开。攻击者利用用户对价格优惠、订单时效和售后处理的关注，通过搜索结果、内容广告或二维码截获需求，再将用户导向虚假活动页、登录页、支付页面或私域客服，实施信息收集、恶意下载或资金欺诈。



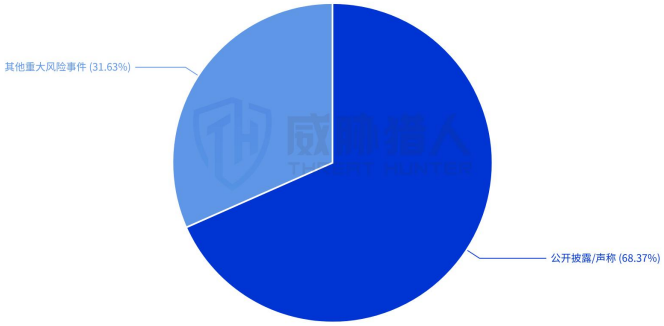
（某仿冒某电商平台网站页面）

3.3 制造业与零售业：重大数据泄露与公开披露风险

2026 年上半年，制造业重大数据泄露风险事件较 2025 年下半年的增长 82.14%；零售业增长 59.26%。制造业增幅更为突出，重大风险事件对企业生产经营、合作关系和公共声誉的潜在影响进一步上升。

在制造业与零售业发现的重大风险事件中，68.3%出现在勒索组织或相关站点的公开发布页面。企业名称、攻击声明和数据样本被公开展示，已成为相关风险进入客户、供应商、合作伙伴及公共传播视野的重要方式。

2026年上半年制造业、零售业重大数据泄露风险事件结构



从 2026 年上半年中国地区制造业与零售业相关公开披露事件看，The Gentlemen 记录 23 起，Qilin 记录 17 起，事件数明显高于其他主体；Akira 与 Inc Ransom 各记录 10 起，LockBit 5.0 与 DragonForce 各记录 9 起。

整体上，相关事件呈现头部主体较为突出，同时参与主体较为分散，制造业与零售业持续成为勒索组织公开挂牌和发布攻击声明的重要目标。

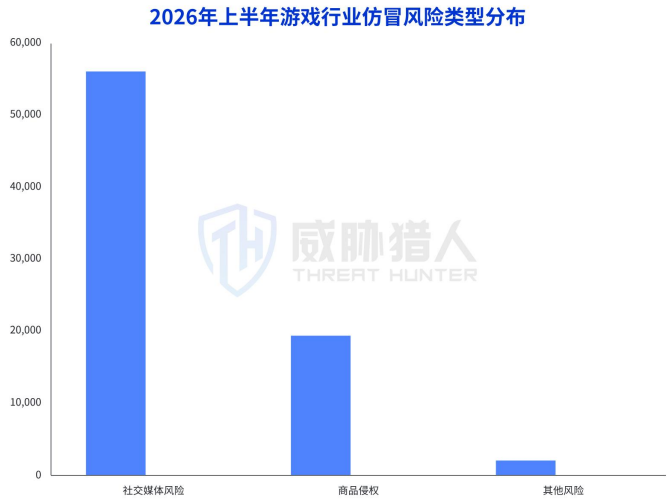
> 注：上述数据仅反映威胁猎人监测范围内中国地区制造业和零售业相关事件，不代表相关组织在全球范围内的整体活跃情况。

2026 年上半年，制造业与零售业重大风险事件中，超过三分之二通过相关组织或站点进入公开传播。这意味着，相关风险的影响已不再局限于企业内部的技术处置。制造业事件可能进一步影响生产安排、供应商协作和业务连续性；零售业事件则可能直接触发消费者对交易安全、个人信息保护及服务可靠性的担忧。随着企业名称、攻击声明和数据样本被公开展示，客户信任、合作伙伴审查、供应链关系和公共声誉均可能受到持续影响。

3.4　游戏行业：社交传播与商品侵权形成独立生态

2026 年上半年共记录相关风险 77,816 起，其中仿冒社交媒体 56,071 起、商品侵权 19,350 起、其他风险 2,395 起。该总量不应与前述数据直接加总或横向比较。

注：游戏行业采用专项监测口径，与其他场景相比，监测对象和统计口径存在差异。



仿冒社交内容通常以福利、兑换码、稀缺资源或版本优势吸引玩家，再引导其进入私域渠道。商品侵权则主要涉及私服、BT 服、修改版、成品账号、外挂、辅助和脚本等电商商品，直接造成收入分流，并可能影响账号安全、游戏公平性和用户体验。

在威胁猎人监测到的 19,350 起商品侵权专项记录中，私服、BT 服及修改版 7,933 起，账号交易 6,305 起，外挂、辅助及脚本 1,198 起；游戏仿冒事件主要聚焦电商平台上的私服、账号和外挂等商品，与前文所述侵权网站属于不同风险形态。

（游戏行业仿冒社交媒体与商品侵权样本）

游戏风险的观察对象主要是社交账号和电商商品，难点在于平台分散、内容变体多、账号重建快和商品反复上架。其识别和处置路径，与金融行业围绕搜索入口、客服和高仿页面的风险路径明显不同。

04

品牌外部风险典型案例

四、品牌外部风险典型案例

品牌外部风险很少停留在单一页面或一条数据记录上。内容发布、跳转控制、数据包装和身份冒用往往分散在不同环节。沿样本继续核验，有助于还原用户最终接触的内容及品牌被冒用的环节。以下是威胁猎人监测到的 2 个典型案例。

4.1 公信力被“劫持”：黑灰产借助权威融媒体渠道引流

2026 年上半年，威胁猎人发现一种利用媒体公信力实施仿冒引流的新型手法。黑灰产不再仅依赖自建网站或低权重社交账号传播，而是以“广告投放”名义接触融媒体、行业媒体及地方资讯类公众号，通过正规内容渠道发布冒用某头部电商品牌的促销文章，借助媒体账号的权威属性降低用户戒备。

相关内容通常采用“即将抵达！请市民做好准备！”等通知式标题，并根据投放地区替换城市名称。同期监测到多条标题结构、活动素材和引流方式高度相似的内容，发布时间和发布渠道分散，呈现出模板化制作、跨地区投放和批量复制特征。

典型文章正文仅包含活动长图和二维码，以连续签到免费领取日用品、小家电及智能数码产品为诱饵，引导用户扫码、下载安装应用并完成注册。经品牌方核验，相关活动并未获得授权，投放方提交的品牌授权文件及授权公章均系伪造。

4.1.1 黑产作恶链路

从作案链路看，黑灰产首先筛选具备一定影响力且承接商业广告的媒体账号，并以单篇约 5,000 元购买广告位；随后使用伪造的授权材料完成形式审核。投放初期，二维码可呈现正常访问结果，使文章通过人工审核和平台机审。待内容正式发布并积累曝光后，攻击者再通过服务端调整中转地址，将后续访问者导向非官方应用下载或其他风险页面。

与传统仿冒网站相比，该手法的风险重点不只在最终落地页面，更在于攻击者利用正规传播渠道完成“信任转移”。用户容易将“发布渠道可信”等同于“活动真实可信”；媒体运营方在广告审核过程中，也往往更关注资质文件、宣传内容和首次扫码结果，难以持续观察二维码背后的访问目标。由于二维码始终指向同一中转入口，服务端换链不需要修改文章内容或二维码图案。审核时看到的页面与用户后续访问的页面可能不同，常规审核和单次扫码因而难以及时发现异常。

该模式体现出三项明显变化：

- **传播渠道可信化。** 黑灰产由低权重账号转向融媒体和地方资讯渠道，利用媒体影响力完成初次背书。
- **诱导内容图片化。** 品牌名称、促销话术和二维码集中在活动长图中，减少可供文本规则识别的风险特征。
- **审核规避动态化。** 二维码入口保持不变，后端访问目标可以分阶段调整，单次核验难以反映后续风险。

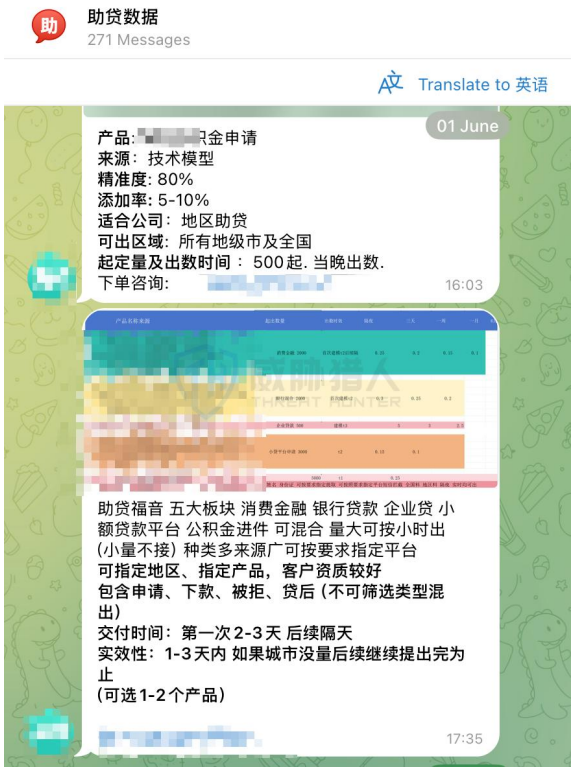
这类攻击会同时影响用户、媒体和被仿冒品牌：用户可能因信任发布渠道而降低核验意识；媒体账号可能在不知情的情况下成为风险流量入口；被仿冒品牌则需承担非官方活动引发的咨询、投诉和信任损耗。其危害已经从单一品牌冒用，进一步延伸至对媒体公信力和品牌渠道秩序的双重侵蚀。

4.2 真实业务信息与仿冒渠道共同制造“官方催收”假象的典型路径

假催收是信息暴露与身份冒用在同一业务场景中结合的典型案例。威胁猎人监测发现，部分诈骗团伙会从非法数据交易市场购买借贷用户数据，在获得用户的申请、放款或逾期信息后，再通过虚假催收短信、客服电话和高仿还款页面接触用户。用户面对的并非一条毫无依据的陌生信息，而是一套同时包含真实业务细节与企业品牌标识的“官方催收”假象。

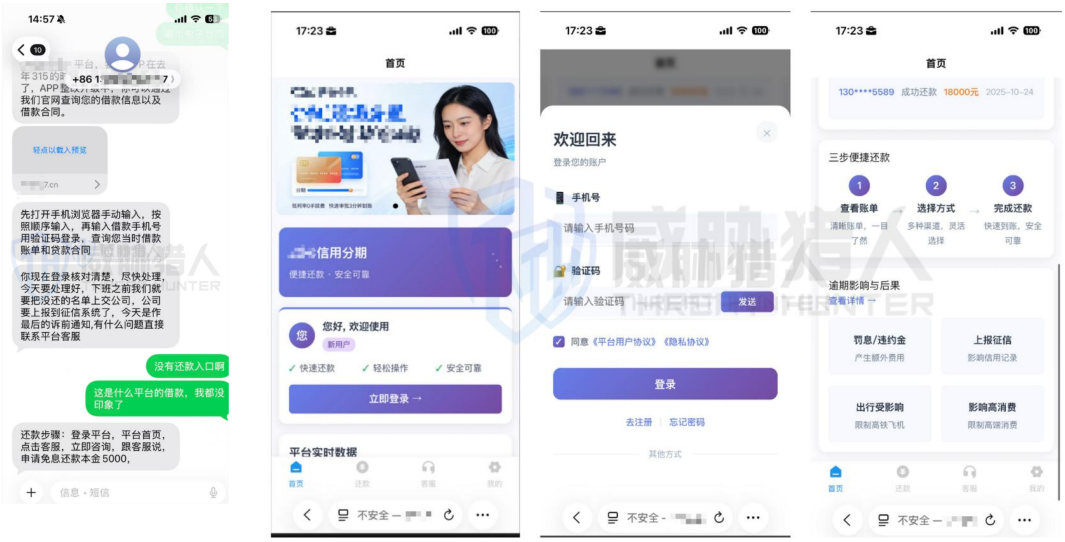
4.2.1 真实业务信息先补足“催收”所需的细节

地下渠道流通的借贷数据通常按申请、放款和逾期等业务状态分类。除姓名、手机号等基础信息外，相关样本还可能包含贷款平台、申请或放款时间、借款金额、逾期状态及银行卡信息。与普通联系方式名单相比，这些字段能够还原用户与某一金融机构之间的真实业务关系，也为后续冒充客服或催收人员提供更具迷惑性的交流依据。



4.2.2 虚假短信和高仿页面共同强化“官方催收”假象

获得相关数据后，诈骗团伙通过催收短信、虚拟号码或社交工具向用户发起接触。短信内容可能直接出现贷款平台、借款金额、申请时间或逾期状态，并附带所谓的“查询合同” “协商还款”链接。用户点击后进入的页面进一步使用企业名称、标识、业务话术和还款流程，使前一环节中的真实业务信息得到视觉和渠道上的“验证”。



4.2.3 用户看到的是一条连续的“官方催收”链路

在这一过程中，真实业务信息回答了用户“对方为什么了解我的情况”，企业名称、短信、客服和还款页面则回答了“对方为什么看起来像官方”。两类信息在连续触点中相互强化，使用户更难识别真实服务主体与非官方渠道。

4.2.4 诈骗发生在企业边界之外，影响却会回到品牌方

假催行为虽发生在企业控制范围之外，但用户接触到的却是企业名称、真实贷款信息和高度相似的服务页面。一旦发生骚扰、信息泄露或资金损失，用户往往会将相关体验与被冒用的金融品牌联系起来，并进一步形成投诉、质疑和对官方催收渠道的不信任。

而即使初始数据暴露入口已经修复，进入地下渠道的历史数据仍可能被复制、转卖，并通过新的短信号码、客服账号和仿冒页面再次利用。因此，相关风险不会随着单一漏洞修复或页面下架自动结束，而可能以新的接触载体持续回到用户侧。

这一案例说明，品牌保护不仅需要识别冒用企业名称的页面、账号和联系方式，也需要关注是否已有足以支撑身份冒用的真实业务信息进入外部渠道。客户关系数据的流通与企业身份的冒用一旦结合，外部欺诈造成的影响便可能沿投诉、舆情和监管等路径持续回流至品牌方。

因此，企业需在风险回流并扩散到品牌层面之前，切断“数据泄露→身份冒用→用户受害→影响回流”的完整链路，也正是品牌保护的核心目标。

结语

本报告由威胁猎人反欺诈情报研究团队基于长期监测数据、真实风险样本与行业治理实践编写。企业品牌外部风险不会止于单一仿冒页面或一次数据泄露，数据暴露、身份冒用、渠道截流与公开传播等风险仍将持续演变，并不断影响企业与用户之间的信任关系。威胁猎人将持续与各行业企业协同，共同提升品牌外部风险的发现、研判与处置能力，守护企业品牌安全与用户权益。

希望本报告能够帮助品牌保护、安全、风控及业务从业者更准确地理解企业品牌外部风险变化，识别不同行业的主要风险结构与形成路径，并为企业制定更具针对性的品牌保护和外部风险治理策略提供参考。

说明：本报告所提供的数据信息系威胁猎人依据大样本数据抽样采集、小样本调研、外部情报数据采集、数据模型预测及其他研究方法估算、分析得出，由于统计分析领域中的任何数据来源和技术方法均存在局限性，依据上述方法所估算、分析得出的数据信息仅供参考。

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