威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

2023年数据泄露风险年度报告

出品方：威胁猎人

目录

Contents

前言

2023 年，各行业全面数字化，加速业务创新发展的同时，确保大量数字资产及云上业务的数据安全，成为不少企业面临的“两难之境”，因数据泄露问题产生的影响及损失进一步扩大，对各行业关键领域造成严重影响。

威胁猎人发布《2023 年数据泄露风险年度报告》，对 2023 年数据泄露风险概况、黑产数据交易市场等进行具体分析，数据显示：

1. 2023 年，全网监测并分析验证有效的数据泄露事件**超过 19500** 起，涉及**金融、物流、航旅、电商、汽车等** 20 余个行业；

2. **金融行业**超过物流行业，成为 2023 年公民个人信息泄露事件数量**最多**的行业；2023 年**航旅行业**公民个人信息泄露事件数量也出现大幅增长，在公民个人信息泄露的行业分布中首次**排名前三**；

3. 从数据泄露渠道来看，主要集中在更加隐蔽和便利的匿名群聊、暗网渠道；值得一提的是，公民个人信息泄露事件的数据交易时间中，**夜间交易的超过 50%，在非工作日交易的超过 30%。**

相关名词定义：

1、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；

2、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，确认为真实、有效的数据泄露事件；

3、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；

4、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；

5、企业敏感代码：指企业的核心代码、算法、技术、密码等敏感信息，具体包括软件源代码、数据库结构、API 密钥、访问凭证、加密算法等；

6、企业敏感资料：指企业的机密文件和敏感资料，包括但不限于合同、商业计划、财务报表、市场调研报告、客户列表等；

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。

01

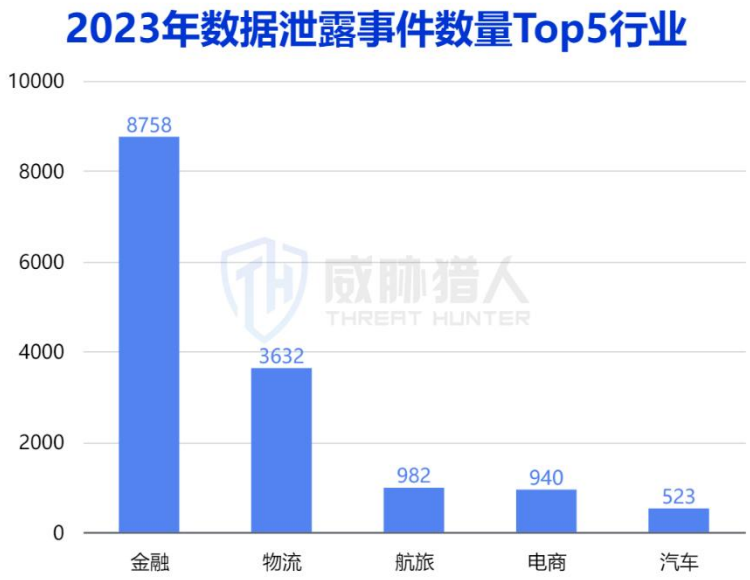
2023 年

数据泄露风险概况

一、2023 年数据泄露风险概况

1.1 2023 年监测数据泄露事件超 19500 起， 金融、物流、航旅等行业是数据泄露重灾区

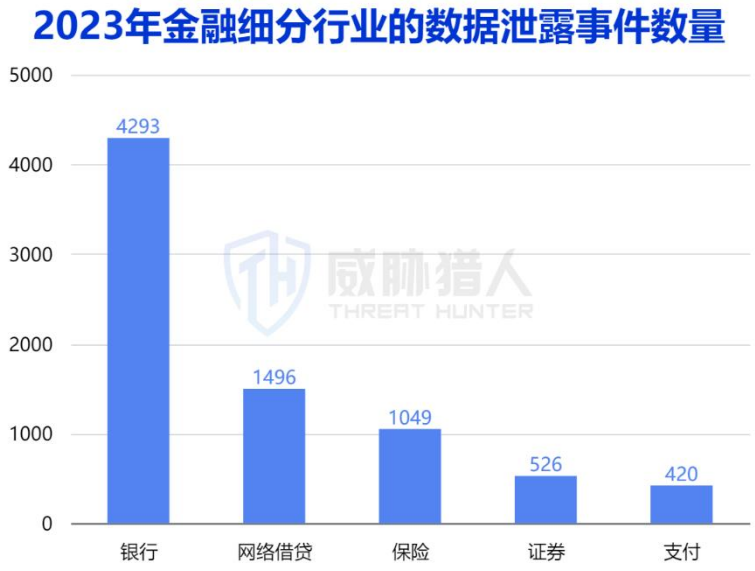
据威胁猎人数据泄露风险监测平台数据显示，2023 年全网监测到的近 1.5 亿条情报中，分析验证有效的的数据泄露事件超过 19500 起。从行业分布来看，2023 年数据泄露事件涉及 20 余个行业，数据泄露事件数量 Top5 行业分别为金融、物流、航旅、电商、汽车。



1.2 金融行业数据泄露事件 8758 起位列第一，航旅行业跃居第三

2023 年，金融行业依旧是个人信息泄露重灾区，数据泄露事件数量 8758 起，涉及银行、保险、证券等行业高净值人群信息，主要源于下游黑产用于营销推广以及诈骗的收益价值更高。

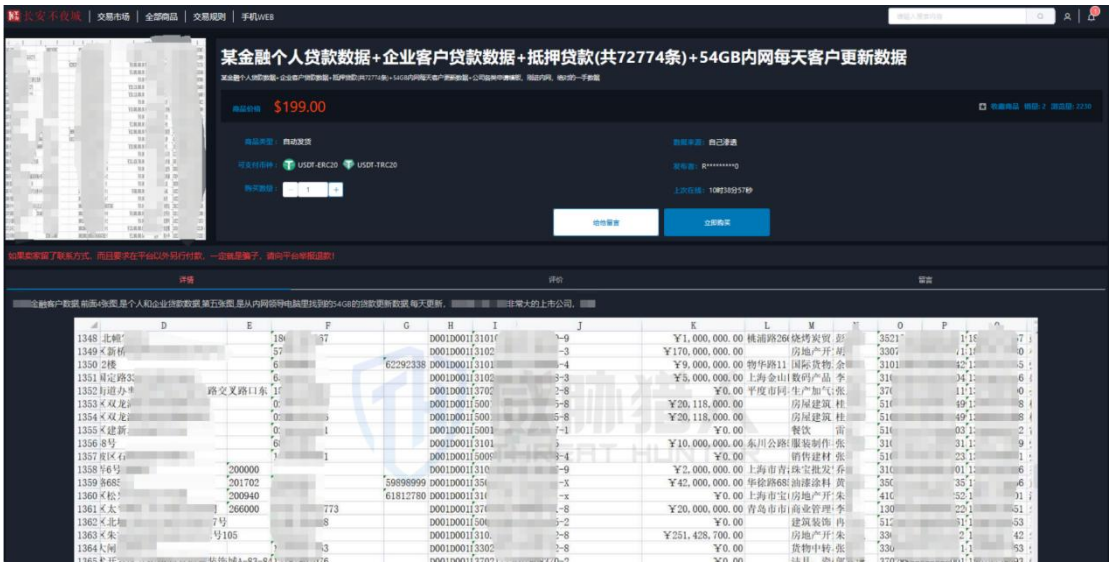
从金融细分行业来看，数据泄露事件数量发生最多的是银行业，全年共发生 4293 起，其次为网络借贷、保险、证券及支付行业。



金融行业典型数据泄露事件案例：

以某金融企业为例，其用户贷款信息等被泄露在某知名中文暗网上，泄露数据量级超过 72000 条，该数量仍在每日不断更新增加，黑产以 199 美元进行售卖，截至目前已成交 2 单，浏览超过 2200 次。

调查发现，黑客通过攻击渗透爬取该金融企业数据，如果企业未能及时感知数据泄露风险，缺乏有效的防御及处置措施，将会带来难以消弭的经济损失及品牌声誉影响。

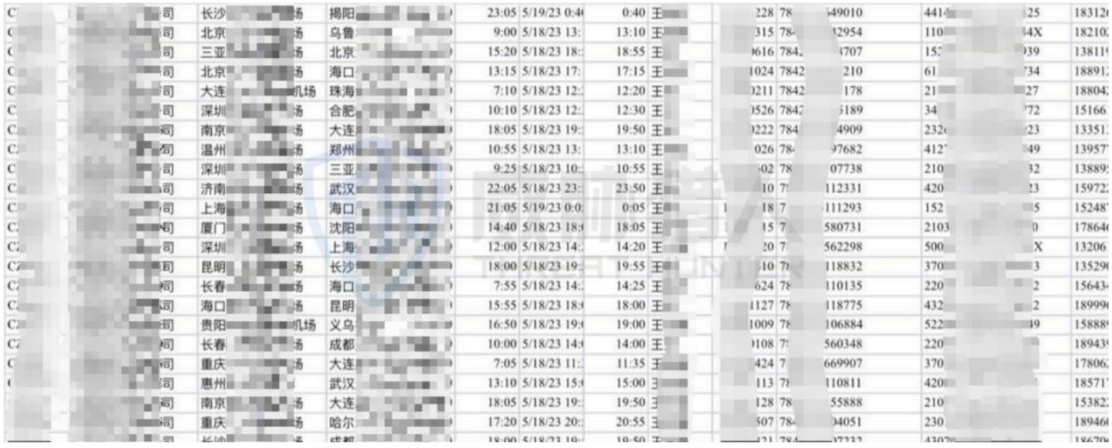


值得一提的是，航旅行业位列第三，成为数据泄露重灾区之一。随着新冠疫情好转，旅游行业回暖态势明显，消费需求得到强劲释放，机票信息、酒店信息等旅客信息数量也出现大幅增长。

威胁猎人安全研究员观察到，2023 年因航班信息泄露而遭遇“退改签”诈骗的事件频发，黑产团伙在精确获得乘客姓名、证件号、航班号等信息后，通过机票改签的方法实施网络诈骗，诈骗成功率较高。

航旅行业典型数据泄露事件案例：

威胁猎人数据泄露风险监测平台在 Telegram 数据交易群“黑客接单”中捕获到黑产发布“实时机票 未登记”的敏感信息，包含了旅客姓名、手机号、身份证号、航班信息等各类敏感信息。



进一步分析发现，该份旅客数据涉及多家航空公司，初步判定为多家航空公司的共有合作方泄露导致。据了解，航旅类用户个人信息的交易单价大部分在 13-15 元不等，其中最高达 20 元。

1.3 数据泄露原因包括运营商通道泄露、内鬼泄露、黑客攻击等

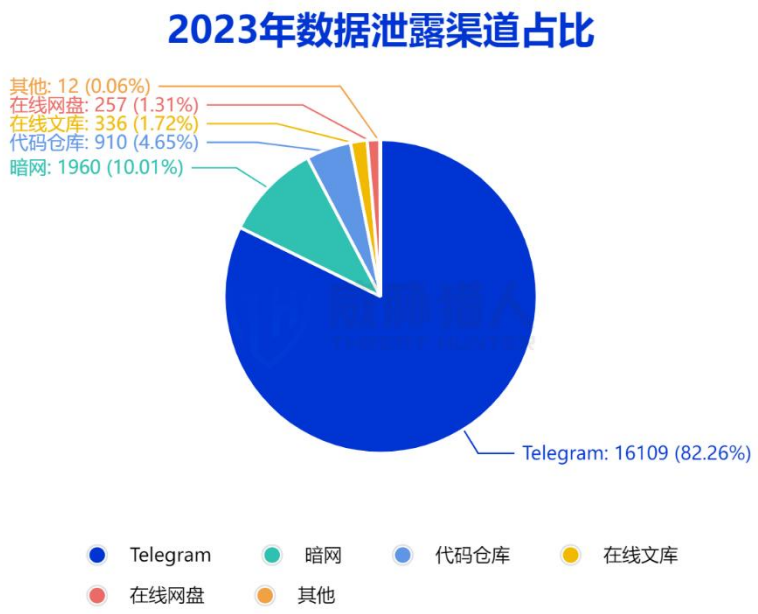
从数据泄露的具体原因来看，2023 年数据泄露原因包括运营商通道泄露、内鬼泄露、黑客攻击、安全意识问题等。其中，因运营商通道泄露引发的数据泄露事件数量最多。

- **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;

- **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，导致敏感信息泄露；
- **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;

1.4 Telegram、暗网是数据泄露的主要渠道，占比高达 92%

2023 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 92%以上，其中 82.26%集中在 Telegram，10.01%发生在暗网，主要原因是 Telegram 及暗网渠道的隐蔽性较高，难以追溯到黑产本人，是黑产沟通和交易的首选渠道。此外，威胁猎人在代码仓库（如 GitHub、GitLab 、Postman 等）、网盘文库等渠道也监测到了数据泄露事件。

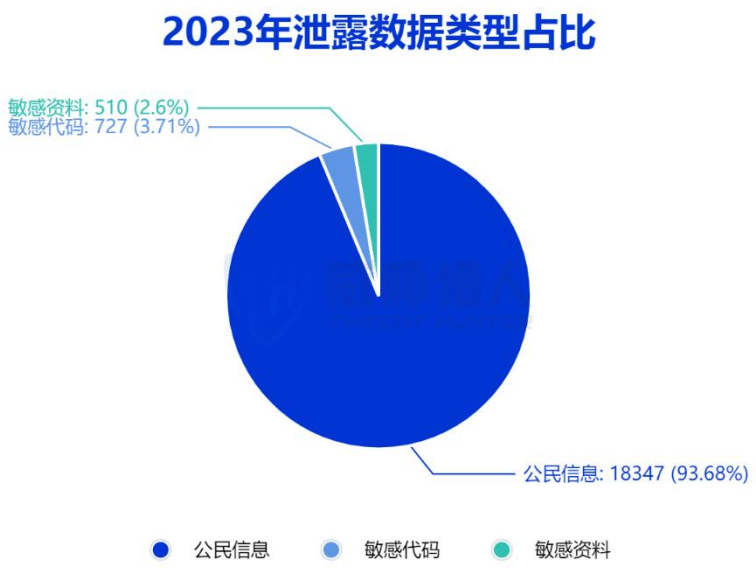


截至 2023 年 12 月，威胁猎人数据泄露监测情报覆盖了 Telegram 近 2 万个频道/群聊，在超过 1700 个频道/群聊中发现公民个人信息泄露风险事件。

1.5 2023 年“公民个人信息”依旧是数据泄露的主要类型，占比超 90%

从数据泄露的类型来看，2023 年泄露数据类型主要有 3 种：公民个人信息共计 18347 起（93.68%）、敏感代码共计 727 起（3.71%）、敏感文件资料共计 510 起（2.6%）。

其中公民个人信息类型的数据泄露占比最高，达 93.68%，作为下游黑灰产主要作恶的数据类型，**下文将针对公民个人信息数据泄露具体分析。**



1.6 2023 年公民个人信息泄露的特征及趋势

1.6.1 包含“手机号”的公民个人信息泄露超过 80%，主要用于精准营销/诈骗作恶

2023 年公民个人信息泄露事件超 18000 余起，其中泄露信息字段包含“手机号”的超过 80%，主要被下游营销/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。

2023 年公民个人信息泄露事件中，“姓名+手机号+身份证号+银行卡号”这类数据字段组合出现的频率最高，相关数据泄露事件出现近 900 起。

从这类数据字段组合出现频率较高的原因来看，一方面下游黑产团伙可以基于完整的数据字段及公民画像信息，进行定向性作恶，使整体作恶成功率及收益更高；

另一方面，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。

泄露字段 TOP10：

泄露字段	事件数
手机号	14425
姓名	12731
身份证号	7095
地址信息	5614
银行卡号	2702
运单号	2297
商品信息	2260
短信内容	1910
运营商	799
时间	459

1.6.2 黑产二次拼接“历史个人数据信息”，并进行多次贩卖的现象频发

威胁猎人对公民个人信息贩卖情况调查后发现，数据交易黑市存在**历史数据信息被黑产中介进行二次整合，并进行多次贩卖**的现象。尽管数据此前已被买家用于作恶，二次作恶效果明显下降，但黑产中介会以较低的价格进行出售，并以此牟利。

首先，黑产通过一些非法渠道获取初步的公民个人信息（如手机号），而后通过包含历史泄露信息的社工库等渠道，进行数据精细化处理，补充数据字段完整性，从而提升公民个人信息的价值及盈利空间，具体方式包括：

1、通过浏览器等公开渠道，查询相应手机号码的具体归属地、运营商信息；

2、利用社工库，通过手机号码进一步查询号主的身份信息；

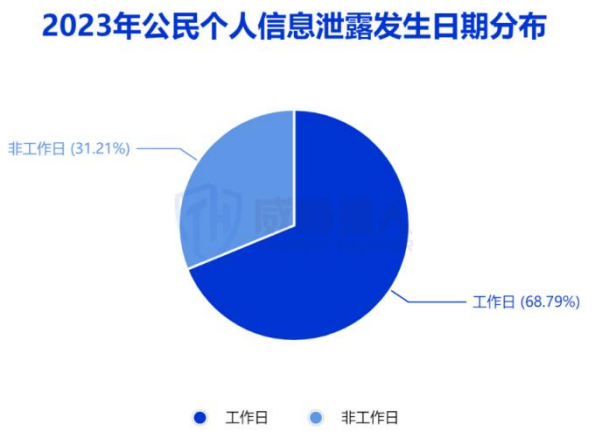
3、针对特定平台网站的用户，中介机构执行校验查询，对数据进行清洗并过滤无效手机号；

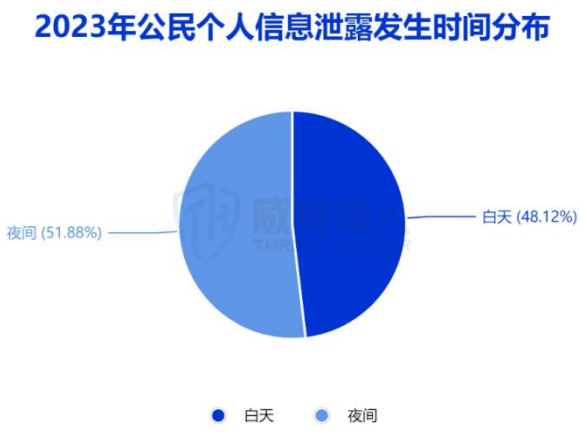
4、运用 Apple 提供的公开 API 以及一些自动化脚本工具，实现全自动检测号码是否注册 iMessage、开通 FaceTime 来区分 IOS 用户等功能，让数据更完整从而提升数据价值。

1.6.3 公民个人信息在夜间交易的超过 50%，在非工作日交易的超过 30%

威胁猎人研究统计发现，2023 年公民个人信息泄露事件中的数据交易时间中，非工作日（周末、节假日）发生的事件数量高达 31.21%，夜间发生的事件占比高达 51.88%，超过一半。（夜间：18:30 至次日 09:30）

在防守最薄弱的时候，企业难以在数据泄露事件爆发时快速感知、及时响应，以至于错过最佳应对时机，给企业资金、品牌声誉及商业竞争带来重大影响。



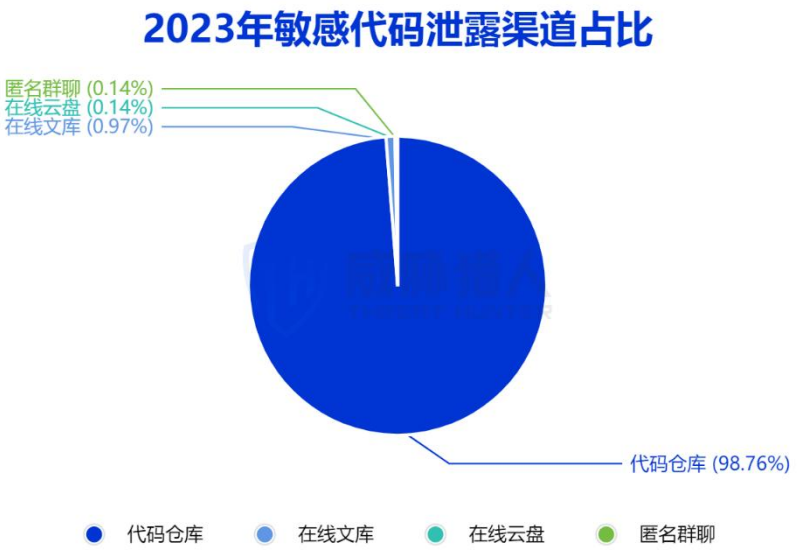


1.7 2023 年除公民个人信息泄露外，敏感代码、资料文件等信息泄露超 1200 起

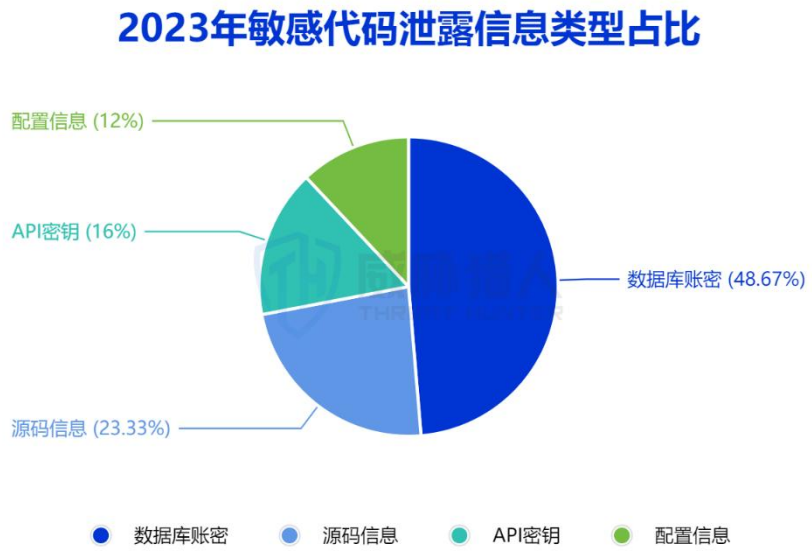
2023 年数据泄露事件类型中，除了公民个人信息之外，还有企业敏感代码、敏感资料文件等信息类型。

1.7.1 敏感代码泄露渠道以代码仓库为主，包括数据库账密、源码等信息

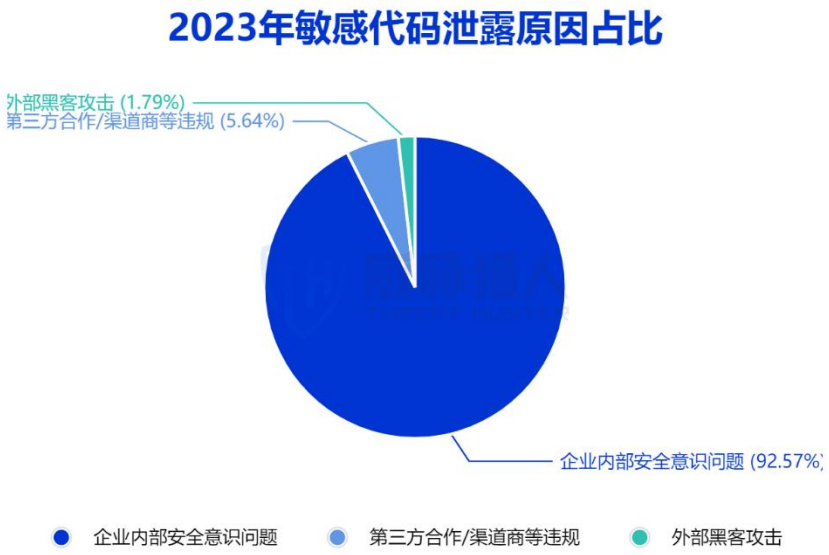
其中，企业敏感代码泄露事件发现超过 727 起，主要集中在 Github、Gitee 等代码仓库平台，占总体量级的 98.76%。



敏感代码泄露的内容类型上，**以数据库账密、源码信息为主**，具体包括内网、公网账号密码等，由于涉及大量内部敏感信息，敏感代码泄露带来的影响和损失同样不容小觑。

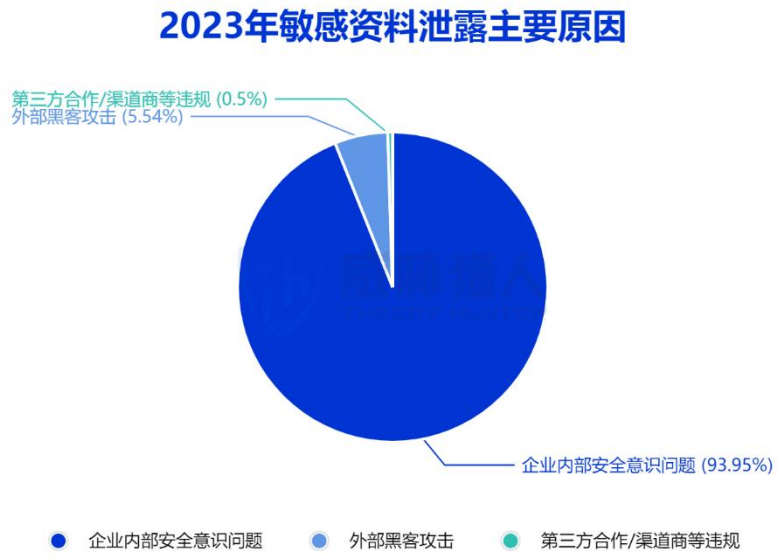


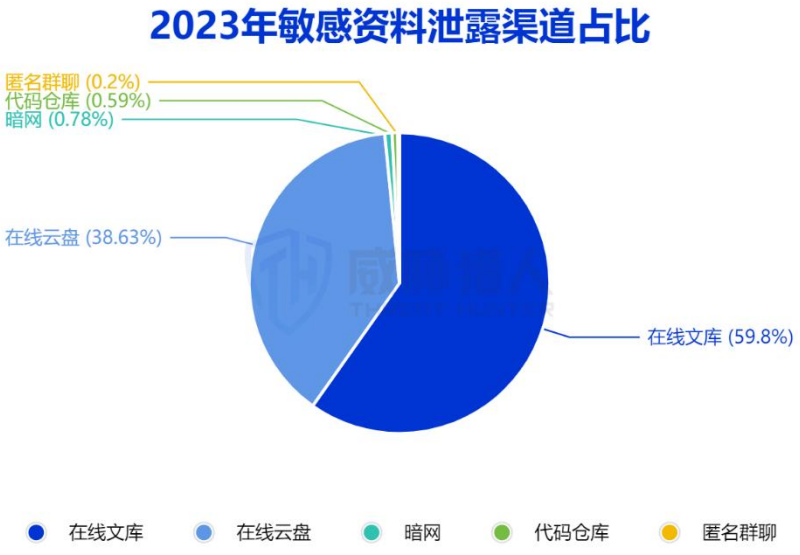
敏感代码泄露的原因主要归结为**企业内部员工安全意识问题、第三方合作泄露及外部黑客攻击**，这一点与公民个人信息类数据交易作恶的原因有所不同。



1.7.2 敏感资料泄露渠道以在线文库/云盘为主，主要由企业内部安全意识问题引发

企业敏感资料泄露事件发现超过 510 起，主要为企业内部安全意识问题引发，例如误上传到在线云盘、文库所导致。





02

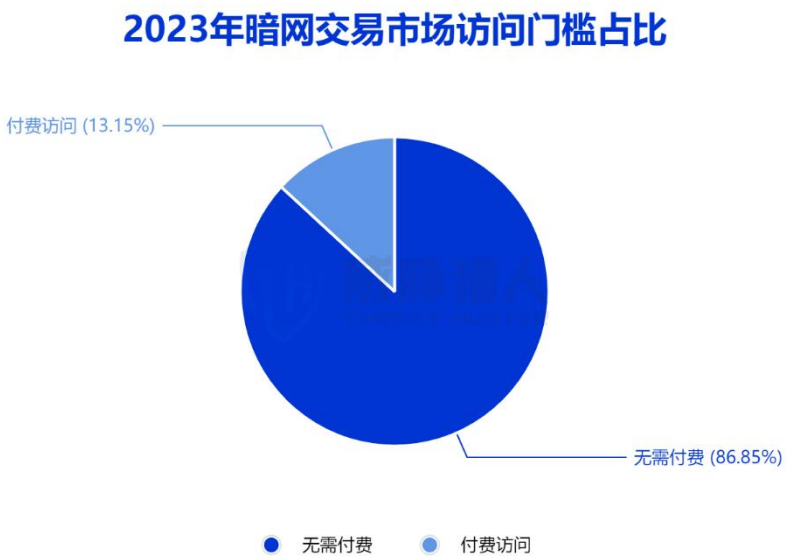
2023 年黑产数据交易市场相关研究

二、2023 年黑产数据交易市场相关研究

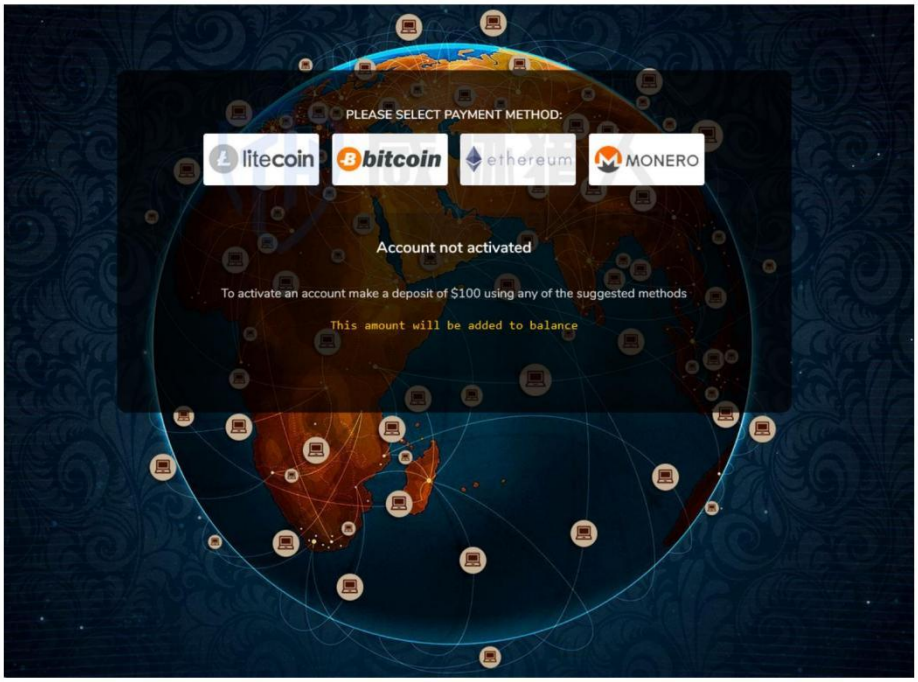
2.1 超过 45 个暗网平台通过“高级会员”等形式提升访问门槛

随着非法数据交易市场和黑客论坛逐渐走向公开化，为了提升访问门槛和增强平台安全性，同时实现更高的经营利润，越来越多的暗网论坛以及交易市场开始升级会员体系，使得更有价值的资源及互动需要付费成为会员才能获取和参与，普通用户仅能享受有限资源和受限互动。

威胁猎人对暗网交易市场以及黑客论坛进行调研，发现有超过 45 个暗网市场以及论坛需通过付费注册、积分解锁、充值会员、邀请码、点赞回复、升级 VIP 等方式进一步查看具体数据交易模块以及相关帖子内容，充值会员、付费查看信息的价格从**数百美元至数千美元**不等。



著名的俄罗斯数据交易论坛“russianmarket”的网站访问需充值 100 美元进行注册



2.2 超过 1500 起风险事件在 Telegram“私域群”发现

上文提到，2023 年威胁猎人监测到的公民个人信息泄露事件中，82.26%集中在 Telegram，10.01%发生在暗网。作为公民个人信息泄露的主要渠道，我们将对 Telegram 及暗网进行进一步分析。

为规避相关法律政策打击，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，威胁猎人在私域群累计发现超过 1500 起风险事件。

此外，为了加强渠道的可信度，确保数据交易顺利进行，一些黑产团伙会组建“公群”，相当于担保机构，如汇旺担保、神马担保等，他们会组织整理资源群、供需群、担保群等，承接项目需求及各项资源对接，在数据交易过程中进行担保。公群也会设置为单独的私域群，交易者通过邀请链接/管理员同意后才能进入。

数据交易频道/群聊 TOP5

频道/群名	事件数
公群****	1508
蟹老板****	234
火凤凰****	212
大boss****	193
爱拼****	167

数据交易黑产团伙 TOP5

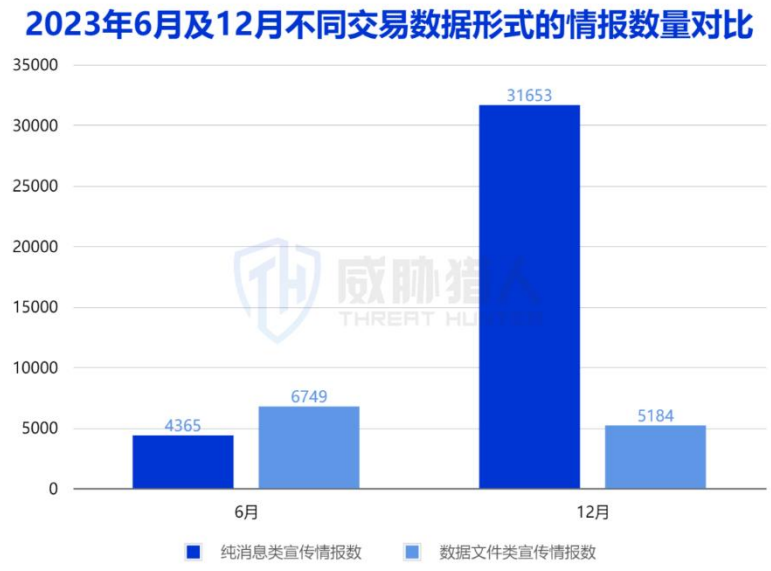
发布者信息	事件数
匿名**	11868
保***	208
Boss**	193
孤独**	162
摇一摇**	141

2.3 黑产交易数据形式逐渐由“数据文件类”转化为更隐蔽的“纯消息类”宣传

在市场监管及政策打击下，黑产数据交易的宣传形式变得更加谨慎，以更好地规避风控和保护自身利益。

以某金融行业为例，威胁猎人对金融行业 2023 年黑产数据交易宣传形式的变化趋势进行分析。2023 年 1 月到 8 月期间，黑产交易主要以**“数据文件类”**宣传为主，黑产交易者通过发布各类数据文件的样本和描述，吸引潜在买家进行交易。

随着监管力度的加大和市场风险的上升，2023 年 9 月，黑产交易宣传形式逐渐转换为以**“纯消息类”**宣传数据交易。黑产交易者通过加密消息、暗号和私密聊天等方式与买家进行交流联络，更加隐蔽而难以被监管机构察觉。



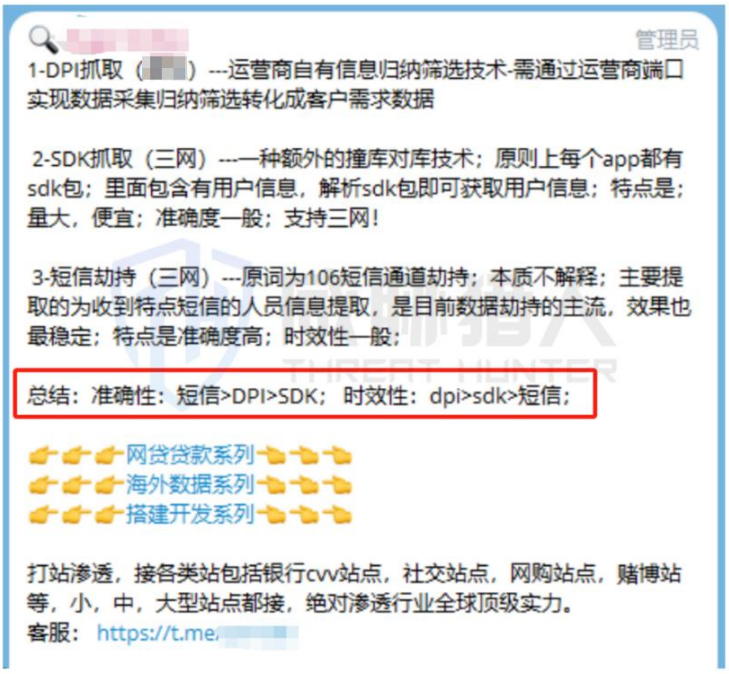
2.4 不同黑产交易数据格式中，短信劫持格式的数据准确性最强

黑产对数据评估的维度主要有两个方面，一是数据的时效性，二是数据的准确性。

威胁猎人对数据交易黑产进行深入调研发现，**不同格式数据的准确性以及时效性均有所不同。**主要为**短信劫持格式、DPI 格式、SDK 格式的信息数据**，据了解每日可稳定产生的数据量高达万余条。

在准确性方面：短信劫持格式的数据>DPI 格式的数据>SDK 格式的数据；

在时效性方面：DPI 格式的数据>SDK 格式的数据>短信劫持格式的数据。



威胁猎人针对该泄露数据样本进行验证后发现，不同格式数据的准确率确实有所不同，结果与数据交易黑产描述的一致，在准确率方面：短信劫持格式的数据>DPI 格式的数据>SDK 格式的数据，具体原因如下：

1、短信劫持格式的数据：包含短信内容，数据真实性方面基本确认为真实接受到短信通知的公民个人信息；

2、DPI 格式的数据：主要为流量解析的数据，主要通过运营商侧获取到的流量数据，因此真实性较低，据威胁猎人调查统计，该类数据的真实性基本不超过 20%；

3、SDK 格式的数据：主要通过解析软件包名信息，再提供到运营商侧获取下载流量，且存在应用市场软件刷量或未进行注册的用户信息的情况，因此真实性最低。

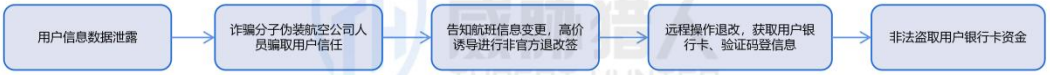
2.5 2023 年黑产数据交易形势变化以及下游作恶新手法

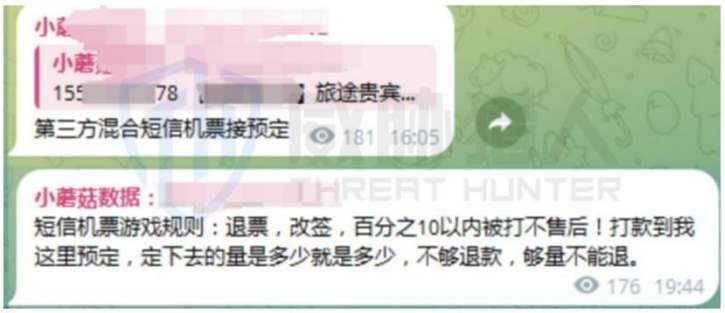
2.5.1 航旅行业“退改签”诈骗事件频发且成功率较高

威胁猎人对数据交易市场下游作恶团伙调研发现，2023 年航旅行业出现大量黑产团伙通过机票改签的方法实施网络诈骗，诈骗成功率较高。

2023 年随着新冠疫情好转，旅游行业回暖态势明显，消费需求得到强劲释放，机票信息、酒店信息等旅客信息也出现大幅增长，航旅出行方面的公民个人信息备受下游黑产诈骗团伙的青睐。

案例：诈骗团伙通过伪装成航空公司工作人员电话联系航班旅客，称航班出现延误，可进行改签或者退票操作，同时以获得“高额理赔”为由诱导用户下载视频会议、远程共享等操作，逐步陷入诈骗团伙的陷阱，通过获取用户的银行卡、支付宝、验证码等敏感信息后，转移盗取旅客资金。



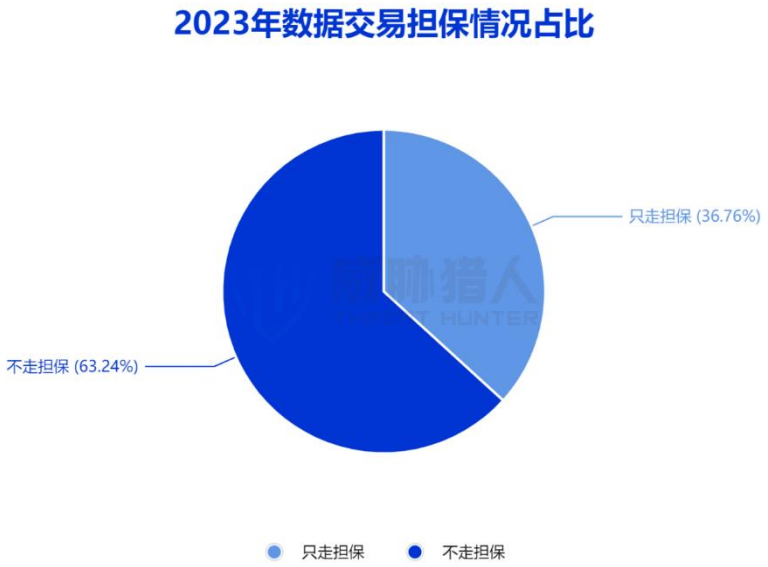


2.5.2 第三方担保、区块链付款为黑产数据交易再添安全保障

第三方担保：

过去，交易双方通常采取一对一的方式，即一方付款，另一方交付数据。由于近年来不断爆发的交易诈骗和交易跑路事件，数据交易市场变得更加混乱，一对一的交易方式变得不再可行。

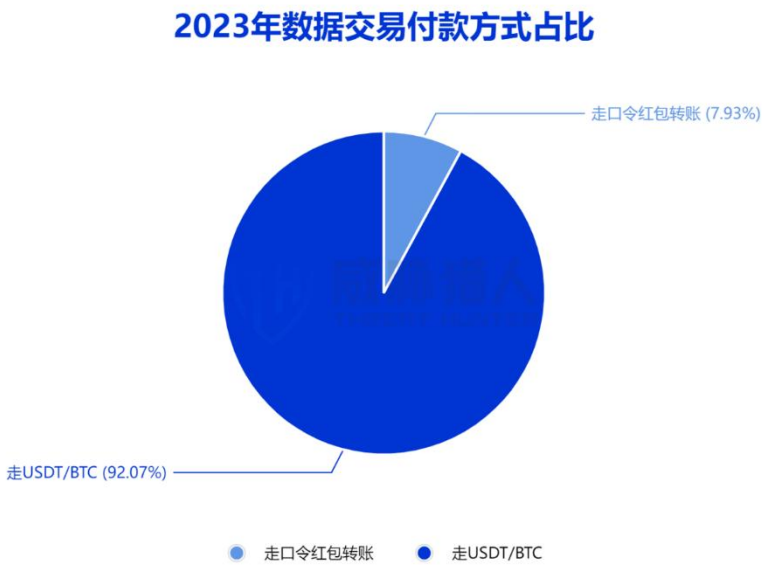
为了避免被骗，数据交易黑产团伙逐渐改变交易方式，开始依赖于中介担保平台和第三方担保平台进行交易，为交易提供了更可靠的保障，使得交易更加安全和可信。



区块链付款：

过去，黑产常常通过口令红包、支付平台转账等方式进行交易付款。由于这些付款方式易被追踪和控制，加上近年来司法机关对数据交易黑产团伙的严厉打击，导致数据交易的黑产团伙不得不改变交易付款方式，逐渐转向只采用加密货币进行支付。

加密货币具有匿名性和去中心化的特点，使得交易双方的身份得以保密，并且很难被监管机构追踪和控制。因此，采用加密货币支付款项成为黑产团伙数据交易的新趋势。这种变化进一步增加了打击黑产团伙数据交易的难度，需要采取更加有力的措施来保护数据交易市场的安全和稳定。



2.5.3 金融行业“全格式”信息数据交易价格最高，单价达 25 元

威胁猎人调研统计发现，在利益的驱动下，上游黑产窃取的数据类型发生了变化。

在金融行业，公民个人信息数据的价值与其所包含的字段数量密切相关。“全格式”信息通常包含身份证、姓名、手机号、银行卡、贷款信息、地址等字段，下游黑产可通过完整的公民画像信息实现精准作恶，**因此“全格式”数据的价格最高，单条数据价格可达 25 元。**相比之下，仅包含手机号字段的公民个人信息数据，由于下游作恶团伙的作恶方式受限，其收益较低，数据价格一般在 3 毛左右。

此外，不同行业的数据价格也存在差异。例如金融行业的公民个人信息针对高净值人群，持有资金较多，因此数据价格较贵；学生信息数据则相对便宜，因为下游作恶收益较低。这种差异性定价反映了不同行业对于公民个人信息的需求和价值认知。

03

多维度提升数据泄露风险监测及预警能力

三、多维度提升数据泄露风险监测及预警能力

从 2023 年数据泄露风险现状来看，企业需要重点关注以下问题：

1、黑产二次拼接“历史个人数据信息”，并进行多次贩卖的现象频发

数据交易市场存在着大量的黑产贩卖虚假数据、拼接数据、历史数据、交易诈骗等行为，企业对数据的真伪校验存在一定的难度。

2、公民个人信息在夜间交易的超过 50%，在非工作日交易的超过 30%

2023 年公民个人信息泄露事件的数据交易时间分布中，非工作日（周末、节假日）发生的事件数量高达 31.21%，夜间发生的事件数量占比高达 51.88%，超过一半。

3、金融行业数据泄露事件数量超 8700 起，在数据泄露行业分布上位列第一

金融行业依旧是个人信息泄露重灾区，数据泄露事件数量超 8700 起，涉及银行、保险、证券等行业高净值人群信息数据，主要源于下游黑产用于营销推广以及诈骗的收益价值更高。

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、加强风险真实性验证：在全网情报监测及深度挖掘的基础上，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。其中，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，帮助企业精准感知风险，为企业和个人提供更可靠的数据安全保护。

2、「7×24×365」应急响应：2023 年 10 月，威胁猎人成立数字风险应急响应中心（DRRC），对企业相关风险情报进行全天候监测、审核和预警，提供「7×24×365」样例获取、情报挖掘、协助溯源、处置下架等服务。

数据泄露风险监测及预警能力需要从多维度持续提升，只有不断加深对企业自身及行业风险态势的全面认知，才能为企业数字化的高效、可持续发展夯实安全底座。

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