威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

2022年API安全研究报告

出品方：威胁猎人

以客户为中心 | 正直 | 求真

THREAT HUNTER

目录

Contents

前言

近年来，数字化浪潮与疫情交织，企业业务线上化被按下了“快进键”。数字化与线上化趋势下，API 接口作为应用连接、数据传输的重要通道，呈现大规模增长趋势，API 应用的增速与其安全发展的不平衡，使其成为**恶意攻击的首选目标**，围绕 API 安全的攻防较量愈演愈烈。

威胁猎人长期致力于 API 安全的研究，重点关注全网针对 API 攻击的各类黑灰产情报。《2022 年 API 安全研究报告》显示，**API 安全已然成为了当下企业面临的最严峻网络安全挑战之一：**

1、2022 年平均每月遭受攻击的 API 数量**超 21 万**，其中**“营销作弊”**场景在 API 攻击的主要场景中占比最大，**金融和政务平台**成为黑产攻击 API 并窃取数据的重要目标；

2、2022 年，**互联网、政务、金融等各行业**发生了多起因 API 安全防护不当引起的 **API 攻击及数据泄漏事件**：如线上政务平台的业务 API 遭黑产攻击，公民隐私数据被爬取；社交平台面临大量扫号、撞库等攻击，大量用户账号被黑产贩卖并用于色情、赌博、诈骗等引流推广。

威胁猎人《2022 年 API 安全研究报告》基于 Karma 情报平台捕获的 API 攻击风险，对过去一年的 API 安全现状和攻击趋势进行了分析，梳理了 2022 年较为常见的 API 安全缺陷、API 攻击方式，并结合 API 安全案例给出相应的防御建议。

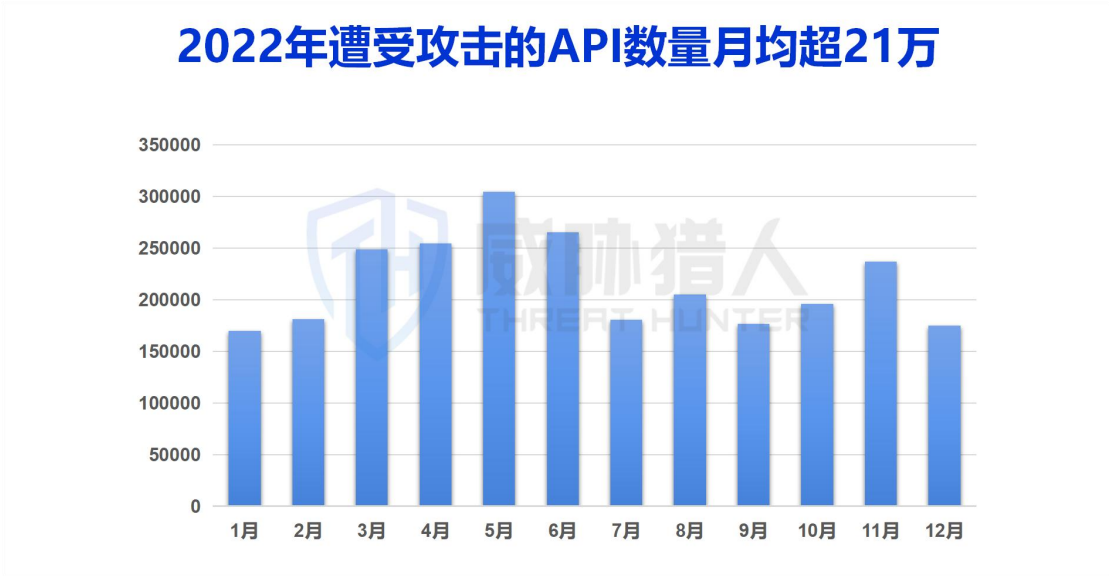
01

API 安全风险概况

一、2022 年 API 安全风险概况

1、2022 年平均每月遭受攻击的 API 数量超 21 万

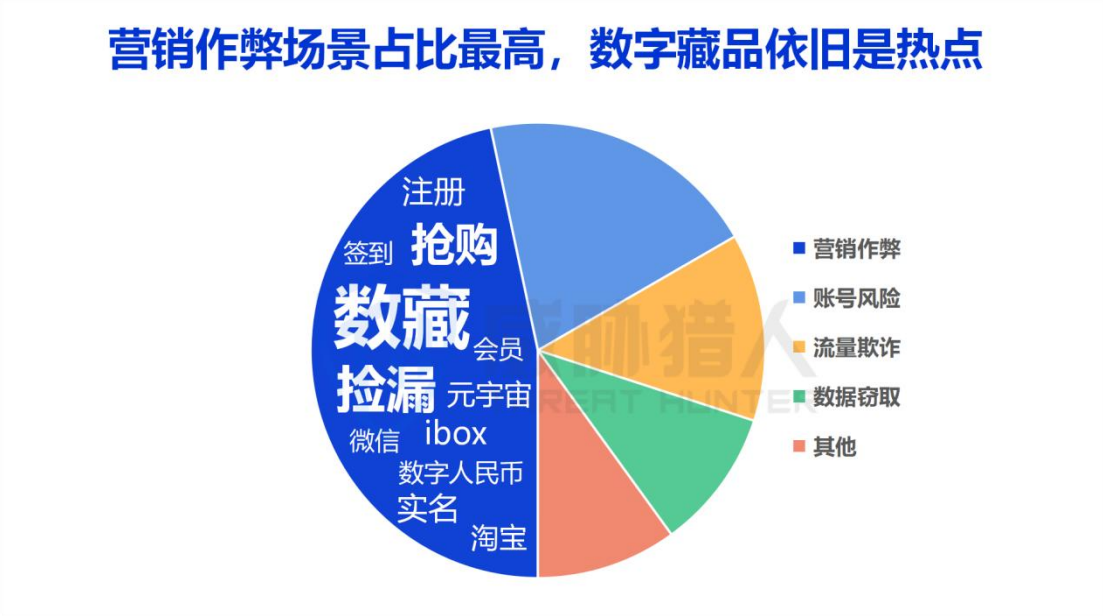
从威胁猎人 Karma 情报平台捕获到的攻击流量来看，2022 年全年平均每月遭受攻击的 API 数量**超过 21 万**，第二季度（4-6 月）遭受攻击的 API 数量达到高峰，月均攻击数量**超过 27 万**。



图：2022 年 1-12 月遭受攻击的 API 数量

2、API 攻击主要集中在四大场景，营销作弊场景占比最大

从 API 遭受攻击的场景来看，主要集中在营销作弊、账号风险、数据窃取和流量欺诈四大场景，其中，**营销作弊**场景攻击量近乎占总攻击量的一半。此外，虚假账号、账号盗取等一系列**账号风险**问题占比高达 20%，成为第二大常见 API 攻击场景。



图：API 攻击的常见场景占比

3、API 攻击遍布各行各业，金融和政务平台是黑产攻击 API 并窃取数据的重要目标

图：2022 年 API 攻击的主要行业

从 2022 年 API 攻击的行业分布数据来看，热度最高的是**数字藏品行业**，2022 年初开始，黑产针对数字藏品活动接口的攻击快速激增，并在 2022 年 Q2 达到高峰。

值得关注的是，威胁猎人情报研究团队通过分析 2022 年 API 攻击流量，发现有多个**金融和政务平台**遭受大规模攻击，黑产通过金融或政务平台有安全缺陷的 API 非法爬取大量涉及公民隐私、金融业务办理等敏感数据。

黑产通过贩卖**金融行业的用户数据**可以获取高额利益，包括但不限于出售给中介“精准”揽客、出售给犯罪分子实施诈骗等；**政务平台的 API 接口**则承载了海量公民隐私数据，如身份证、住址、医保社保等敏感信息，也是黑产疯狂攻击的对象。

此外，**游戏、社交、电商、制造**等行业的 API 接口也遭到黑产的大规模攻击，具体如下所示：

游戏：游戏行业 API 接口被攻击的主要场景是**账号风险**问题。黑产长期对注册、登录、找回密码等接口，发起扫号、撞库和暴破攻击，盗取玩家账号和虚拟资产。其中针对某些热门游戏的全网攻击规模达到数亿次。

社交：社交平台 API 接口被攻击的主要场景是**流量欺诈**问题。黑产通过攻击平台的业务接口，制造虚假阅读量、点赞量、评论等。网络水军可借此控制舆情，引流团伙则借此给赌博、诈骗等网络犯罪行为引流。

电商：电商平台面临着**营销作弊**以及商家刷单、黄牛抢购等**流量欺诈**问题。尤其每年的双11，双 22 等电商节日，以及疫情期间口罩、抗原等热门商品的抢购时段，各家平台的 API 接口往往会遭受到黑产的大规模攻击。

制造：汽车、家电等传统制造业在 2022 年进一步深化数字化转型，其线上业务的 API 接口也被黑产盯上，带来了**营销作弊、数据窃取**等安全问题。

02

API 安全缺陷分析

二、2022 年 API 安全缺陷分析

API 攻击事件频发，其根本原因仍是 API 存在安全缺陷。威胁猎人基于 API 安全管控平台 2022 年流量审计结果，从**危害性、可利用性、普遍性**三个维度，梳理了企业需关注的五大 API 安全缺陷。

2022年需重点关注的五大API安全缺陷

缺陷类型	危害性	可利用性	普遍性
未授权访问	**极高**	**高**	**高**
允许弱密码	**高**	**高**	**高**
敏感数据过度暴露	**高**	**高**	中
错误提示不合理	中高	中高	**高**
安全配置不合理	**极高**	**高**	中

注：极高 > 高 > 中高 > 中

1、未授权访问

从 2022 年的审计结果来看，**「未授权访问」**依然是危害性最大的 API 安全缺陷之一。API 存在未授权访问缺陷，**可能会导致系统权限失陷**。威胁猎人情报研究员曾在 2022 年 Q1 发现某公司内部系统的 API 接口，该接口开放了外网访问且访问无需任何授权，传入任意账号都可以获取到该账号的密码。

这属于非常严重的安全漏洞，一旦遭到攻击，攻击者可轻易获取到管理员的账号密码，并拿到系统的最高权限。

该缺陷也**可能会引发大规模数据失窃**。威胁猎人在 2022 年 Q3 对 48 家银行信用卡业务的 API 接口进行安全评估，发现**至少有 20 家银行的 API 接口存在未授权访问缺陷**：在未经授权的情况下，可以查询到任意用户的信用卡办理信息，而黑产团伙也利用该缺陷对多家银行的 API 接口发起了大规模的自动化攻击，批量窃取用户隐私信息。

安全建议：

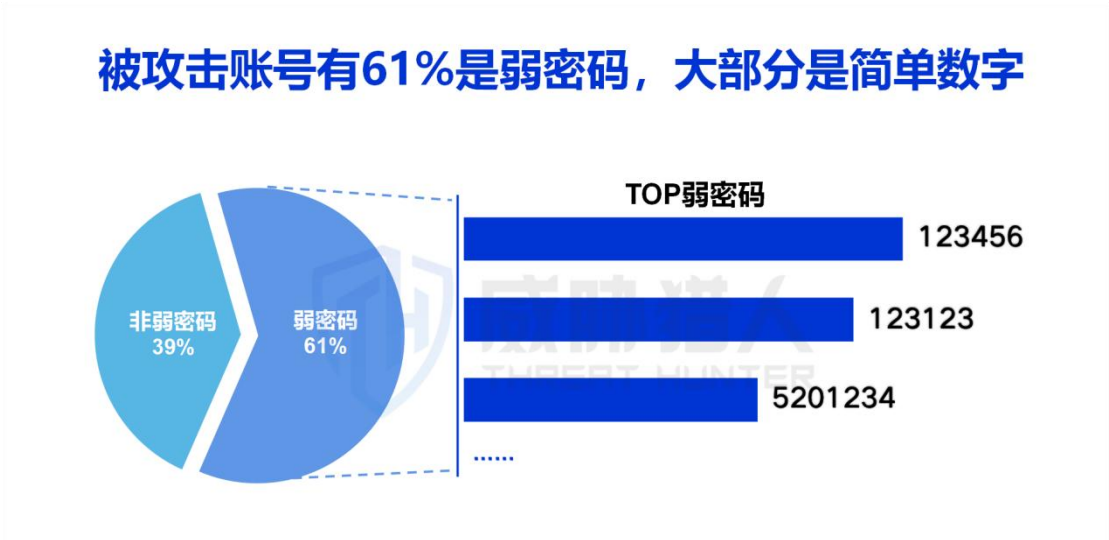
1）除非资源完全对外开放，否则访问默认都要授权，尤其是访问用户的资源或者受限制资源；

2）通过白名单的方式来严格控制无需授权的 API 接口的访问。

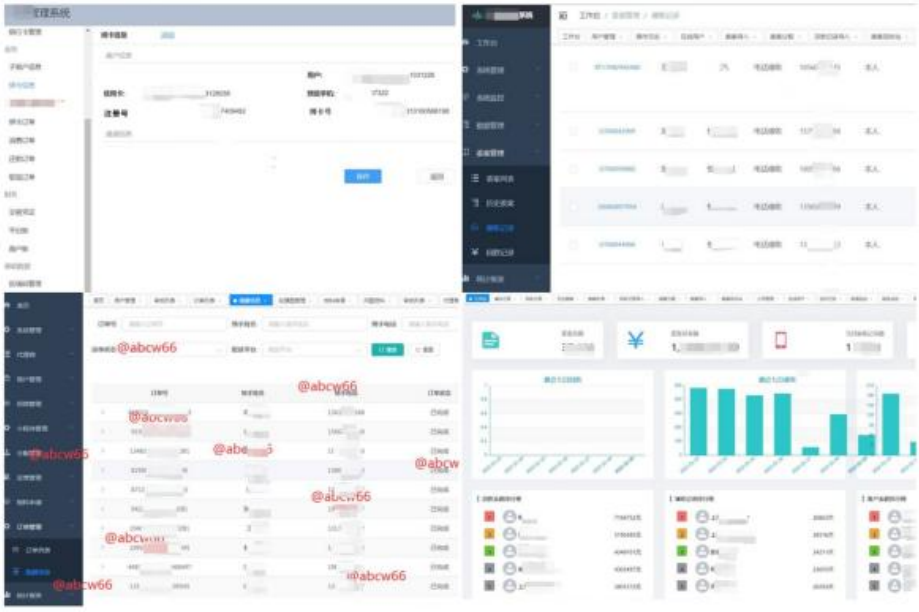
2、允许弱密码

「允许弱密码」是危害性、普遍性和可利用性都非常高的一种缺陷，是黑产盗取账号的主要手段之一。尽管很多安全开发规范都有提到密码设置需满足一定的强度，但从 2022 年的整体情况来看，仍有不少的 API 接口，甚至是**部分管理后台的登录接口**，存在允许弱密码的缺陷。

API 接口存在允许弱密码的缺陷**容易导致严重的账号风险。**以某游戏平台为例，该平台由于存在弱密码缺陷，遭受到黑产团伙长期撞库和暴破攻击，被黑产成功盗取的账号中**超过 61%是弱密码**，且排名靠前的都是一些非常简单的纯数字组合。



后台 API 接口存在该缺陷可能会导致**系统权限失陷。**在某数据泄露事件中，威胁猎人情报研究员多次发现由不法分子流传出来的管理后台截图，初步判断攻击者就是利用弱密码缺陷，暴破出了登录后台的账号密码。



安全建议：

1）在用户注册、登录、密码重置等场景中对密码复杂度进行检查，建议密码长度不低于 8 位，且包含大小写字母、数字及特殊符号；

2）密码不允许设置为账号、邮箱、生日等关联信息；

3）对于高权限账号，建议引入一段时间内强制修改密码的机制。

3、敏感数据过度暴露

「敏感数据过度暴露」指 API 接口不加任何限制或过滤，把后端存储的敏感数据返回到前端，一旦被黑产攻击，会带来严重的数据泄露问题。

威胁猎人情报实验室经研究发现，存在敏感数据过度暴露缺陷的 API，往往出现在**企业的信息公示页面**上。虽然页面只展示了必要信息和脱敏信息，但背后的 API 接口却返回了大量不必要的明文敏感数据，部分 API 接口一次性返回**几百甚至上千条**用户的涉敏数据。

以某互联网公司营销活动为例：

某互联网公司营销活动的中奖公示页面上，只展示了中奖用户的头像、昵称、城市和脱敏手机号，但 API 接口却返回了很多页面没有展示的敏感数据，包括中奖人的**真实姓名、收货地址、明文手机号**等。公示的中奖信息任何人都可以查看，极易被不法分子获取并利用。

另一个关于 API 敏感数据过度暴露的真实例子：

在某数字化转型企业官网的供应商公示页面上，只展示了供应商的公司名、公司图片、营业执照等基本信息，但 API 接口却返回很多无需公示的非常敏感的个人隐私数据，包括**供应商法人的身份证号、手机号、紧急联系人**等。这些敏感数据被不法分子窃取后，不仅会危害到供应商法人的个人安全，也会给企业数字化转型带来阻力和打击。

安全建议：

API 接口要对返回到前端的敏感数据进行严格的过滤，只返回前端需要的数据。

4、错误提示不合理

「错误提示不合理」指 API 接口返回的错误提示，会无意间暴露用户的注册账号、手机号、邮箱等敏感数据。从 2022 年的审计结果来看，错误提示不合理依然被黑产**广泛应用于扫号攻击**当中，威胁猎人情报研究员发现了多家金融借贷平台的 API 接口遭受黑产团伙攻击，导致平台大量用户手机号泄漏。

以某金融借贷平台 API 攻击事件为例：

威胁猎人情报研究员对攻击流量分析发现，在用户发起借贷申请时会引导用户先填入手机号进行注册。点击申请后，前端会根据接口返回的值，向用户返回不同的提示（如下所示）。

不少攻击者利用这一点实施扫号攻击，在接口参数中传入不同的手机号，再通过接口返回值（True/False）进行筛选，从而获取到大量平台注册用户的手机号，**批量攻击存在错误提示不合理的 API 接口。**如果不能及时发现并阻断攻击，黑产完全可以遍历完 11 位手机号，从而获取到平台所有用户的注册手机号。

安全建议：

1）针对登录、注册、验证码发送、密码找回等接口的错误提示信息进行模糊化处理，比如返回“用户名或密码不正确”；

2）针对上述接口，对于调用量过大及调用频率过高等异常行为加强监控。

5、安全配置不合理

「安全配置不合理」指由于开发或运维人员的疏忽，导致对外暴露不应公开的 API 接口，使用旧版本存在漏洞的 API 接口，或接口访问使用默认密码或密钥等问题。

2022 年，威胁猎人对部分企业的后台组件和服务进行了安全审计，从审计结果来看，安全配置不合理这个缺陷普遍存在，其中不乏 **Spring Boot Actuator 、Elasticsearch 配置错误**等较为严重的安全配置错误。

据了解，2022 年 11 月，开源 API 接口管理平台 YApi 曝出执行任意命令高危漏洞，**其中一个重要原因就是使用了默认的密钥**，导致攻击者可以成功获取到系统权限，如图所示：

```
41
42  const defaultSalt = 'abcde';
43
44  exports.getToken = function getToken(token, uid){
45    if(!token)throw new Error('token 不能为空')
46    yapi.WEBCONFIG.passsalt = yapi.WEBCONFIG.passsalt || defaultSalt;
47    return aseEncode(uid + '|' + token, yapi.WEBCONFIG.passsalt)
48  }
49
50  exports.parseToken = function parseToken(token){
```

如果没有配置密钥，
就会使用默认密钥

安全建议：

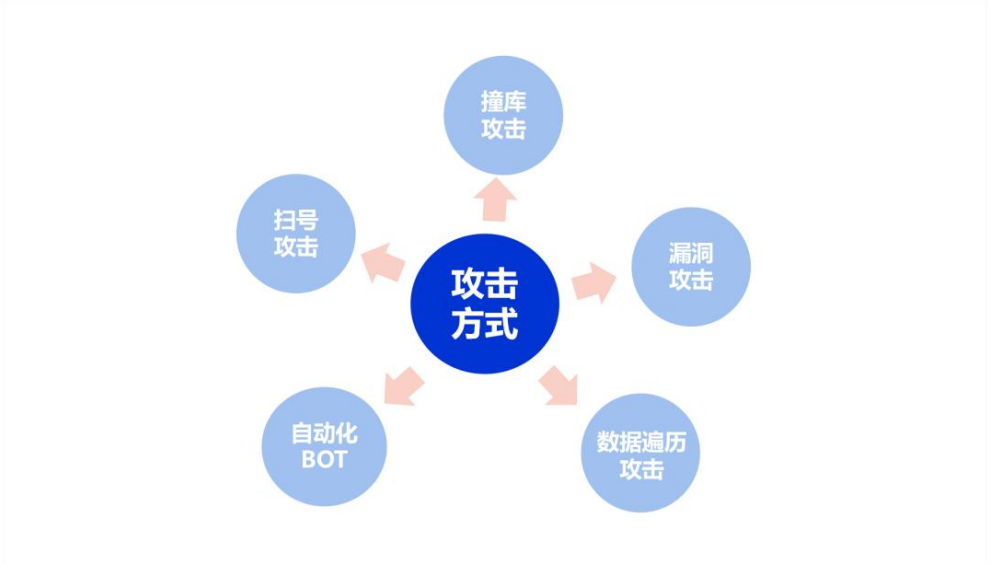
1）全面排查使用的组件/服务的版本，尽量升级到最新版本；

2）全面检查配置是否正确，避免出现组件/服务暴露未授权访问 API，避免使用默认密码或秘钥。

03

API 攻击方式分析

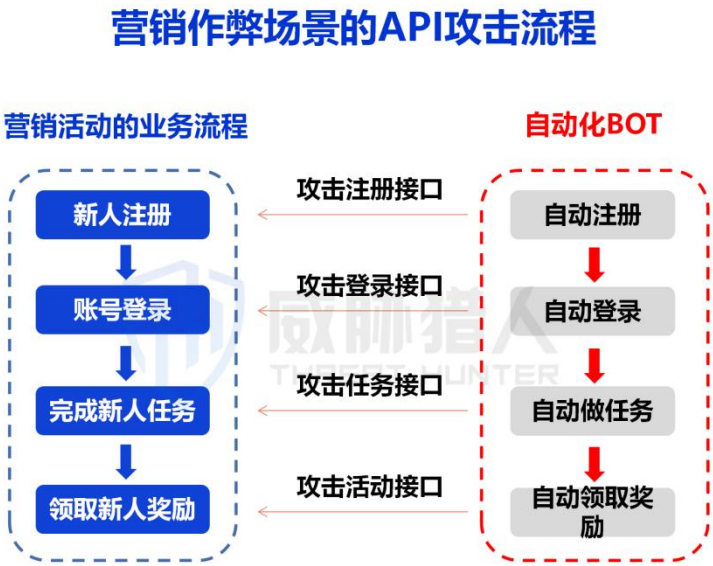
三、2022 年 API 攻击方式分析



1、自动化 BOT

「自动化 BOT」是 2022 年最为常见的 API 攻击方式之一，主要出现在**营销作弊**和**流量欺诈**场景当中。黑产通过自动化脚本等方式模拟真人操作，伪造出完整的业务流程，进而按照真实的业务访问顺序攻击多个 API 接口。

以营销作弊场景的 API 攻击为例：



专业的黑产团伙往往具备丰富的攻防对抗经验，其发起的自动化 BOT 攻击，从流量和行为上不会出现明显异常，很难识别出是真人还是机器人。因此，对于自动化 BOT 的攻击方式，我们需要从海量的接口访问数据中，将其和正常用户的请求区分开来。

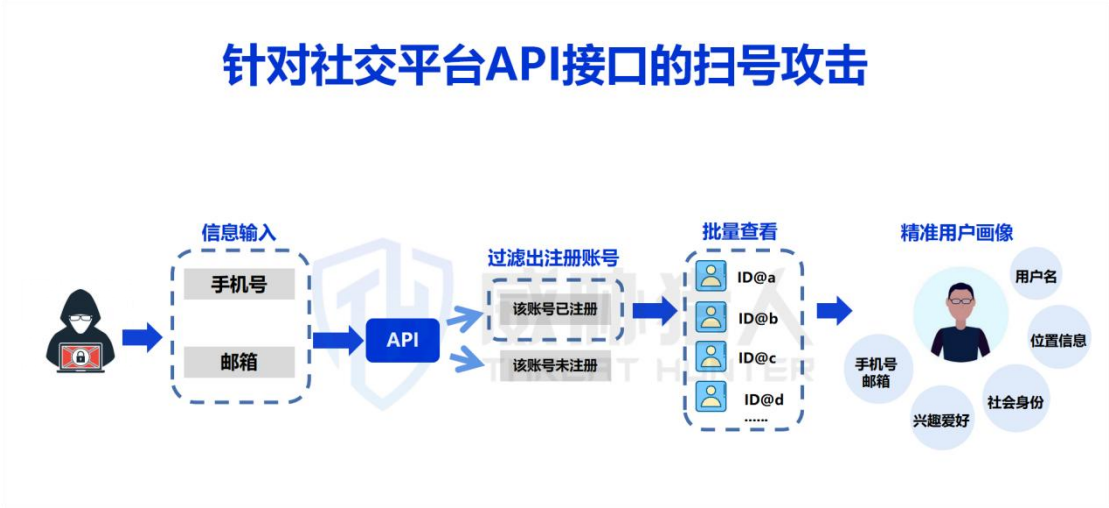
自动化 BOT 攻击主要包括以下几个识别维度：

自动化BOT攻击的主要识别维度

识别维度	有经验的BOT攻击	如何绕过攻防
UA	无聚集	随机伪造和终端匹配的UA
IP	无聚集	通过动态代理/秒拨切换IP地址
设备	无聚集	通过改机技术更改设备参数
行为	和真人操作的请求参数和序列完全一致	通过抓包破解的方式获取接口请求参数和序列

2、扫号攻击

「扫号攻击」指黑产团伙以**“注册、登录、找回密码”** 等 API 接口为目标，通过注册、登录等接口的返回值，如“账号已存在”或“账号不存在”等来判断某个账号（用户名、邮箱、手机号等）是否在该平台注册过。黑产团伙通过遍历 11 位手机号，就可以筛选出平台所有注册用户的手机号，这些数据一旦在黑市上出售，手机号主就会遭受到电销骚扰甚至电话诈骗。

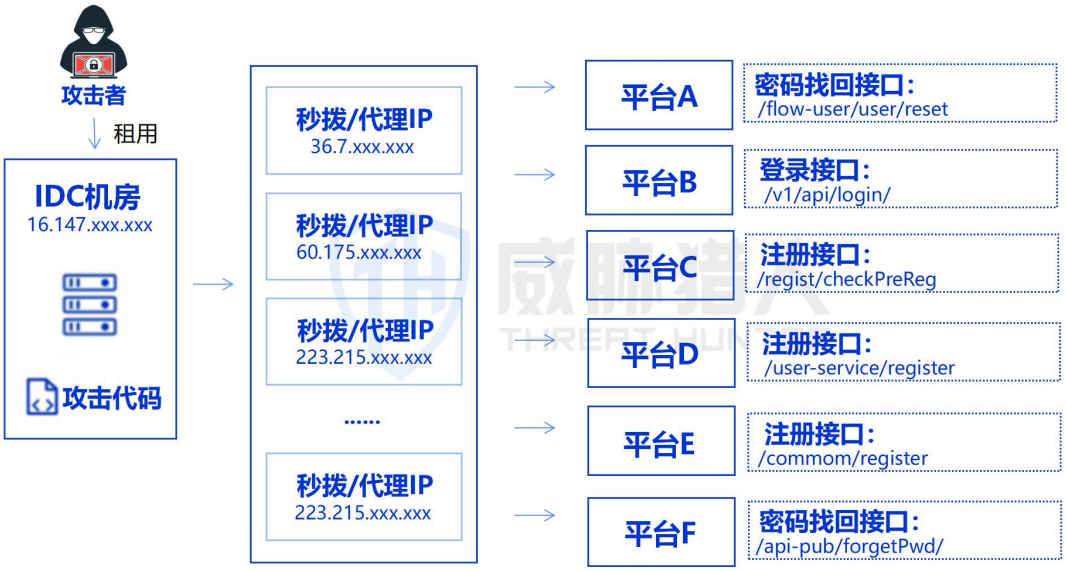


在 API 安全缺陷分析中提到，如果接口存在**错误提示不合理**的缺陷，很可能会遭到黑产团伙的扫号攻击。

金融行业是扫号攻击的重点行业，一方面这些数据会卖给金融中介或其他平台的推广人员用于“精准营销”“精准获客”；另一方面这些数据也会卖给诈骗团伙实施精准诈骗，最典型的套路就是确认受害人在某个金融平台借贷后，打电话诱导受害人以**“保证金”、“服务费”、“手续费”**等名义往犯罪分子控制的银行账户打款。

威胁猎人 Karma 情报平台在 2022 年捕获到了**多起针对金融借贷平台 API 接口的扫号攻击**，并对其中一个较为活跃的黑产团伙的攻击过程进行了详细分析。该团伙先是在国内某 IDC 机房租用服务器，将攻击代码部署在服务器上，然后对多个平台的 API 接口发起大规模的自动化攻击，如下图所示：

针对金融借贷平台API接口的扫号攻击



为了尽可能多的获取用户数据，该团伙会高频攻击这些接口，同时为了避免被发现，该团伙通过黑产资源平台获取到的动态代理和秒拨频繁切换 IP，**超过 35%的 IP 甚至只发起一次攻击。**从实际的攻击结果来看，遭受到攻击的平台当中，没有 1 个平台可以识别或阻断攻击，**攻击成功率达到 100%。**

3、撞库攻击

「撞库攻击」指黑产团伙以登录接口或其他接口为目标，通过一些自动化工具批量提交大量曾泄露的**用户名/密码组合**，记录下其中能成功登录的组合，从而盗取该账号并接管其权限。

游戏行业是撞库攻击的重点行业，黑产通过撞库攻击盗号成功之后，通常会登录账号查看玩家账号等级、资产、装备等信息（晒号），若账号不存在二次验证，黑产会在极短的时间将金币等资产、装备进行转移，甚至分解掉不能转移的装备（洗号），不仅给玩家造成财产损

失，也给游戏平台口碑及生态造成破坏。此外，威胁猎人研究人员调查发现，**部分大型社交平台也多次遭遇撞库攻击。**

很多企业为降低撞库攻击的风险，对于登录接口会有严格的安全限制。但“道高一尺魔高一丈”，专业的黑产团伙会采用针对性的攻击策略：

1、为避免被发现，攻击团伙对登录接口进行低频撞库攻击，如**平均 3-4 分钟才发起 1 次攻击**，因不易被发现，因此可以保持长期攻击；

2、为提高撞库攻击效率，攻击团伙会结合扫号攻击，先通过扫号筛选出已注册账号，**针对已注册账号进一步发起撞库攻击**；

3、为进一步提高攻击效率，黑产通过路径扫描等方式进行 API 资产探测，**找到老旧登录接口进行攻击**，老旧接口可能因无人维护而缺乏安全限制，更容易被攻击。

4、数据遍历攻击

「数据遍历攻击」通常以存在“未授权访问缺陷” 或“越权访问缺陷” 的 API 接口为目标，黑产通过攻击这些 API 接口，批量窃取平台的用户数据或业务数据。数据遍历攻击也逐渐成为导致数**据泄漏事件的重要原因之一。**

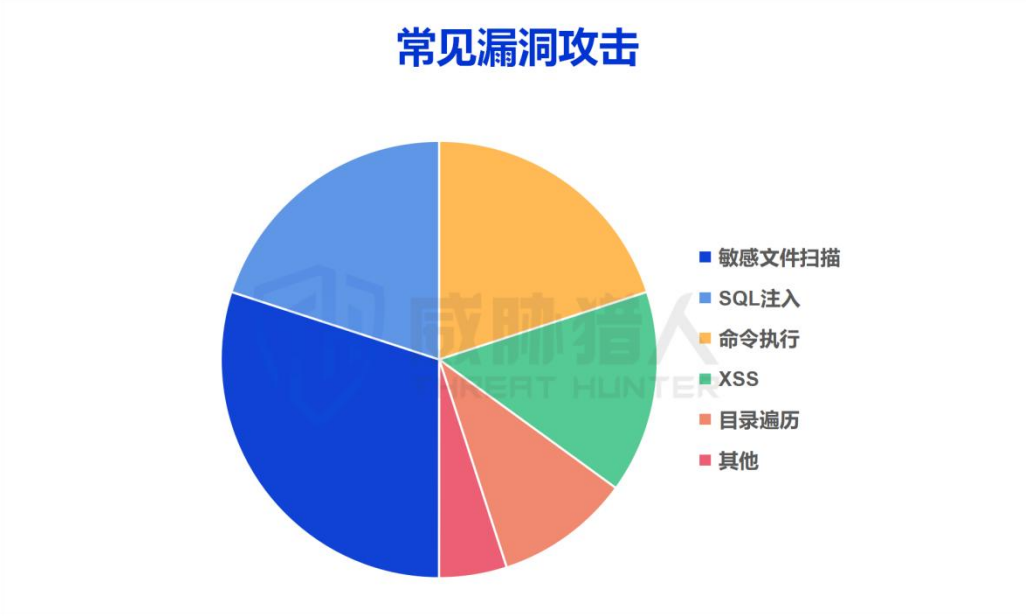
政务平台是数据遍历攻击的重点行业，为提升业务办理效率及服务体验，各地政府机关都推出了线上政务服务，然而很多业务的 API 接口由于存在安全缺陷，成为网络犯罪分子的重点攻击目标。

2022 年针对政府平台的数据遍历攻击更加猖獗。威胁猎人情报实验室曾发现某非法窃取数据的大型网络犯罪团伙，经调查发现，该团伙开发了**数十款自动化攻击工具**，利用政府平台 API 接口存在的安全缺陷，通过数据遍历攻击**大规模非法窃取公民隐私数据。**

黑产通过对 API 接口进行数据遍历攻击，窃取的敏感数据主要类型如下：

5、漏洞攻击

「漏洞攻击」通常指“SQL 注入漏洞，命令执行漏洞”等一些常见的 Web 漏洞，被用于攻击 API 接口。2022 年，威胁猎人情报研究人员对部分企业的流量进行了审计研究，发现**“敏感文件扫描、SQL 注入、命令执行、XSS、目录遍历”**等漏洞出现频率较高。



互联网每天存在大量由扫描器发起漏洞攻击，攻防演练期间，“漏洞攻击”更是攻击方的重要“杀手锏”，攻击方通过漏洞扫描器发起扫描，在目标资产中快速找到脆弱点。由于扫描数量庞大，安全设备难以实现精准告警，**容易产生大量误报。**因此，防守方需要定位到漏洞点，及时感知风险并做出防御措施，防止风险进一步扩大。

以较为经典的“SQL 注入”为例：

结合 HTTP 请求及响应，可以分析出一些 SQL 注入漏洞是否攻击成功，若请求参数中存在 updatexml()等函数，同时响应体中又存在"XPATH syntax error"这样的关键词，那么基本可以判定是在进行 SQL 报错注入，且已经攻击成功。

04

API 攻击案例

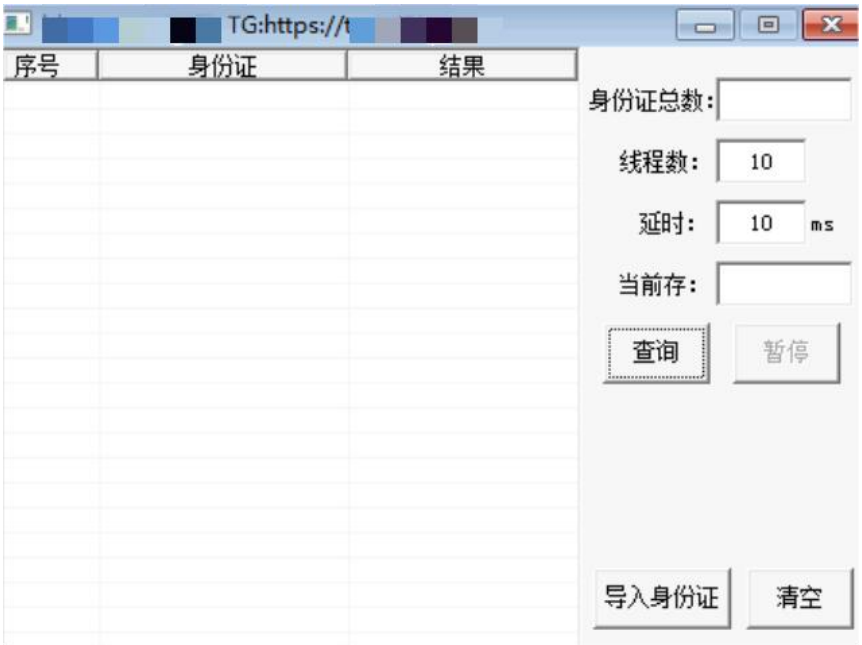
四、2022 年值得关注的 API 攻击案例

1、线上政务平台的业务 API 遭受黑产攻击，公民隐私数据被爬取

线上政务给广大民众带来极大的便利，但线上政务的背后往往关联大量公民隐私数据，**数据访问限制、身份授权等**都需要经过仔细的设计和严格的审核，大量 API 暴露在互联网上无疑增加了公民隐私**数据泄露的风险。**

关于攻击者利用 API 获取敏感数据的真实案例：

2022 年 9 月，威胁猎人 Karma 情报平台捕获到一款名为**“**名下证”**的自动化攻击工具，攻击者通过该工具对**广东某线上政务平台**的数据查询 API 接口展开攻击，遍历爬取该平台用户信息。



威胁猎人研究员通过对攻击工具进行分析，从复现的攻击代码中发现，攻击者只需要在函数中构造好身份证参数，**无需任何授权就能查询任意用户基本信息**，包括公民的姓名、身份证、结婚证、儿童出生证明、户口簿、社会保障卡、不动产权等。

攻击者会持续扫描发现系统 API 存在的安全漏洞、利用大量动态代理 IP、借助自动化工具来进行敏感数据爬取，**极易引发大规模数据泄露**，复现的 API 攻击代码如下：

```python
    # 获取指定身份证公民的证件信息列表
    resp = requests.post(url, data = postPattern.encode("utf-8"), headers=headers, verify=False)
    print(resp.text)
    if resp.text == "[]":
        print("未查询到结果")
        return
    j = json.loads(resp.text)
    for index in range(len(j)):
        fileId = j[index]["fileId"]
        if fileId == None:
            continue
        getLicenseFileStream(fileId,idCard)
        time.sleep(5)
```

爬取的敏感信息样例如下：

JSON ▾ 取消自动换行 复制


```
      "fileName": "居民身份证",
        "licenseCode": "440000201802******",
        "type": "0",
        "materialUnid": "",
        "fileId": "440000201802******_100208101_1144060631507697******111187000",
        "licenseItemCode": "100208***"
    },
    {
        "fileName": "广东省居民户口簿",
        "licenseCode": "440000201902******",
        "type": "0",
        "materialUnid": "",
        "fileId": "440000201902******_100210301_1144060631507697******111187000",
        "licenseItemCode": "100210***"
    }
]
```

安全建议：

1）限制政务平台信息查询的接口只有登录后的用户才可以查询，并且只有当前用户绑定的身份证与查询的身份证一致时才能够查到用户个人信息；

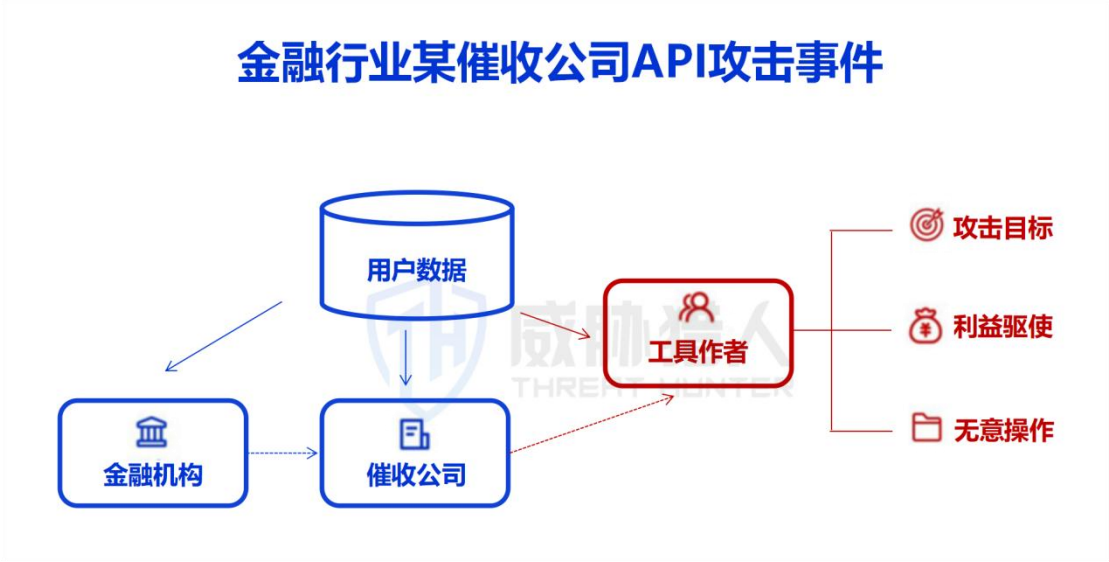
2）如不可避免直接通过身份证查询用户个人信息，建议该接口不要暴露到互联网，只允许内网访问，并且限定人员的访问权限，做好日志记录。

2、金融行业第三方合作中存 API 安全隐患，多家金融机构面临数据泄漏风险

为降低借款客户逾期赖账的风险，金融机构往往会**委托第三方公司进行催收**，将自身催收系统的权限开放给催收公司，同时会将借款人的身份证、手机号、住址、联系人、借款金额等数据交给第三方催收公司，如何保障数据安全成为各金融机构不可回避的问题。

以金融行业某催收公司 API 攻击事件为例：

2022 年，威胁猎人 Karma 情报平台监控到某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**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，不受系统访问权限和操作限制的影响。



以某款工具为例，“催收辅助工具”访问以下接口时可直接获取**借款人名字、身份证、借款数量、住址**等数据，还支持将数据下载到本地。

一方面，催收公司员工可登录系统并查看借款客户的信息，给**潜在内鬼批量窃取数据**提供了便利；另一方面，获得数据访问权限的工具作者，也将成为攻击者的攻击目标之一，**扩大了数据暴露面**，给金融机构带来了新的数据泄露风险。

工具访问的接口	接口说明	接口返回数据明细
https://cs.xxx.com:8080/ajax/case/list.json	拉取借款列表	data.count 借款数量 data[i].caseNo 借款编号 data[i].debtorName 借款人名字
https://cs.xxx.com:8080/ajax/case/detail/info.json	获取借款人详细信息	data.baseInfo.overdueAmount 逾期金额 data.baseInfo.overdueDays 逾期时间 data.userInfo.certificateNo 身份证 data.userInfo.workUnit 工作单位 data.userInfo.unitAddress 住址 ... ...

安全建议：

1) 在 API 资产梳理及 API 缺陷检测过程中，对于传输业务敏感数据或用户敏感数据的 API 接口，需进行完备的安全审计并进行严格的安全限制，避免出现未授权访问、越权访问等缺陷；

2) 基于情报的 API 风险识别能力，提取“催收辅助工具”发起的 API 请求特征等行为方式，及时发现涉敏数据的异常流动及账号的违规行为；

3) 金融行业需加强对合作催收公司的安全治理：2022 年全网攻防演练中新增了数据获取的评判维度，其中包括“通过供应链企业获取敏感数据信息”，催收公司作为金融机构催收服务的供应商，也属于供应链企业，未来会成为重点攻击目标。

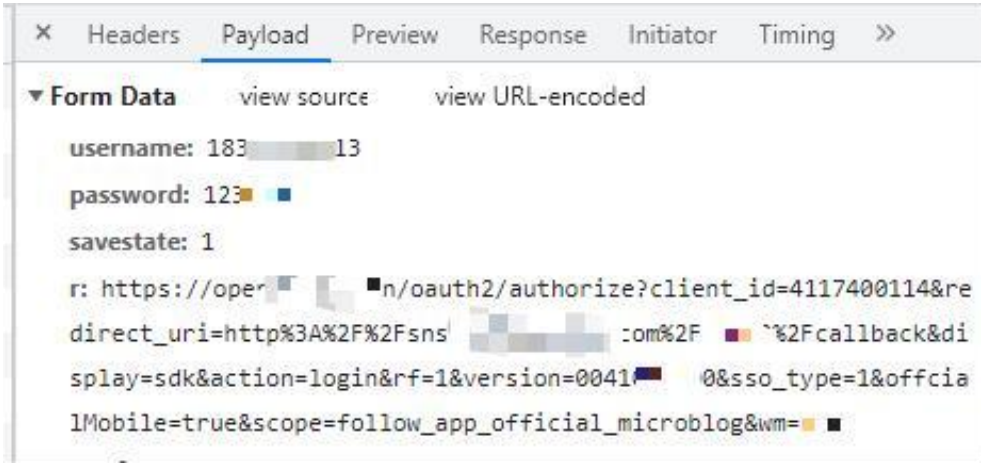
3、互联网社交平台受到撞库攻击，贩卖账号被用于引流推广

2022 年，威胁猎人 Karma 情报平台监测到大量针对社交平台的扫号、撞库等攻击，其中不乏专业黑产团伙的参与。**部分大型社交平台**因 API 接口存在问题而屡遭攻击，账号安全事件接二连三。

以某大型社交平台撞库攻击为例：

2022 年 8 月，威胁猎人 Karma 情报平台监测到攻击者对**国内某大型社交平台**发起撞库攻击，并成功盗取到不少平台用户的账号密码。这些账号密码被攻击者用于贩卖获利，主要被用于**色情、赌博、诈骗引流推广**等。由于大多都是正常用户长期使用的账号，不是黑产批量注册的虚假账号，从而增加了平台的治理难度。

从威胁猎人蜜罐捕获的攻击流量发现，从 2022 年 8 月到 10 月，攻击者使用代理 IP，对某社交平台的登录 API 发起攻击共计**超 500 万次，盗取账号数千个。**通过进一步分析发现，该社交平台存在多个登录 API 接口，如下图所示，**部分登录 API 接口中账号密码参数并未进行加密，均为明文传输**，这些的登录 API 接口也成为了黑产发起撞库攻击的主要对象。



从 2022 年 9 月到 10 月，威胁猎人 Karma 情报平台共捕获到**黑产通过发卡平台交易共计 3000 余个社交账号**，通过对账号卖方的行为统计研究发现，捕获到的黑产交易的账号与撞库流量可以成功匹配，进一步确认了黑产盗取社交账号进行交易的行为。

安全建议：

1）使用统一登录 API，能够实现对登录入口的统一管理，减少攻击面，安全策略能够集中控制，遇到风险也能及时响应；

2）登录 API 的账号、密码要进行加密后再传输，同时加强强弱密码的校验；

3）使用验证码等人机识别，虽然攻击者会使用打码平台来绕过，不断强化的验证码策略会提高攻击者的攻击门槛。

4、智慧停车平台 API 接口存在漏洞，车主信息泄露事件频现

近几年，“智慧停车”平台蓬勃发展，停车场接入“智慧停车”系统后，车主用手机扫一扫、输入车牌号即可线上查询和缴费。智慧停车平台在为广大车主带来便利的同时，业务安全问题也逐渐暴露。

关于攻击者利用“查询 API 接口”获取车主隐私的真实案例：

威胁猎人情报研究员在蜜罐监测到的流量中，发现针对多个“智慧停车”系统的持续性攻击行为，**被攻击的“智慧停车平台”基本覆盖了市民能接触到的大多数停车场**，通过分析发现，这些智慧停车平台的缴费查询 API 接口均存在**“未授权访问漏洞”**，攻击者利用该漏洞爬取了大量用户停车信息。

多个省市智慧停车系统APP遭受攻击（部分）

工具名	对应公司	攻击接口
A .exe	深圳市 有限公司	http://mops. com.cn/v3/Bussiness/GetParkInfo
R .exe	广西 科技有限公司	https://plate- /plate
E a.exe	深 有限公司	https://api.a /gateway
H .exe	北京 科技有限公司	http://www /v1/api/parking/lookup?licence_plate
J .exe	深圳市 股份有限公司	https:// com.cn/core-gateway/order/carno/pay/index
L .exe	兰州 运营有限公司	https:// .com/parking_orders/wx_get_car_orders
T .exe	武汉 科技有限公司	https://mpapi. /kesb_req
X .exe	浙江 科技有限公司	https://u. n/parkingLot/getCurrentChargeBill
Y .exe	广东 科技股份有限公司	https://wxy .xin/user/charge/charge/parkingCharge.do

为进一步验证，威胁猎人情报研究员对其中一个被攻击的智慧停车平台进行分析，发现黑产团伙**通过 IP 代理平台获取大量 IP**，并对智慧停车平台的**查询 API 接口**进行频繁、批量攻击。

黑产团伙利用该 API 缺陷**任意输入一个车牌号**，在不需要车主授权的情况下，便可查询到该车辆在系统内每个时段的停车信息，包括**入场时间、入场位置、入场照片等**信息，在摸清任意车辆的行驶轨迹的同时，还能“顺藤摸瓜”获取车主的家庭住址、手机号、工作单位等更多隐私数据。

黑产通过相关渠道进行信息售卖或者提供定位服务来获利，车主的信息有可能被用于各种用途，轻则账号被盗，重则伪造身份进行借贷，给市民财产安全造成威胁。

威胁猎人情报实验室发现，某黑产团伙在 Telegram 群中提供车辆信息查询服务：

安全建议：

1）限制车辆停车的信息接口需要先进行身份验证，比如绑定微信号、手机号等才可以进行查询；

2）对接口查询做好频率限制，比如短时间内单个身份查询的车牌号不能超过 2 个。

在数字化转型与发展过程中，企业所面临网络安全管理的实际问题远不止于此，遭遇的 API 攻击也更加复杂多变。对于企业而言，一旦出现数据泄露情况，不仅面临经济损失和名誉损失，还会面临违法风险甚至更严厉的处罚。结合不同行业/场景下的 API 攻击案例可以看出，**企业需要加强自身的安全建设，尤其是针对 API 安全建设。**

05

安全建议

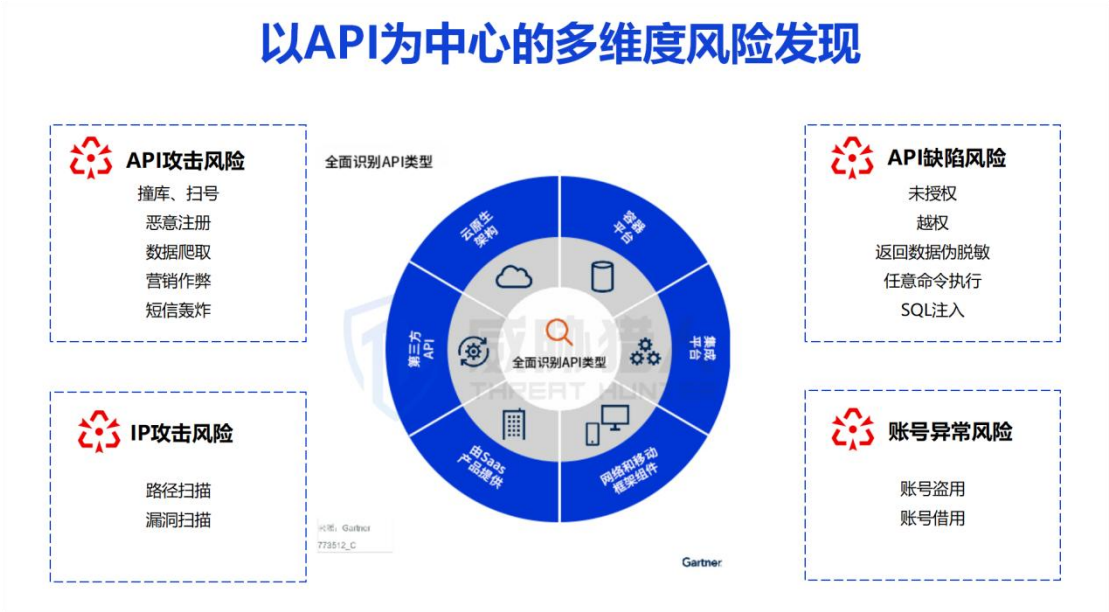
五、安全建议

面对不断更新变化的内外部 API 攻击，企业该如何识别 API 安全建设路径的关键？威胁猎人认为，“业务优先”是企业发展的前提，企业的整体安全建设应遵循：

第一、业务优先；第二、解决可见性；第三、做到整体可控。

在“业务优先”的基础上，威胁猎人安全专家建议从 API 的上线运营阶段入手，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，要务是**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。**从业务安全角度来讲，这也是企业能够健康发展的前提。

之后再通过安全左移，将视角转到 API 上线前的**设计、开发、测试**等阶段，从而更好地实现 API 全生命周期管理，过程中结合上线后的安全实践总结，可更加有的放矢，避免盲目投入。



据 Google Cloud 研究表明，与低成熟度的企业相比，API 安全成熟度高的企业在数字化转型方面遥遥领先。显然，技术领导者已经意识到了 API 带来的价值，**API 安全最终需要成为整体端到端安全战略的一部分。**

威胁猎人 API 安全管控平台将攻击防御能力与 AI 智能数据分析能力全面融合，**基于“情报”构建 API 访问的行为基线**，且不受 AI 流量波动影响，可以快速判定 API 存在的风险攻击事件，帮助企业全面梳理 API 资产、预防发现阻断 API 攻击、提升风险事件的响应速度、防止流动敏感数据泄漏，更好地护航企业的业务和数据安全，**以情报构筑数字化安全基石。**

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