

# 一、威胁情报与

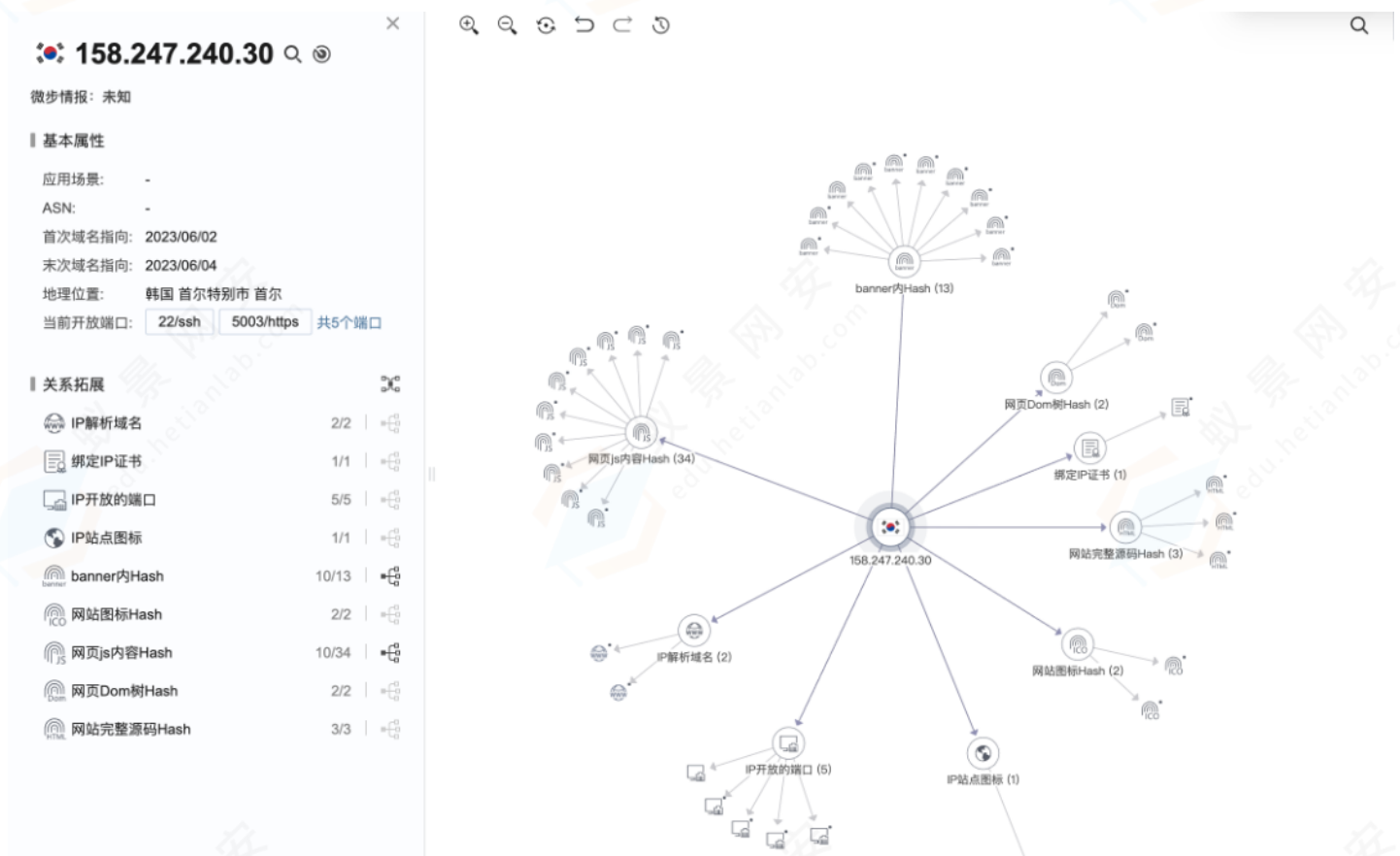
## 1. 威胁情报

威胁情报是有关组织可能面临的潜在攻击以及如何检测和阻止这些攻击的信息。执法部门有时会分发带有嫌疑人信息的“通缉”海报；同样，网络威胁情报包含有关当前威胁是什么样子以及它们来自何处的信息。

在数字安全术语中，“威胁”是一种恶意行为，可能导致数据在未经许可的情况下被盗、丢失或更改。该术语指的是潜在的和实际的攻击。威胁情报使组织能够针对威胁采取行动，而不仅仅是提供数据。每一条威胁情报都有助于检测和预防攻击。

某些类型的威胁情报可以输入防火墙、Web 应用程序防火墙 (WAF)、安全信息和事件管理 (SIEM) 系统以及其他安全产品，使它们能够更有效地识别和阻止威胁。其他类型的威胁情报更为通用，可帮助组织做出更大的战略决策。

- 奇安信威胁情报平台 <https://ti.qianxin.com/>
- 微步威胁情报 <https://x.threatbook.com/>
- 腾讯安全威胁情报平台 <https://tix.qq.com/>



## 2. IP

(1) 物理定位

A. asn

自治系统或自治域(AS)是在一个或多个网络运营商代表单个管理实体或域的控制下连接的互联网协议(IP)路由前缀的集合，它为互联网提供了一个通用且明确定义的路由策略。每个AS都分配有一个唯一的自治系统编号(ASN)，用于边界网关协议(BGP)路由。

ASN号的分配是由互联网地址分配机构（IANA）先将未分配的ASN块分配给各个区域互联网注册管理机构（RIRs），各地区RIR将进一步将收到的ASN块分配给本地互联网注册机构(LIR)和最终用户组织。IANA还维护一个保留供私人使用的ASN注册表（因此不应向全球互联网公布）。被分配的AS号有16比特和32比特的整数值两种表示类型。16比特的AS号的长度范围介于 0 和 65535 之间，32比特的AS号的长度范围介于0 和 4294967294 之间。目前普遍使用的是16比特整数值表示的类型，最多能被分配给65536个自治系统。

知道这个IP是哪个国家、哪个地区，就是通过asn定位的。

<https://zh-hans.ipshu.com/>

国家或地区代码	国家或地区名称	IP数量	全球排名
AD	 - 安道尔	62,309	178
AE	 - 阿联酋	4,240,588	58
AF	 - 阿富汗	239,576	135
AG	 - 安提瓜和巴布达	44,779	186
AI	 - 安圭拉	10,442	217
AL	 - 阿尔巴尼亚	382,707	123

B. 公开定位接口

一般不准，给你一个ip，就想通过这种免费的方式实现GPS级的定位，还是洗洗睡吧

https://www.chaipip.com/aiwen.html

chaipip

首页

Q 查询1-埃文

Q 查询2-互联网

Q 新手上云

IP 58.20.23.44

点击按钮进行验证

查询

今日: 3,082 昨日: 3,175 总共: 4,816,915

每人每天限查20个IP, 多了永久黑名单

查询2收费, 可查高德、搜狗、腾讯3家的高精度IP 点我查询

埃文科技-IP访问

IP为: 58.20.23.44

级别: 街道 算法定位 中国联通

该IP可能在以下1个区域内分布:

地区1

半径: 7114.6米

纬度: 28.225417

经度: 112.862017

详细: 湖南省 长沙市 岳麓区

显示周围 全屏查看 谷歌地图

时间: 2023-10-19 22:07:37

IPINET

地址: 中国 湖南 长沙 联通

qqzeng

IP2Region

地址: 中国 湖南 长沙市 联通

Geolp2

地址: 中国 湖南 长沙 (国外准)

纯真IP

地址: 湖南 长沙市 联通

注意事项

接口由埃文科技的街道级别-IP访问服务提供 官网http://ipplus360.com/

https://www.ipuu.net/

公安版 商业版 区县级 城市级

此IP分布在以下一个区域

大洲	亚洲
国家/地区代码	CN
国家	中国
省份	湖南省
城市	长沙市
区 (县)	岳麓区
详细地址	湖南省长沙市岳麓区东方红中路
经度	112.86821
纬度	28.219741
半径	9.1088KM
精度	街道
邮编	410013
时区	UTC+8

C. 经纬度信息

```
options = {
  enableHighAccuracy: true,
  timeout: 5000,
  maximumAge: 0,
};

success(pos{
```

```

    crd = pos.coords;

    console.log("Your current position is:");
    console.log("Latitude : " + crd.latitude);
    console.log("Longitude: " + crd.longitude);
    console.log("More or less " + crd.accuracy + " meters.");
  }

  error(err){
    console.warn("ERROR(" + err.code + "): " + err.message);
  }

  navigator.geolocation.getCurrentPosition(success, error, options);

```

```

>> ▼ var options = {
  enableHighAccuracy: true,
  timeout: 5000,
  maximumAge: 0,
};

function success(pos) {
  var crd = pos.coords;

  console.log("Your current position is:");
  console.log("Latitude : " + crd.latitude);
  console.log("Longitude: " + crd.longitude);
  console.log("More or less " + crd.accuracy + " meters.");
}

function error(err) {
  console.warn("ERROR(" + err.code + "): " + err.message);
}

navigator.geolocation.getCurrentPosition(success, error, options);

```

← undefined

Your current position is:

Latitude : 28.212490441074078

Longitude: 112.88094046908702

More or less 42 meters.

>>

获取到经纬度信息

Latitude : 28.212490441074078 维度

Longitude: 112.88094046908702 经度

经纬度转地图

<https://lbs.amap.com/demo/javascript-api/example/geocoder/regeocoding>

境内地图不允许使用GPS坐标，但是设备定位获取的坐标均为GPS坐标，所以实际会有很大误差，一般是与GPS存在西北方向偏移

感兴趣可以了解下坐标，境内使用的是GCJ02国测局坐标，其他地区是WGS84坐标（GPS角度坐标），也有特殊的，比如百度地图用自己的BD-09坐标





## (2) 用了代理怎么办

- 挟持用户ping（漏洞或钓鱼）

一般使用的代理软件都是socks协议、http协议代理，均工作在应用层，无法代理icmp流量，所以ping命令发出的流量是自己的互联网IP

```
root@vultr:~# tcpdump -n icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enpl0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
14:49:51.174491 IP 220.202.233.202 > 158.247.240.30: ICMP echo request, id 17652, seq 0, length 64
14:49:51.174542 IP 158.247.240.30 > 220.202.233.202: ICMP echo reply, id 17652, seq 0, length 64
14:49:52.176798 IP 220.202.233.202 > 158.247.240.30: ICMP echo request, id 17652, seq 1, length 64
14:49:52.176853 IP 158.247.240.30 > 220.202.233.202: ICMP echo reply, id 17652, seq 1, length 64
```

- 挟持用户访问境内网站（jsonp）

有些代理具有代理规则，如代理境外网站。

<https://www.chaip.org/>

检测点	检测结果	解释说明
国内	220.202.233.202 湖南省长沙市联通	一般显示的是本机的IP地址，如 192.168.1.1，则显示的是 192.168.1.1 的IP地址
国外	218.255.175.153 香港汇港电讯 (WTTHK)	左侧IP就是您用来访问国外普通网站（没一 网站）的IP地址
Google	218.255.175.153	左侧若空白，则说明不能 显示IP则代表可以
IPv6		

### 3. 端口扫描

端口扫描是最有效的溯源方法（威胁情报都在用），通过端口扫描，能够发现攻击者开启的相关攻击工具监听服务，如teamserver、metasploit、frp、awvs、http等等，如果使用了默认密码或匿名访问，可以获取到攻击者非常多的信息

端口扫描的方法

```
namp -sT -Pn -p1-65535 -T4 你想扫描的
namp -sS -p1-65535 -T4 你想扫描的
```

### 4. 社会工程学

#### (1) 公开资源

专业名词称为 公开资源情报（OSINT）

- 注册网站检测

# 你注册过哪些网站？


邮箱/手机号

🔍

手机换号，如何保护您的数据？

- 网站历史

https://archive.org/web/



INTERNET ARCHIVE

Explore more than 846 billion [web pages](#) saved over time


BROWSE HISTORY

Find the Wayback Machine useful? [DONATE](#)

- 社交软件

https://checkusernames.com/

这个网站其实弊端很明显，第一都是境外的社交软件，第二是很多安全工作者喜欢用的twitter现在变成了x，但该网站没有适配



Check the use of your brand or username on 160 Social Networks:

Check User Name

To check the availability of your username **on over 50 social networks** check out our new, updated site at: [KnowEm.com](#).

KnowEm also offers a **Premium Service** which will create profiles for you on up to 300 popular social media sites

You Tube

Wikipedia

Linked In

Twitter

Ebay

Tumblr

Pinterest

Blogger

Live Leak

Zimbio

Houzz

My Space

Game Spot

Cracked

Behance

Sky Rock

APSense

Folkd

Watt Pad

Empire Avenue

Spark People

N4G

Veoh

Ebaums World

Design Float

Stock Twits

Fotki

Trend Hunter

Ads Of The World

Eventful

Tiny Chat

Shock Wave

- 信息泄露

https://haveibeenpwned.com/

- Google Dorks

intext:xxx

## (2) 社交媒体

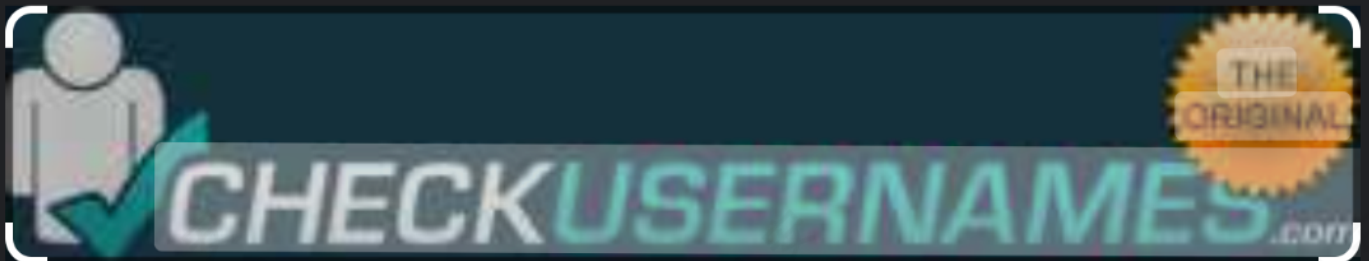
github、csdn、微博、推特、Facebook、支付宝、小红书、抖音、Bilibili、微信、QQ、网易云等等

```
xxx site:twitter.com  
xxx site:github.com  
xxx site:csdn.com
```

技巧：谷歌搜图

Google

🔍 查找图片来源



搜索

文字

翻译

技巧：个人博客

很多安全工作者会在个人博客的about me中留下丰富的个人信息，然后进行交叉查询