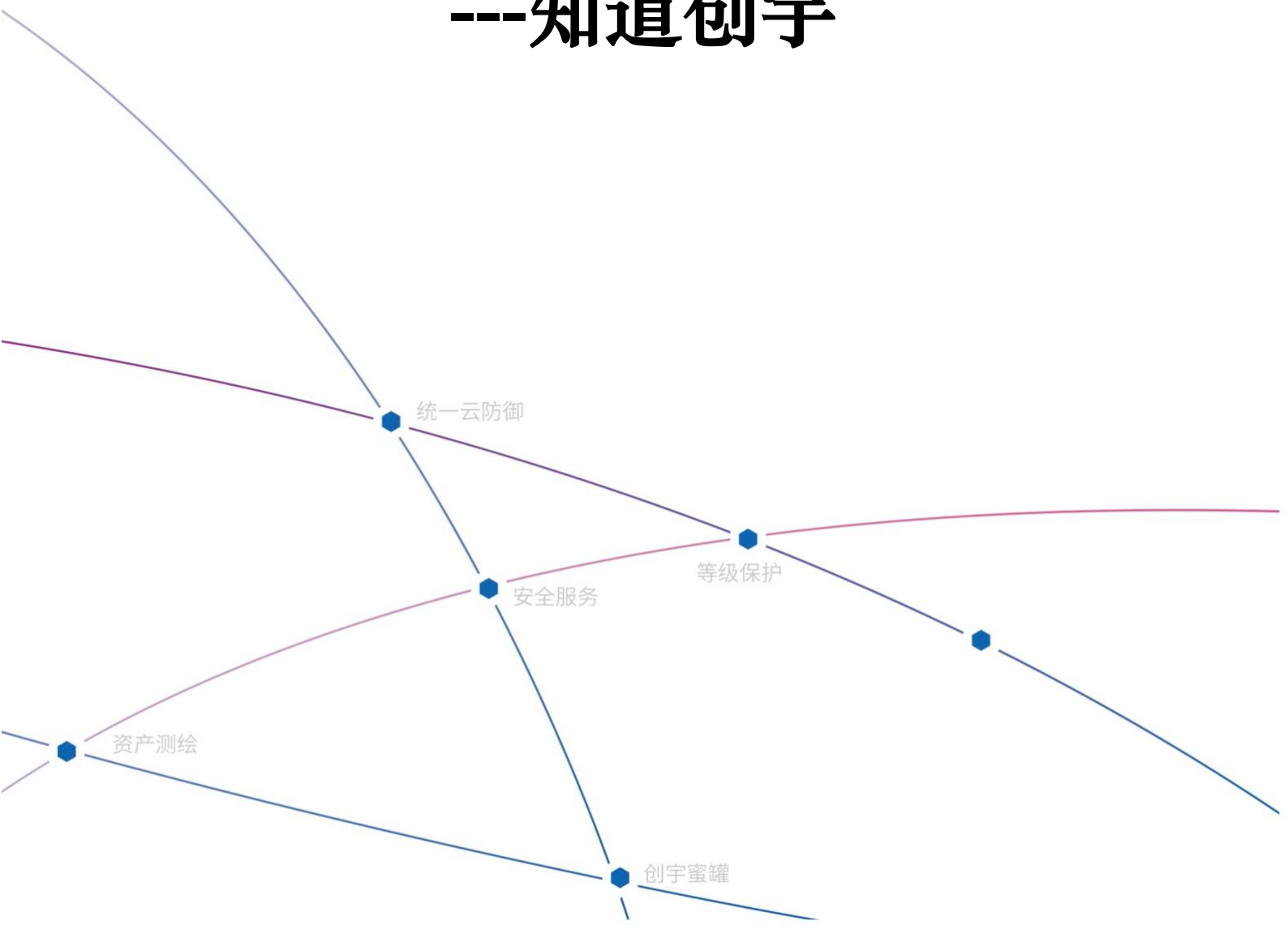
Zoomeye 使用手册

---知道创宇



文档信息

文档名称	版本号	保密级别
Zoomeye 使用手册—知道创宇	1.0	内部公开

版本说明

修订人	修订内容	修订时间	版本号	审阅人
田世辉	Zoomeye 使用手册—知道创宇	2021.06.16	1.0	裴文成
裴文成	修订格式	2021.06.16	1.1	马超

版权说明

目录

1. 前言

ZoomEye（“钟馗之眼”）——全球网络空间测绘的领导者，是知道创宇旗下 404 实验室驱动打造的中国第一款，同时也是全球著名的网络空间搜索引擎。通过分布在全球的大量测绘节点，针对全球范围内的 IPv4、IPv6 地址库及网站域名库进行 24 小时不间断探测、识别，根据对多个服务端口协议进行测绘，最终实现对整体或局部地区的网络空间画像。通过多年的发展不停的技术改造，目前 ZoomEye 拥有的自主研发网络空间搜索核心引擎已拥有世界领先网络空间测绘能力，并积累了大量的测绘数据进行趋势分析最终实现跨时空式的动态网络空间测绘画像。

本文主要对 ZoomEye 的使用方法进行详细讲解，所有搜索示例均已亲自测试通过。

2. 账户

ZoomEye 拥有四种账户类型，包括：注册用户、高级用户、VIP 用户、企业用户。

普通用户自行注册即可成为注册用户，注册用户购买会员服务即可成为高级用户、VIP 用户。各种用户可使用的功能、数据额度等均有差异，具体对比可以参考链接：https://www.zoomeye.org/business#recharge

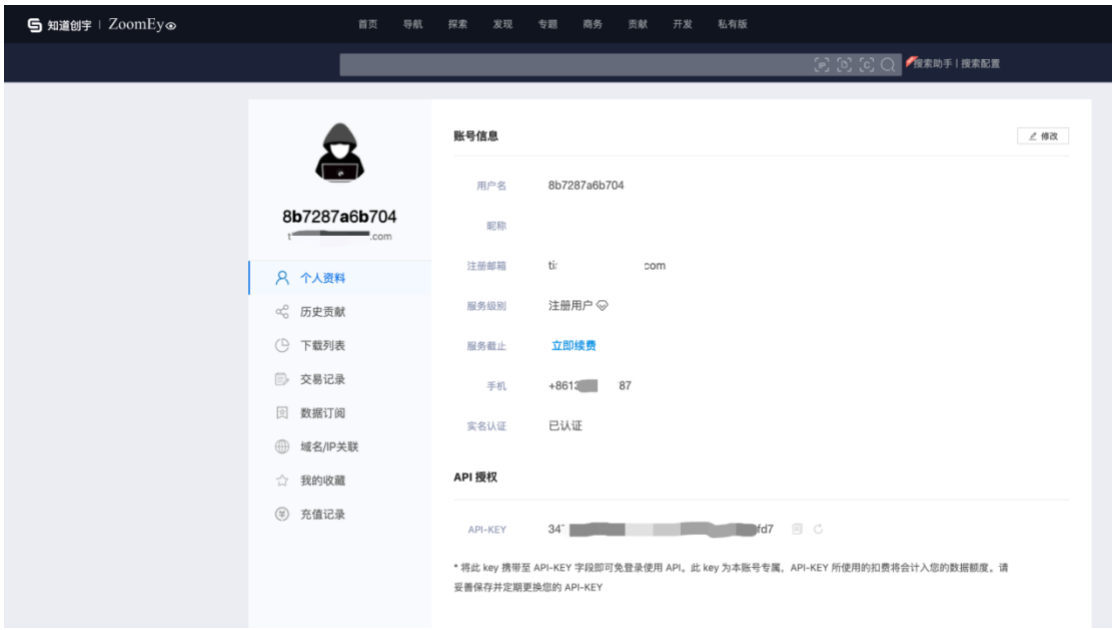
功能及价格	注册用户 ¥0 /月 每月赠与用户10,000条数据	高级用户 ¥500 /月 立即购买	VIP用户 ¥1000 /月 立即购买	企业商务 专属定制服务 联系商务
套餐1 (3个月) 9折	-	¥1350 (¥450/月)	¥2700 (¥900/月)	-
套餐2 (6个月) 8.5折	-	¥2550 (¥425/月)	¥5100 (¥850/月)	-
套餐3 (一年) 8折	-	¥4800 (¥400/月)	¥9600 (¥800/月)	-
查询结果展示量	400 条	1000 条	2000 条	数据查询定制
API数据总额度	免费 10000 条/月	免费 10000 条/月 +20000 条/月	免费 10000 条/月 +30000 条/月	专属定制
API查询结果数据比率	100%	100%	100%	专属定制
数据订阅规格	2 个订阅/20 个订阅 IP	5 个订阅/50 个订阅 IP	10 个订阅/256 个订阅 IP	专属定制
icon检索 NEW	✓	✓	✓	✓
文件检索 NEW	✓	✓	✓	✓
域名关联 NEW	✓	✓	✓	✓
数据订阅	✓	✓	✓	✓
分词测试	✓	✓	✓	✓

3. 个人资料

3.1. API-KEY

https://www.zoomeye.org/profile

登录后访问上述链接即可查看个人资料，其中包含了自己账户的一些信息、历史贡献、下载列表等信息。其中需要注意的是 API-KEY 将此 key 携带至 API-KEY 字段即可免登录使用 API。此 key 为本账号专属，API-KEY 所使用的扣费将会计入您的数据额度。请妥善保存并定期更换您的 API-KEY。

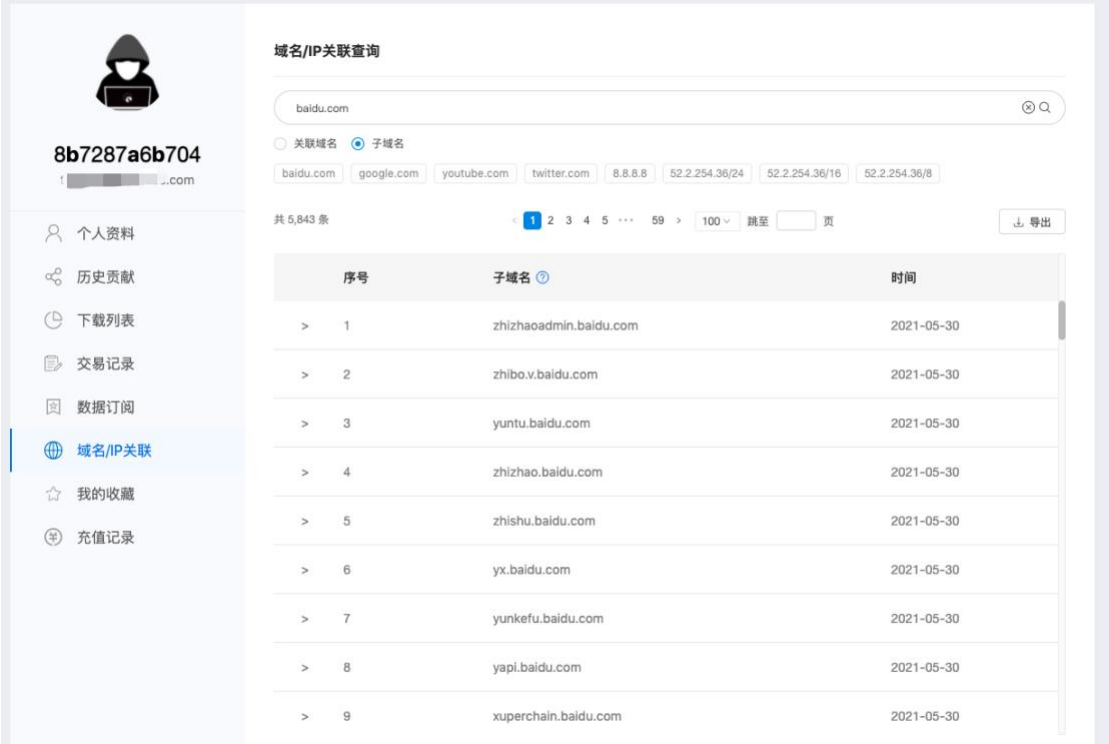


3.2. 域名/IP 关联查询

该功能模块位于个人资料目录下，地址为：

https://www.zoomeye.org/profile/domain

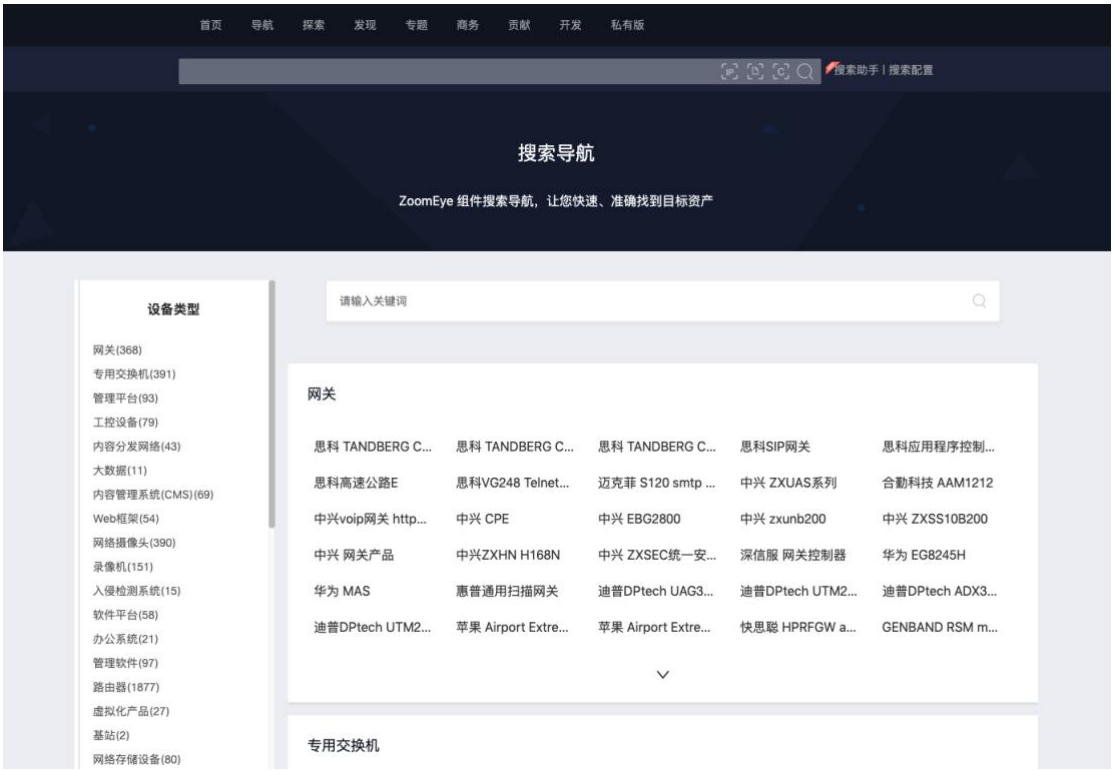
可以查询域名/IP 关联信息，也可以查询子域名信息，并且支持 TXT 和 Json 格式导出（目前支持单次 20000 条数据的免费导出）：



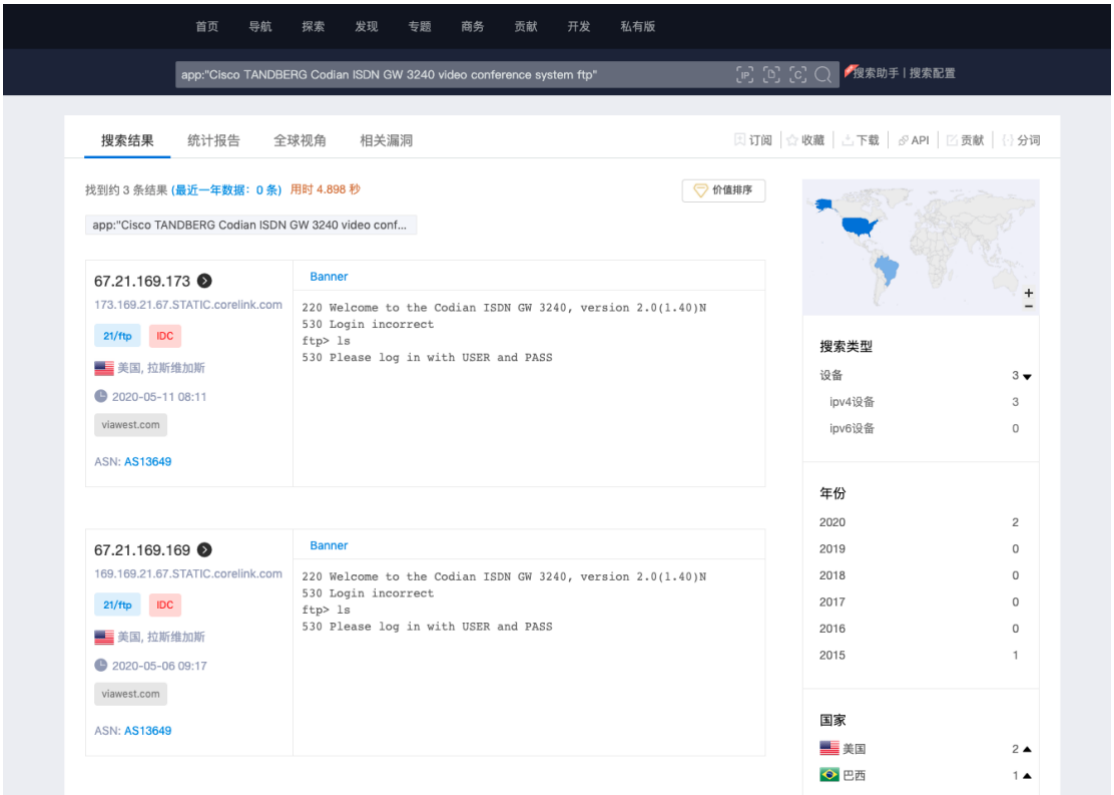
4. 导航

导航功能地址为：https://www.zoomeye.org/component

导航功能为用户提供了已经收录好的常用网关、专用交换机、工控设备等常用设备的搜索语法。



点击对应设备名称，即可自动生成对应的搜索语法进行搜索：



5. 探索

地址：https://www.zoomeye.org/statistics

探索功能是 Zoomeye 提供的可视化资产测绘展示，以 IP 分布、Web 应用、Web 框架、设备、端口等维度展示了 Zoomeye 测绘的能力。

6. 发现

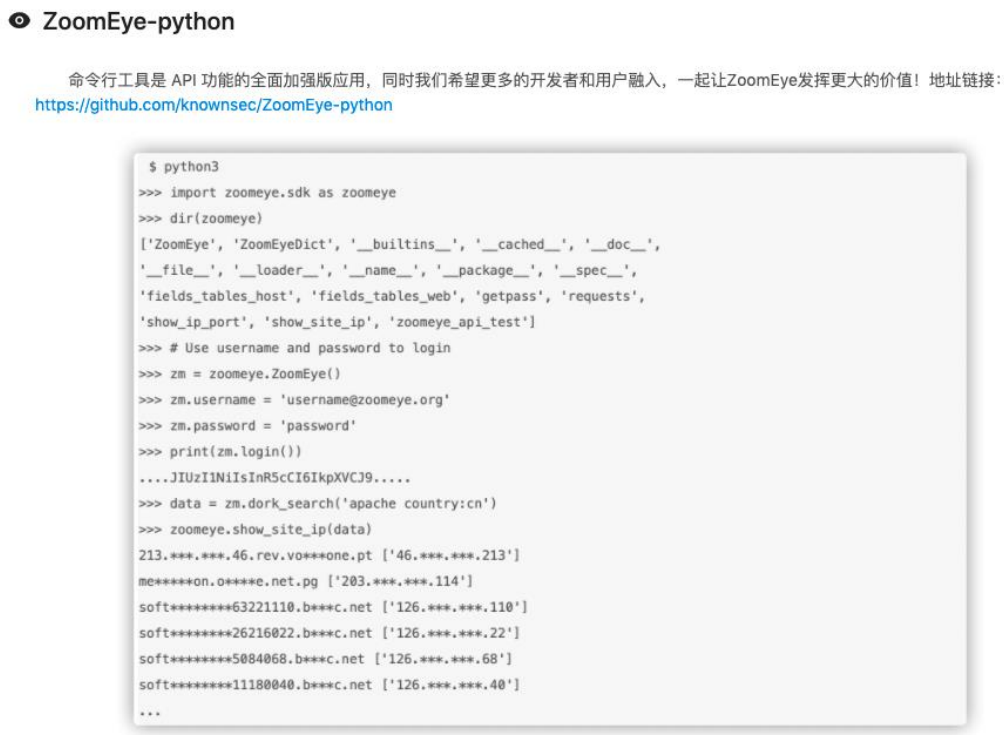
地址：https://www.zoomeye.org/discover

介绍了一些 Zoomeye 的独家特性。

6.1. ZoomEye-python

命令行工具是 API 功能的全面加强版应用。

地址链接：https://github.com/knownsec/ZoomEye-python



6.2. 恶意 ip 标记

ZoomEye 与创宇安全大脑深度合作，将所有主动发起网络攻击的 IP 记录在册，并且标记在 IP 信息中。提醒用户对目标进一步进行甄别，使得 IP 的标记更加具备实用性，避免用户因盲目攻击目标从而给自身带来相关风险。

6.3. 高精地理信息

ZoomEye 支持对 ip 所在地理位置进行解析，地理位置精确到楼宇级别，误差在 50m 以内，让用户从更多维度了解 ip 信息。（仅支持中国大陆地区）

6.4. 行业识别

ZoomEye 拥有强大的线上数据处理能力，可以结合 ip 的多维度数据信息判断出精准的行业信息，深度剖析 ip 数据，赋予数据灵魂，让 ip 信息不再是简单的数字。

6.5. API-KEY

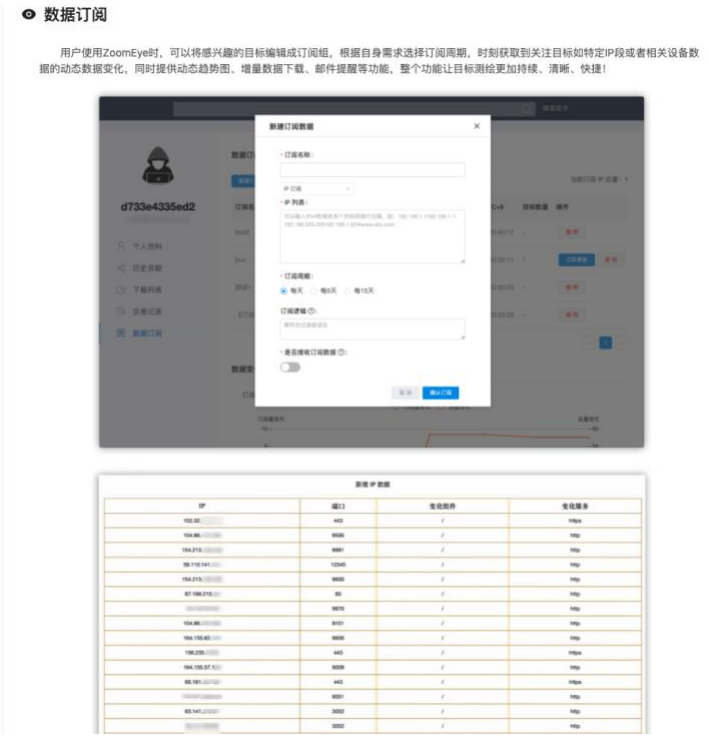
ZoomEye 在 20 年 8 月份取消了 api 接口数据输出限制 ,开放 100%的数据输出。目前不仅支持用户名密码登录调取数据，还支持 API-KEY 的用户登录认证模式，从此不再依赖单一的用户名及密码，让开发者与用户更加安全方便的使用 API 接口。

6.6. 可视化查询

ZoomEye 为初学者以及不熟悉 ZoomEye 搜索语法的用户量身打造了可视化查询功能。可视化查询功能将 ZoomEye 专业的搜索语法变成通俗易懂的或且非，更方便用户使用，让搜索更加简单。

6.7. 数据订阅

用户使用 ZoomEye 时，可以将感兴趣的目标编辑成订阅组，根据自身需求选择订阅周期，时刻获取到关注目标如特定 IP 段或者相关设备数据的动态数据变化，同时提供动态趋势图、增量数据下载、邮件提醒等功能，整个功能让目标测绘更加持续、清晰、快捷！



6.8. 302 跳转

在我们访问某个 IP 或者域名的 HTTP 服务时，经常会遇到跳转到其他页面的情况，转跳后的 banner 数据难以获取。ZoomEye 实现了通过动态解析获取转跳页面的办法，大幅度提升了转跳 banner 的数据获取能力，现在的 ZoomEye 获取跳转后的 banner 信息易如反掌。

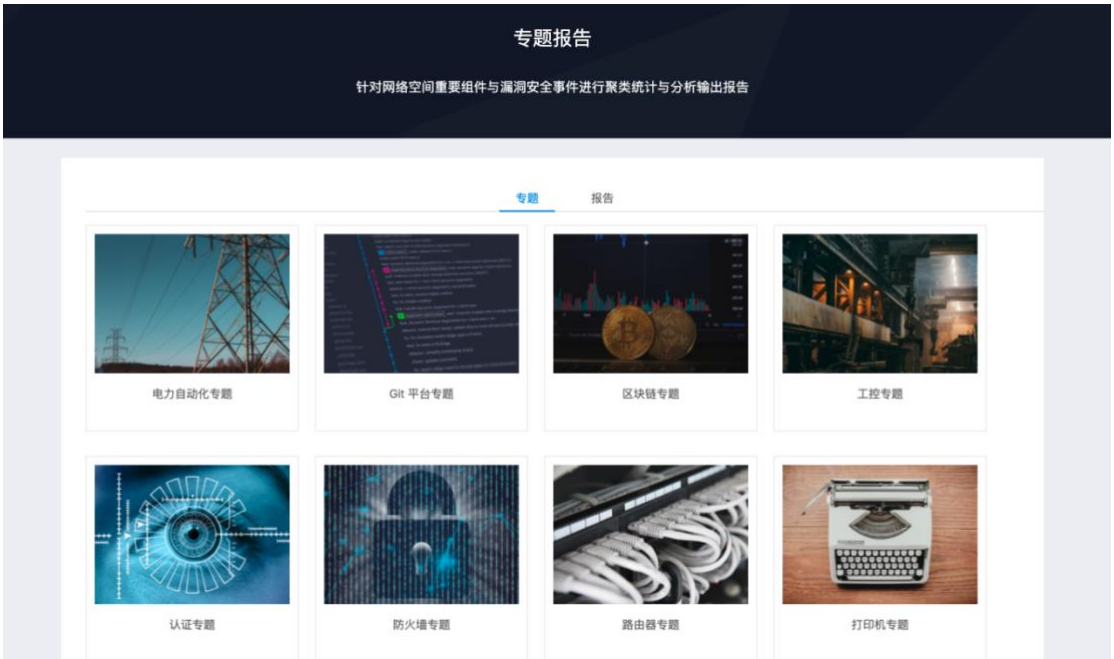
6.9. 历史数据

ZoomEye 作为元老级别的网络搜索引擎系统。累积了从 2008 年至今近 13 年的海量网络空间资产数据 ,并且对于搜索到的网络资产数据会一直保留并展示。

7. 专题

地址：https://www.zoomeye.org/topics。

针对网络空间重要组件与漏洞安全事件进行聚类统计与分析输出报告。



HP

描述：惠普打印机作为惠普公司下设三大业务集团之一。旗下产品包括包括碳粉打印机、墨水打印机、连供打印机、大型打印机、数字印刷机、3D打印机等等。其特有的HP Smart应用可以帮助用户设置、扫描、打印、共享和管理HP打印机。

筛选器条件：app:"HP Officejet Pro 8600 printer smbd"
app:"HP OFFICEJET PRO 8610 E-ALL-IN-ONE httpd"

说明：包含Officejet Pro系列激光打印机、Photosmart系列、Laserjet系列、Officejet系列、Color LaserJet系列、Designjet系列以及适合家用的Deskjet系列无线打印一体机等等。

Samsung

描述：Samsung是韩国最大的跨国企业集团，旗下的打印机产品一直致力于发现并满足用户的各种办公需求，主要包括黑白激光打印机、黑白多功能一体机和彩色激光打印机、彩色多功能一体机等等。

筛选器条件：app:"Samsung SL-J1760FW printer httpd"
app:"Samsung ML-2251N printer http config"

说明：包含Samsung CLX系列彩色激光打印机、Samsung ML系列黑白激光打印机等众多型号，具有机器稳定、打印速度快、效果好等特点。

FUJI-Xerox

描述：富士施乐公司是全球最大数字与信息技术产品生产商，且是复印技术的发明公司，具有悠久的历史。在复印机市场尤其是彩色机器市场占有率极高，其彩色技术方面属于全球领袖地位。

筛选器条件：app:"FUJI XEROX DocuPrint 2100 printer httpd"
app:"Xerox Phaser 3500"

说明：包含Xerox Phaser系列、XEROX DocuPrint系列、Fuji Xerox ApeosPort-V系列等多种型号打印机。较适用于中小型办公环境，具有高效的生产力和强大的稳定性。

Sharp

描述：夏普公司以复印功能为基础，聚集打印、扫描、传真等功能，利用数码园里。采用激光打印进行文件的输出，包括黑白超高速机、黑白高速机、黑白中高速机、黑白中低速机、黑白复印机以及多功能一体机等多类型机器。

筛选器条件：app:"Sharp MX-2700N printer"
app:"Sharp AR-M550N printer http config"

说明：包含Sharp AR、Sharp MX等系列。夏普复印机与模拟复印机的区别主要是在光学扫描与静电潜像方式上，其它地方可能有少许变化。

Kyocera

描述：京瓷办公信息系统株式会社是由京瓷株式会社出资的企业，拥有复印机和打印机两个领域资产的企业，主要从事黑白、彩色网络复合机、打印机、软件解决方案的开发、制造和销售,是一家办公文档解决方案公司。

筛选器条件：app:"Kyocera FS-3900DN printer http config"
app:"Kyocera 4050 printer http config"

说明：包含Kyocera FS系列打印机、Kyocera TASKalfa系列多功能数码复合机、Kyocera KM系列打印机、Kyocera Ecosys系列激光打印机、Kyocera MFP系列等等。

Citizen

描述：西铁城成立于1930年，旗下有四大产品线：手表、机床、设备及零部件和电子产品。

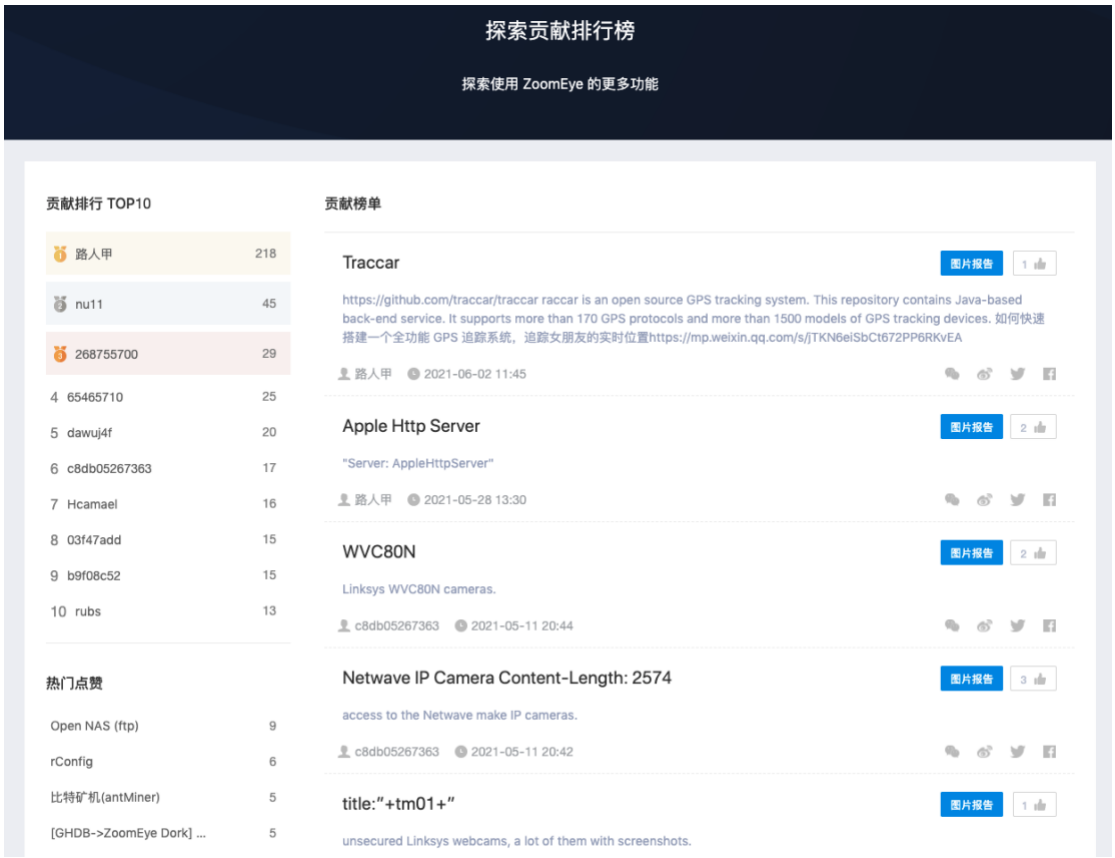
筛选器条件：app:"Citizen CLP-521 or Kyocera Mita KM-1530 printer http config"

说明：包含Citizen CLP-521条码打印机等型号，具有高性能、稳定可靠，经济实用的特点。

8. 贡献

地址：https://www.zoomeye.org/share。

Zoomeye 提供了贡献功能，用户可以向 Zoomeye 贡献独特的搜索语法：



9. 搜索指南

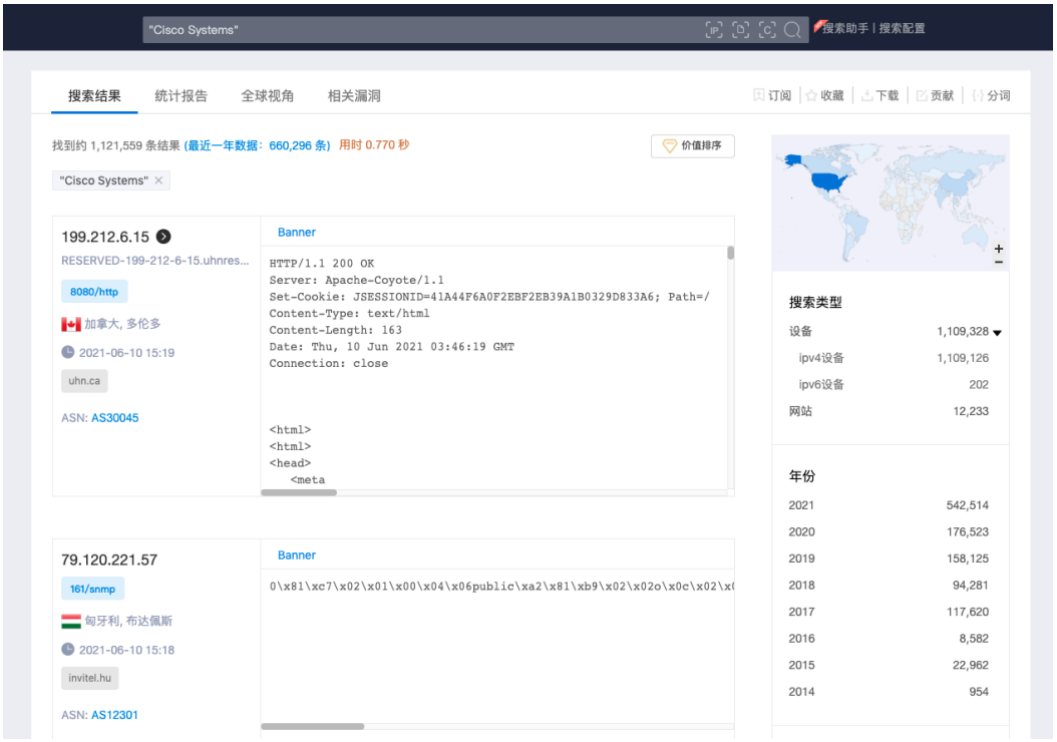
9.1. 搜索范围

搜索范围覆盖设备(IPv4、IPv6)及网站(域名)，可以提交 URL 参数 t 进行指定类型 t=v4 为 IPv4，t=v6 为 IPv6，t=web 为域名（或可通过搜索结果侧栏点击对应搜索内容）。

9.2. 字符串搜索

搜索字符串不区分大小写，直接输入搜索字符串会认定为“全局”进行匹配搜索关键词，会从 http 等协议内容(包括 http 头、html 内容等)、ssl 证书、组件名等进行匹配搜索。

搜索字符串请使用引号（如"Cisco Systems"或'Cisco Systems'），如不然空格会认定为逻辑 or 运算符，如果搜索字符串里存在引号可以使用 \ 进行转义 比如: "a\"b",如果搜索字符串里存在括号可以使用 \ 进行转义 比如: portinfo\(\)。



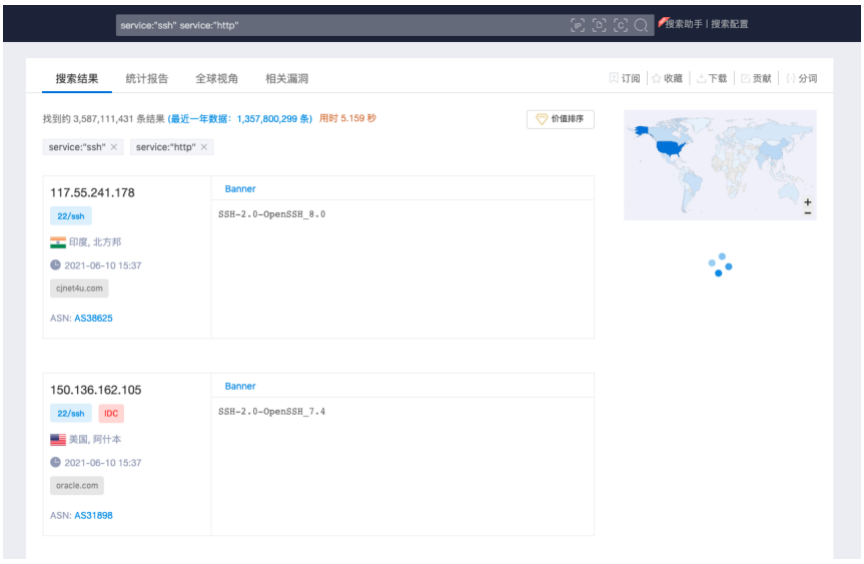
9.3. 逻辑运算

9.3.1. 空格

在搜索框中输入“空格”则表示“或”的运算逻辑。

示例：搜索 ssh 或 http 协议的数据。

service:"ssh" service:"http"。

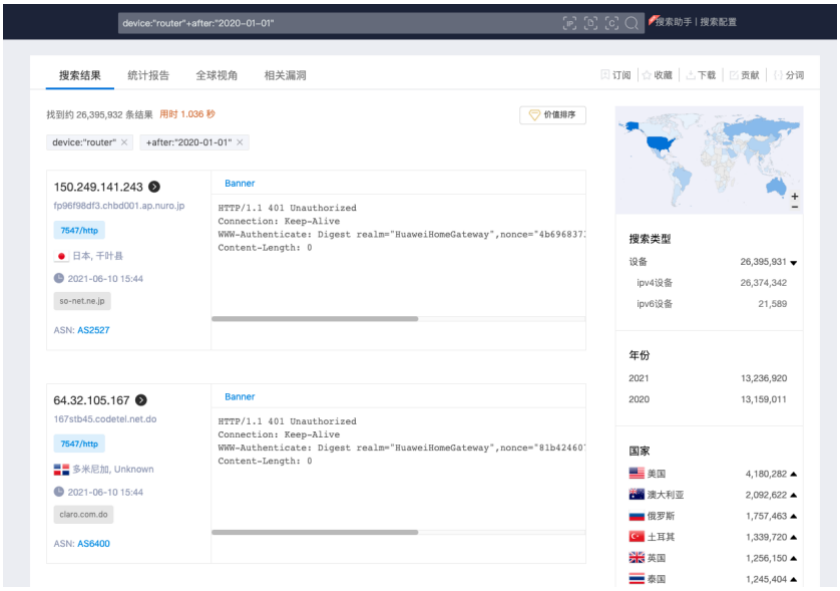


9.3.2. +

在搜索框中输入“+”则表示“且”的运算逻辑。

示例：搜索 2020-01-01 后路由器的数据。

device:"router"+after:"2020-01-01"。

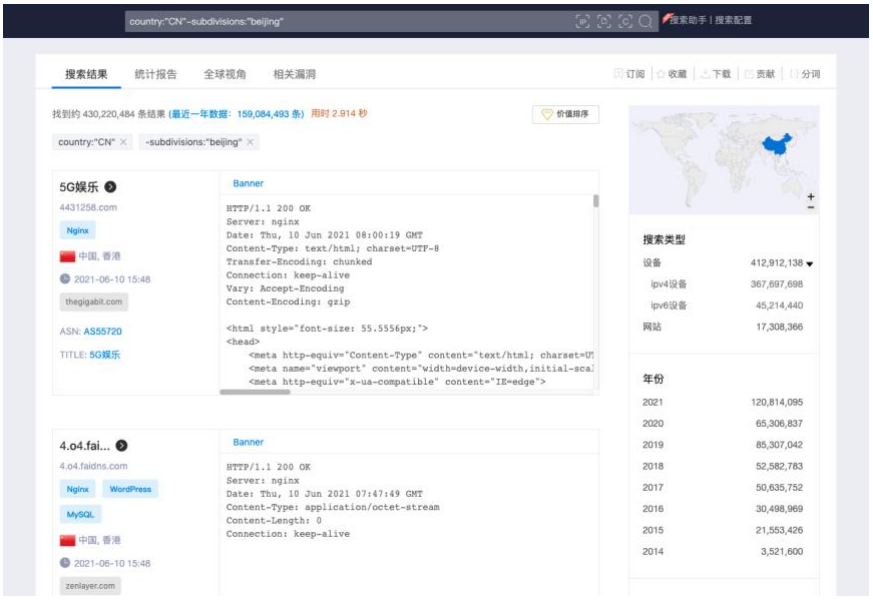


9.3.3. -

在搜索框中输入“-”则表示“非”的运算逻辑。

示例：搜索中国地区内除北京的数据。

country:"CN"-subdivisions:"beijing"。

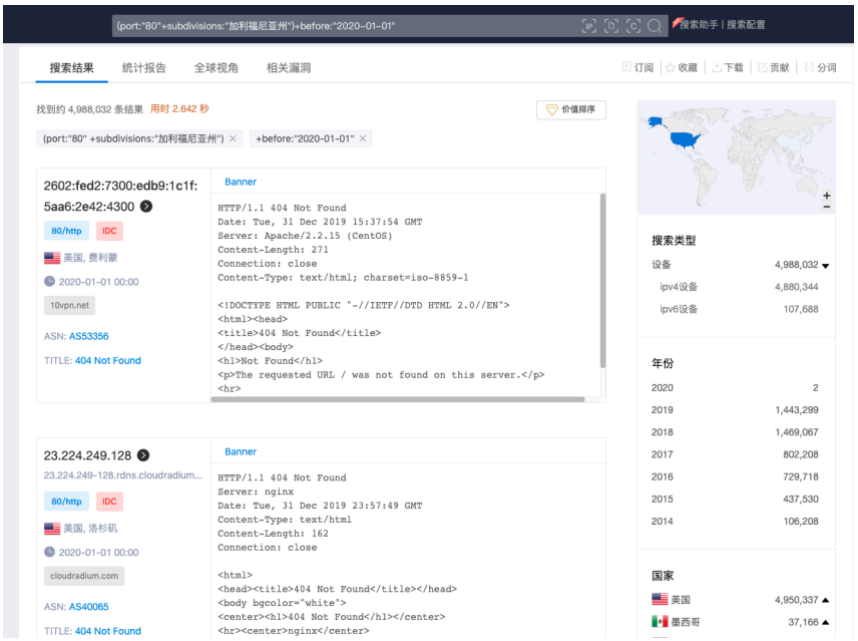


9.3.4. ()

在搜索框中输入“()”则表示“优先处理”的运算逻辑。

示例：搜索 2020-01-01 前在加利福尼亚州开放的 80 端口数据。

(port:"80"+subdivisions:"加利福尼亚州")+before:"2020-01-01"。



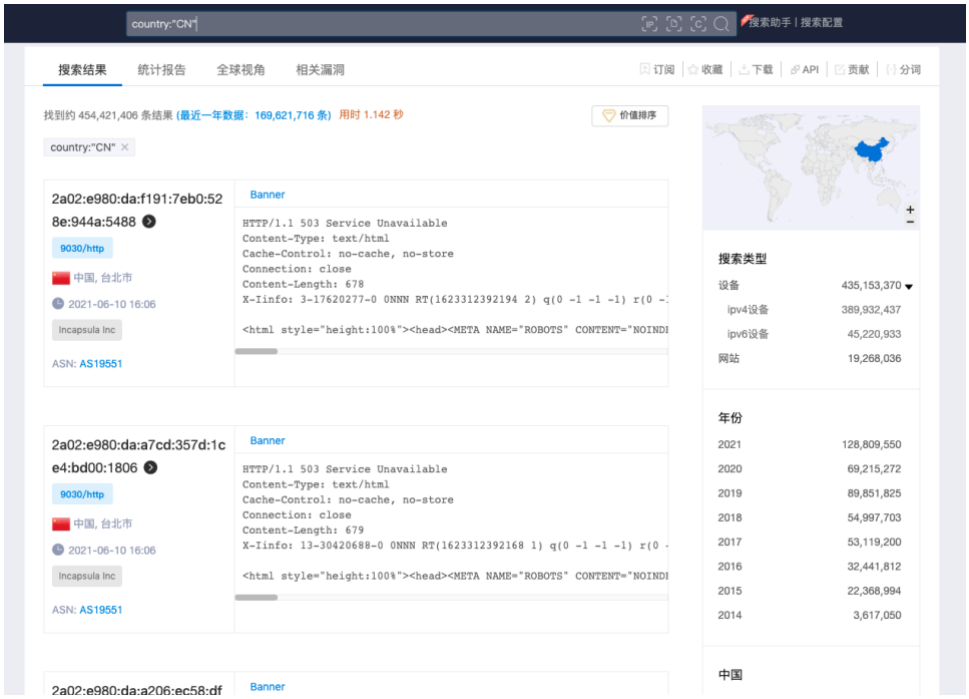
9.3.5. 简易化查询逻辑

9.4. 地理位置

注意：中国地区资产只对中国 IP 及手机号码认证用户开放。

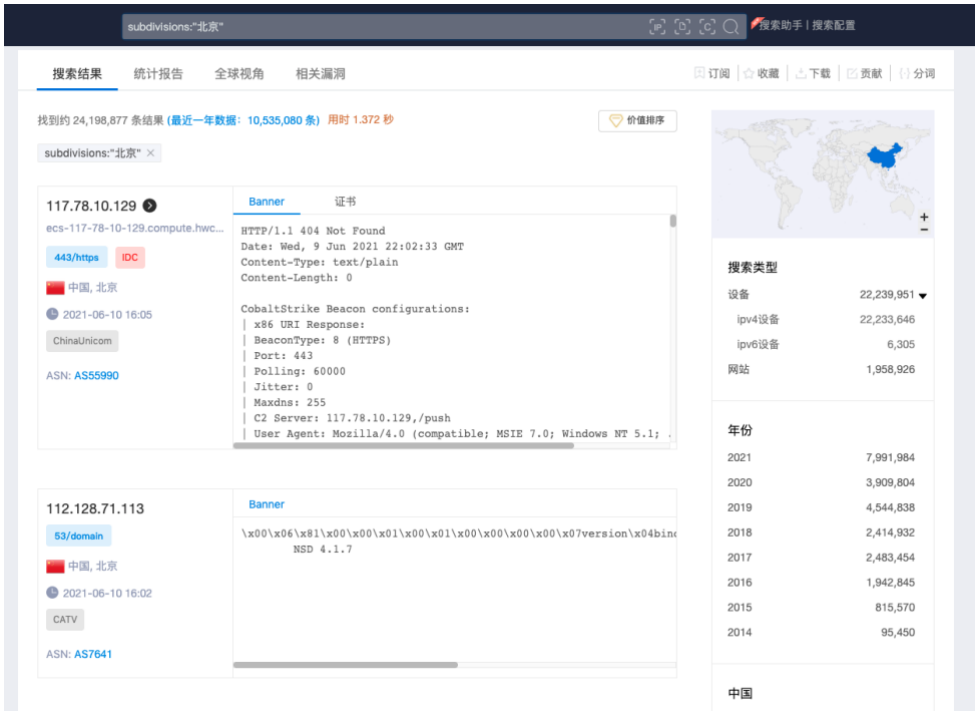
9.4.1. 搜索国家地区资产

可以使用国家缩写 country:"CN"，也可以使用中/英文全称如 country:"中国" country:"china"。



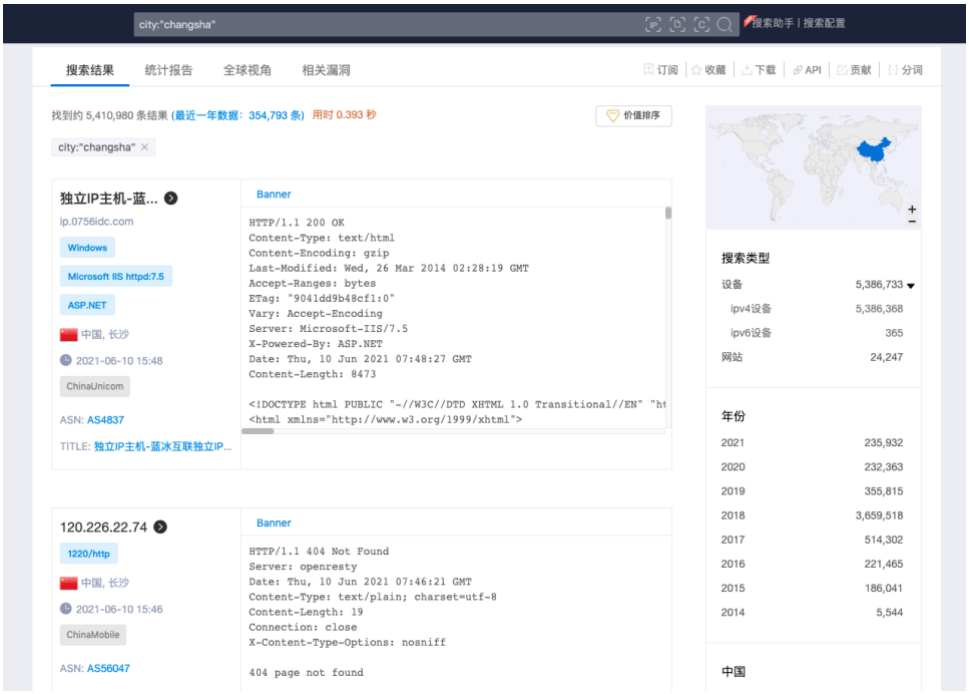
9.4.2. 搜索相关指定行政区的资产

中国省会支持中文及英文描述搜索如 subdivisions:"北京" subdivisions:"beijing"。



9.4.3. 搜索相关城市资产

中国城市支持中文及英文描述搜索如 city:"changsha" city:"长沙"。

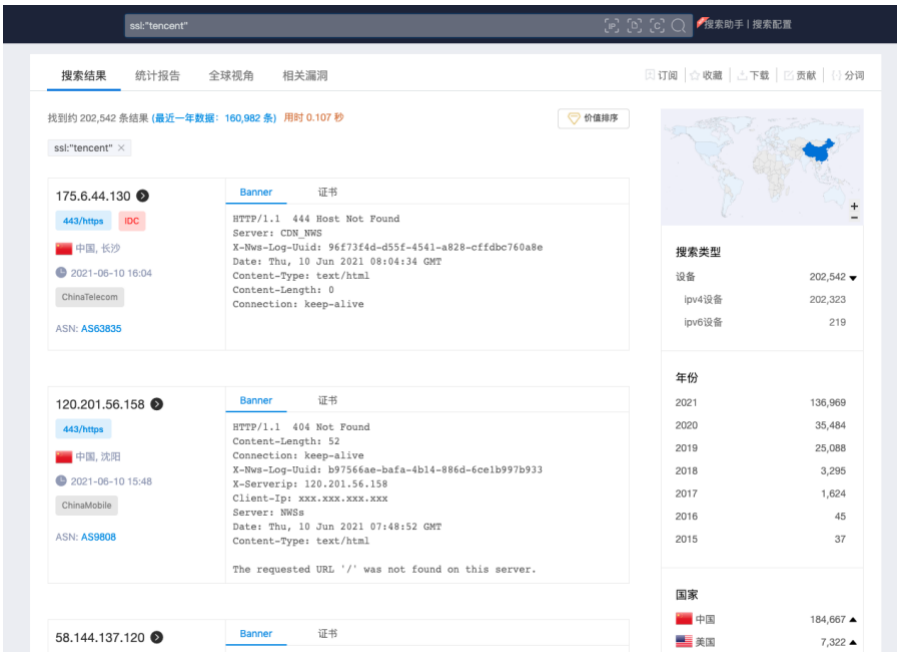


9.5. 证书搜索

常常用来提过产品名及公司名搜索对应目标。

示例：搜索 ssl 证书存在"tencent"字符串的资产。

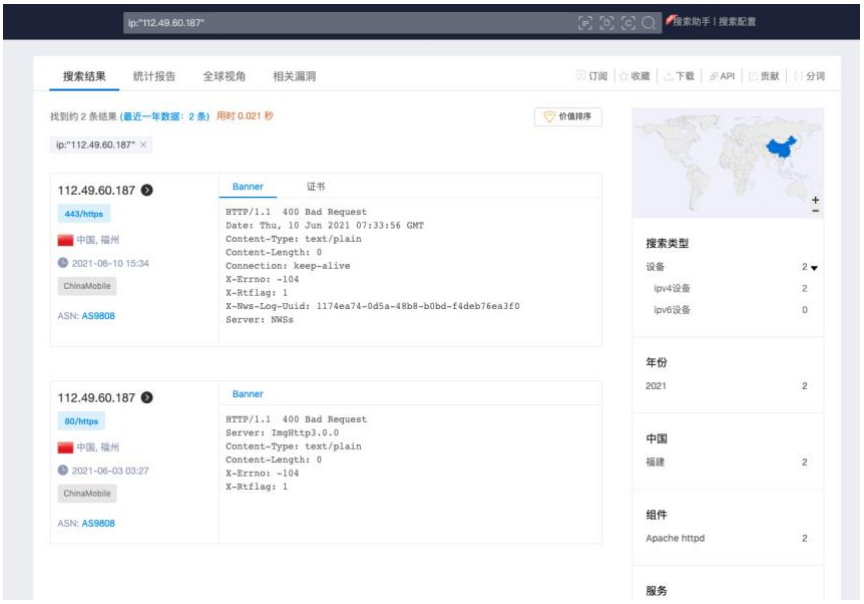
ssl:"tencent"。



9.6. IP 及域名信息相关搜索

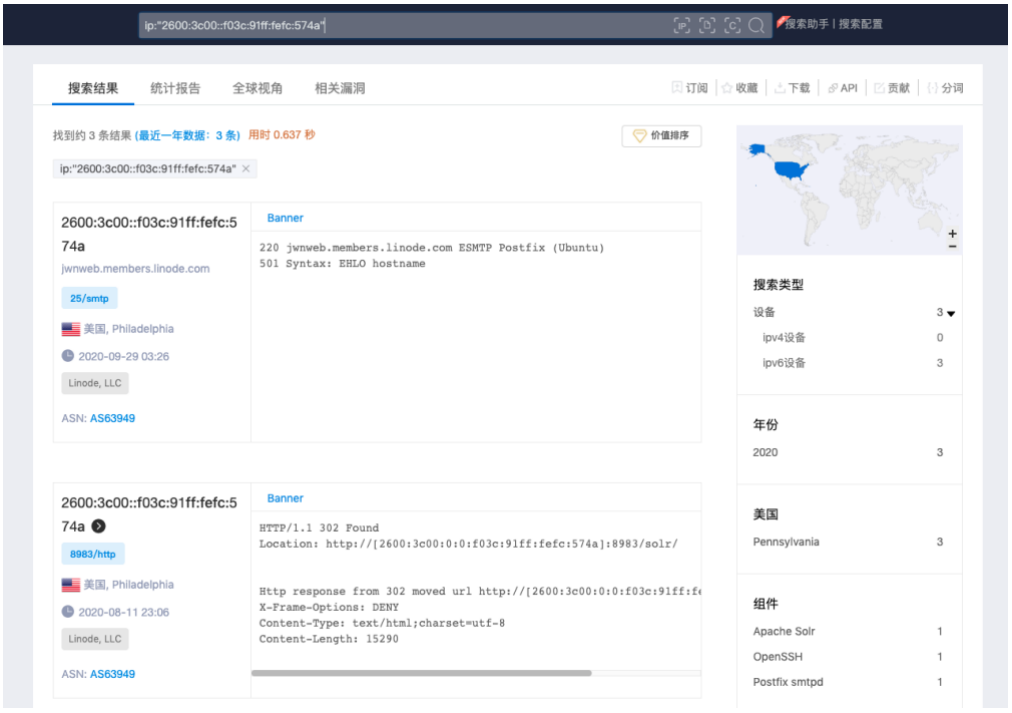
9.6.1. 搜索指定 IPv4 地址相关资产

ip:"112.49.60.187"。



9.6.2. 搜索指定 IPv6 地址相关资产

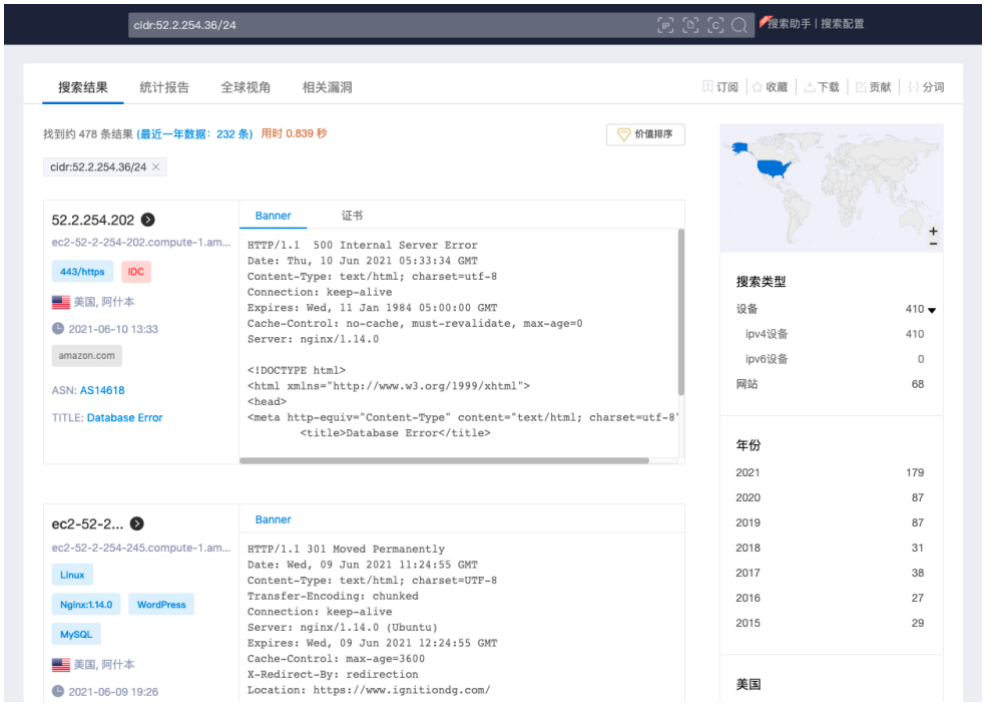
ip:"2600:3c00::f03c:91ff:fefc:574a"。



9.6.3. 搜索 IP 的 C 段资产

cidr:52.2.254.36/24。

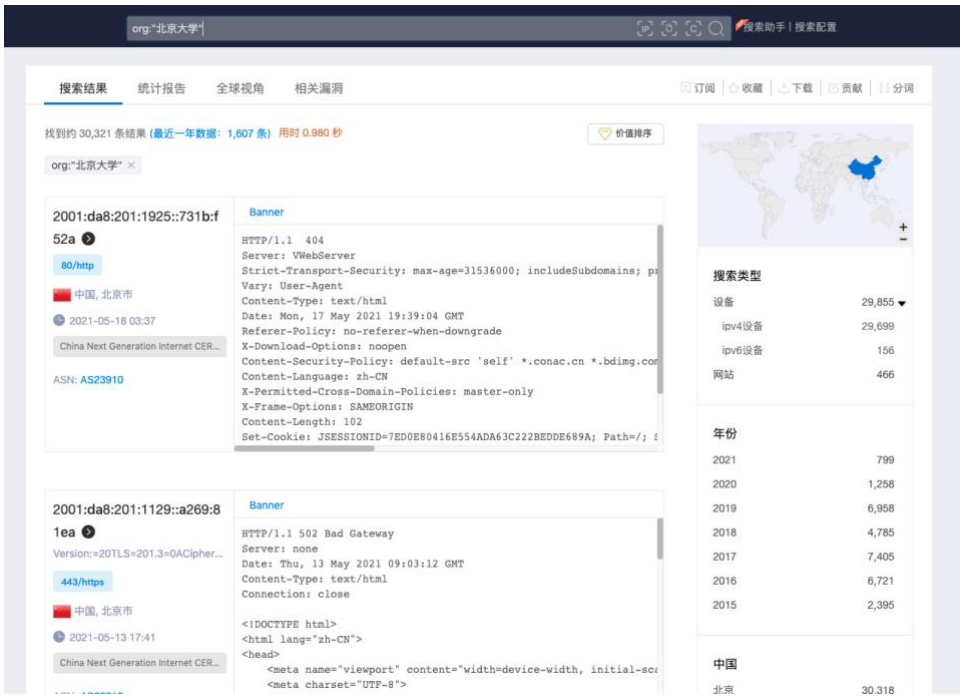
同理，cidr:52.2.254.36/16 为 IP 的 B 段资产， cidr:52.2.254.36/8 为 IP 的 A 段资产。



9.6.4. 搜索相关组织(Organization)的资产

常常用来定位大学、结构、大型互联网公司对应 IP 资产。

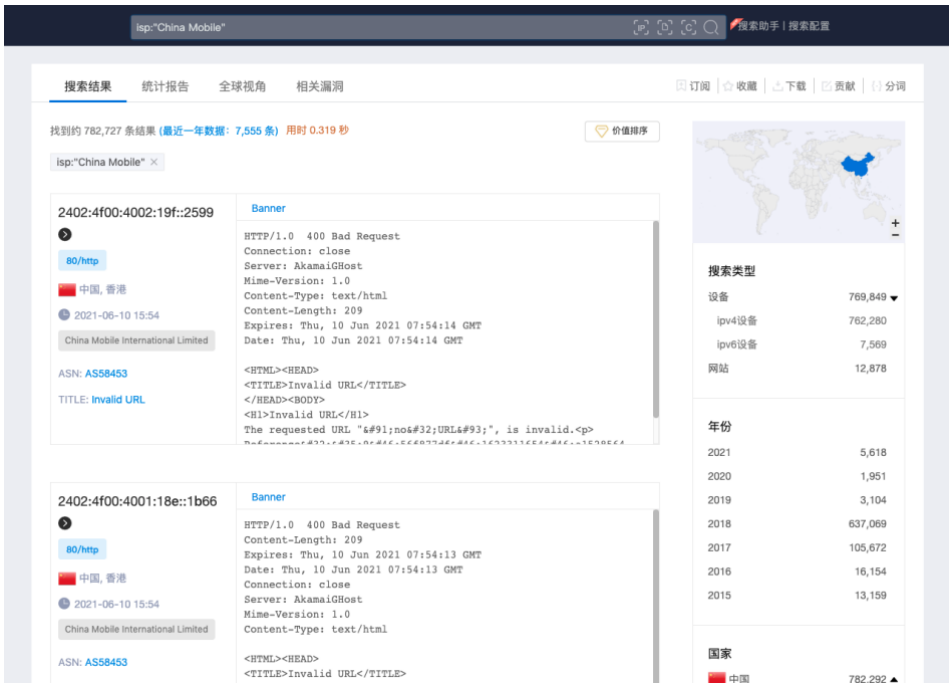
org:"北京大学" 或者 organization:"北京大学"。



9.6.5. 搜索相关网络服务提供商的资产

可结合 org 数据相互补充。

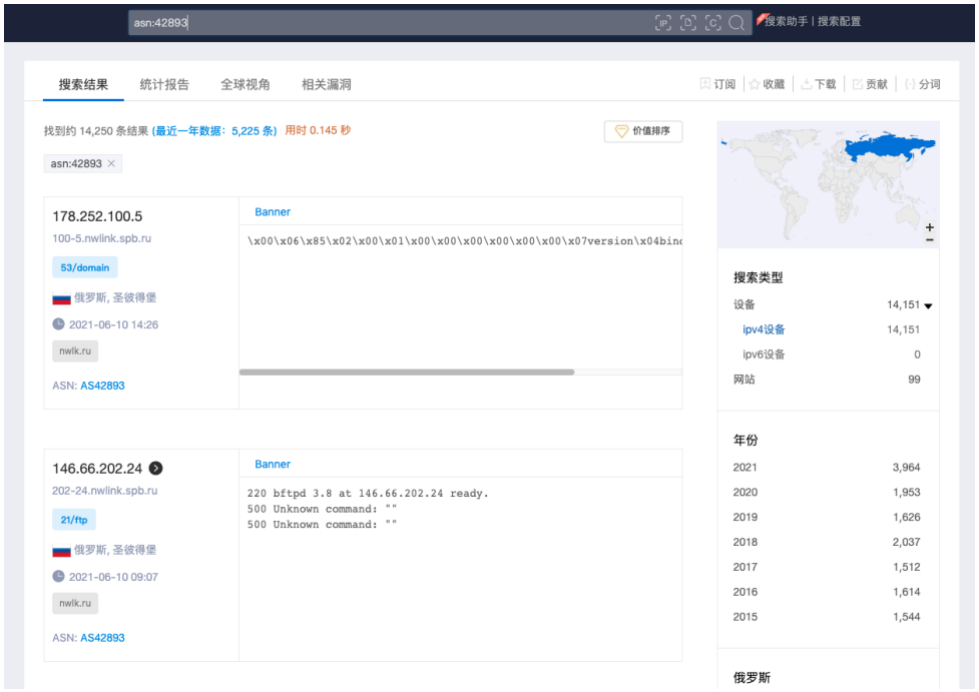
isp:"China Mobile"。



9.6.6. 搜索 ASN

搜索对应 ASN（Autonomous system number）自治系统编号相关 IP 资产。

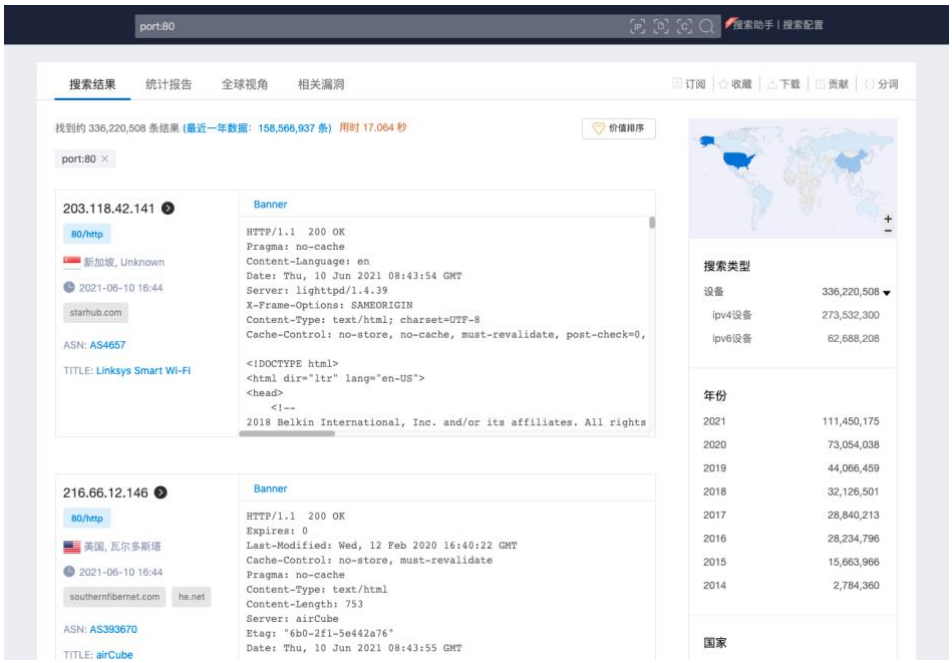
asn:42893。



9.6.7. 搜索相关端口资产

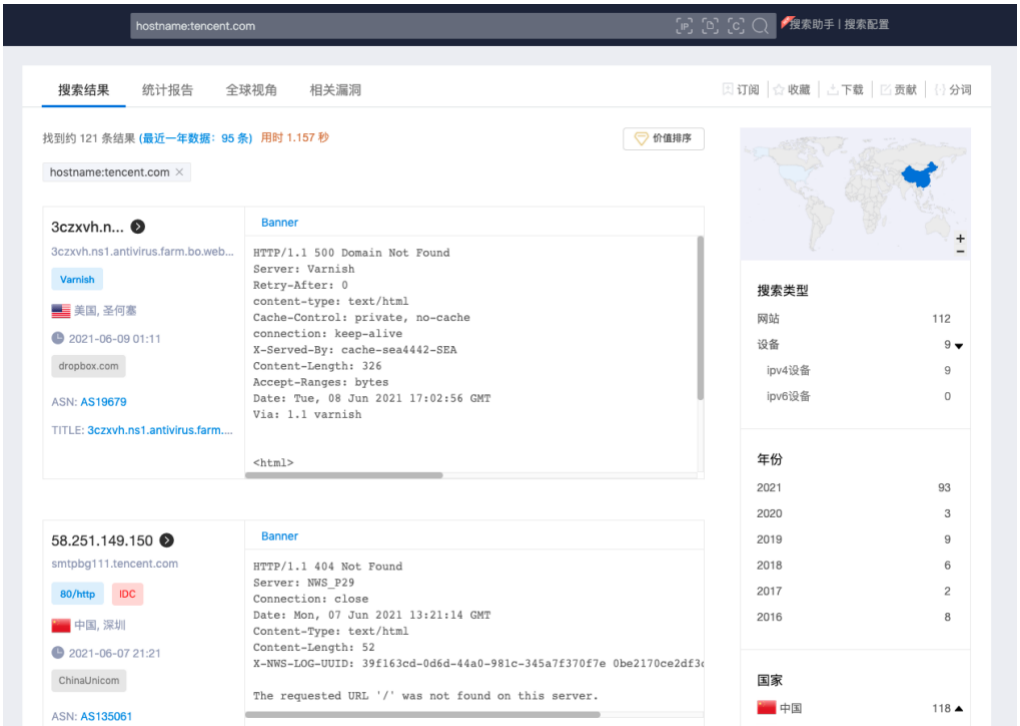
目前不支持同时开放多端口目标搜索。

port:80。



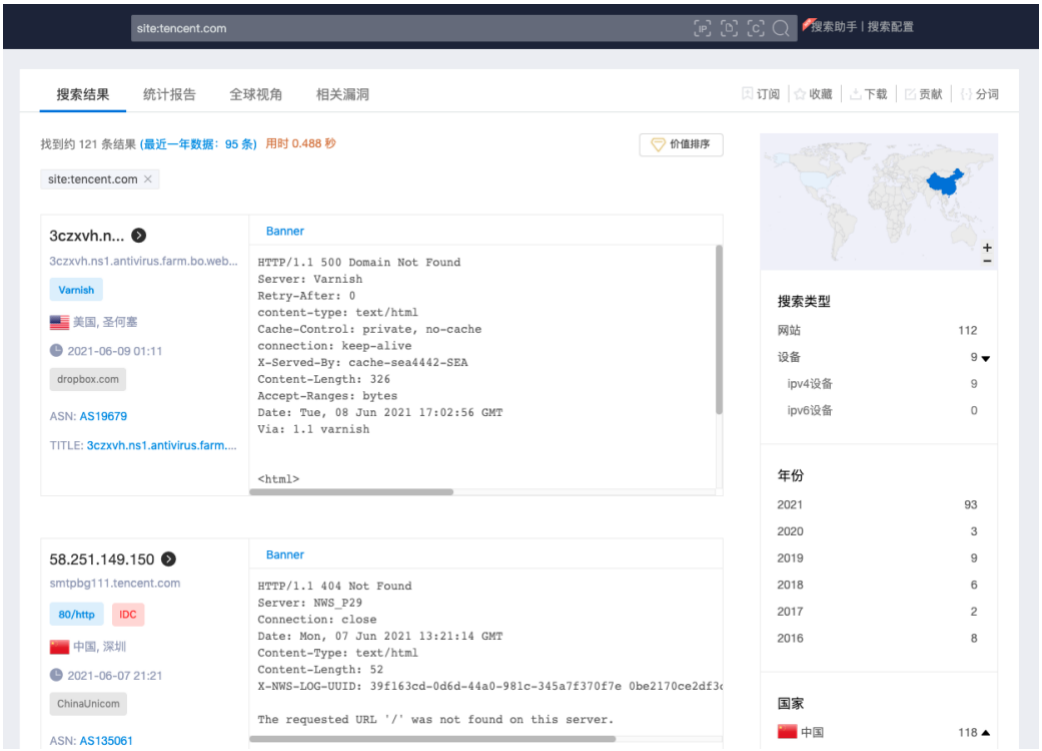
9.6.8. 搜索相关 IP"主机名"的资产

hostname:tencent.com。



9.6.9. 搜索域名相关的资产

site:tencent.com。

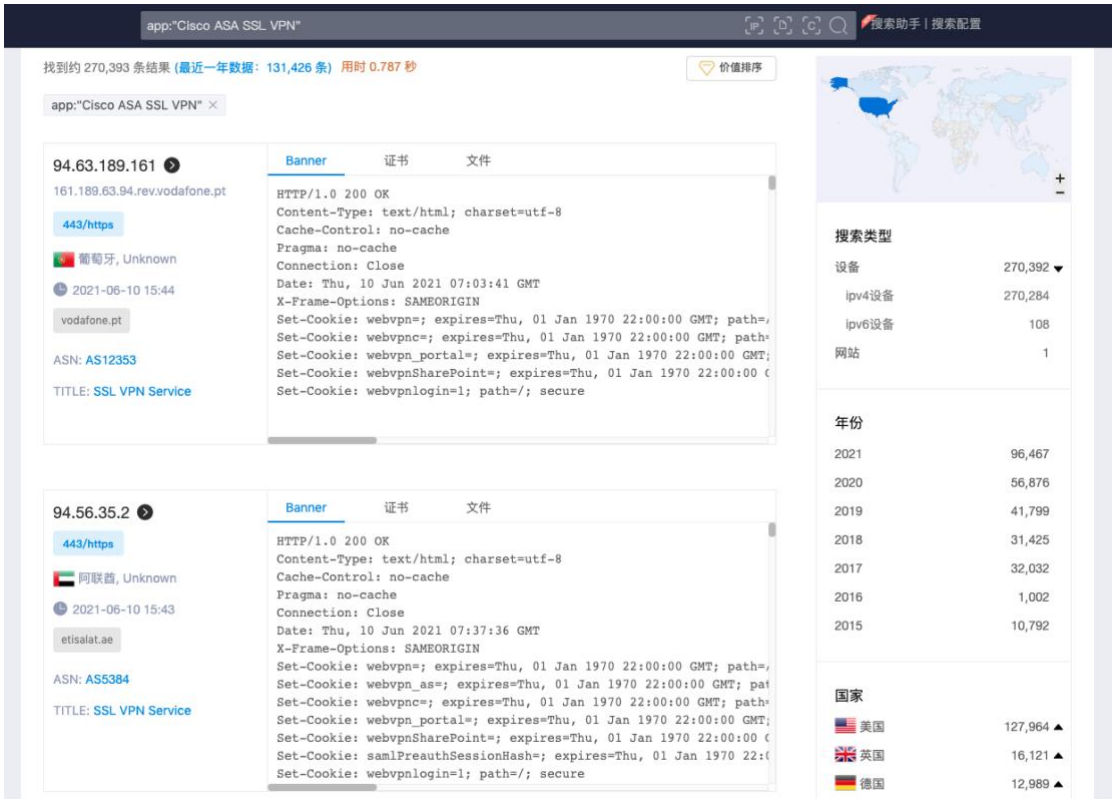


9.7. 指纹相关搜索

9.7.1. app

搜索思科 ASA-SSL-VPN 的设备。

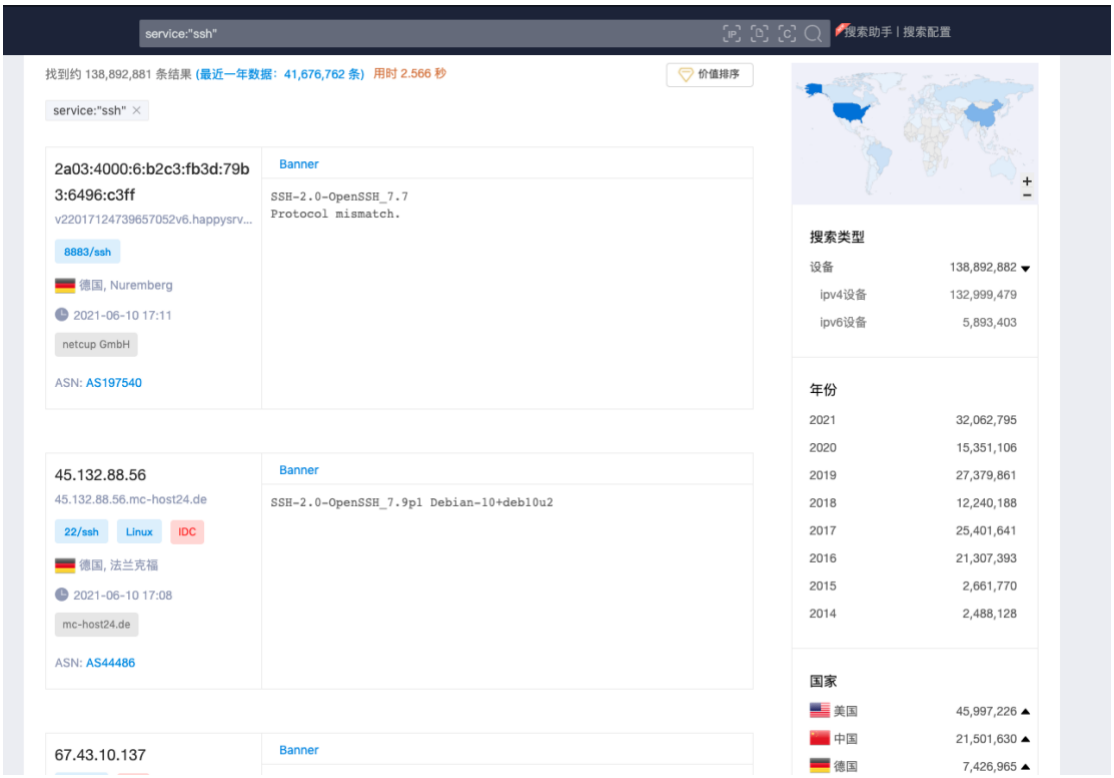
app:"Cisco ASA SSL VPN"。



9.7.2. service

搜索对应服务协议的资产，常见服务协议包括：http、ftp、ssh、telnet 等等(其他服务可参考搜索结果域名侧栏聚合展示）

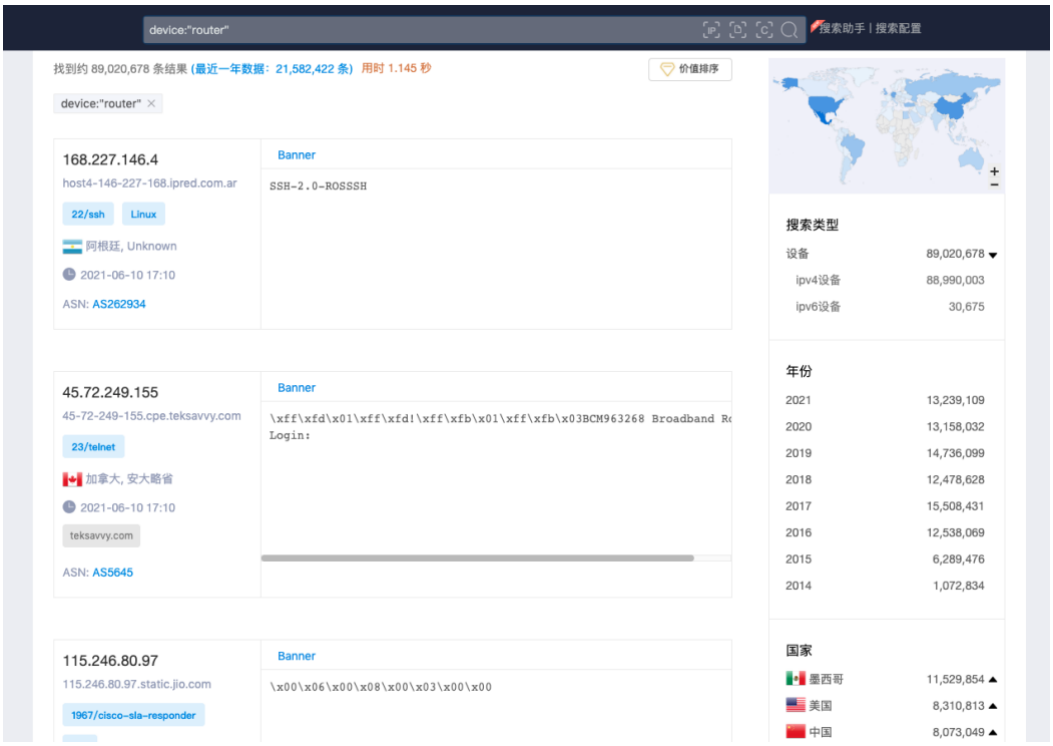
service:"ssh"



9.7.3. device

搜索路由器相关的设备类型 ,常见类型包括 router(路由器)、switch(交换机)、storage-misc(存储设备)等等(其他类型可参考搜索结果域名侧栏聚合展示)。

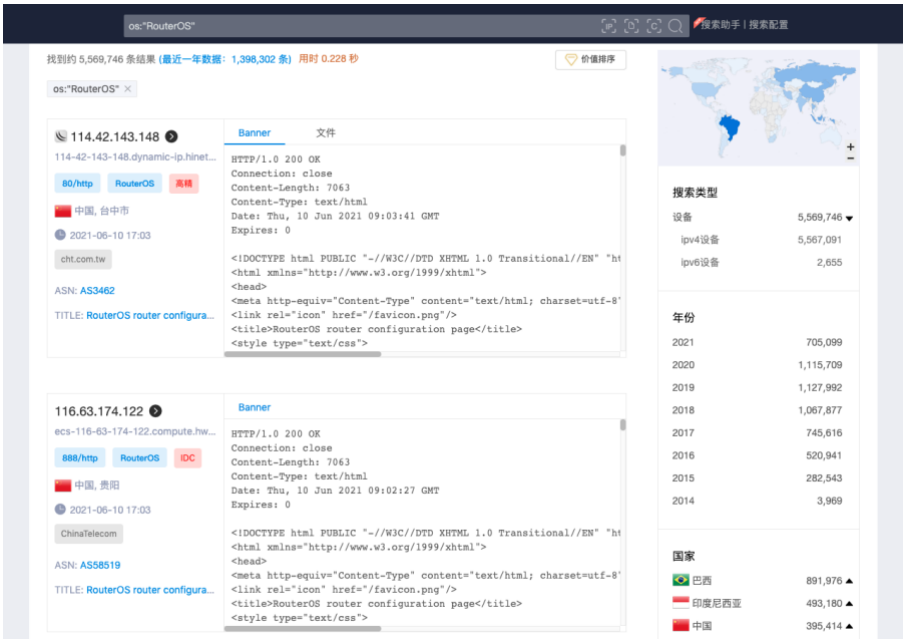
device:"router"。



9.7.4. os

搜索相关操作系统，常见系统包括 Linux、Windows、RouterOS、IOS、JUNOS 等等(其他系统可参考搜索结果域名侧栏聚合展示)。

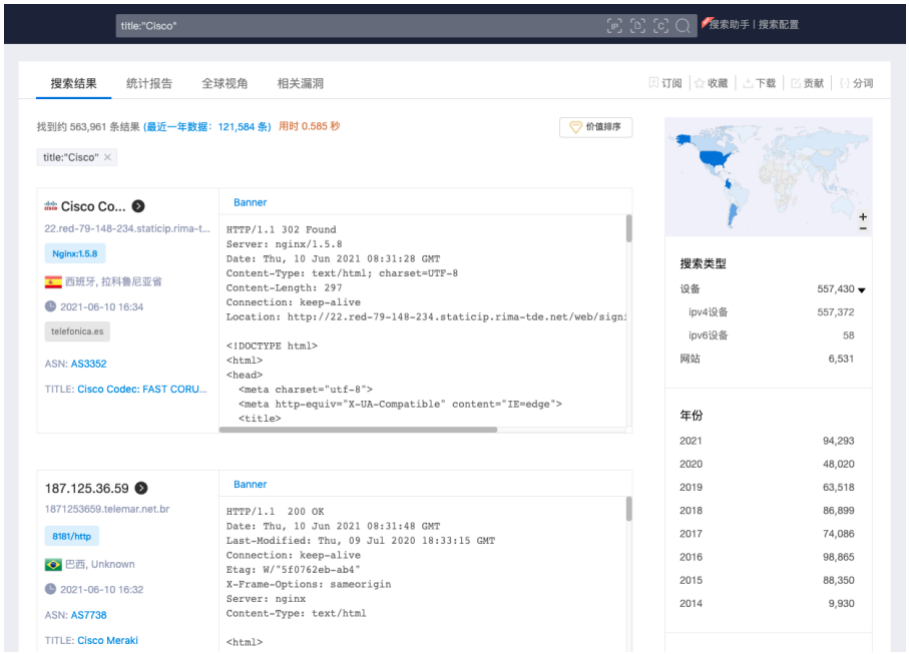
os:"RouterOS"。



9.7.5. title

搜索 html 内容里标题中存在"Cisco"的数据。

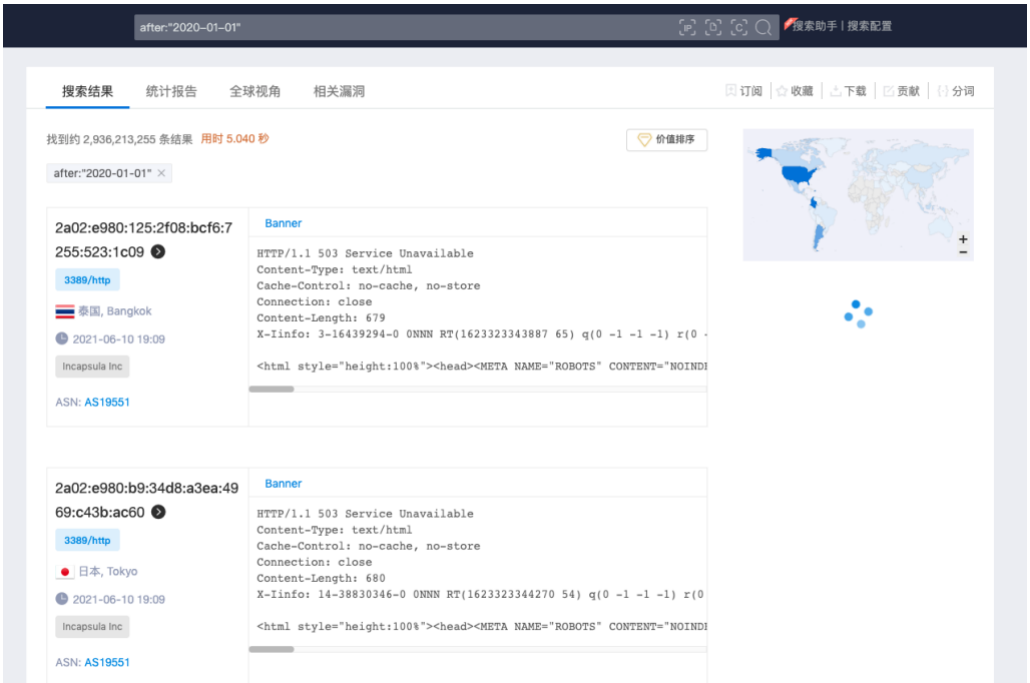
title:"Cisco"。



9.8. 时间节点区间搜索

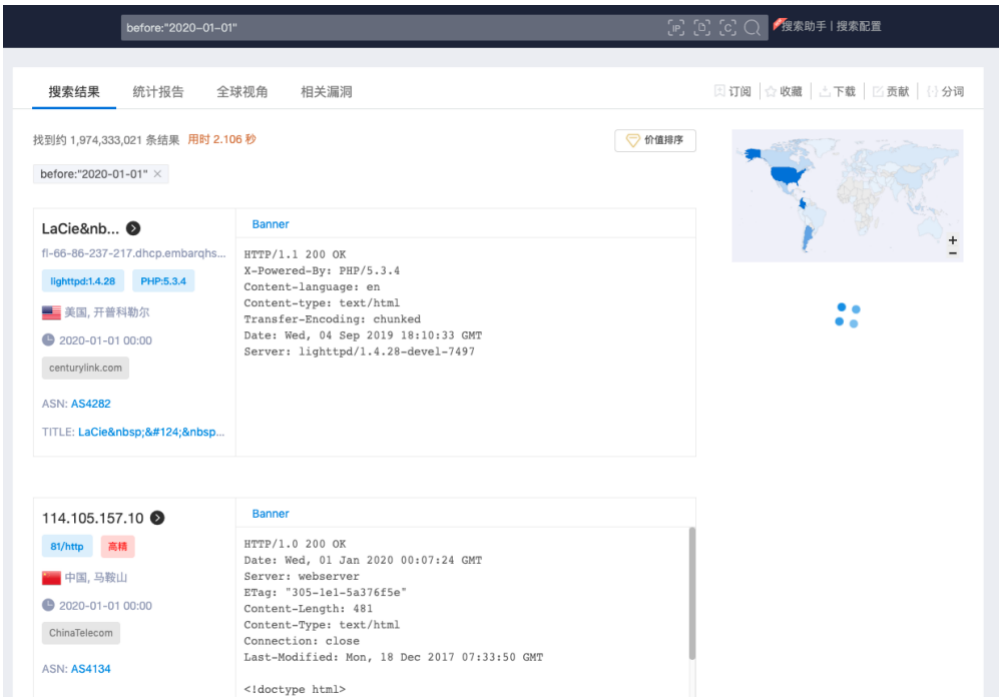
搜索更新时间为"2020-01-01"以后的资产。

after:"2020-01-01"。



搜索更新时间在"2020-01-01"以前的资产。

before:"2020-01-01"。



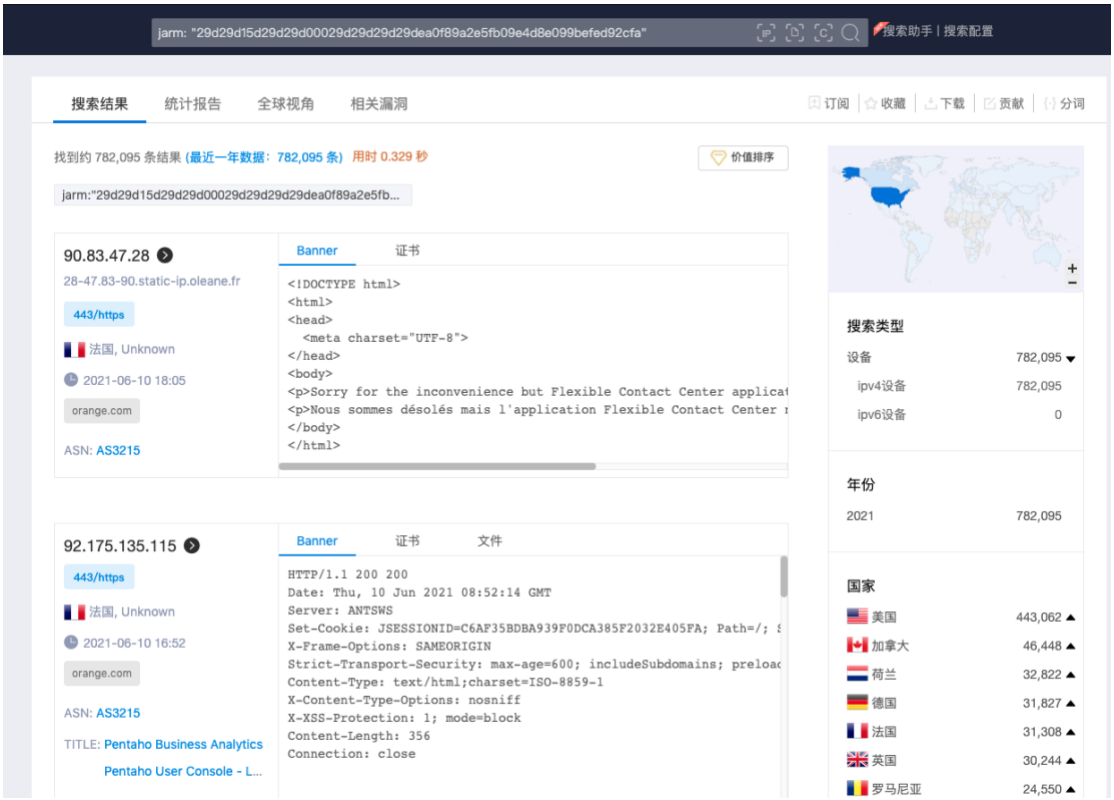
after 与 before 常常配合使用。

9.9. Jarm

Jarm 是一个活动的传输层安全性（TLS）服务器指纹识别工具，详情参考：https://github.com/salesforce/jarm

搜索相关 jarm 内容的资产

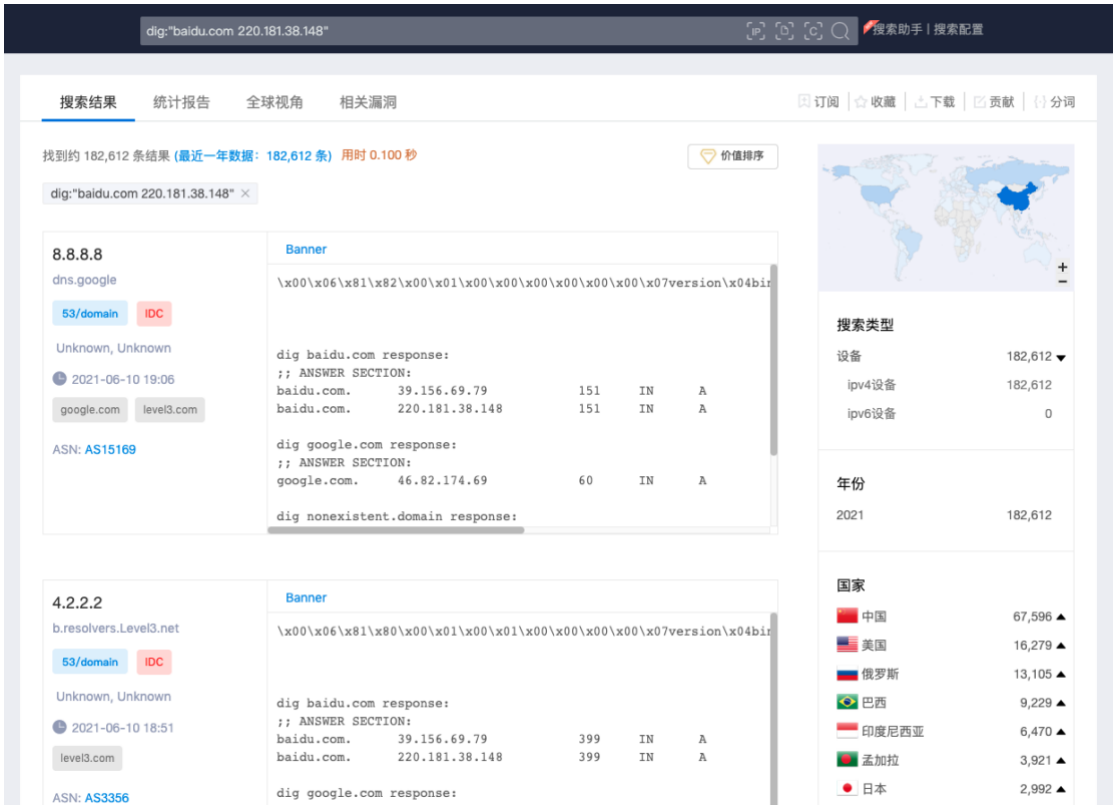
jarm:"29d29d15d29d29d00029d29d29d29dea0f89a2e5fb09e4d8e099befed92cfa"


jarm: "29d29d15d29d29d00029d29d29d29dea0f89a2e5fb09e4d8e099befed92cfa"
搜索助手 | 搜索配置
搜索结果
统计报告
全球视角
相关漏洞
订阅
收藏
下载
贡献
分词
找到约 782,095 条结果 (最近一年数据：782,095 条) 用时 0.329 秒
价值排序
jarm:"29d29d15d29d29d00029d29d29d29dea0f89a2e5fb...
90.83.47.28
28-47.83-90.static-ip.oleane.fr
443/https
法国, Unknown
2021-06-10 18:05
orange.com
ASN: AS3215
Banner
证书
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
</head>
<body>
<p>Sorry for the inconvenience but Flexible Contact Center applicat
<p>Nous sommes désolés mais l'application Flexible Contact Center
</body>
</html>
92.175.135.115
443/https
法国, Unknown
2021-06-10 16:52
orange.com
ASN: AS3215
TITLE: Pentaho Business Analytics
Pentaho User Console - L...
Banner
证书
文件
HTTP/1.1 200 200
Date: Thu, 10 Jun 2021 08:52:14 GMT
Server: ANTSWS
Set-Cookie: JSESSIONID=C6AF35BDBA939F0DCA385F2032E405FA; Path=/;
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=600; includeSubdomains; preload
Content-Type: text/html;charset=ISO-8859-1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 356
Connection: close
搜索类型
设备 782,095
ipv4设备 782,095
ipv6设备 0
年份
2021 782,095
国家
美国 443,062
加拿大 46,448
荷兰 32,822
德国 31,827
法国 31,308
英国 30,244
罗马尼亚 24,550

9.10. Dig

搜索相关 dig 内容的资产

dig:"baidu.com 220.181.38.148"

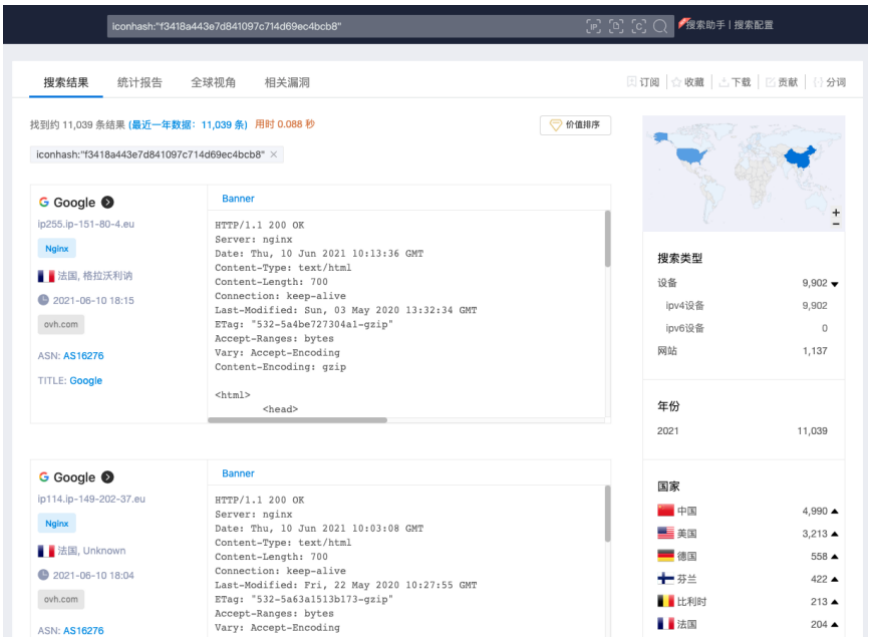


9.11. Iconhash

通过 md5 方式对目标数据进行解析，根据图标搜索相关内容的资产。

搜索包含“google”图标的相关资产

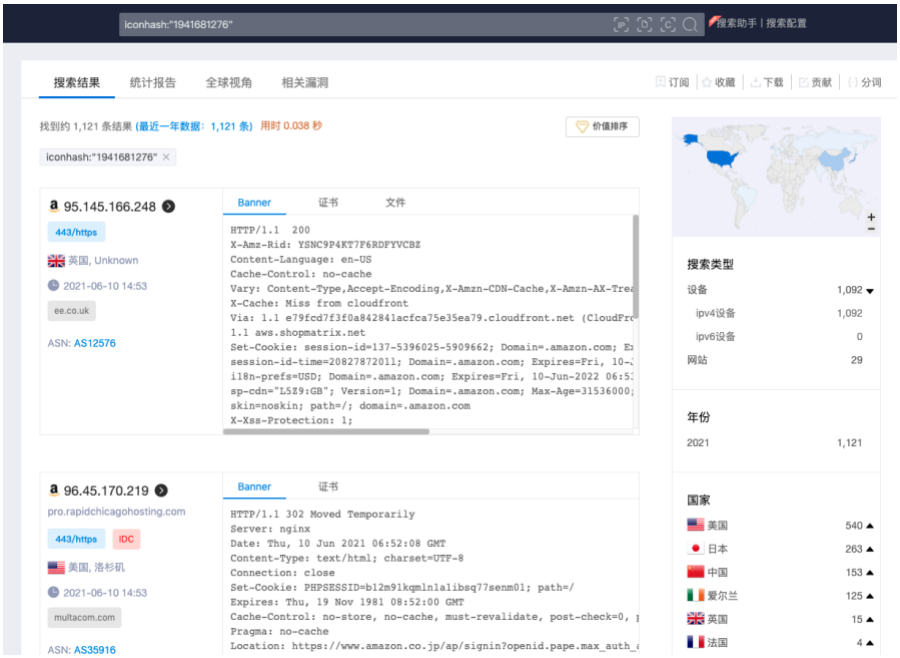
iconhash:"f3418a443e7d841097c714d69ec4bcb8"



通过 mmh3 方式对目标数据进行解析，根据图标搜索相关内容的资产。

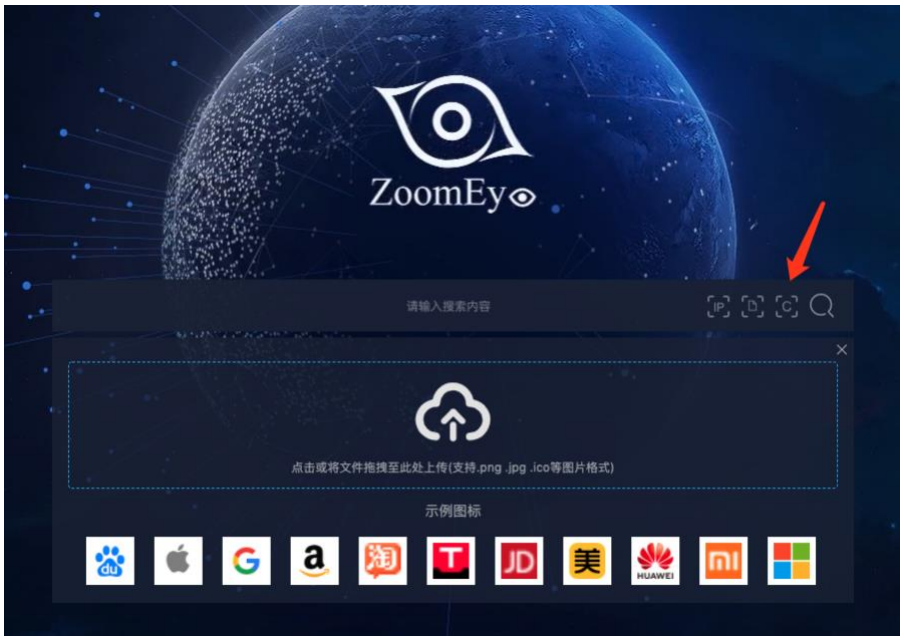
搜索包含“amazon”图标的相关资产

iconhash:"1941681276"



9.11.1. 图标搜索

如果觉得计算图标hash比较困难的话，可以直接使用首页的图片搜索功能。

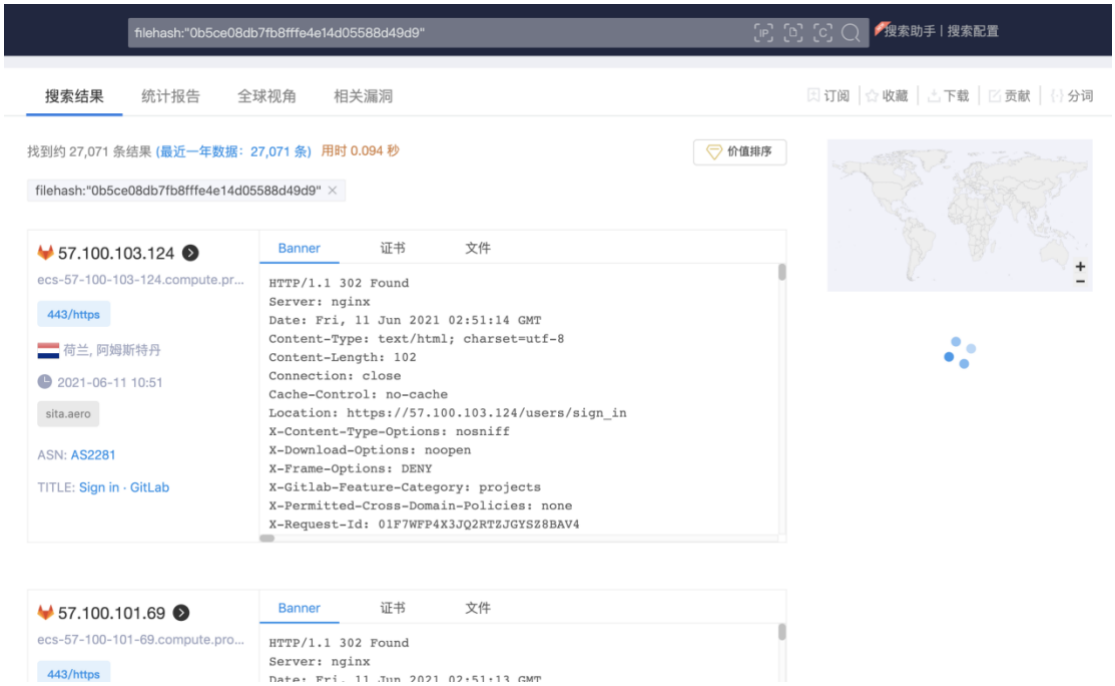


9.12. Filehash

通过上传方式进行查询，根据解析的文件数据搜索相关内容的资产。

示例：搜索包含“Gitlab”解析的相关资产

filehash:"0b5ce08db7fb8fffe4e14d05588d49d9"



9.12.1. 文件搜索

如果计算文件 hash 不方便的话，也可以直接使用文件搜索功能：

9.13. IP 批量搜索

9.14. ZoomEye-python

地址链接：https://github.com/knownsec/ZoomEye-python。

9.14.1. 安装步骤

可直接从 pypi 进行安装：

pip3 install zoomeye。

也可以通过 github 进行安装：

pip3 install git+https://github.com/knownsec/ZoomEye-python.git。

9.15. 使用 cli

在成功安装 ZoomEye-python 后，可以直接使用 zoomeye 命令，如下：

```
~ » zoomeye -h                                                    cy@PiodeMac
usage: zoomeye [-h] [-v] {info,search,init,ip,history,clear} ...

positional arguments:
  {info,search,init,ip,history,clear}
    info                Show ZoomEye account info
    search              Search the ZoomEye database
    init                Initialize the token for ZoomEye-python
    ip                  Query IP information
    history             Query device history
    clear               Manually clear the cache and user information

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit
```

9.15.1. 初始化 token

在使用 ZoomEye-python cli 前需要先初始化用户 token ,该凭证用于验证用户身份以便从 ZoomEye 查询数据；zoomeye 提供了两种认证方式：

1.username/password

2.APIKEY (推荐)

可以通过 zoomeye init -h 查看帮助，下面通过 APIKEY 来进行演示：

```
~ » zoomeye init -apikey "3(                                    d7"
Role: developer
Quota: 10000
successfully initialized
```

用户可以通过登陆 ZoomEye 在个人信息中(https://www.zoomeye.org/profile)获取 APIKEY；APIKEY 不会过期，用户可根据需求在个人信息中进行重置。

除此之外，zoomeye 还提供了 username/password 的初始化方式，通过这种方式认证后会返回 JWT-token，具有一定的时效性，失效后需要用户重新登陆。

示例：

```
curl -X POST https://api.zoomeye.org/user/login -d
'{
      "username": "foo@bar.com",
      "password": "foobar"
}'
```

{"access_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZGVudGl0eSI6MSwiaWF0IjoxNDU1NzE4
NDcwLCJuYmYiOjE0N... ..."}

9.15.2. 查询配额

用户可以通过 info 命令查询个人信息以及数据配额，如下：

```
~ » zoomeye info
Role: developer
Quota: 10000
```

9.15.3. 搜索

搜索是 ZoomEye-python 最核心的功能，通过 search 命令进行使用。search 命令需要指定搜索关键词(dork)，下面我们进行简单的搜索：

```
~ » zoomeye search "telnet" -num 1                          cy@PiodeMacBook-Pro
ip:port                 service             country             app
                banner
133.35.44.71:80         mysql               Japan               MySQL
                HTTP/1.1  200 OK\nDate:...
133.43.124.201:80       http                Japan               Apache httpd
                HTTP/1.1  200 OK\nDate:...
133.205.107.117:80      https               Japan               Apache httpd
                HTTP/1.1  200 OK\nServe...
133.186.213.35:80       mysql               Republic of Korea   MySQL
                HTTP/1.1  200 OK\nDate:...
133.186.241.201:80      mysql               Republic of Korea   MySQL
                HTTP/1.1  200 OK\nConte...
133.242.131.57:80       https               Japan               Apache httpd
                HTTP/1.1  200 OK\nDate:...
133.242.151.193:80      http                Japan               Apache httpd
                HTTP/1.1  200 OK\nConte...
133.242.180.211:80      http                Japan               Apache httpd
                HTTP/1.1  200 OK\nConte...
133.242.189.56:80       http                Japan               Apache httpd
                HTTP/1.1  200 OK\nX-Pow...
133.242.129.33:80       https               Japan               nginx
                HTTP/1.1  200 OK\nX-Pow...
133.242.208.84:80       http                Japan               Apache httpd
                HTTP/1.1  200 OK\nConte...
133.242.155.169:80      https               Japan               Apache httpd
                HTTP/1.1  200 OK\nConte...
133.242.226.123:80      mysql               Japan               MySQL
                HTTP/1.1  200 OK\nConne...
133.242.143.54:80       mysql               Japan               MySQL
                HTTP/1.1  200 OK\nConte...
133.242.133.215:80      https               Japan               nginx
                HTTP/1.1  200 OK\nServe...
133.242.144.232:80      http                Japan               Apache httpd
                HTTP/1.1  200 OK\nConte...
133.242.149.129:80      mysql               Japan               MySQL
                HTTP/1.1  200 OK\nDate:...
133.242.206.215:80      http                Japan               Apache httpd
                HTTP/1.1  200 OK\nDate:...
133.242.52.244:80       http                Japan               Apache httpd
                HTTP/1.1  200 OK\nDate:...
133.242.139.49:80       mysql               Japan               MySQL
                HTTP/1.1  200 OK\nDate:...

total: 20/59314794
```

使用 search 命令和使用浏览器在 ZoomEye 进行搜索一样简单，在默认情况下显示了较为重要的 5 个字段，用户可以使用这些数据了解目标信息：

1.ip:port　ip 地址和端口
2.service　该端口开放的服务
3.country　该 ip 地址所属国家
4.app　　识别出的应用类型

5.banner　该端口的特征响应报文

在以上演示中，使用 -num 参数指定了显示的数量，除此之外，search 还支持以下参数(zoomeye search -h)，以便用户对数据进行处理，我们将在下文进行说明和演示：

-num　设置显示/搜索的数量，支持 all
-count 查询该 dork 在 ZoomEye 数据库的总量
-facet　查询该 dork 全量数据的分布情况
-stat　统计数据结果集的分布情况
-filter　查询数据结果集中某个字段的详情，或根据内容进行筛选
-save　可按照筛选条件将结果集进行导出
-force　忽略本地缓存文件，直接从 ZoomEye 获取数据
-type　指定搜索源，host 或 web

```
~ » zoomeye search -h                                    cy@PiodeMacBook-Pro
usage: zoomeye search [-h] [-num value] [-facet [field]]
                      [-filter [field=regexp]] [-stat [field]]
                      [-save [field=regexp]] [-count] [-figure {pie,hist}]
                      [-type {host,web}] [-force]
                      dork

positional arguments:
  dork                  The ZoomEye search keyword or ZoomEye exported file

optional arguments:
  -h, --help            show this help message and exit
  -num value            The number of search results that should be returned,
                        support 'all'
  -facet [field]        Perform statistics on ZoomEye database, host field:
                        [app,device,service,os,port,country,city] web field:
                        [webapp,component,framework,server,waf,os,country]
  -filter [field=regexp]
                        Output more clearer search results by set filter
                        field, host field: [app,version,device,port,city,count
                        ry,asn,banner,timestamp,*] web field: [app,headers,key
                        words,title,site,city,country,webapp,component,framewo
                        rk,server,waf,os,timestamp,*]
  -stat [field]         Perform statistics on search results, host field:
                        [app,device,service,os,port,country,city] web field:
                        [webapp,component,framework,server,waf,os,country]
  -save [field=regexp]  Save the search results with ZoomEye json format, if
                        you specify the field, it will be saved with JSON
                        Lines
  -count                The total number of results in ZoomEye database for a
                        search
  -figure {pie,hist}    Pie chart or bar chart showing data, can only be used
                        under facet and stat
  -type {host,web}      Select web search or host search(default host)
  -force                Ignore the local cache and force the data to be
                        obtained from the API
```

9.15.4. 数据数量

通过 -num 参数可以指定我们搜索和显示的数量，指定的数目即消耗的配额数量。而通过 -count 参数可以查询该 dork 在 ZoomEye 数据库的总量，如下：

```
~ » zoomeye search "telnet" -count
59314794
```

注意：-num 参数消耗的配额为 20 的整数倍，这是因为 ZoomEye API 单次查询的最小数量为 20 条。

9.15.5. 数据聚合

我们可以通过 -facet 和 -stat 进行数据的聚合统计，使用 -facet 可以查询该 dork 全量数据的聚合情况(由 ZoomEye 聚合统计后通过 API 获取)，而 -stat 可以对查询到的结果集进行聚合统计。两个命令支持的聚合字段包括：

 # host search
app 按应用类型进行统计
device 按设备类型进行统计
service 按照服务类型进行统计
os 按照操作系统类型进行统计
port 按照端口进行统计
country 按照国家进行统计
city 按照城市进行统计
 # web search
webapp 按照 Web 应用进行统计
component 按照 Web 容器进行统计
framework 按照 Web 框架进行统计
server 按照 Web 服务器进行统计
waf 按照 Web 防火墙(WAF)进行统计
os 按照操作系统进行统计
country 按照国家进行统计

示例：使用 -facet 统计全量 telnet 设备的应用类型

```
~ » zoomeye search "telnet" -facet app
 ----------------------------------------
ZoomEye total data:59314794
 ---------------app Top 10---------------
app                                  count
[unknown]                            28208031
BusyBox telnetd                      10723193
Linux telnetd                        3312989
Cisco IOS telnetd                    1607888
MikroTik router config httpd         1376630
Huawei Home Gateway telnetd          1286494
Huawei telnetd                       1013632
Busybox telnetd                      960468
Apache httpd                         702392
Pocket CMD telnetd                   646787
```

使用 -stat 统计查询出来的 20 条 telnet 设备的应用类型：

```
~ » zoomeye search "telnet" -stat app
 ----------------------------------------
current total data:20
 ----------------app data----------------
app                                    count
Apache httpd                           11
MySQL                                  7
nginx                                  2
 ----------------------------------------
```

9.15.6. 数据筛选

使用 -filter 参数可以查询数据结果集中某个字段的详情，或根据内容进行筛选，该命令支持的字段包括：

# host/search	
app	显示应用类型详情
version	显示版本信息详情
device	显示设备类型详情
port	显示端口信息详情

city	显示城市详情
country	显示国家详情
asn	显示 as number 详情
banner	显示特征响应报文详情
timestamp	显示数据更新时间
*	在包含该符号时，显示所有字段详情

 # web/search

app	显示应用类型详情
headers	HTTP 头
keywords	meta 属性关键词
title	HTTP Title 标题信息
site	site 搜索
city	显示城市详情
country	显示国家详情
webapp	Web 应用
component	Web 容器
framework	Web 框架
server	Web 服务
waf	Web 防火墙(WAF)
os	操作系统
timestamp	显示数据更新时间
*	在包含该符号时，显示所有字段详情

相比较默认情况下的省略显示，所以通过 -filter 可以查看完整的数据，如下：

```
~ » zoomeye search "telnet" -num 1 -filter banner          cy@PiodeMacBook-Pro ]
ip                          banner
133.35.44.71                HTTP/1.1  200 OK\nDate: Tue, 15 Jun 2021 06:49:17
GMT\nServer: Apache/2.4.46 (Unix) PHP/7.4.11\nX-Powered-By: PHP/7.4.11\nContent-
Type: text/html; charset=UTF-8\n\n<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 T
ransitional//EN" "DTD/xhtml1-transitional.dtd">\n<html xmlns="http://www.w3.org/
1999/xhtml"><head>\n<style type="text/css">\nbody {background-color: #fff; color
: #222; font-family: sans-serif;}\npre {margin: 0; font-family: monospace;}\na:l
ink {color: #009; text-decoration: none; background-color: #fff;}\na:hover {text
-decoration: underline;}\ntable {border-collapse: collapse; border: 0; width: 93
4px; box-shadow: 1px 2px 3px #ccc;}\n.center {text-align: center;}\n.center tabl
e {margin: 1em auto; text-align: left;}\n.center th {text-align: center !importa
nt;}\ntd, th {border: 1px solid #666; font-size: 75%; vertical-align: baseline;
padding: 4px 5px;}\nth {position: sticky; top: 0; background: inherit;}\nh1 {fon
t-size: 150%;}\nh2 {font-size: 125%;}\n.p {text-align: left;}\n.e {background-co
lor: #ccf; width: 300px; font-weight: bold;}\n.h {background-color: #99c; font-w
eight: bold;}\n.v {background-color: #ddd; max-width: 300px; overflow-x: auto; w
ord-wrap: break-word;}\n.v i {color: #999;}\nimg {float: right; border: 0;}\nhr
{width: 934px; background-color: #ccc; border: 0; height: 1px;}\n</style>\n<titl
e>PHP 7.4.11 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NO
ARCHIVE" /></head>\n<body><div class="center">\n<table>\n<tr class="h"><td>\n<a
href="http://www.php.net/"><img border="0" src="
oAAAANSUhEUgAAAHkAAABACAYAAAA+j9gsAAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5cc
llPAAAD4BJREFUeNrsnXtwXFUdx8/dBGihKrQDY6oZZykon/gY5qizjgM2KQMfzFAOioOA5KEh+
j4R9oZH7zT6MAMKrNphZFSQreKHRgZmspLHSCJ2Co6tBtJk7Zps7tJs5t95F5/33PvWU4293F29ybdlP
zaM3df2XPv+Zzf4/zOuWc1tkjl+T0HQ3SQC6SBSlD6WKN4rusGm9F1ps/o5mPriOf8dd0YoNfi0nt4nt
B1PT4zYwzQkf3kR9/sW4xtpS0CmE0SyPUFUJXFMIxZcM0jAZ4xrKMudQT7963HBF0n6EaUjkP0vI9K9O
EHWqJLkNW1s8mC2WgVTwGAqWTafJzTWTKZmQuZ/k1MpAi2+eys6mpWfVaAPzcILu8EVKoCAaYFtPxrAX
o8qyNwzZc7gSgzgN9Hx0Ecn3j8xr4lyHOhNrlpaJIgptM5DjCdzrJ0Jmce6bWFkOpqs0MErA4gXIBuAm
Y53gFmOPCcdaTXCbq+n16PPLXjewMfGcgEttECeouTpk5MplhyKsPBTiXNYyULtwIW7Cx1vlwuJyDLR9
L0mQiVPb27fhA54yBbGttMpc1OWwF1cmKaH2FSF7vAjGezOZZJZ9j0dIZlMhnuRiToMO0c+N4X7oksas
gEt9XS2KZCHzoem2Ixq5zpAuDTqTR14FMslZyepeEI4Ogj26n0vLj33uiigExgMWRpt+CGCsEePZqoeP
M738BPTaJzT7CpU0nu1yXpAXCC3VeRkCW4bfJYFZo6dmJyQTW2tvZc1nb719iyZWc5fmZ6Osu6H3uVzi
t52oBnMll2YizGxk8muFZLAshb/YKtzQdcaO3Y2CQ7eiy+YNGvLN+4+nJetm3bxhKJxJz316xZw1pbW9
kLew+w1944XBEaPj6eYCeOx1gqNe07bK1MwIDbKcOFOR49GuePT5fcfOMX2drPXcQ0zf7y2tvbWVdXF/
v1k2+yQ4dPVpQ5P0Um/NjoCX6UBMFZR6k+u7qMYVBYDIEqBW7eXAfPZX19zp2/oaGBHysNMGTFinPZik
9fWggbI5Omb13zUDeB3lLsdwaK/YPeyAFU0i8Aw9/2Dwyx4SPjFQEYUlf3MTYw4Jx7CIVCbHR0oqIDNM
D+FMG+ZE0dO/tsHlvAWnYS6H4qjfMC+Zld/wg92/tuv2WeeYT87j+H2aFDxysGLuSy+o/z49DQkONnmp
qa2MjRyoYsZOXKGnb5Z+vZqlUrxUsAvI9At/oK+elnBpoNw+Dai9TekSMxDrgSh0KrSYshTprc2NhoRf
1JtlikqirAVl98AddsSavDBDrsC+QdT7/TSoB344tzOZ39+70RbporVerqasyw1MEnC8iV6I9VTDi0uq
bmfPFSq2W+gyUHXuEdb3WR5rab5jnD3i/BNMN8ChNaqsTiKa55KmBWX+Tuj0XQdQVF307nhTH0CPls+O
0UPbaT5TQG/8qX68u6LpV67LQ6dNknaYgaYyPDx2TzvYGCsnhRkH8b/rsF2GDj1MCInkvxvRjOuCUlip
WD/zrKx7ZOwBF0vfSSM2ShyaqAAOC1Nw+zt9/5YNbrN1zfwIdpfgnqebv/A6pnWAn4qlW1HPgHQ6OeoG
3N9RO/+StMdDtmV2LxJPfBpQCGfwTgrVu38jFrKaW2tpZt2LCBdXR0sEgkwhv21u9cxQsyW3ZB1+DgoO
M54btU6tu8eTPr6elhy5fr7IZNDey+e76e9/fCLcAllHpdKKinpaUlX8+111xB9VzNrYxqUAY/XVVVJY
MOekLu2fFGM8VWYQRYiYkU9bD4vPlHFYnH4/zvkb1CgwACHgMoUpdyw3sFXcXUh4YHaNSHDqaxdL5jwV
TXBpeXVY9oF3RcUQ+O09NT7Cayfld+4RJlP42gTIq8w66Qf/X4a6FTSSMMDcaE/NhYecMM+MdyG90OAh
```

使用 -filter 进行筛选时，语法为：key1,key2,key3=value，其中 key3=value 为筛选条件，而展示的内容为 key1,key2 例：

```
~ » zoomeye search telnet -num 1 -filter port,app,banner=Telnet
ip                              port                            app

133.35.44.71                    80                              MySQL


total: 1
```

在上面的示例中 :banner=Telnet 为筛选的条件 ,而 port,app 为展示的内容。如果需要展示 banner，筛选语句则是这样：

```
zoomeye search telnet -num 1 -filter port,app,banner,banner=Telnet
```

9.15.7. 数据导出

-save 参数可以对数据进行导出，该参数的语法和 -filter 一样，并将结果按行 json 的格式保存到文件中，如下：

$ zoomeye search "telnet" -save banner=telnet

save file to telnet_1_1610446755.json successful!

$ cat telnet_1_1610446755.json

{'ip': '218.223.21.91', 'banner': '\\xff\\xfb\\x01\\xff\\xfb\\x03\\xff\\xfd\\x03TELNET session now in ESTABLISHED state\\r\\n\\r\\n'}

9.15.8. 数据图像化

-figure 参数为数据图像化参数，该参数提供了 pie(饼图) 和 hist(柱状图) 两种展示方式，在没有进行指定依旧显示数据，在指定 -figure 时，只会显示图形。饼图如下：

```
(venv) ➜  ZoomEye-python git:(master) ✗ zoomeye search telnet -facet country -figure pie
------------------------------
ZoomEye total data:57313229
-----------------Top 10-----------------

                                    China : 50%
        # # # # # # #                 United States: 12%
      # # # # # # # # #               Brazil: 9%
    # # # # # # # # # # #             Republic of Korea: 6%
  # # # # # # # # # # # # #           Argentina: 4%
  # # # # # # # # # # # # #           India : 4%
  # # # # # # # # # # # # #           Russia: 3%
  # # # # # # # # # # # # #           Italy : 3%
  # # # # # # # # # # # # #           Japan : 3%
  # # # # # # # # # # # # #           Mexico: 2%
    # # # # # # # # # # # #
      # # # # # # # # # #
        # # # # # # # #
```

```
(venv) ➜  ZoomEye-python git:(master) ✗ zoomeye search telnet -stat country -figure pie
------------------------------
current total data:20
-------------current data--------------
country                          count

                                    South Africa: 60%
        # # # # # # #               Germany: 30%
      # # # # # # # # #             Kenya : 5%
    # # # # # # # # # # #           Thailand: 5%
  # # # # # # # # # # # # #
  # # # # # # # # # # # # #
  # # # # # # # # # # # # #
  # # # # # # # # # # # # #
  # # # # # # # # # # # # #
  # # # # # # # # # # # # #
    # # # # # # # # # # # #
      # # # # # # # # # #
        # # # # # # # #
```

柱状图如下：

```
(venv) ➜  ZoomEye-python git:(master) ✗ zoomeye search telnet -facet country -figure hist
------------------------------
ZoomEye total data:57313229
-----------------Top 10-----------------

China              [19768794]  ########################################
United States      [ 4703769]  ##########
Brazil             [ 3617285]  ########
Republic of Korea  [ 2486195]  #####
Argentina          [ 1711641]  ####
India              [ 1653985]  ####
Russia             [ 1520672]  ####
Italy              [ 1303083]  ###
Japan              [ 1255294]  ###
Mexico             [ 1075128]  ###
```

```
(venv) ➜  ZoomEye-python git:(master) ✗ zoomeye search telnet -stat country -figure hist
------------------------------
current total data:20
-------------current data--------------
country                          count

South Africa  [12]  ########################################
Germany       [ 6]  ####################
Kenya         [ 1]  ####
Thailand      [ 1]  ####
```

注意：仅能在 -facet 和 -stat 数据聚合的情况使用。

9.15.9. IP 历史数据查看

ZoomEye-python 提供了 IP 历史设备数据查询功能，使用命令 history [ip] 便能查询 IP 设备历史数据，使用方式如下：

```
$zoomeye history "207.xx.xx.13" -num 1
207.xx.xx.13
Hostnames:                  [unknown]
Country:                    United States
City:                       Lake Charles
Organization:               fulair.com
Lastupdated:                2021-02-18T03:44:06
Number of open ports:       1
Number of historical probes:  1
timestamp                          port/service                    app
raw_data
2021-02-18  03:44:06               80/http                         Apache  httpd
HTTP/1.0 301 Moved Permanently...
```

在默认情况下向用户较为重要的六个字段：

1. time 记录的时间
2. service 开放的服务
3. port 端口
4. app Web 应用
5. banner 原始的指纹信息

使用 zoomeye history -h 可以查看 history 提供的参数。

```
[~ » zoomeye history -h                                    1 ↵ cy@PiodeMacBook-Pro
usage: zoomeye history [-h] [-filter [filed=regexp]] [-force] [-num value] ip

positional arguments:
  ip                    search historical device IP

optional arguments:
  -h, --help            show this help message and exit
  -filter [filed=regexp]
                        filter data and print raw data detail. field:
                        [timestamp,port,service,country,banner,*]
  -force                ignore the local cache and force the data to be
                        obtained from the API
  -num value            The number of search results that should be returned
```

下面对 -filter 进行演示：

$zoomeye history "207.xx.xx.13" -filter "time=^2019-08,port,service"

207.xx.xx.13

Hostnames: [unknown]

Country: United States

City: Lake Charles

Organization: fulair.com

Lastupdated: 2019-08-16T10:53:46

Number of open ports: 3

Number of historical probes: 3

time	port	service
2019-08-16 10:53:46	389	ldap
2019-08-08 23:32:30	22	ssh
2019-08-03 01:55:59	80	http

-filter 参数支持以下五个字段的筛选：

1.time 扫描时间

2.port 端口信息

3.service 开放的服务

4.app Web 应用

5.raw 原始指纹信息

6.* 在包含该符号时，显示所有字段详情

在展示时添加了一个 id 字段的展示，id 为序号，为了方便查看，并不能作为筛选的字段。

注意：目前只开放了上述五个字段的筛选。使用 history 命令时同样会消耗用户配额，在 history 命令中返回多少条数据，用户配额就相应扣除多少。例如：IP "8.8.8.8" 共有 944 条历史记录，查询一次扣除 944 的用户配额。

9.15.10. 查询 IP 信息

可以通过 zoomeye ip 命令查询指定 IP 的信息，例如：

```
~ » zoomeye ip 39.156.69.79                                    cy@PiodeMacBook-Pro
39.156.69.79
Hostnames:                  [unknown]
Isp:                        ChinaMobile
Country:                    China
City:                       Beijing
Organization:               [unknown]
Lastupdated:                2021-06-11T23:00:50
Number of open ports:       2{80, 443}

port      service       app                  banner
80        http          Apache httpd         HTTP/1.1 200 OK\r\nDate...
443       https         Baidu Front End httpd  HTTP/1.1 405 Not Allowe...
```

zoomeye ip 命令同样支持筛选参数 -filter, 语法和 zoomeye search 的筛选语法一致。例如：

```
$ zoomeye ip "185.*.*.57" -filter "app,app=ntpd"
Hostnames:                  [unknown]
Isp:                        [unknown]
Country:                    Saudi Arabia
City:                       [unknown]
Organization:               [unknown]
Lastupdated:                2021-02-17T02:15:06
Number of open ports:       0
Number of historical probes:  1

app
ntpd
```

filter 参数支持的字段有:

port	端口信息
service	运行服务
app	应用
banner	指纹信息

注意 :此功能根据不同用户等级 ,对每个用户每天查询次数做了一定的限制。

注册用户和开发者每天能够查询 10 次

高级用户每天可查询 20 次

VIP 用户每天可以查询 30 次

每天的次数使用完之后 ,24 小时后刷新 ,即从第一次查 IP 的时间开始计算，24 小时后刷新次数。

9.15.11. 清理功能

用户每天都会搜索大量的数据 ,这样就导致缓存文件夹所占的存储空间逐渐增大；如果用户在公共服务器上使用 ZoomEye-python 可能会导致自己的 API KEY 和 ACCESS TOKEN 泄漏。 为此 ZoomEye-python 提供了清理命令 zoomeye clear，清理命令可以缓存数据和用户配置进行清空。使用方式如下：

```
~ » zoomeye clear -h
usage: zoomeye clear [-h] [-setting] [-cache]

optional arguments:
  -h, --help  show this help message and exit
  -setting    clear user api key and access token
  -cache      clear local cache file
```

9.15.12. 缓存机制

ZoomEye-python 在 cli 模式下提供了缓存机制，位于 ~/.config/zoomeye/cache 下，尽可能的节约用户配额；用户查询过的数据集将在本地缓存 5 天，当用户查询相同的数据集时，不会消耗配额。

9.16. 使用 SDK

9.16.1. 初始化 token

同样，在 SDK 中也支持 username/password 和 APIKEY 两种认证方式，如下：

user/pass

```
from zoomeye.sdk import ZoomEye
zm = ZoomEye(username="username", password="password")
```

APIKEY

```
from zoomeye.sdk import ZoomEye
zm = ZoomEye(api_key="01234567-acbd-00000-1111-22222222222")
```

9.16.2. SDK API

以下是 SDK 提供的接口以及说明：

```
1.login()
    使用 username/password 或者 APIKEY 进行认证
2.dork_search(dork, page=0, resource="host", facets=None)
    根据 dork 搜索指定页的数据
3.multi_page_search(dork, page=1, resource="host", facets=None)
    根据 dork 搜索多页数据
4.resources_info()
    获取当前用户的信息
```

5.show_count()

获取当前 dork 下全部匹配结果的数量

6.dork_filter(keys)

从搜索结果中提取指定字段的数据

7.get_facet()

从搜索结果中获取全量数据的聚合结果

8.history_ip(ip)

查询某个 ip 的历史数据信息

9.show_site_ip(data)

遍历 web-search 结果集，并输出域名和 ip 地址

10.show_ip_port(data)

遍历 host-search 结果集，并输出 ip 地址和端口

9.16.3. 使用示例

```
$ python3
>>> import zoomeye.sdk as zoomeye
>>> dir(zoomeye)
['ZoomEye', 'ZoomEyeDict', '__builtins__', '__cached__', '__doc__',
'__file__', '__loader__', '__name__', '__package__', '__spec__',
'fields_tables_host', 'fields_tables_web', 'getpass', 'requests',
'show_ip_port', 'show_site_ip', 'zoomeye_api_test']
>>> # Use username and password to login
>>> zm = zoomeye.ZoomEye()
>>> zm.username = 'username@zoomeye.org'
>>> zm.password = 'password'
>>> print(zm.login())
....JIUzI1NiIsInR5cCI6IkpXVCJ9.....
>>> data = zm.dork_search('apache country:cn')
>>> zoomeye.show_site_ip(data)
213.***.***.46.rev.vo***one.pt ['46.***.***.213']
me*****on.o****e.net.pg ['203.***.***.114']
soft********63221110.b***c.net ['126.***.***.110']
```

```
soft********26216022.b***c.net ['126.***.***.22']
soft********5084068.b***c.net ['126.***.***.68']
soft********11180040.b***c.net ['126.***.***.40']
...
```

9.16.4. 数据搜索

如上示例，我们使用 dork_search() 进行搜索，我们还可以设置 facets 参数，以便获得该 dork 全量数据的聚合统计结果，示例如下：

```
>>> data = zm.dork_search('telnet', facets='app')
>>> zm.get_facet()
{'product': [{'name': '', 'count': 28323128}, {'name': 'BusyBox telnetd', 'count': 10180912}, {'name': 'Linux telnetd', .....
```

9.16.5. 数据筛选

在 SDK 中提供了 dork_filter() 函数，我们可以更加方便对数据进行筛选，提取指定的数据字段，如下：

```
>>> data = zm.dork_search("telnet")
>>> zm.dork_filter("ip,port")
[['180.*.*.166', 5357], ['180.*.*.6', 5357], .....
```

9.17. 接口

9.17.1. 搜索过滤器

搜索过滤器，提供给用户筛选搜索结果的功能，用户根据它能够更精准的定位所需结果。一般使用 key-value 的格式，如 foo:bar 。并且能够组合不同的过滤器，达到更高级的筛选功能。获取更精准的结果。

9.17.1.1. 主机设备搜索过滤器

名称	类型	说明	示例
app	string	应用，产品	app: ProFTPD
ver	string	版本	ver:2.1

device	string	设备类型	device:router
os	string	操作系统	os:windows
service	string	服务类型	service:http
ip	string	IP 地址	ip:192.168.1.1
cidr	string	CIDR 格式地址	cidr:192.168.1.1/24
hostname	string	主机名称	hostname:google.com
port	string	端口号	port:80
city	string	城市名称	city:beijing
country	string	国家名称	country:china
asn	integer	ASN 号码	asn:8978

9.17.1.2. Web 应用搜索过滤器

名称	类型	说明	示例
app	string	Web 应用信息	webapp:wordpress
header	string	HTTP headers	header:server
keywords	string	meta 属性关键词	keywords:baidu.com
desc	string	HTTP description 属性	desc:hello
title	string	HTTP Title 标题信息	title: baidu
ip	string	IP 地址	ip:192.168.1.1
site	string	site 搜索	site:baidu.com
city	string	城市名称	city:beijing
country	string	国家名称	country:china

9.17.2. 用户相关

9.17.2.1. 登录

权限: 注册用户及以上

登录获取 access_token

POST /user/login

参数

名称	类型	说明	是否必需	示例
username	string	用户名（**必须为邮箱**）	必需	foo@bar.com
password	string	密码	必需	foopass

返回值

名称	类型	说明
access_token	string	用户的 access token

状态码

状态码	说明
200	登录成功
401	需要登录
400	非法请求参数，请求参数为空
400	非法请求参数，缺少用户名（邮箱）或者密码

cURL 示例

```
curl -X POST -i https://api.zoomeye.org/user/login -d
'{
      "username": "foo@bar.com",
      "password": "foopass"
}'
```

响应示例

```
HTTP/1.1 200 OK
Date: Tue, 20 Feb 2016 06:14:49 GMT
Content-Length: 188
Content-Type: application/json; charset=UTF-8
```

{"access_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZGVudGl0eSI6MSwiaWF0IjoxNDU1NzE4
NDcwLCJuYmYiOjE0N... ..."}

9.17.3. 资源信息

权限: 注册用户及以上

账户资源信息，资源额度及套餐类型

```
GET /resources-info
```

返回值

名称	类型	说明
plan	string	套餐类型
resources	object	资源详情

状态码

状态码	说明
200	请求资源信息成功
401	需要登录授权

cURL 示例

```
curl -X GET -i https://api.zoomeye.org/resources-info \ -H "Authorization:
JWT eyJhbGciOiJIUzI1NiIsInR..."
```

响应示例

```
HTTP/1.1 200 OK
Date: Tue, 01 Mar 2016 10:08:09 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 72
Connection: keep-alive
Etag: "f3fdef1e608ffc4b48cd306f068550ff046652c1"
{"plan": "developer", "resources": {"host-search": 9, "web-search": 40}}
```

9.17.4. 主机设备搜索

权限: 注册用户及以上

搜索主机设备

GET /host/search

参数

名称	类型	说明	是否必需	示例
query	string	查询关键词	必需	port:80 nginx
page	integer	翻页参数(默认为 1)	可选	7
facets	string	统计项目，如果为多个，使用,号分隔各个统计项	可选	app,device
sub_type	string	获取数据类型，默认为ipv4,ipv6 全选	可选	sub_type:v4

支持统计项

统计项	类型	说明
app	string	应用，设备等
device	string	设备类型
service	string	服务类型
os	string	操作系统
port	string	端口号
country	string	国家
city	string	城市

返回值

名称	类型	说明
matches	string	结果集

facets	string	统计结果
total	integer	结果总数

状态码

状态码	说明
200	请求成功
400	非法请求参数，请参考文档确认后重试
400	非法请求参数，缺少 query(查询) 参数
422	非法请求参数，包含不支持参数项

cURL 示例

```
curl -X GET 'https://api.zoomeye.org/host/search?query=port:21%20city:beijing&page=1&facet=app,os' \ -H "Authorization: JWT eyJhbGciOiJIUzI1NiIsInR5..."
```

响应示例

```
HTTP/1.1 200 OK
Date: Tue, 23 Feb 2016 07:12:59 GMT
Content-Length: 64683
Etag: "9ef67c54a6639ada78da34ce4198a750908c6f61"
{ "matches": [ {
    "geoinfo": {
        "asn": 45261,
        "city": {
            "names": {
                "en": "Brisbane",
                "zh-CN": "\u5e03\u91cc\u65af\u73ed"
            }
        },
        "continent": {
            "code": "OC",
            "names": {
```

```
                    "en": "Oceania",
                    "zh-CN": "\u5927\u6d0b\u6d32"
                }
            },
            "country": {
                "code": "AU",
                "names": {
                    "en": "Australia",
                    "zh-CN": "\u6fb3\u5927\u5229\u4e9a"
                }
            },
            "location": {
                "lat": -27.471,
                "lon": 153.0243
            }
        },
        "ip": "192.168.1.1",
        "portinfo": {
            "app": "",
            "banner": "+OK Hello there.\r\n-ERR Invalid command.\r\n\n",
            "device": "",
            "extrainfo": "",
            "hostname": "",
            "os": "",
            "port": 110,
            "service": "",
            "version": ""
        },
        "timestamp": "2016-03-09T16:14:04"
        }, ... ...],
    "facets": {
    },
     "total": 28731397
}
```


结果属性

嵌套属性结构 ,使用 '.' 成员访问符表示 ,如{'foo': {'bar': 'zoo'}} 中的 bar 使用 foo.bar 表示

固定属性

名称	类型	说明	示例
ip	string	IP 地址	192.168.1.1
geoinfo.asn	integer	ASN 号	4134
geoinfo.city	string	城市	Guangzhou
geoinfo.country.code	string	国家码	CN
geoinfo.country.name	string	国家名	China
geoinfo.continent.code	string	洲际码	AS
geoinfo.continent.name	string	洲际名	Asia
geoinfo.location.latitude	float	纬度	23.0268
geoinfo.location.longitude	float	经度	113.1315
port	integer	端口号	80
banner	string	端口指纹信息	HTTP/1.1 403 Forbidden...
portinfo.app	string	产品名称	HTTP/1.1 403 Forbidden...
portinfo.hostname	string	主机名	foo.com
portinfo.os	string	操作系统名称	Windows
portinfo.version	string	产品，应用版本信息	v1.0
portinfo.info	string	额外信息	ssl/http
portinfo.device	string	设备类型	router

9.17.5. Web 应用搜索

权限: 注册用户及以上

搜索 Web 应用

GET /web/search

参数

名称	类型	说明	是否必须	示例
query	string	查询关键词	必须	port:80 nginx
page	integer	翻页参数(默认为 1)	可选	7
facets	string	统计项目，如果为多个，使用, 号分隔各个统计项	可选	app,device

支持统计项

统计项	类型	说明
webapp	string	Web 应用
component	string	Web 容器
framework	string	Web 框架
frontend	string	前端组件
server	string	Web 服务器
waf	string	Web 防火墙(WAF)
os	string	操作系统
country	string	国家
city	string	城市

返回值

名称	类型	说明

matches	string	结果集
facets	string	统计结果
total	integer	结果总数

状态码

状态码	说明
200	请求成功
400	非法请求参数，请参考文档确认后重试
400	非法请求参数，缺少 query(查询) 参数
422	非法请求参数，包含不支持参数项

cURL 示例

```
curl -X GET 'https://api.zoomeye.org/web/search?query=city:beijing%20app:DedeCMS&page=1&facets=app,os' \ -H "Authorization: JWT eyJhbGciOiJIUzI1NiIsInR5..."
```

响应示例

```
HTTP/1.1 200 OK
Date: Tue, 23 Feb 2016 07:12:59 GMT
Content-Length: 64683
Etag: "9ef67c54a6639ada78da34ce4198a750908c6f61"

{ "matches": [{
        "check_time": "2016-2-23T14:58:41.979769",
        "db": [
            {
                "chinese": "MySQL",
                "name": "MySQL",
                "version": null
            }
        ],
        "description": "",
```

```
"domains": [
    "wordpress.org"
],
"geoinfo": {
    "asn": 32475,
    "city": {
        "names": {
            "en": "",
            "zh-CN": ""
        }
    },
    "continent": {
        "code": "EU",
        "names": {
            "en": "Europe",
            "zh-CN": "\u6b27\u6d32"
        }
    },
    "country": {
        "code": "RO",
        "names": {
            "en": "Romania",
            "zh-CN": "\u7f57\u9a6c\u5c3c\u4e9a"
        }
    },
    "location": {
        "lat": 46.0,
        "lon": 25.0
    }
},
"ip": [
    "109.73.238.102"
],
"keywords": "",
"language": [
    "PHP"
],
"plugin": [
```

```
                    {
                        "based": "WordPress",
                        "chinese": "twentyfifteen",
                        "name": "twentyfifteen",
                        "version": "1.3"
                    }
                ],
                "server": [
                    {
                        "chinese": "Nginx",
                        "name": "nginx",
                        "version": null
                    }
                ],
                "site": "socketdigital.com",
                "title": "My Blog &#8211; My WordPress Blog",
                "webapp": [
                    {
                        "chinese": "WordPress",
                        "name": "wordpress",
                        "url": "http://socketdigital.com/",
                        "version": "4.4.2"
                    }
                ],
                "headers": "Server: nginx\r\nDate: Tue, 23 Feb 2016 06:55:40 GMT\r\nContent-Type: text/html; charset=UTF-8\r\nTransfer-Encoding: chunked\r\nConnection: keep-alive\r\n"
            }

     ]
    "total": 1271948
}
```


结果属性

嵌套属性结构 ,使用 '.' 成员访问符表示 ,如{'foo': {'bar': 'zoo'}} 中的 bar 使用 foo.bar 表示

固定属性

名称	类型	说明	示例
site	string	网站地址	foo.com
ip	string	IP 地址	foo.com
headers	string	HTTP 请求头	HTTP/1.1...
title	string	HTTP 标题	Hello Welcome...
description	strine	HTTP meta description 属性	foo
keyword	string	HTTP meta 关键词	foo
domains	string	站点包含子域	a.com
waf.name	string	Web 防火墙名称	jiasule
waf.version	string	Web 防火墙名称版本	v1.0
server.name	string	Web 服务器名称	nginx
server.version	string	Web 服务器版本	1.9.2
component.name	string	Web 容器名称	mod_ssl
component.version	string	Web 容器版本	v1.0
language	string	Web 编程语言	php
db.name	string	数据库名称	MySQL
db.version	string	数据库版本	v1.0
frontend.name	string	前端组件名称	jQuery
frontend.version	string	前端组件版本	v1.0

thirdparty	string	第三方组件名称	v1.0
plugin.url	string	插件 url	www.google.com/analysics
plugin.name	string	插件名称	google analysics
plugin.version	string	插件版本	v1.0
webapp.url	string	web 应用 url	wordpress.org
webapp.name	string	Web 应用名称 name	wordpress
webapp.version	string	Web 应用版本	wordpress version
html	string	HTTP HTML 请求体	
geoinfo.asn	string	ASN 号	4134
geoinfo.isp	string	运营商	China Telecom Guangdong
geoinfo.city	string	城市	Guangzhou
geoinfo.country.code	string	国家码	CN
geoinfo.country.name	string	国家名称	China
geoinfo.continent.code	string	洲际码	AS
geoinfo.continent.name	string	洲际名称	Asia
geoinfo.location.latitude	float	纬度	23.0268
geoinfo.location.longitude	float	经度	113.1315

9.17.6. 设备历史接口

权限: 高级用户，VIP 用户

搜索 设备历史

```
GET /both/search
```

参数

名称	类型	说明	是否必须	示例
ip	string	查询设备的 IP	必须	ip=1.2.3.4
history	string	查询历史数据	必须	history=true

返回值

名称	类型	说明
data	string	结果集
count	integer	结果总数

状态码

状态码	说明
200	请求成功
400	非法请求参数，请参考文档确认后重试
400	非法请求参数，缺少查询参数
422	非法请求参数，包含不支持参数项

cURL 示例

```
curl -X GET 'https://api.zoomeye.org/both/search?history=true&ip=1.2.3.4' \ -H "Authorization: JWT eyJhbGciOiJIUzI1NiIsInR5..."
```

响应示例

```
HTTP/1.1 200 OK
```

Date: Tue, 31 Dec 2019 07:12:59 GMT
Content-Length: 64683
Etag: "9ef67c54a6639ada78da34ce4198a750908c6f61"

{ {
"count": 28,
"data": [
{
"component": [],
"db": [],
"description": "",
"domains": [],
"framework": [],
"geoinfo": {
"PoweredBy": "IPIP",
"asn": null,
"aso": null,
"base_station": "",
"city": {
"geoname_id": null,
"names": {
"en": "",
"zh-CN": ""
}
},
"continent": {
"code": "",
"geoname_id": null,
"names": {
"en": null,
"zh-CN": null
}
},
"country": {
"code": "",
"geoname_id": null,
"names": {
"en": "APNIC.NET",

```
                    "zh-CN": "APNIC.NET"
                }
            },
            "idc": "IDC",
            "isp": "",
            "location": null,
            "organization": "apnic.net",
            "organization_CN": "apnic.net",
            "subdivisions": {
                "code": null,
                "geoname_id": null,
                "names": {
                    "en": "APNIC.NET",
                    "zh-CN": "APNIC.NET"
                }
            }
        },
        "headers": "HTTP/1.1 302 Redirect\r\nContent-Type: text/html; charset=UTF-8\r\nLocation: https://fileex.bdo.a
t\r\nServer: Microsoft-IIS/8.5\r\nX-Frame-Options: sameorigin\r\nStrict-Transport-Security: max-age=31536000\r\nDate: Tue
, 29 Oct 2019 04:54:00 GMT\r\nContent-Length: 144\r\n",
        "ip": [
            "1.2.3.4",
            "80.240.225.208",
            "4.4.4.4",
            "9.8.7.6",
            "80.120.17.23",
            "8.8.8.8"
        ],
        "keywords": "",
        "language": [
            "ASP"
        ],
        "server": [
            {
                "chinese": "Microsoft IIS httpd",
                "name": "Microsoft IIS httpd",
```

```
                        "version": "8.5"
                    }
                ],
                "site": "puresaon.com",
                "system": [
                    {
                        "chinese": "Windows",
                        "distrib": null,
                        "name": "Windows",
                        "release": null,
                        "version": null
                    }
                ],
                "timestamp": "2019-10-29T12:55:30.295349",
                "title": "Document Moved",
                "waf": [],
                "webapp": []
            },
......
}
```


结果属性

嵌套属性结构，使用 '.' 成员访问符表示，如{'foo': {'bar': 'zoo'}} 中的 bar 使用 foo.bar 表示

属性说明

名称	类型	说明	示例
site	string	网站地址	foo.com
ip	string	IP 地址	8.8.8.8
headers	string	HTTP 请求头	HTTP/1.1...
title	string	HTTP 标题	Hello Welcome...

description	strine	HTTP meta description 属性	foo
keyword	string	HTTP meta 关键词	foo
domains	string	站点包含子域	a.com
waf.name	string	Web 防火墙名称	jiasule
waf.version	string	Web 防火墙名称版本	v1.0
server.name	string	Web 服务器名称	nginx
server.version	string	Web 服务器版本	1.9.2
component.name	string	Web 容器名称	mod_ssl
component.version	string	Web 容器版本	v1.0
language	string	Web 编程语言	php
db.name	string	数据库名称	MySQL
db.version	string	数据库版本	v1.0
frontend.name	string	前端组件名称	jQuery
frontend.version	string	前端组件版本	v1.0
thirdparty	string	第三方组件名称	v1.0
plugin.url	string	插件 url	www.google.com/analysics
plugin.name	string	插件名称	google analysics
plugin.version	string	插件版本	v1.0
webapp.url	string	web 应用 url	wordpress.org

webapp.name	string	Web 应用名称 name	wordpress
webapp.version	string	Web 应用版本	wordpress version
html	string	HTTP HTML 请求体	
geoinfo.PoweredBy	string	提供商	IPIP
geoinfo.asn	string	ASN 号	4134
geoinfo.isp	string	运营商	China Telecom Guangdong
geoinfo.base_station	string	基站标识	BS
geoinfo.idc	string	IDC 标识	IDC
geoinfo.city	string	城市	Guangzhou
geoinfo.country.code	string	国家码	CN
geoinfo.country.name	string	国家名称	China
geoinfo.continent.code	string	洲际码	AS
geoinfo.continent.name	string	洲际名称	Asia
geoinfo.location.latitude	float	纬度	23.0268
geoinfo.location.longitude	float	经度	113.1315
port	integer	端口号	80
banner	string	端口指纹信息	HTTP/1.1 403 Forbidden...
portinfo.app	string	产品名称	HTTP/1.1 403 Forbidden...
portinfo.hostname	string	主机名	foo.com

portinfo.os	string	操作系统名称	Windows
portinfo.version	string	产品，应用版本信息	v1.0
portinfo.info	string	额外信息	ssl/http
portinfo.device	string	设备类型	router

9.18. 浏览器插件 Zoomeye Tools

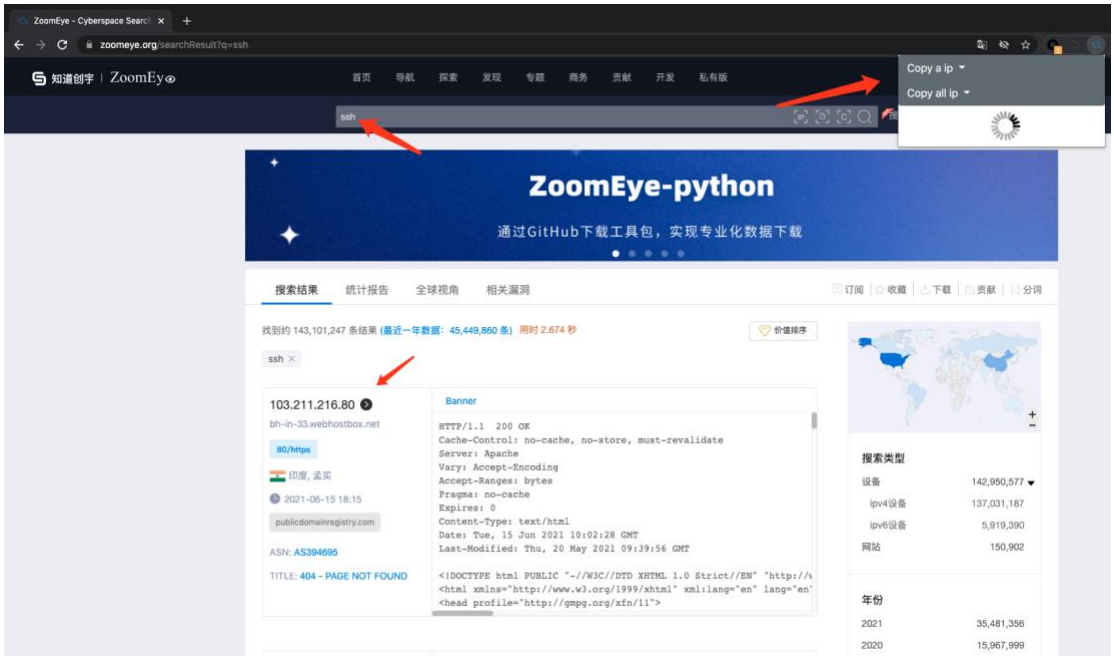
地址：

https://chrome.google.com/webstore/detail/zoomeye-tools/bdoaeiibkccgkbjbmmmoemghacnkbklj

9.18.1. zoomeye 辅助工具

首先第一个功能是配合 Zoomeye 的，只会在 Zoomeye 域下生效，这个功能不需要登录 zoomeye。

当我们打开 Zoomeye 之后搜索任意 banner，等待页面加载完成后，再点击右上角的插件图标，就能看到多出来的两条选项。



如果我们选择 copy all ip with LF，那么剪切板就是

23.225.23.22:8883

23.225.23.19:8883

23.225.23.20:8883

149.11.28.76:10443

149.56.86.123:10443

149.56.86.125:10443

149.233.171.202:10443

149.11.28.75:10443

149.202.168.81:10443

149.56.86.116:10443

149.129.113.51:10443

149.129.104.246:10443

149.11.28.74:10443

149.210.159.238:10443

149.56.86.113:10443

149.56.86.114:10443

149.56.86.122:10443

149.100.174.228:10443

149.62.147.11:10443

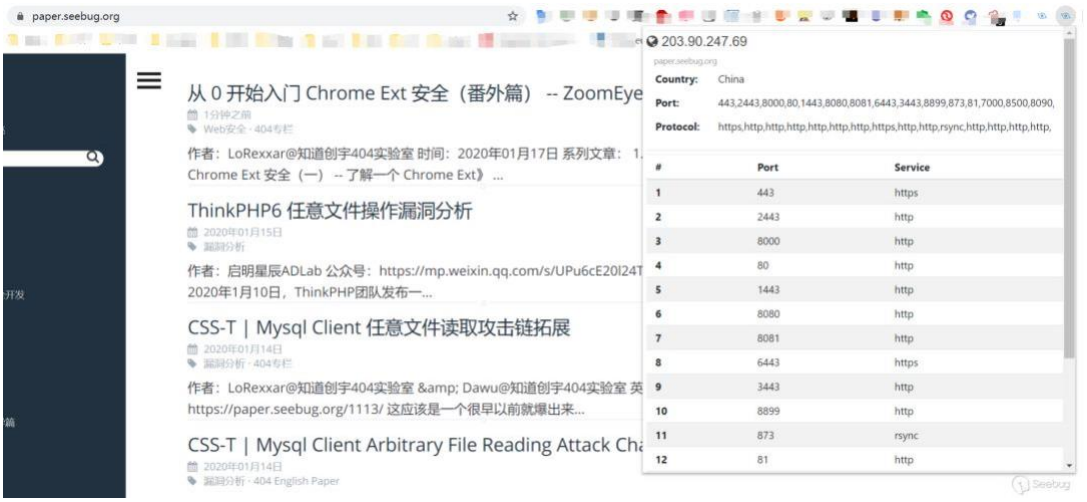
149.11.130.74:10443

9.18.2. Zoomeye Preview

第二个功能是一个简易版本的 Zoomeye，这个功能需要登录 Zoomeye。

在任意域我们点击右上角的 Login Zoomeye，如果你之前登陆过 Zoomeye 那么会直接自动登录，如果没有登录，则需要在 telnet404 页面登录。登录完成后等待一会儿就可以加载完成。

在访问网页时，点击右上角的插件图标，我们就能看到相关 ip 的信息以及开放端口


paper.seebug.org
从 0 开始入门 Chrome Ext 安全（番外篇） -- ZoomEye
作者：LoRexxar@知道创宇404实验室 时间：2020年01月17日 系列文章：1.
Chrome Ext 安全（一） -- 了解一个 Chrome Ext》...
ThinkPHP6 任意文件操作漏洞分析
作者：启明星辰ADLab 公众号：https://mp.weixin.qq.com/s/UPu6cE20I24T
2020年1月10日，ThinkPHP团队发布一...
CSS-T | Mysql Client 任意文件读取攻击链拓展
作者：LoRexxar@知道创宇404实验室 & Dawu@知道创宇404实验室 英
https://paper.seebug.org/1113/ 这应该是一个很早以前就爆出来...
CSS-T | Mysql Client Arbitrary File Reading Attack Cha
203.90.247.69
Country: China
Port: 443,2443,8000,80,1443,8080,8081,6443,3443,8899,873,81,7000,8500,8090,
Protocol: https,http,http,http,http,http,http,https,http,http,rsync,http,http,http,http,
Port Service
1 443 https
2 2443 http
3 8000 http
4 80 http
5 1443 http
6 8080 http
7 8081 http
8 6443 https
9 3443 http
10 8899 http
11 873 rsync
12 81 http

;

知道创宇云安全事业群
解决方案交付中心