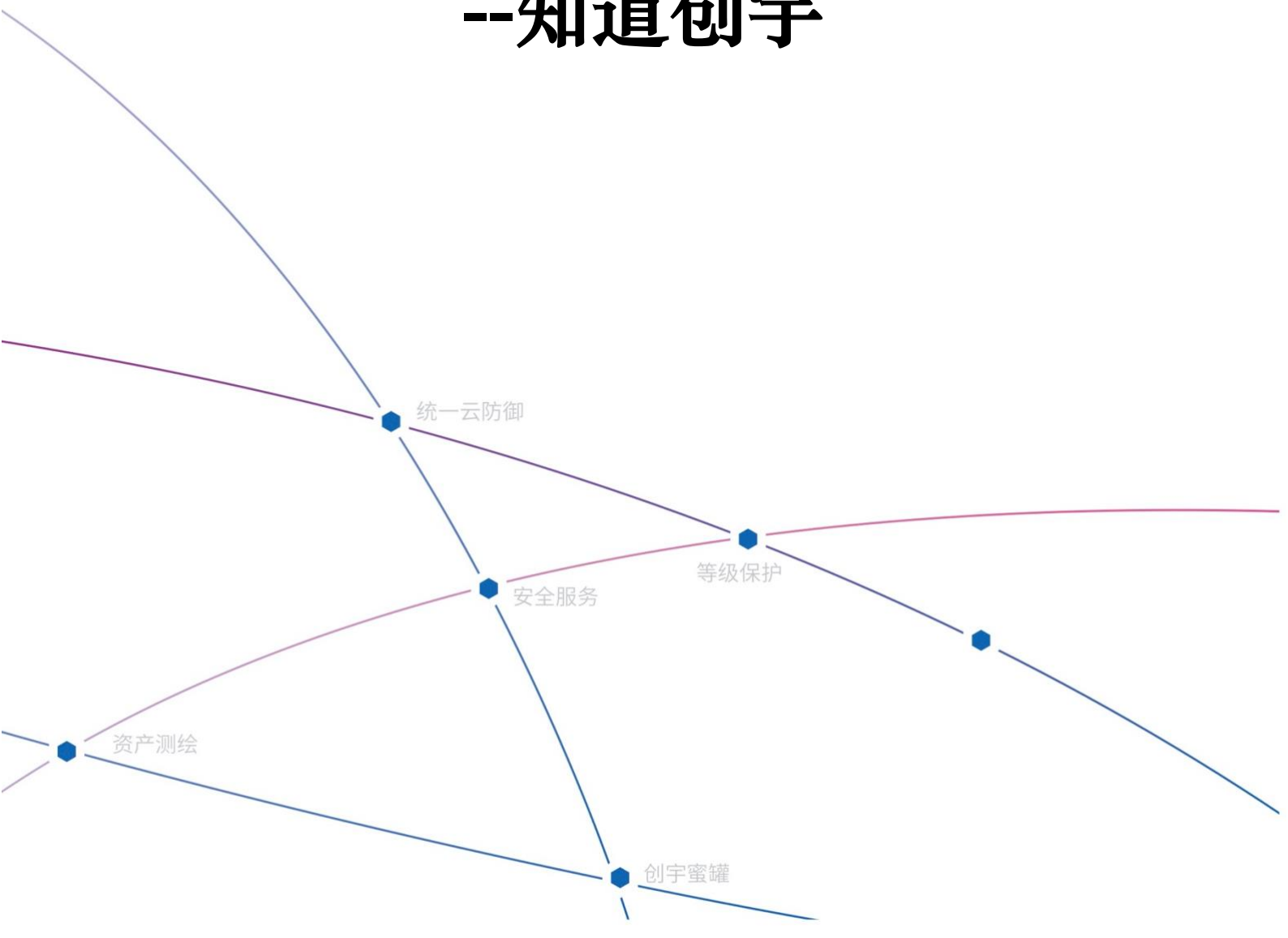
FoFa 使用手册

--知道创宇



文档信息

文档名称	版本号	保密级别
FoFa 使用手册—知道创宇	1.1	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
屈林成	FoFa 使用手册—知道创宇	2021.6.16	1.0	裴文成
裴文成	修订格式	2021.6.19	1.1	马超

版权说明

目录

1. 介绍

随着网络安全的普及，黑客的攻击手段也日新月异，越来越多的企业对网络安全产品与服务的需求有了新的变化。那么，在险象丛生的互联网世界之中企业如何能够更加有效的保护自己的网络空间资产呢？FOFA 给出了相应的解决方案。与传统扫描相比，企业更需要一款能够根据特征、检索条件迅速进行全网资产匹配的搜索引擎。“佛法无边”通常比喻神通广大，无所不能，企业用户终于可以安心的“抱佛脚”了，FOFA 可以迅速进行网站资产匹配，加快后续工作进程，如漏洞影响范围分析，应用分布统计，应用流行度排名统计等。

1.1. 什么是 FOFA

FOFA（网络空间资产检索系统）是世界上数据覆盖更完整的 IT 设备搜索引擎，拥有全球联网 IT 设备更全的 DNA 信息。探索全球互联网的资产信息，进行资产及漏洞影响范围分析、应用分布统计、应用流行度态势感知等。

1.2. 什么是 F 币

F 币，全称 FOFA 币，是由 FOFA 推出的一种虚拟货币。通常它的兑价是 1F 币=10 人民币，用于下载数据一般都是 1F 币=30 元，充值 6 个以上（含 6 个）是 6.7 折，充值 20 个以上（含 20 个）是 5 折。

它可以用来下载数据 :10000 条数据/1F 币 ;也可以调用 API 查询数据 :10000 条数据/1F 币。

1.3. 什么时候能用到 FOFA

- 我想知道我司产品在互联网的部署情况？
- 如何获取一个根域名所有子域名网站？如何根据 IP 确认企业？
- 如何根据一个子域名网站找到跟他在一个 IP 的其他网站？
- 全网漏洞扫描，一个新的漏洞全网的影响范围。

1.4. FOFA 具备哪些优势

- 包括标签在内的 HTML 代码级全文索引和检索，其检索内容更丰富，效果更快速、更精准。
- 预置超过 50000 条产品特征规则，且用户可以随时自行动态增加，灵活度更高。
- 深厚的全网数据积累，同高效的数据检索技术，快速提高用户的网络资产发现能力。
- 实际应用场景中稳定运行超过 4 年，成功部署于各类企业用户的生产环境中，发挥重要作用。

1.5. 会员权益

成为 FOFA 会员可免费查询海量的数据，并拥有稳定的数据资源及丰富的 API 接口，目前 FOFA 会员分普通会员和高级会员，是终身会员。各等级会员区分如下：

https://fofa.so/static_pages/vip。


FOFA
API
会员
登录
选择一个会员以开始使用FOFA
特权与功能
企业会员
立即加入
高级会员
立即加入
普通会员
立即加入
注册用户
立即加入
数据获取
网站查询数据量
10,000条
10,000条
10,000条
50条
API查询数据
免费前100,000条/次
免费前10000条/次
免费前100条/次
1F币（最多10,000条）/次
数据存储时长
30天
14天
7天
获取IP标签接口
获取structinfo数据
一键排除干扰数据
证书有效性提取验证
蜜罐数据提取及分析
仿冒/欺诈数据提取及分析
查询语法
自定义语法查询
正则表达式语法查询
精准匹配icon
模糊匹配icon

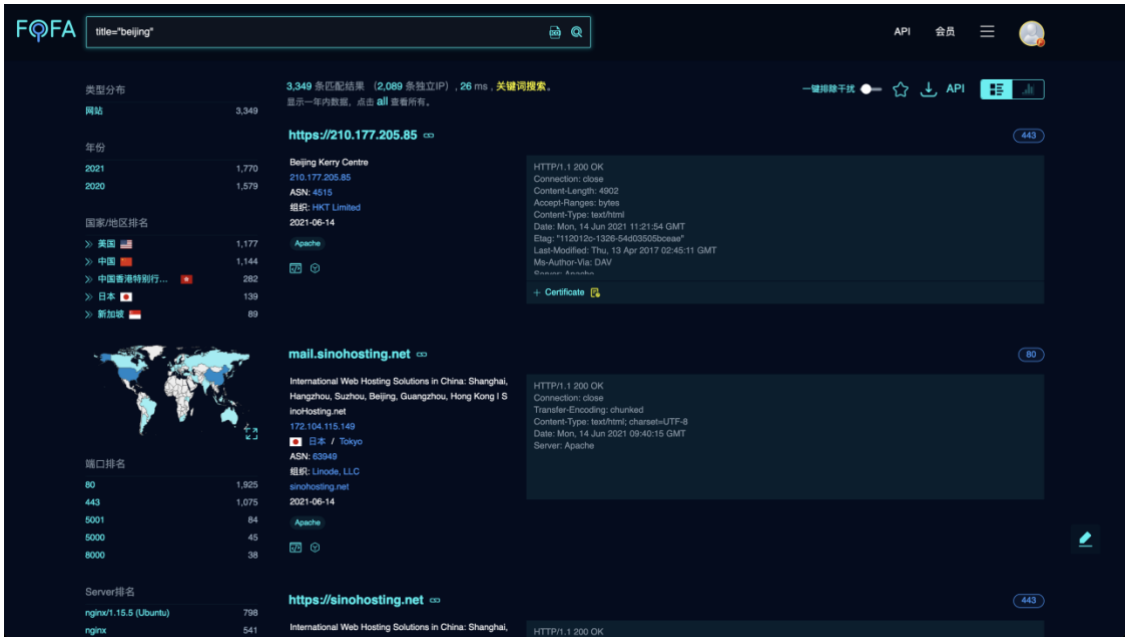
2. 查询语法

FOFA 作为一个搜索引擎，我们要熟悉它的查询语法，类似 google 语法，FOFA 的语法也是简单易懂，主要分为检索字段以及运算符，所有的查询语句都是由这两种元素组成的。

直接输入查询语句，将从标题，html 内容，http 头信息，url 字段中搜索

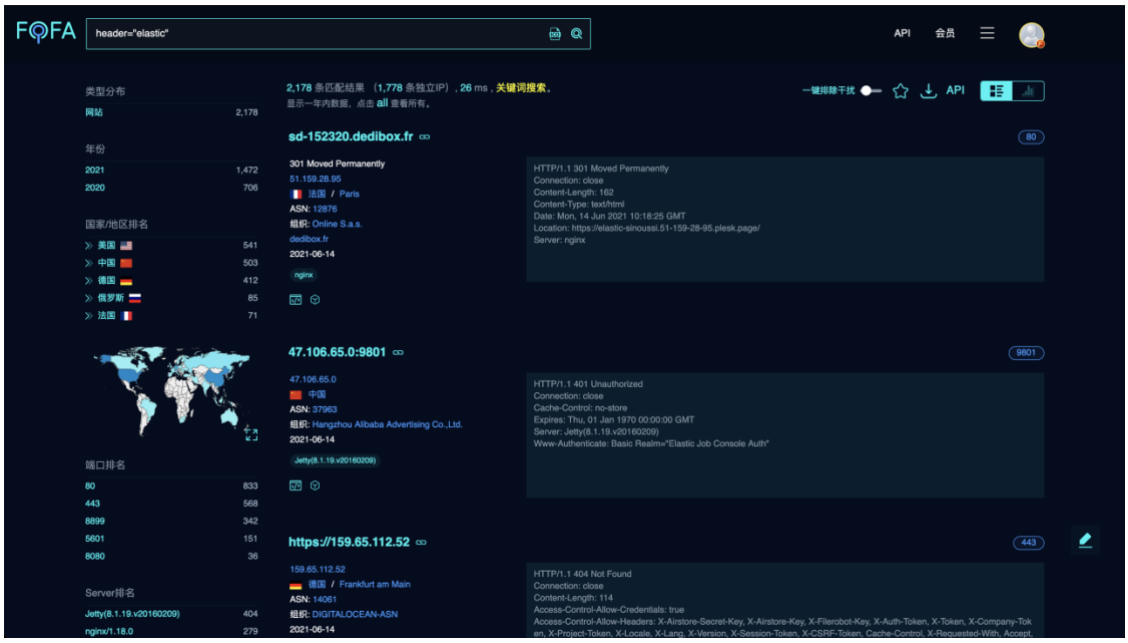
2.1. 从标题中搜索“北京”

title="beijing"



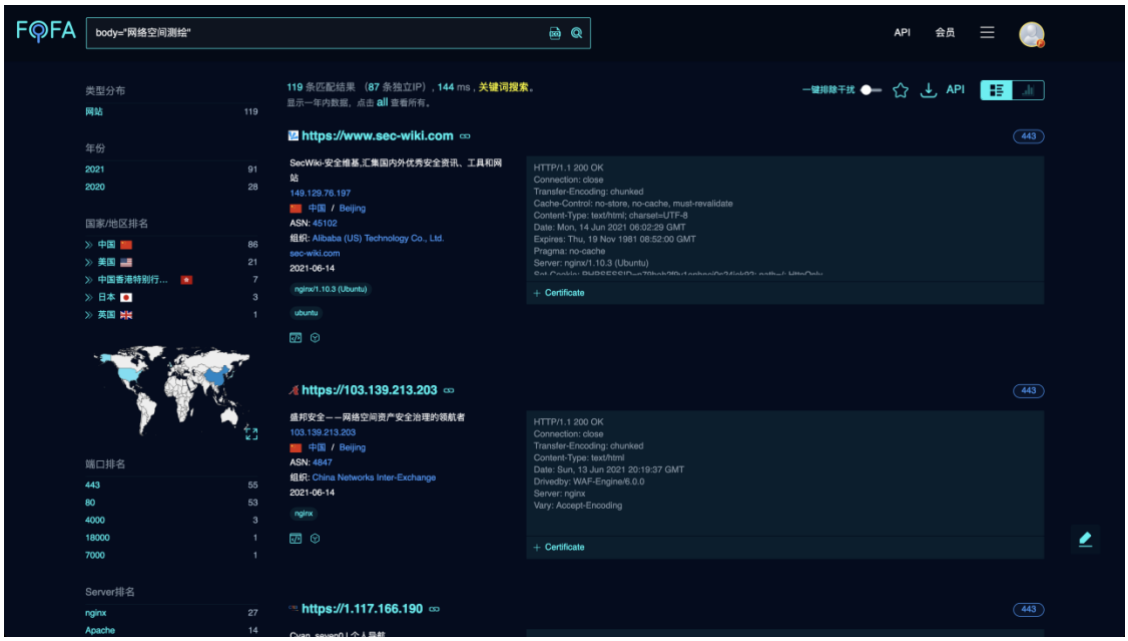
2.2. 从 http 头中搜索“elastic”

header="elastic"



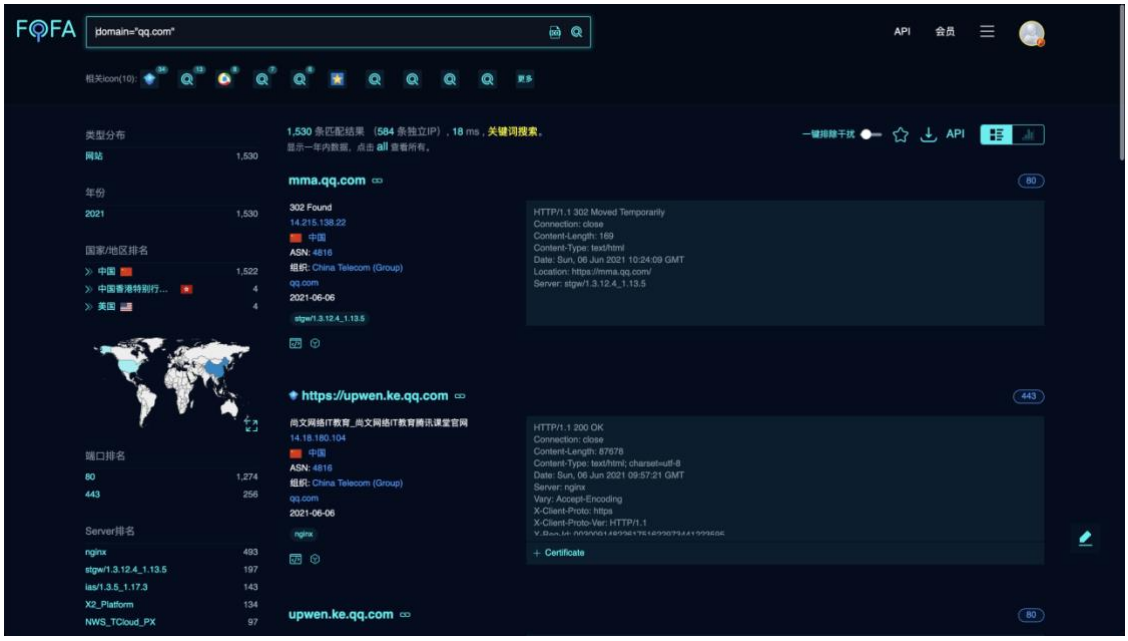
2.3. 从 html 正文中搜索“网络空间测绘”

body="网络空间测绘"



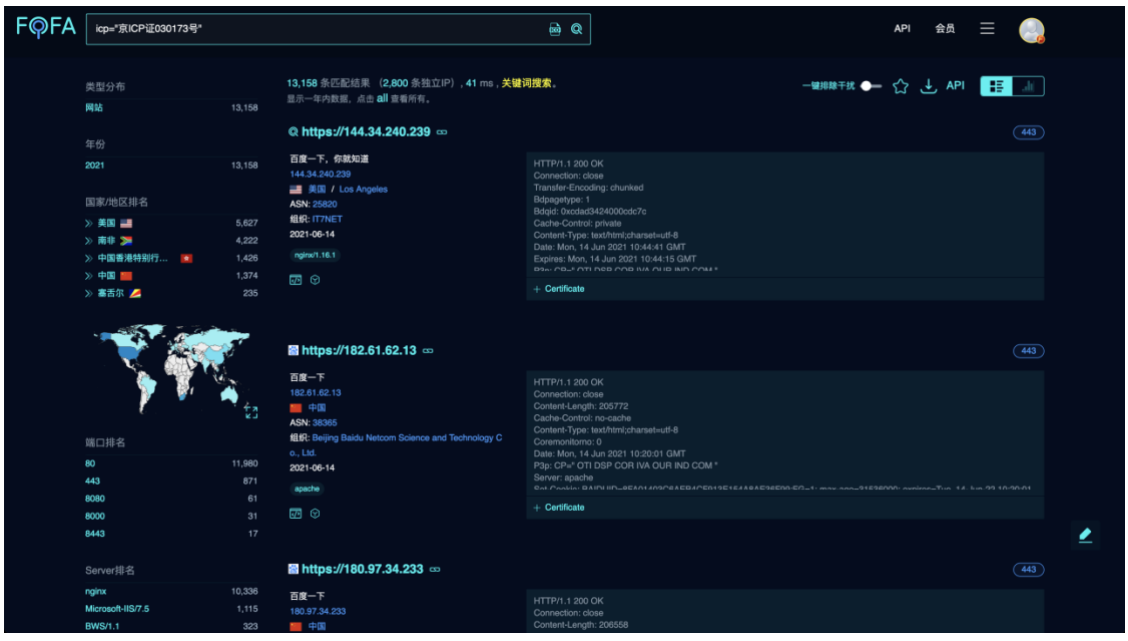
2.4. 搜索根域名带有 qq.com 的网站

domain="qq.com"



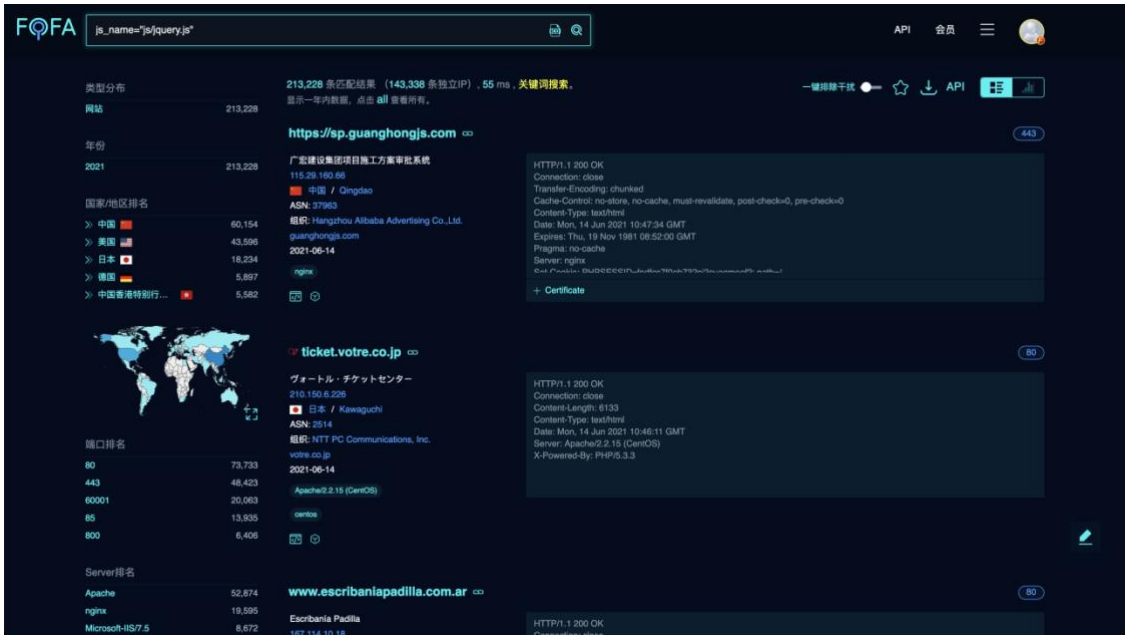
2.5. 查找备案号为“京 ICP 证 030173 号”的网站

icp="京 ICP 证 030173 号"



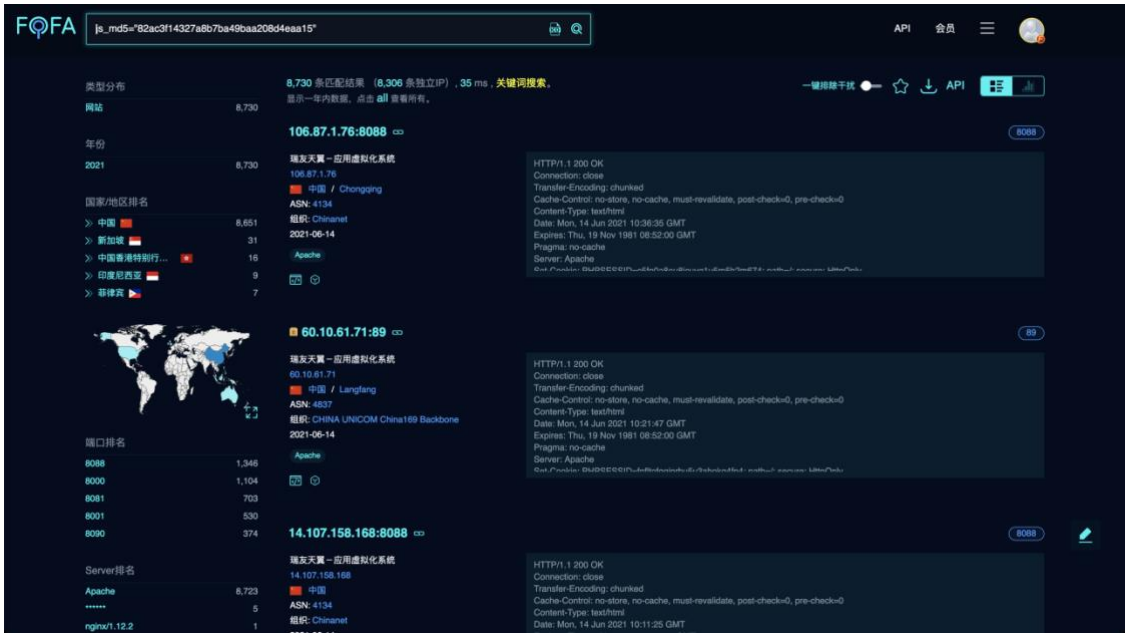
2.6. 查找网站正文中包含 js/jquery.js 的资产

js_name="js/jquery.js"



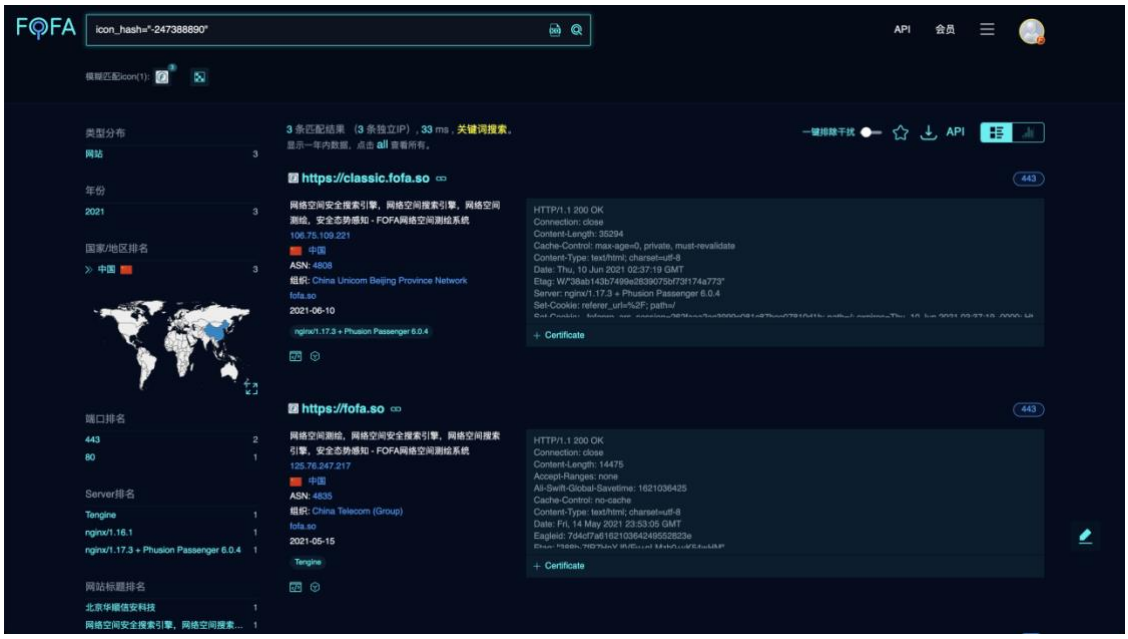
2.7. 查找 js 源码与之匹配的资产

js_md5="82ac3f14327a8b7ba49baa208d4eaa15"



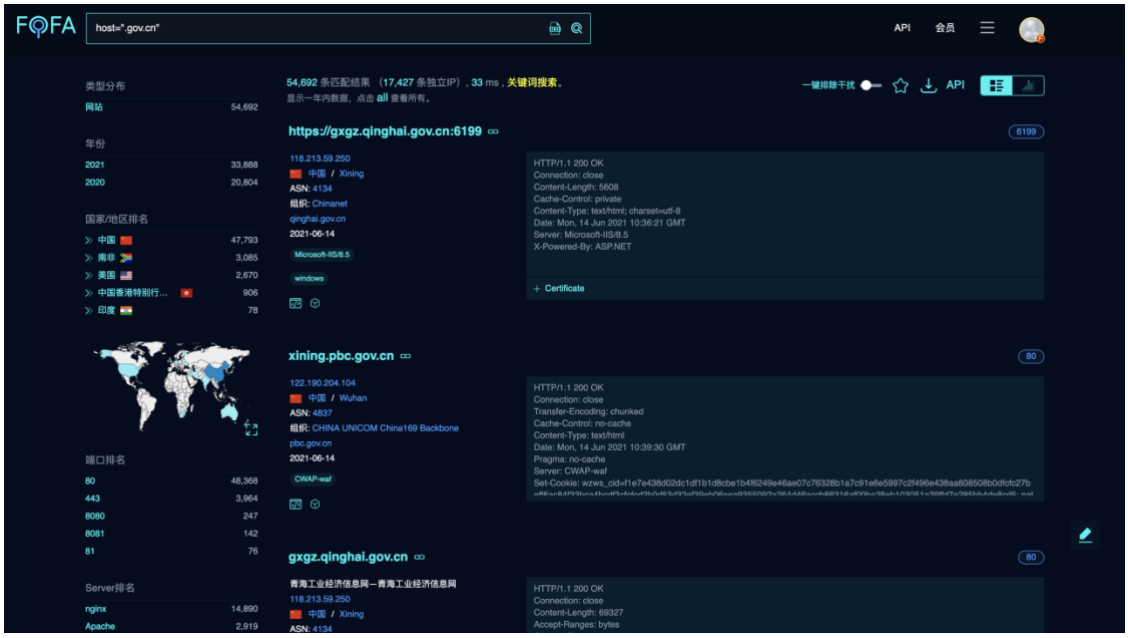
2.8. 搜索使用此 icon 的资产。

icon_hash="-247388890"



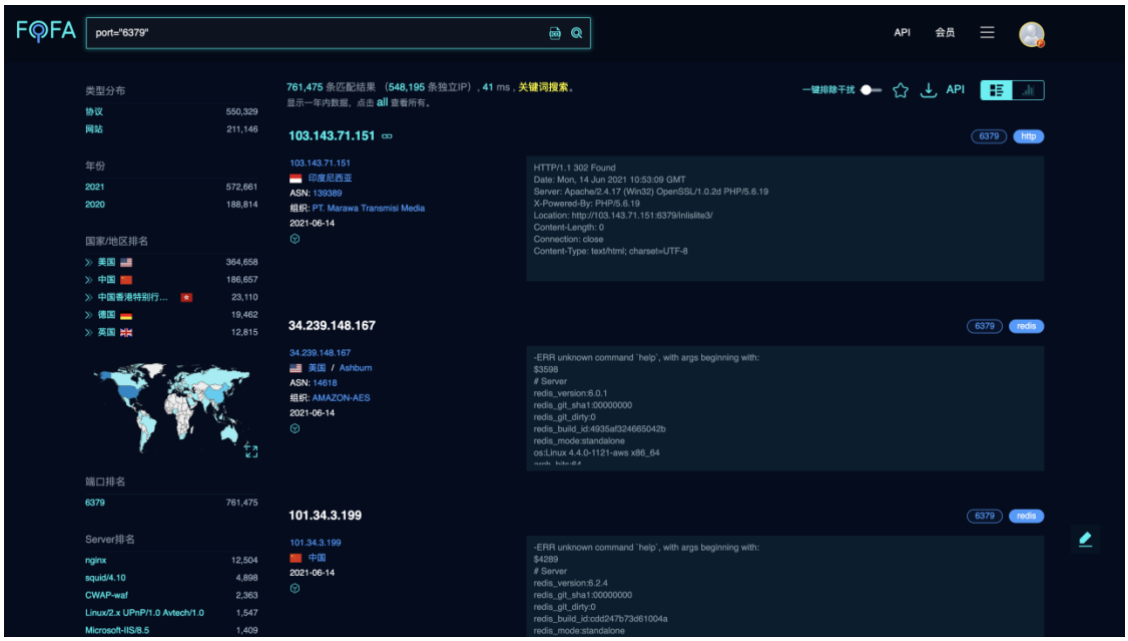
2.9. 从 url 中搜索”.gov.cn”

host=".gov.cn"



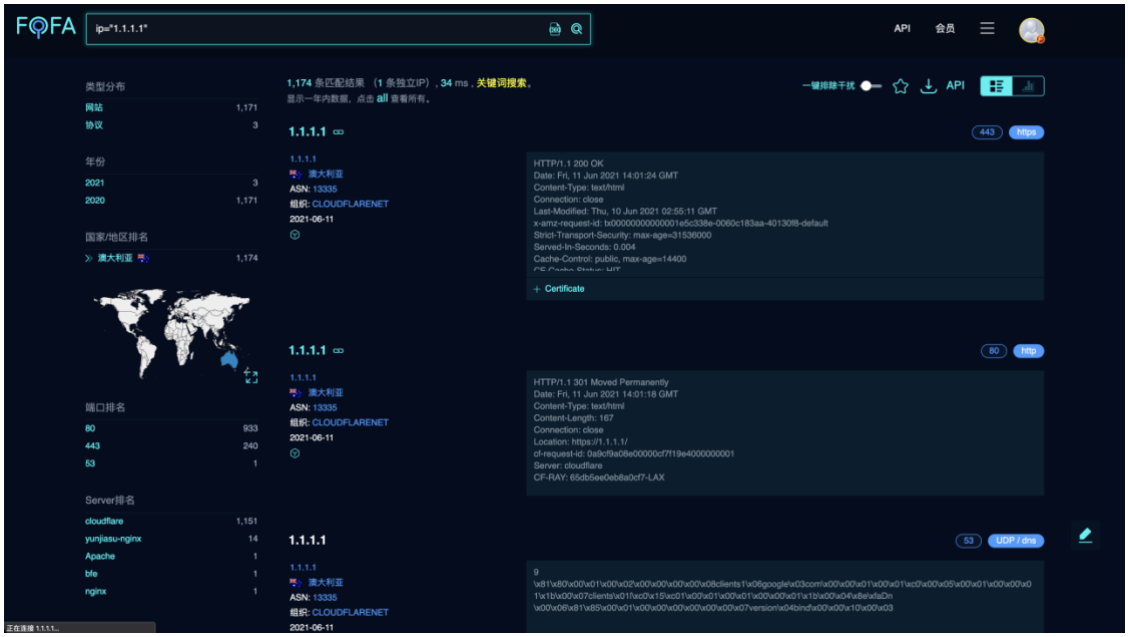
2.10. 查找对应“6379”端口的资产

port="6379"



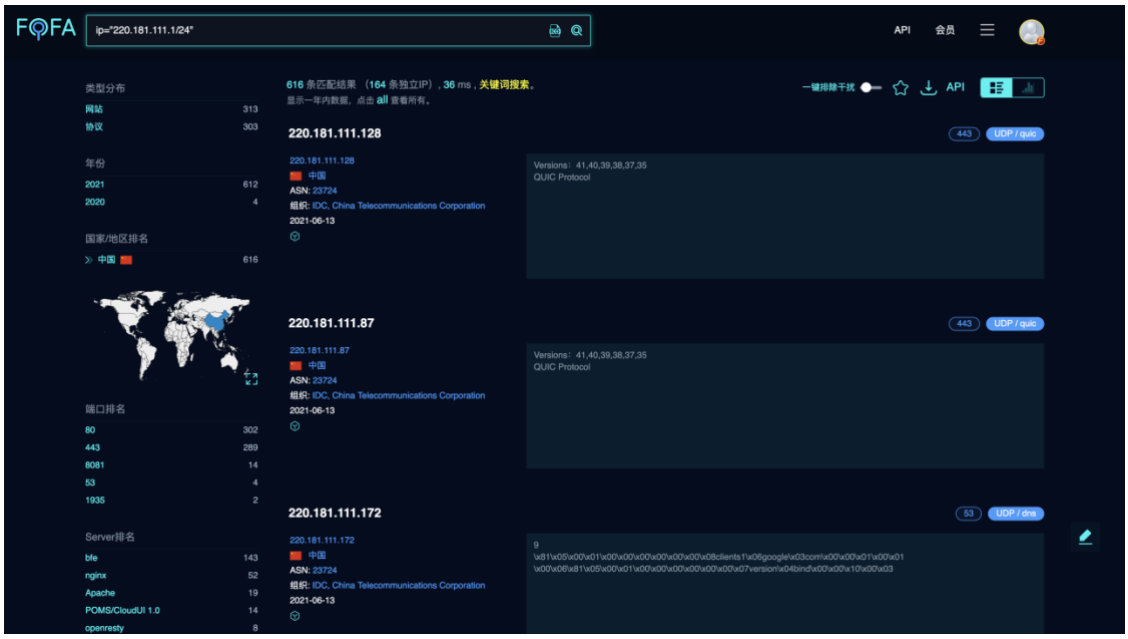
2.11. 从 ip 中搜索包含“1.1.1.1”的网站

ip="1.1.1.1"



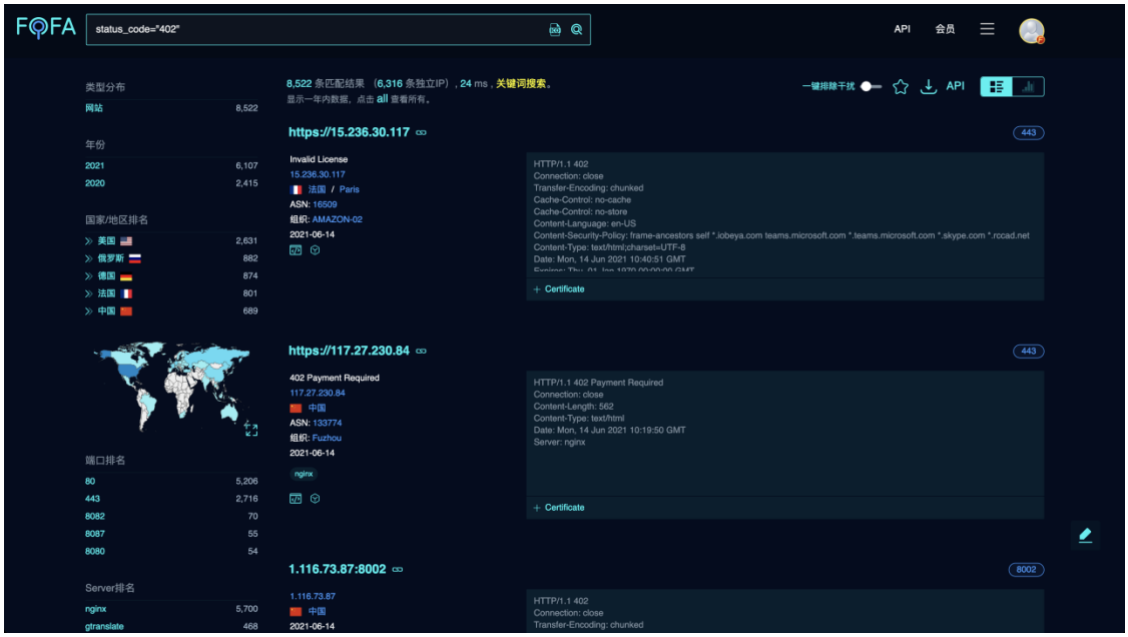
2.12. 查询 IP 为“220.181.111.1”的 C 网段资产

ip="220.181.111.1/24"



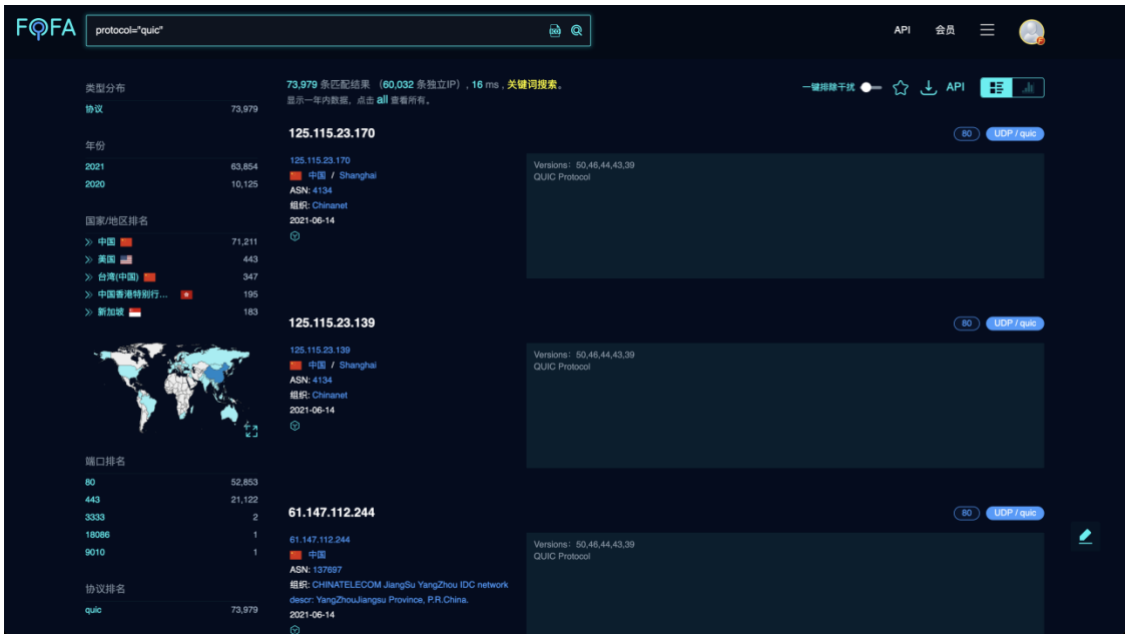
2.13. 查询服务器状态为“402”的资产

status_code="402"



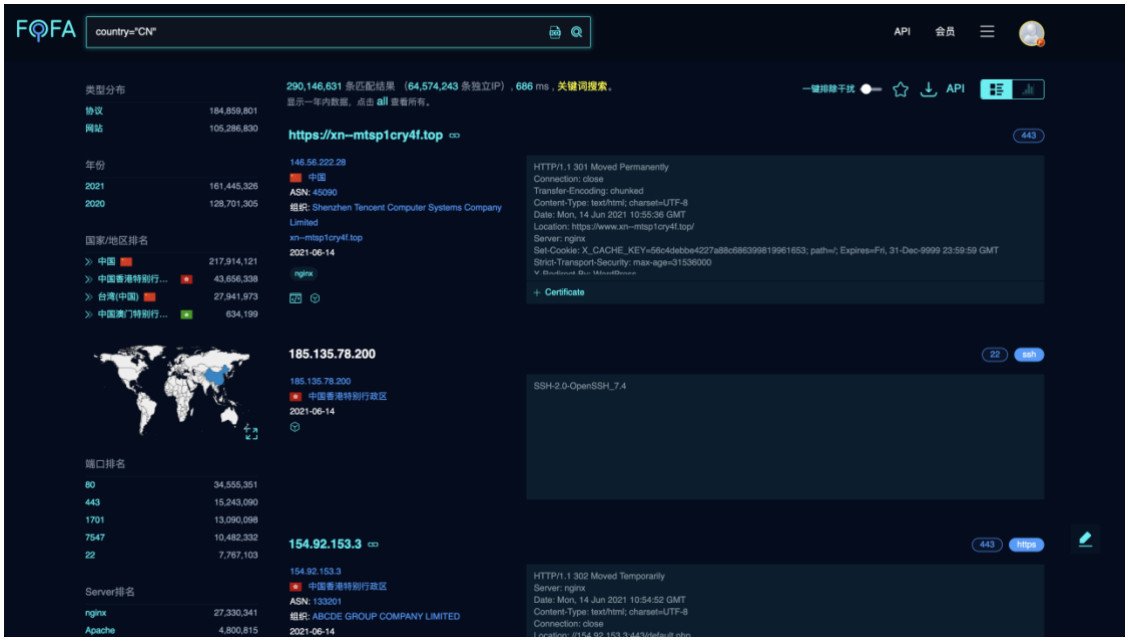
2.14. 查询 quic 协议资产

protocol="quic"



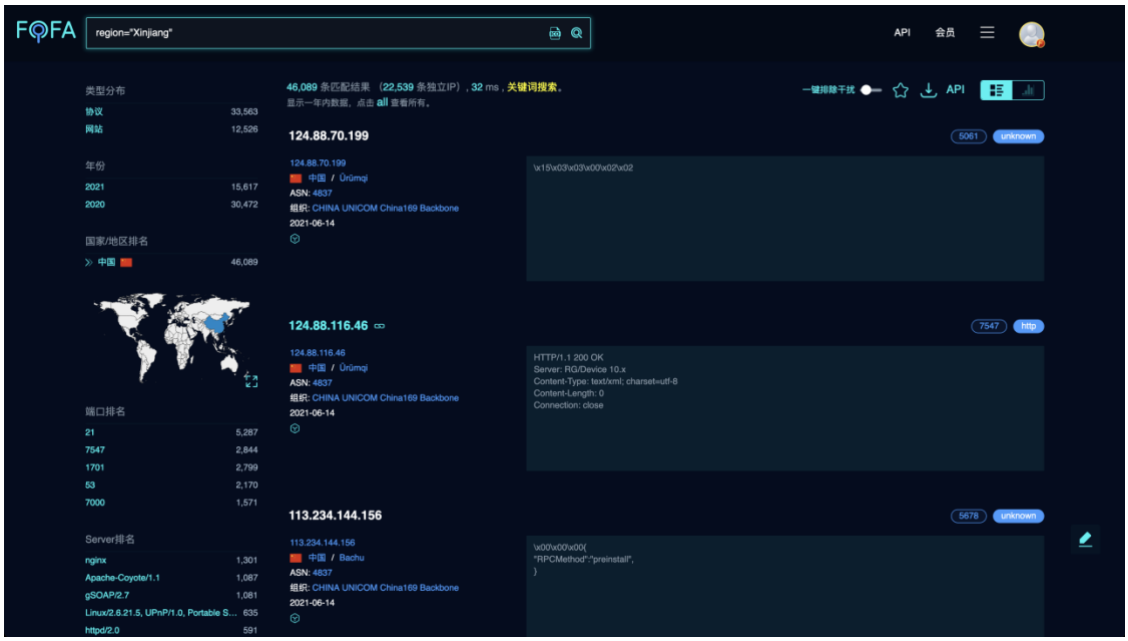
2.15. 搜索指定国家(编码)的资产。

country="CN"



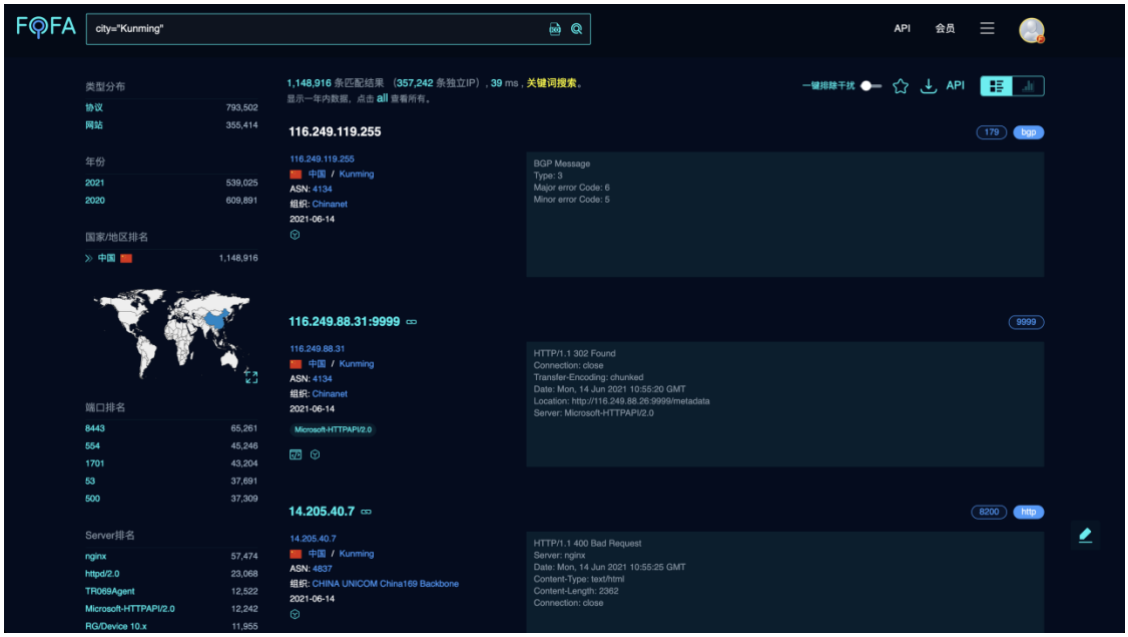
2.16. 搜索指定行政区的资产。

region="Xinjiang"



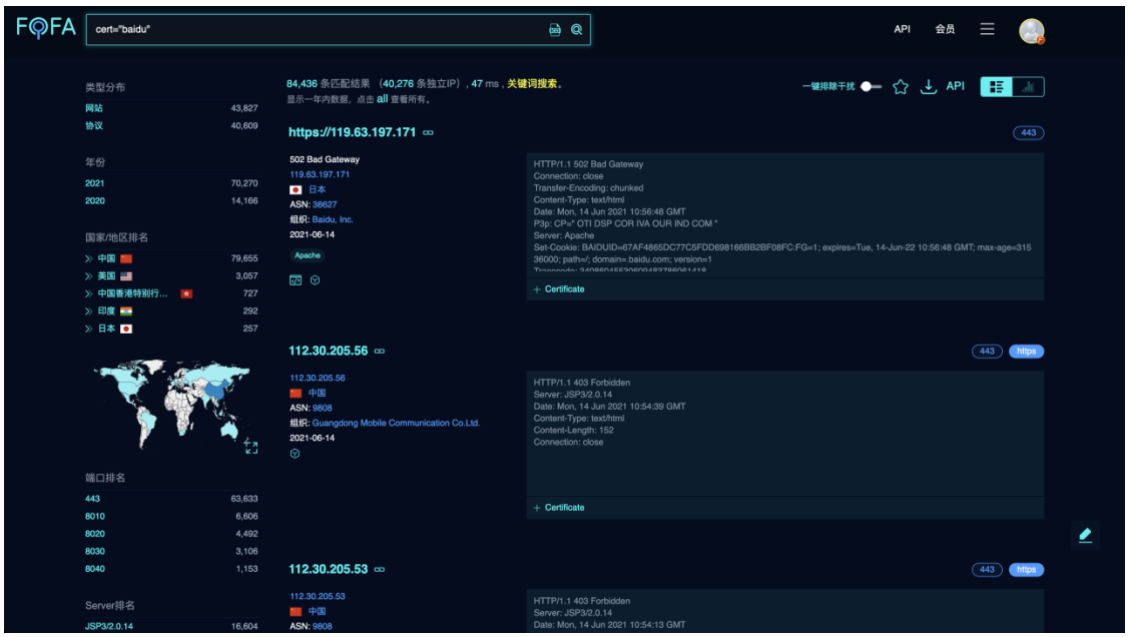
2.17. 搜索指定城市的资产。

city="Kunming"



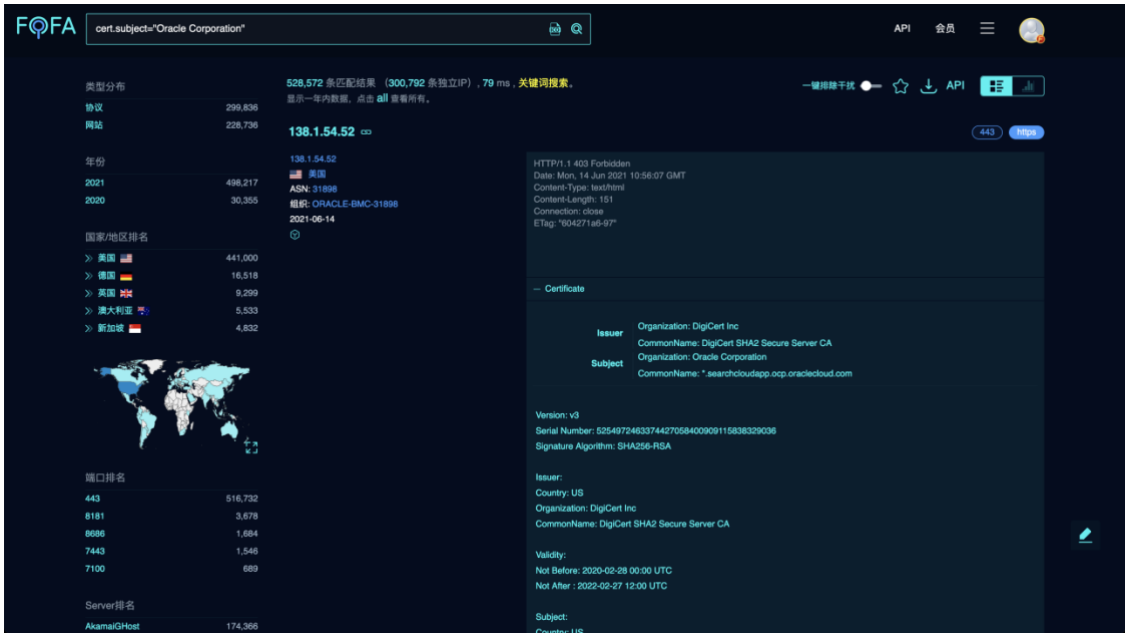
2.18. 搜索证书(https 或者 imaps 等)中带有 baidu 的资产。

cert="baidu"



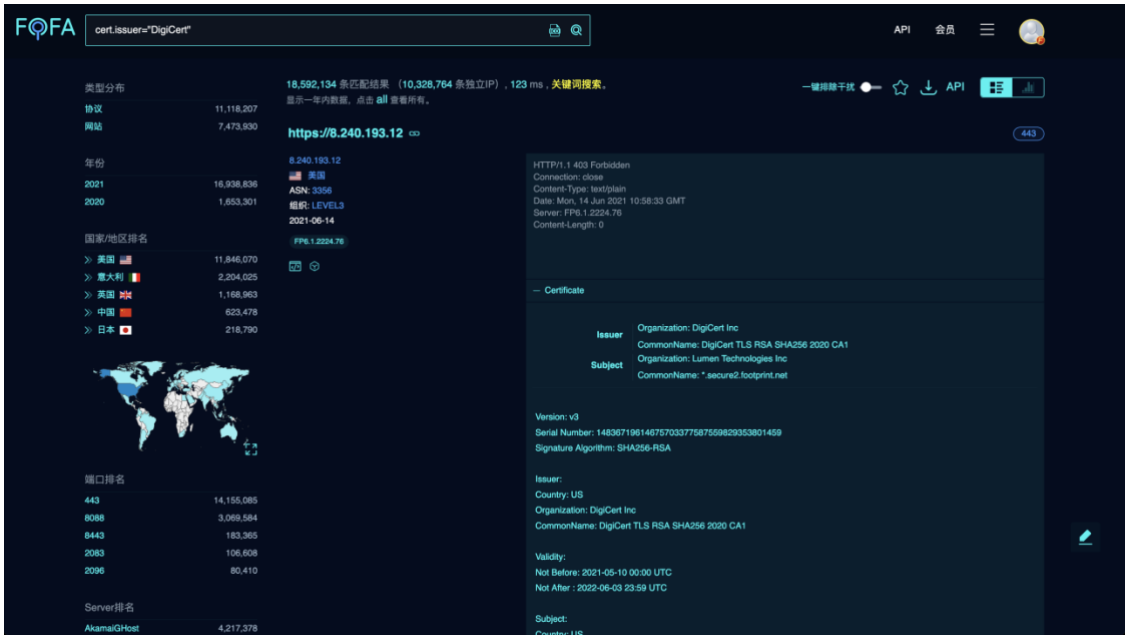
2.19. 搜索证书持有者是 Oracle Corporation 的资产

cert.subject="Oracle Corporation"



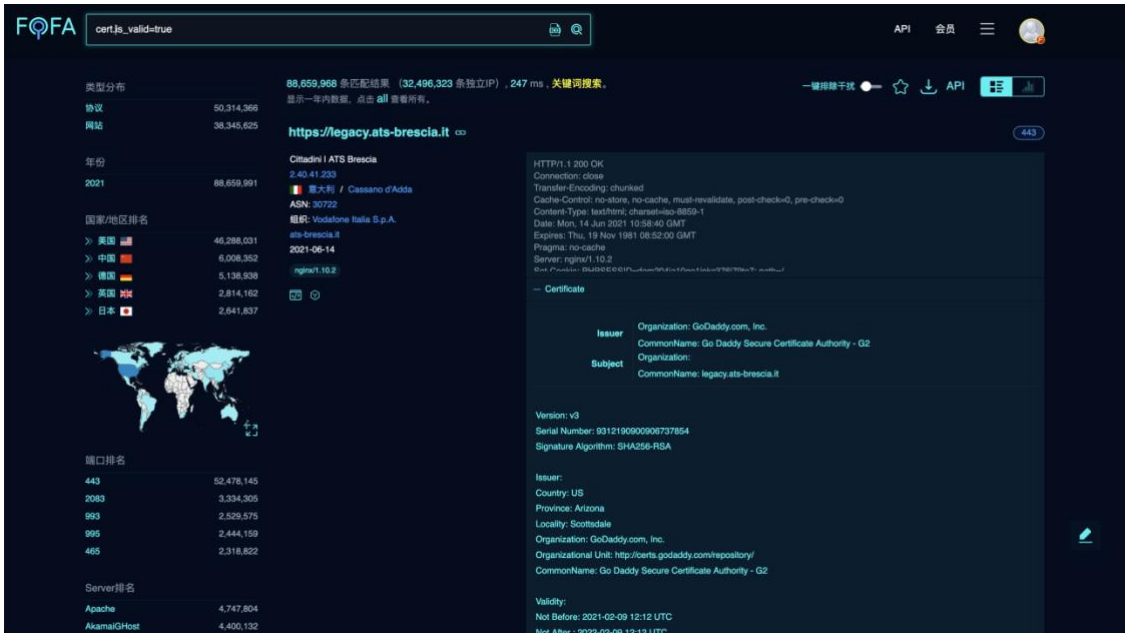
2.20. 搜索证书颁发者为 DigiCert Inc 的资产

cert.issuer="DigiCert"



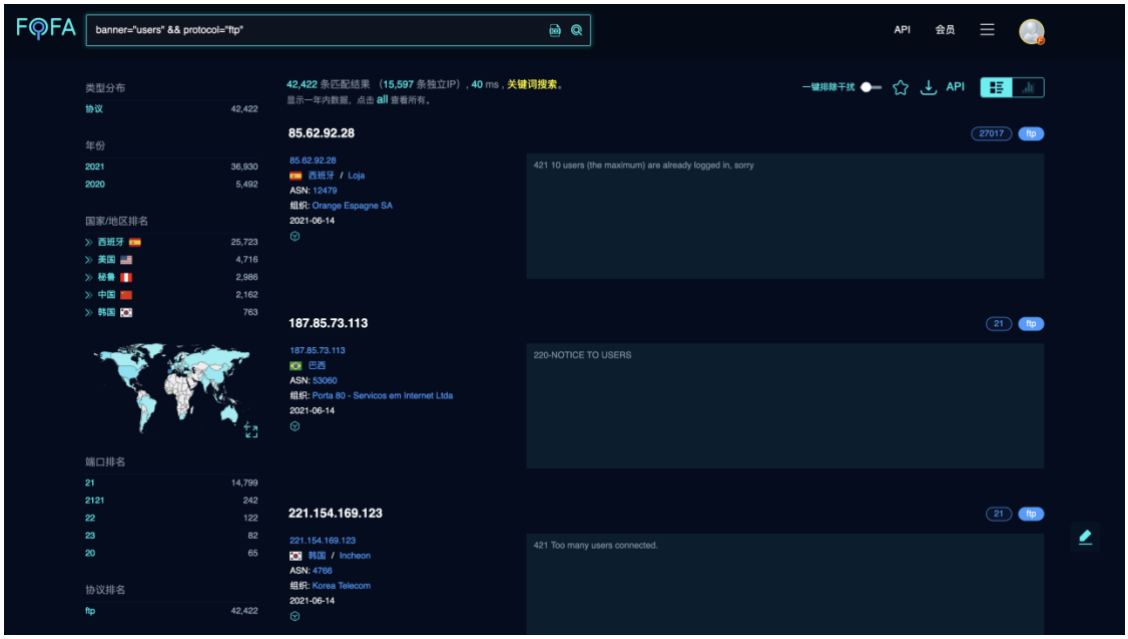
2.21. 验证证书是否有效，true 有效，false 无效

cert.is_valid=true



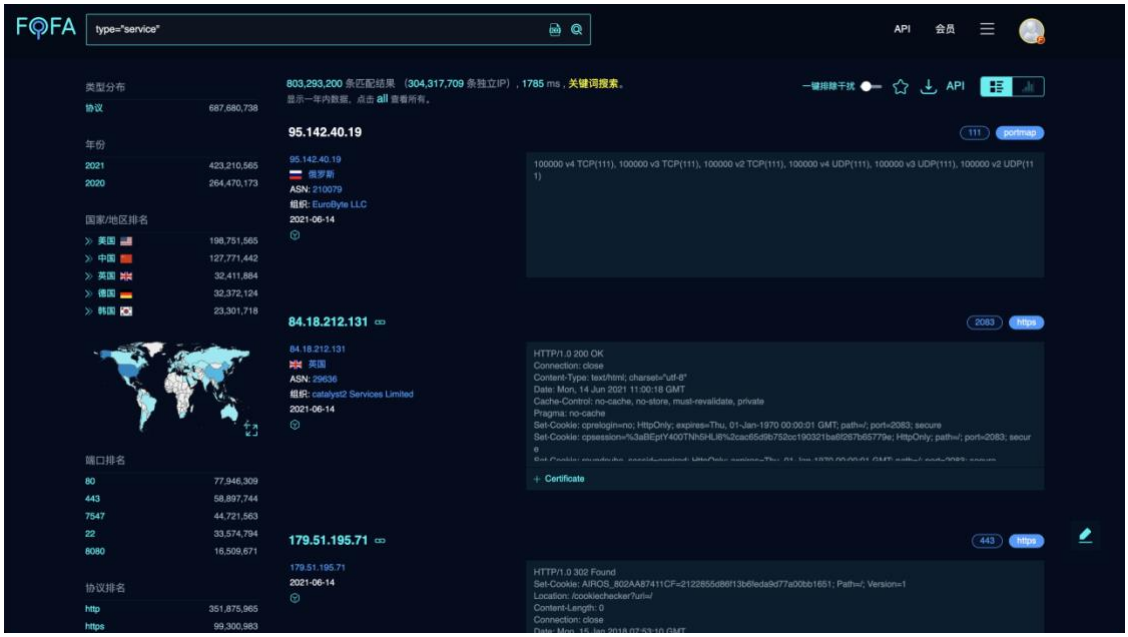
2.22. 搜索 FTP 协议中带有 users 文本的资产。

banner=users && protocol=ftp



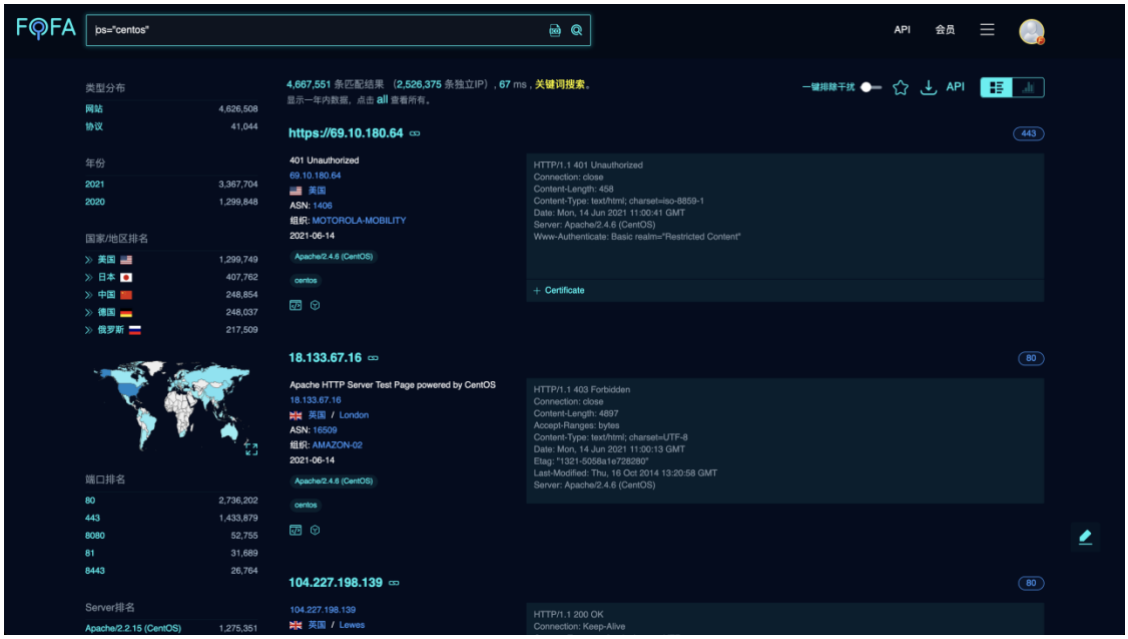
2.23. 搜索所有协议资产，支持 subdomain 和 service 两种

type=service



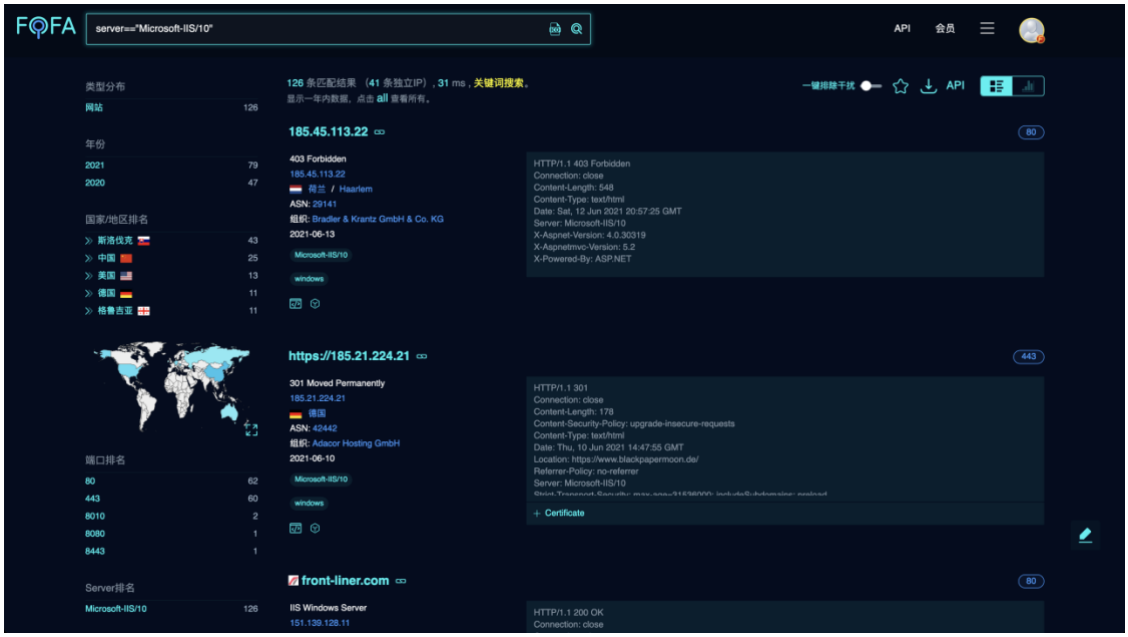
2.24. 搜索 CentOS 资产。

os="centos"



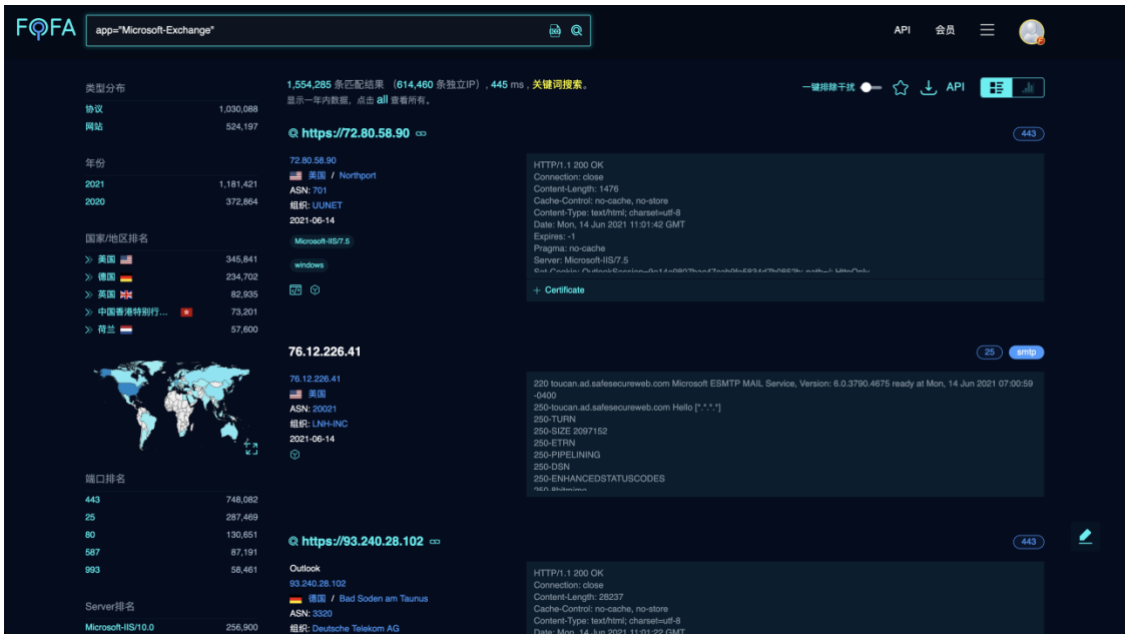
2.25. 搜索 IIS 10 服务器。

server=="Microsoft-IIS/10"



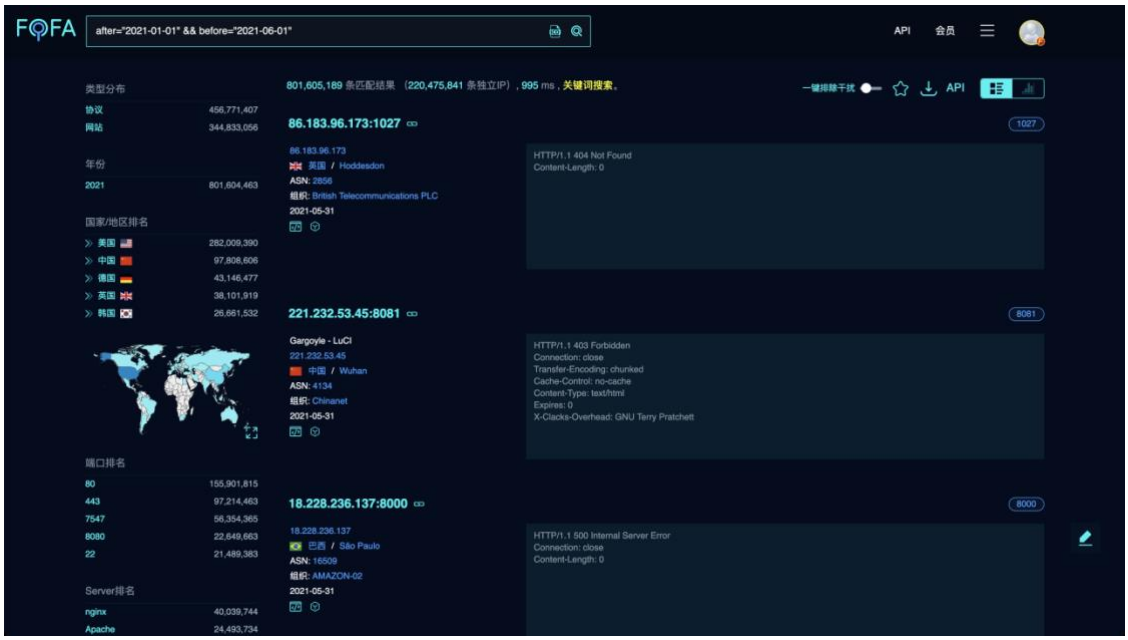
2.26. 搜索 Microsoft-Exchange 设备

app="Microsoft-Exchange"



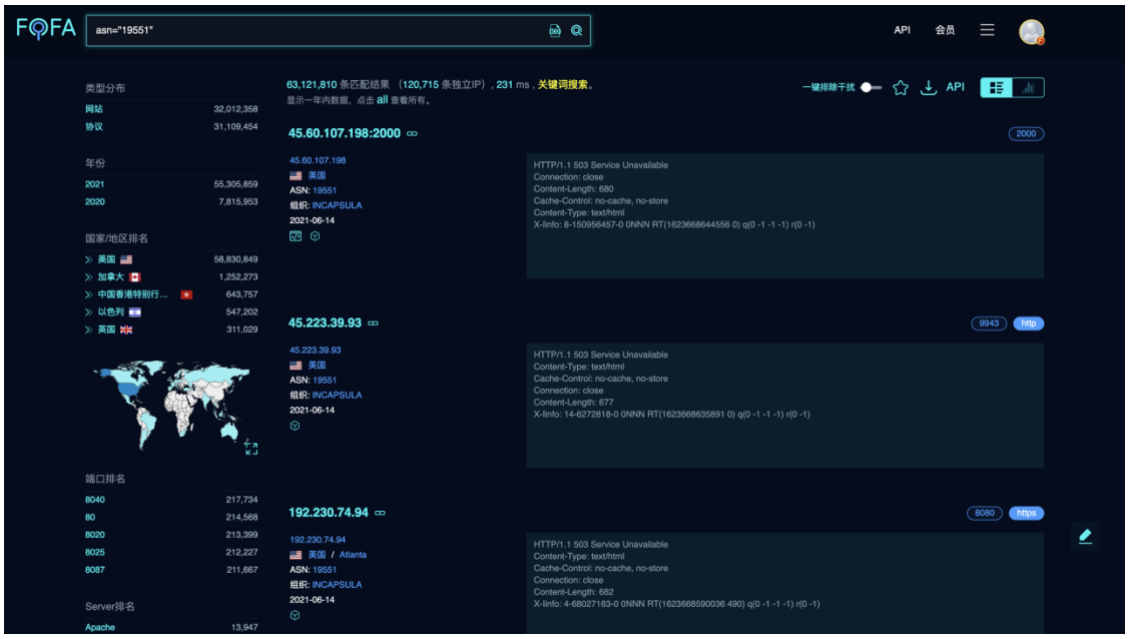
2.27. 时间范围段搜索

after="2021" && before="2021-06-01"



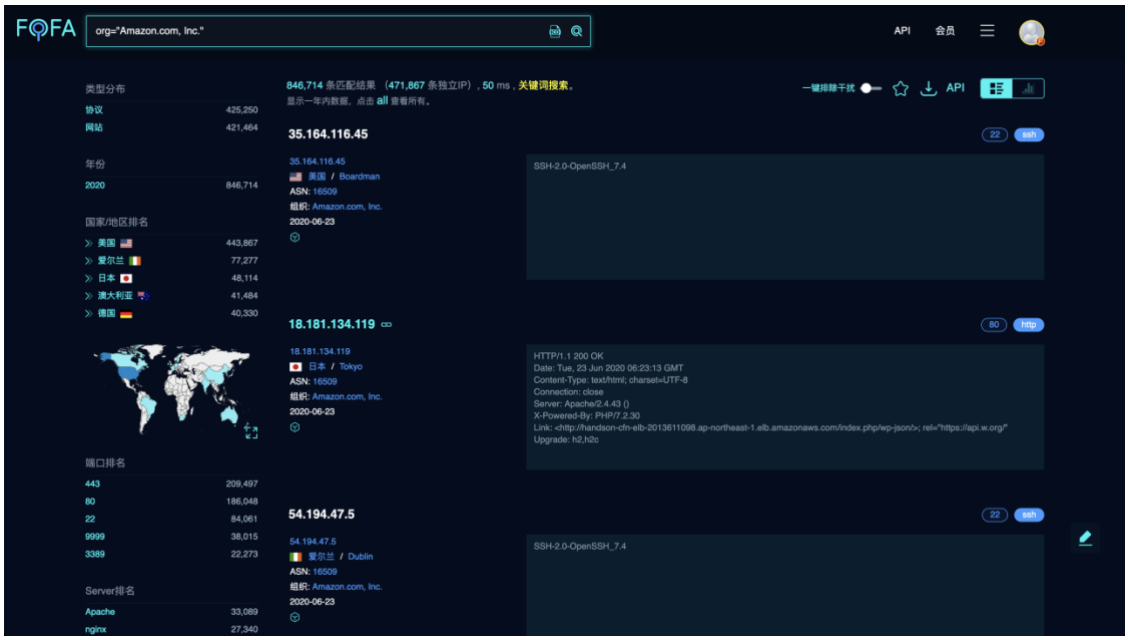
2.28. 搜索指定 asn 的资产。

asn="19551"



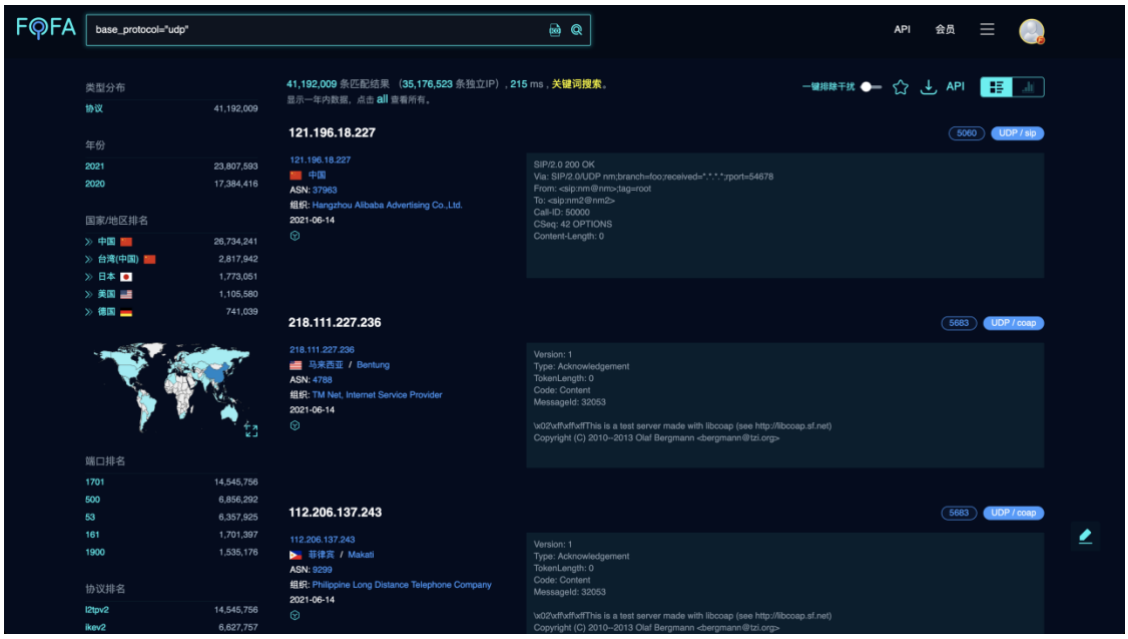
2.29. 搜索指定 org(组织)的资产。

org="Amazon.com, Inc."



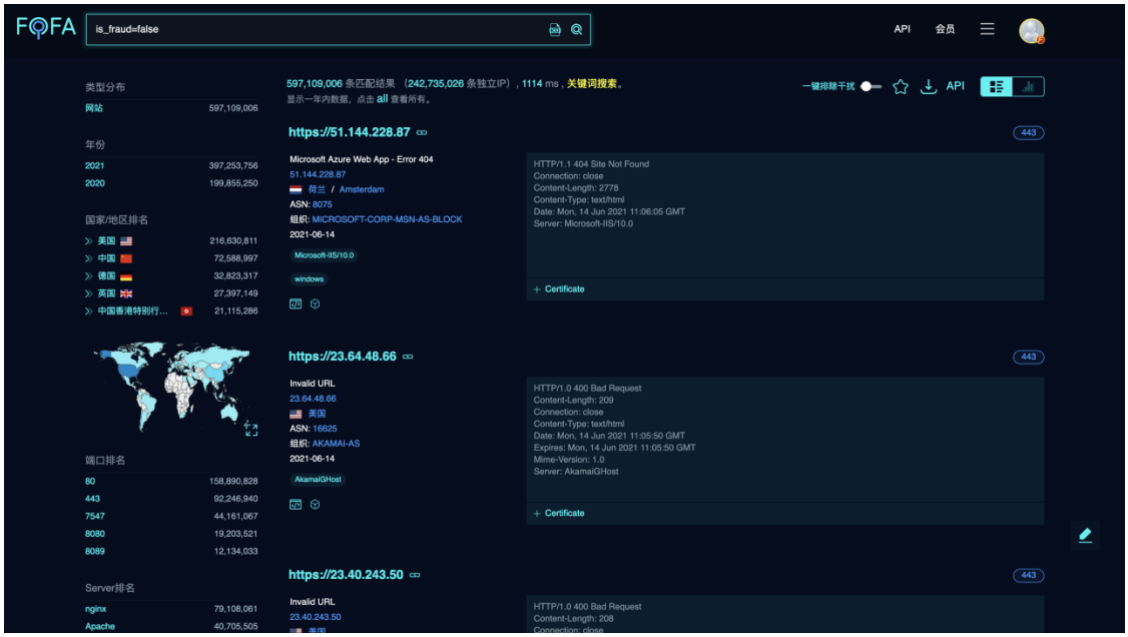
2.30. 搜索指定 udp 协议的资产。

base_protocol="udp"



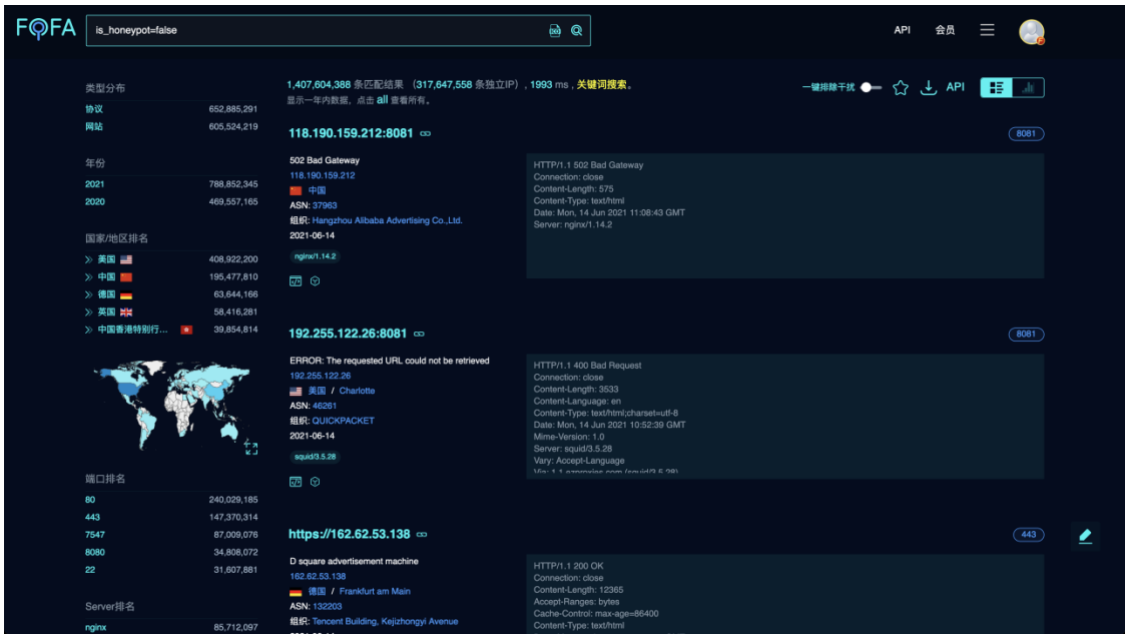
2.31. 排除仿冒/欺诈数据

is_fraud=false



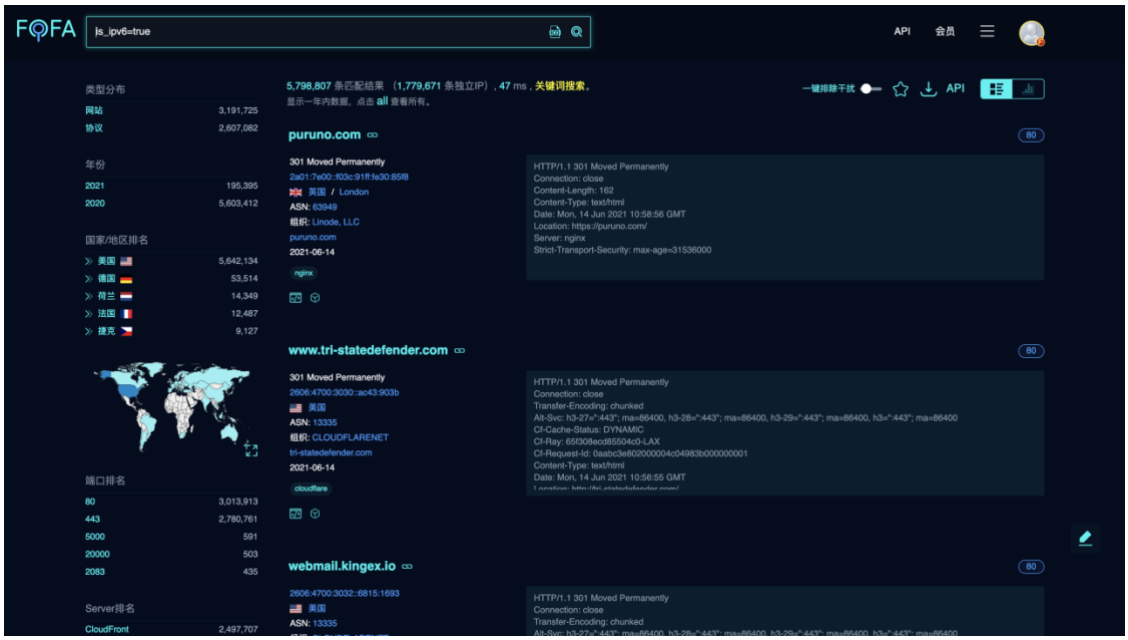
2.32. 排除蜜罐数据

is_honeypot=false



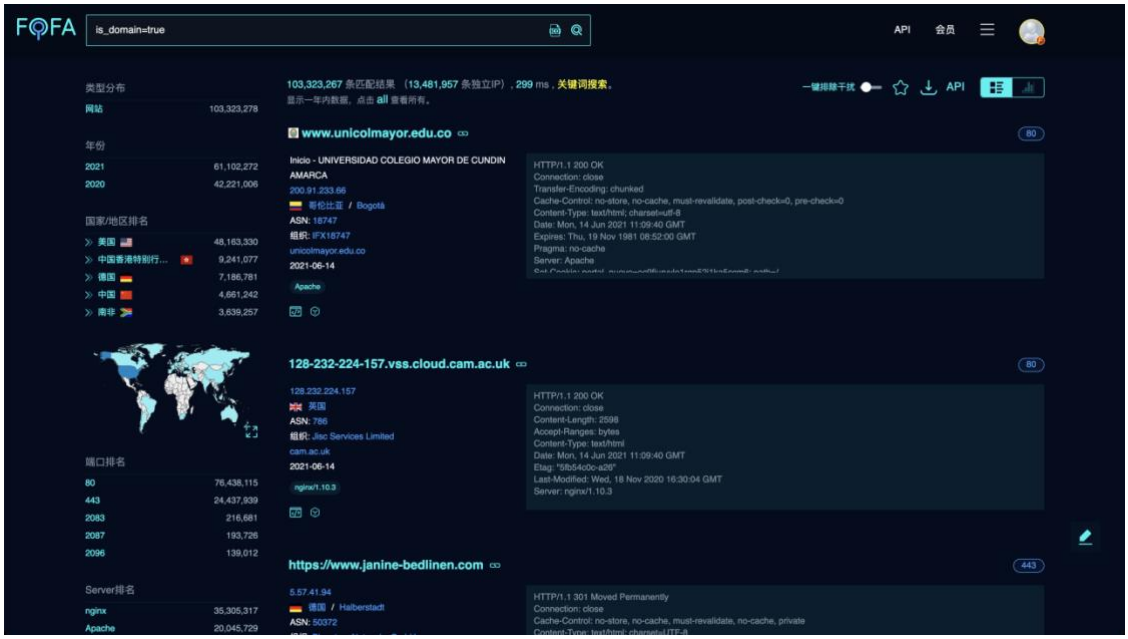
2.33. 搜索 ipv6 的资产

is_ipv6=true



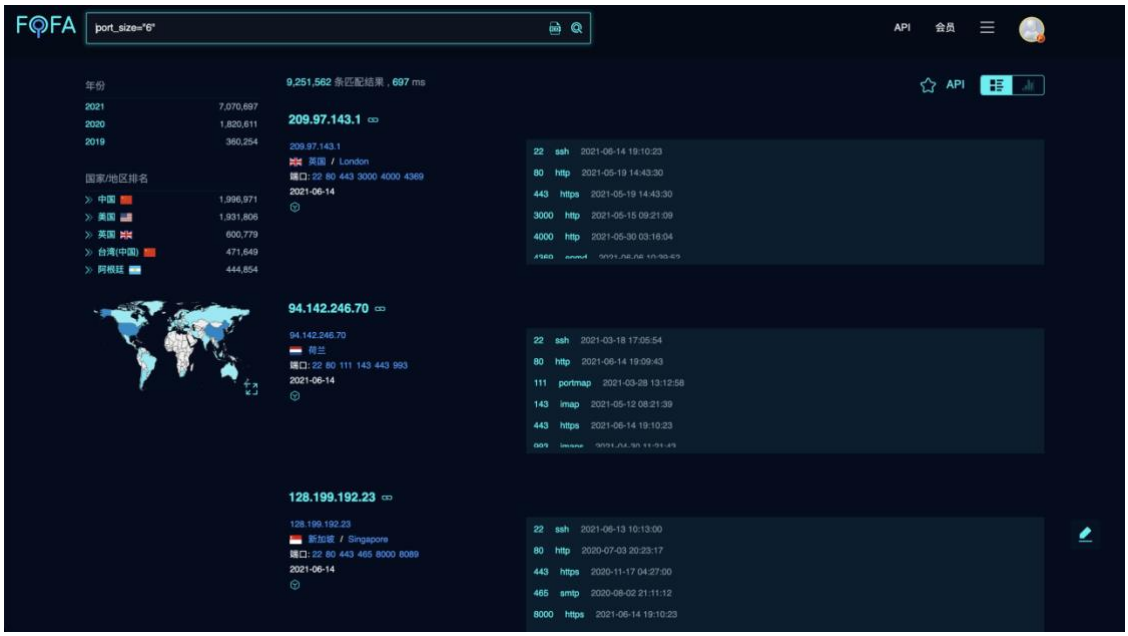
2.34. 搜索域名的资产

is_domain=true



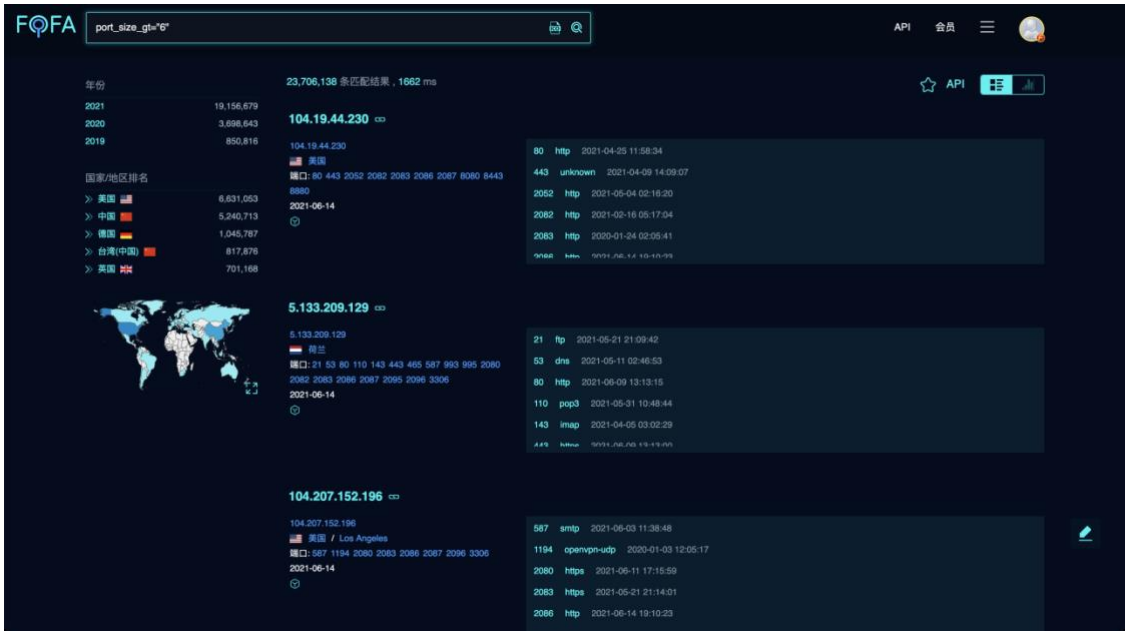
2.35. 查询开放端口数量等于"6"的资产

port_size="6"



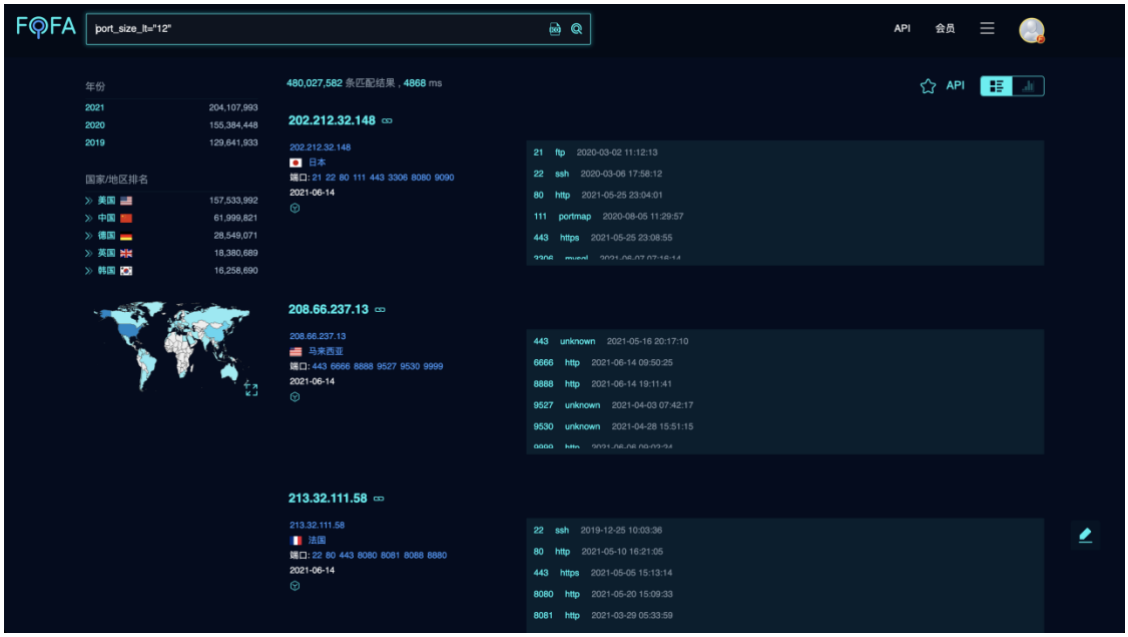
2.36. 查询开放端口数量大于"6"的资产

port_size_gt="6"



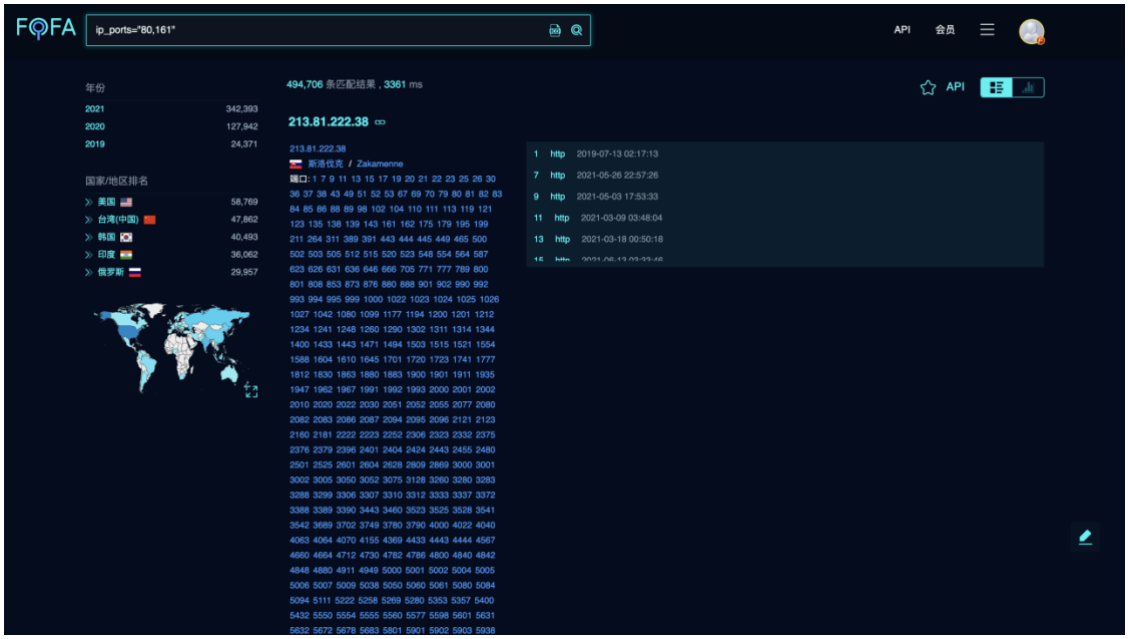
2.37. 查询开放端口数量小于"12"的资产

port_size_lt="12"



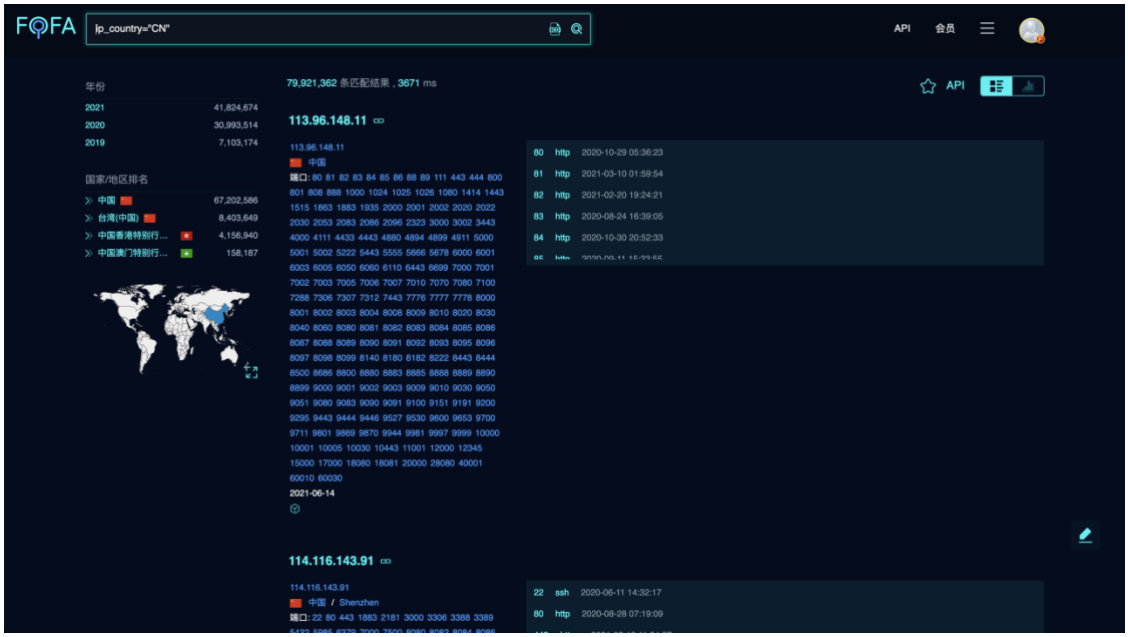
2.38. 搜索同时开放 80 和 161 端口的 ip

ip_ports="80,161"



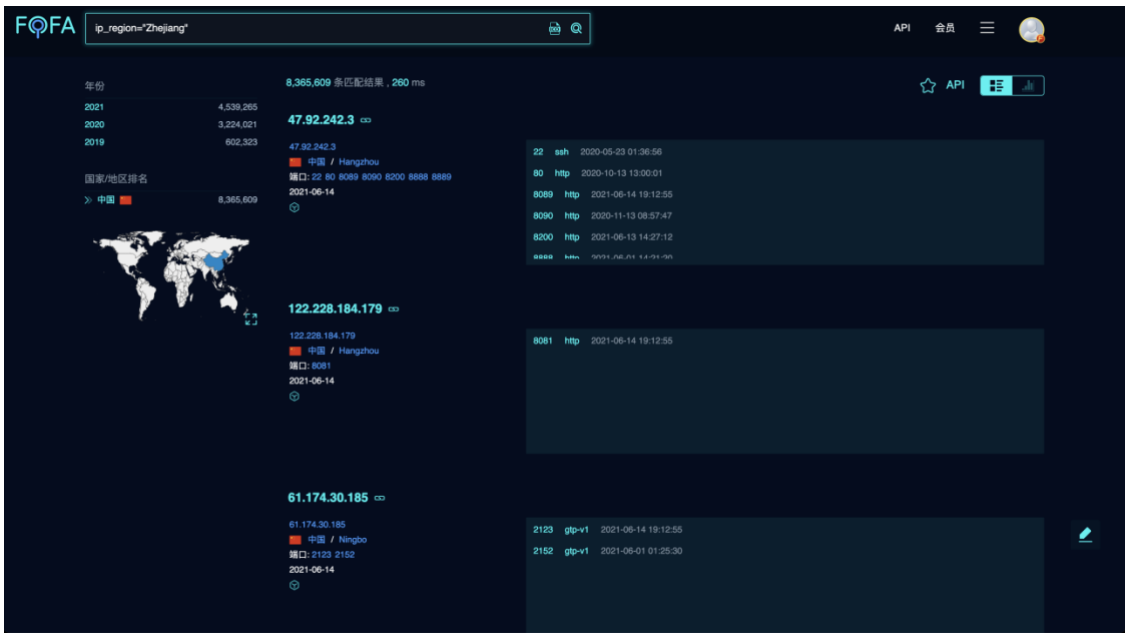
2.39. 搜索中国的 ip 资产(以 ip 为单位的资产数据)。

ip_country="CN"



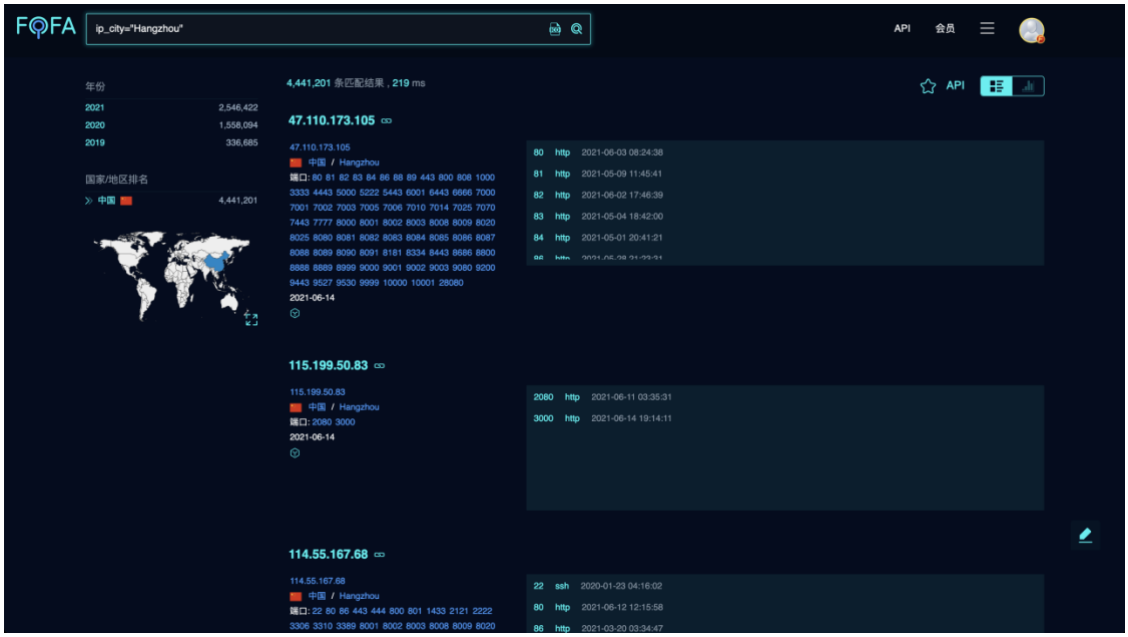
2.40. 搜索指定行政区的 ip 资产(以 ip 为单位的资产数据)。

ip_region="Zhejiang"



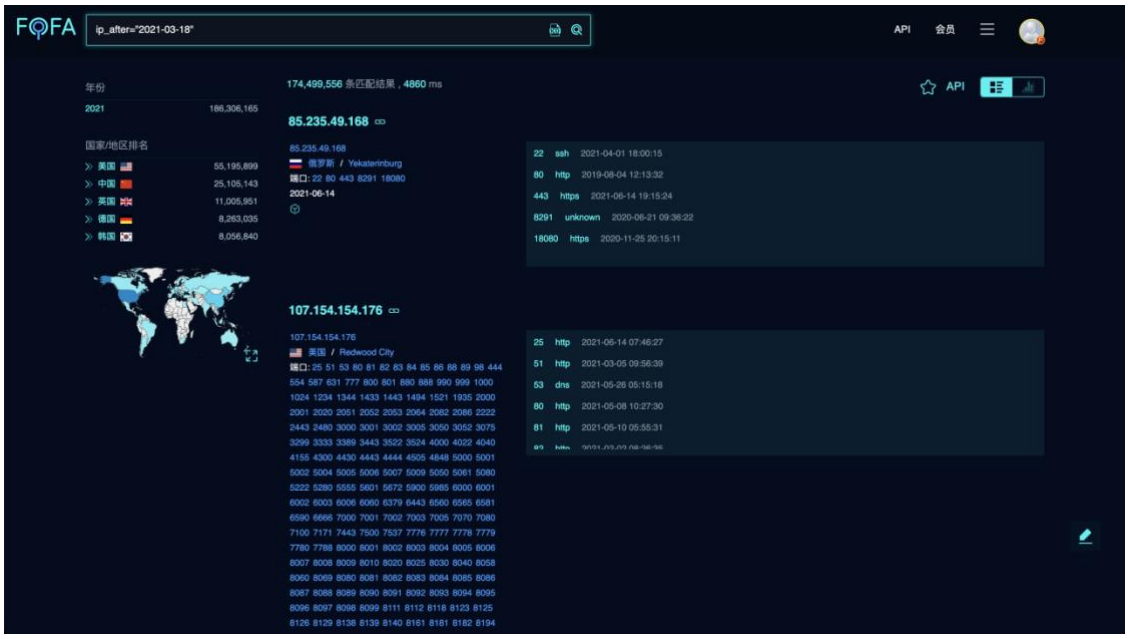
2.41. 搜索指定城市的 ip 资产(以 ip 为单位的资产数据)。

ip_city="Hangzhou"



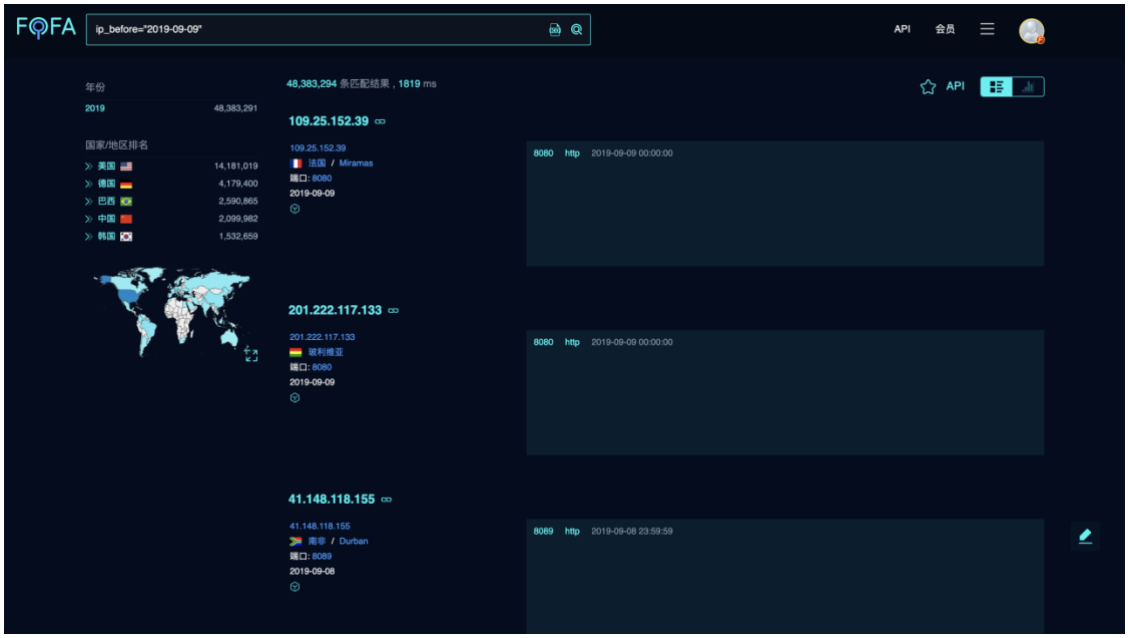
2.42. 搜索 2021-03-18 以后的 ip 资产(以 ip 为单位的资产数据)。

ip_after="2021-03-18"



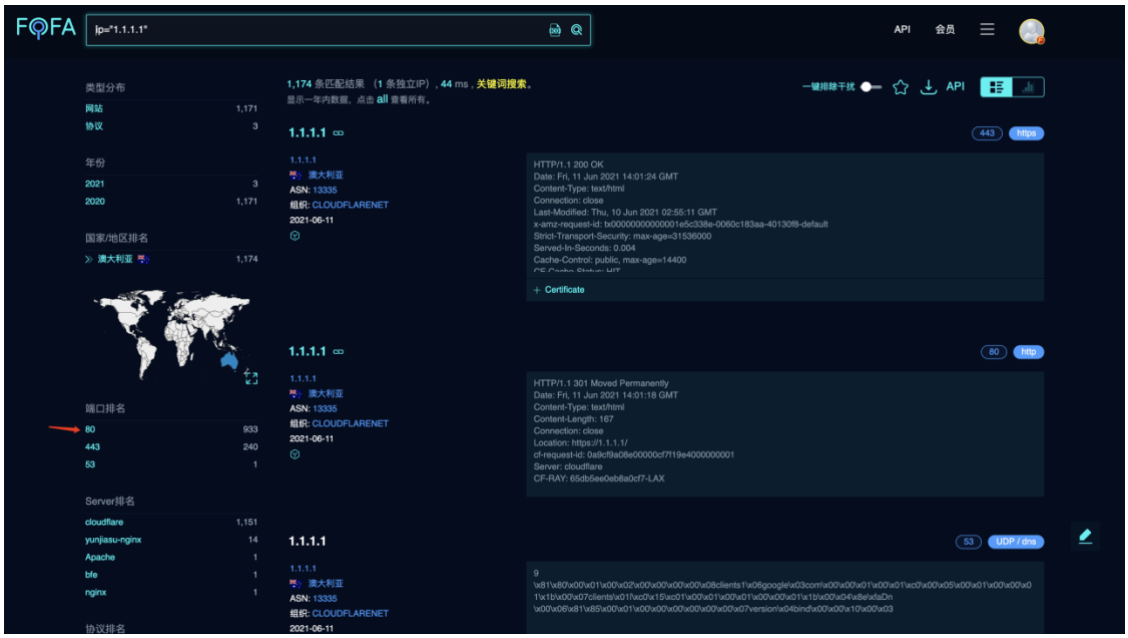
2.43. 搜索 2019-09-09 以前的 ip 资产(以 ip 为单位的资产数据)。

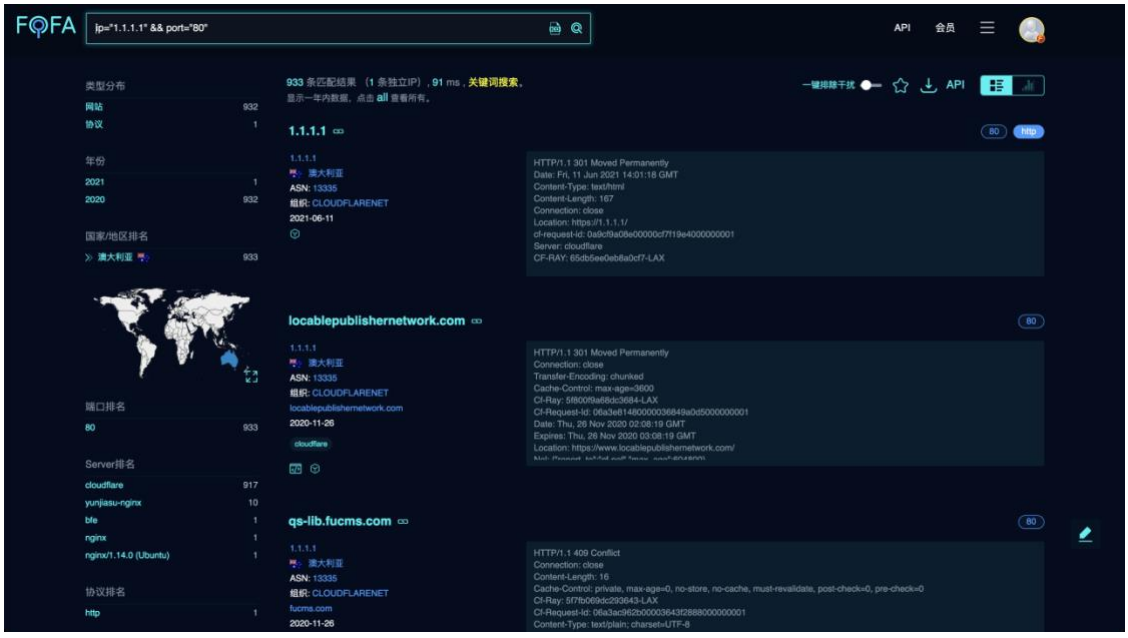
ip_before="2019-09-09"



2.44. 注释

查询过程中，可通过点击左侧栏中的分类进行辅助查询，会自动构建对应的查询语句。





3. 高级搜索

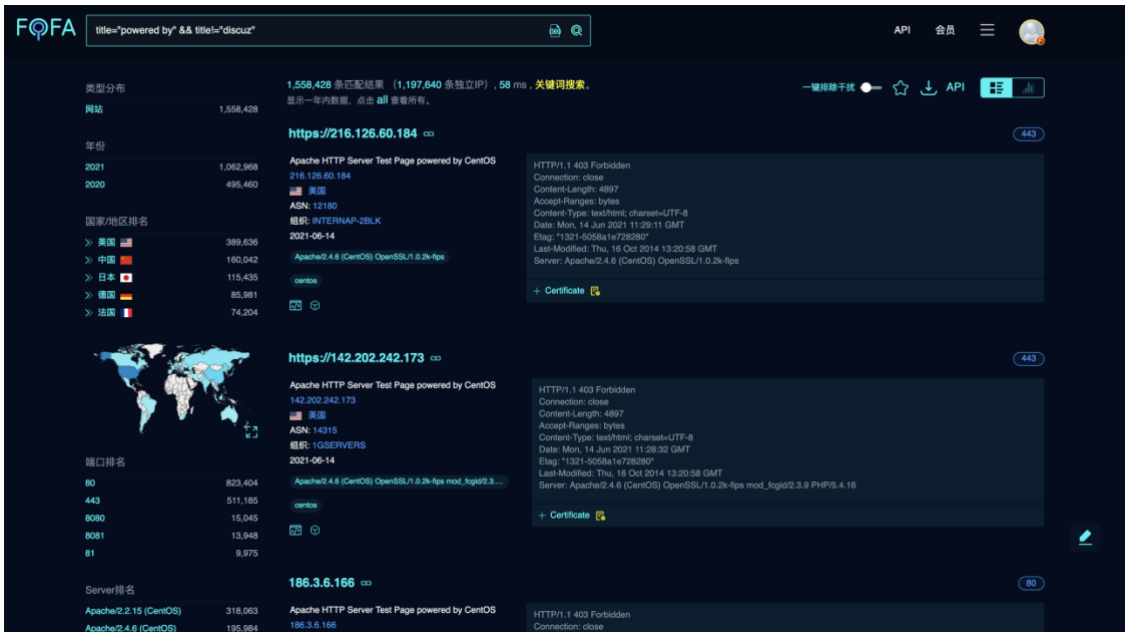
3.1. 逻辑运算符

如果查询表达式有多个与或关系，尽量在外面用（ ）包含起来

逻辑运算符	说明	其他
&&	与	同时满足
||	或	满足其中一个
!=	非	不等于
==	等	全等

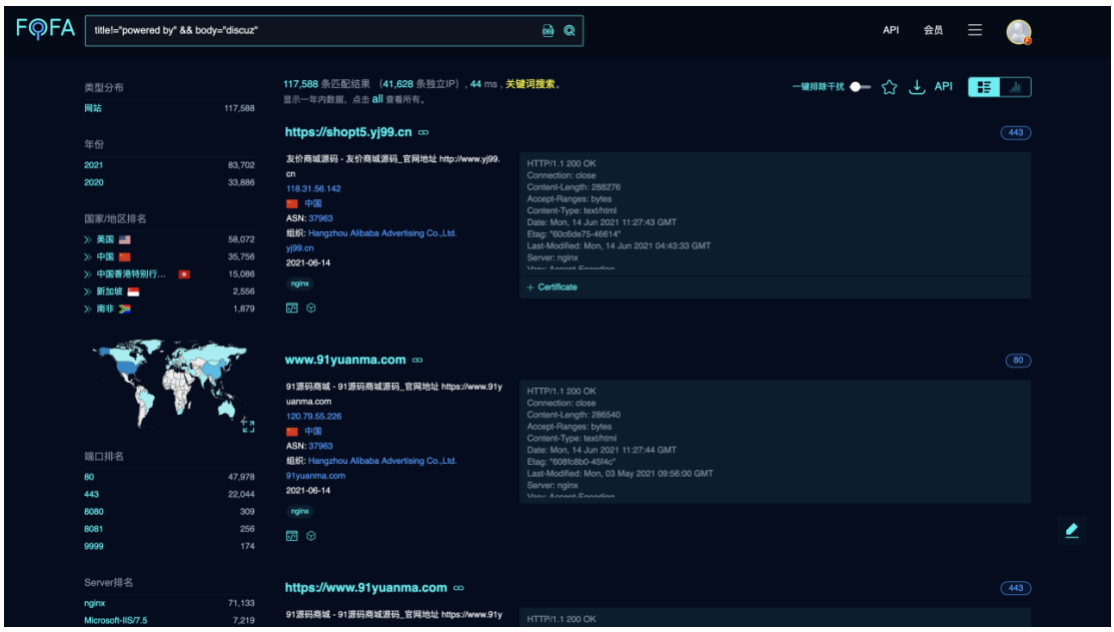
3.2. 标题中包含 powered by 且标题中不包含 discuz

title="powered by" && title!=discuz



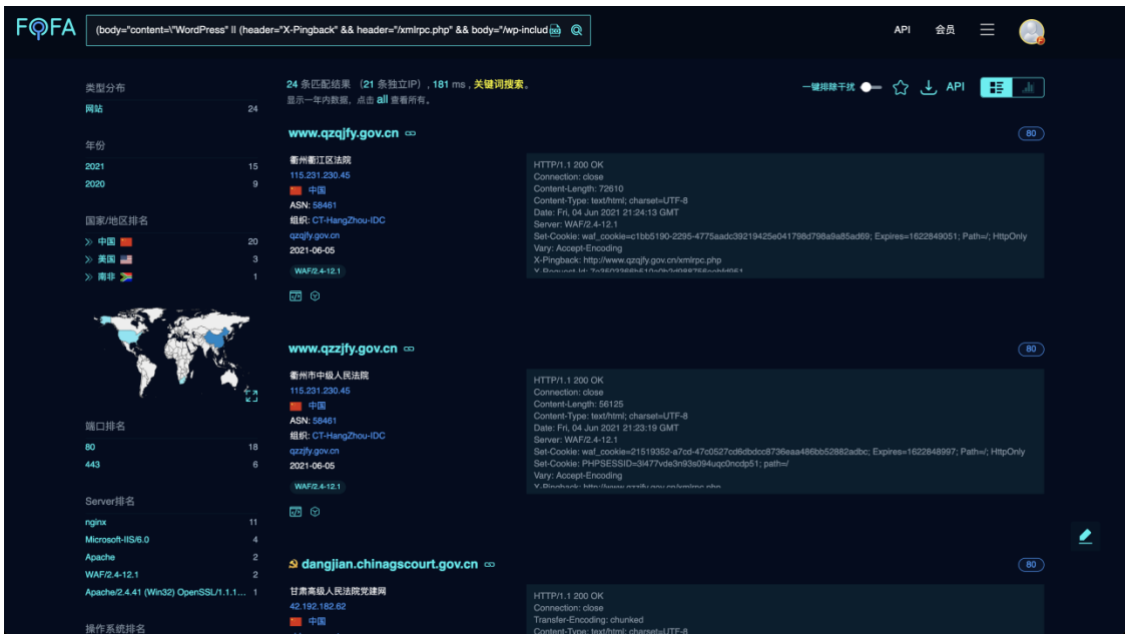
3.3. 标题中不包含 powered by 且 html 正文中包含 discuz

title!="powered by" && body=discuz



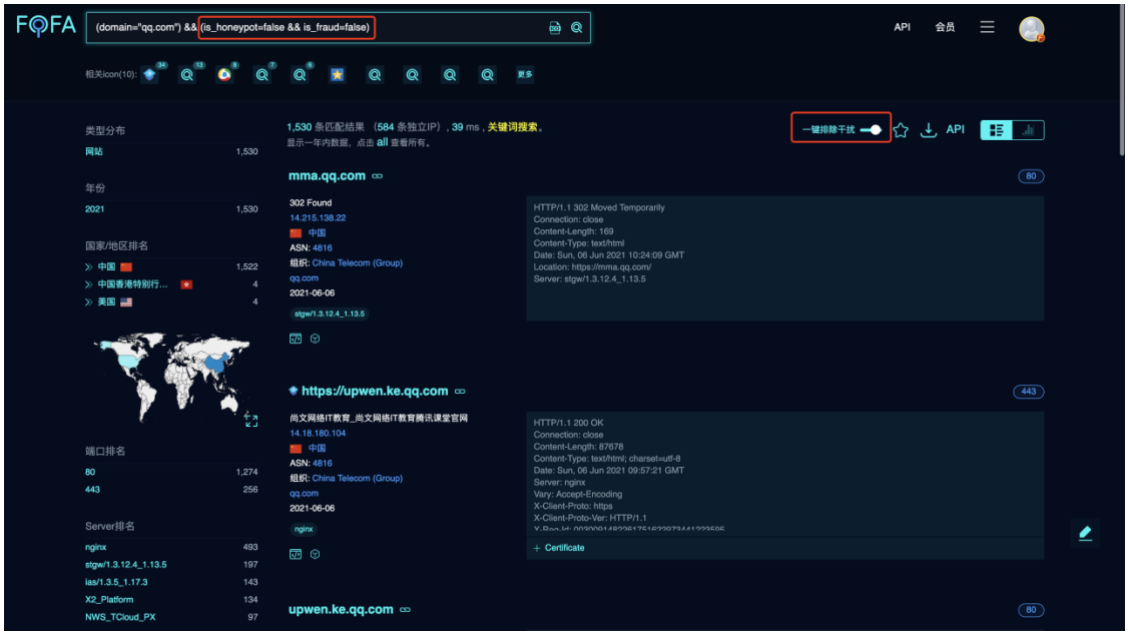
3.4. 寻找 Wordpress 搭建的站点且从 url 中搜索".gov.cn"

(body="content=\"WordPress" || (header="X-Pingback" && header="/xmlrpc.php" && body="/wp-includes/")) && host="gov.cn"



3.5. 排除干扰

使用规则 is_honeypot=false && is_fraud=false 可排除排除仿冒/欺诈数据和蜜罐数据。



4. 规则专题

https://fofa.so/subject

5. 规则列表

FOFA 可以从不同维度搜索网络组件，例如地区，端口号，网络服务，操作系统，网络协议等等。目前 FOFA 支持了多个网络组件的指纹识别，包括建站模块、分享模块、各种开发框架、安全监测平台、项目管理系统、企业管理系统、视频监控系统、站长平台、电商系统、广告联盟、前端库、路由器、SSL 证书、服务器管理系统、CDN、Web 服务器、WAF、CMS 等等。

https://fofa.so/library

6. API

通过 API 可快速从网站中获取数据，便于进行程序间的自动化查询、处理功能，进行进一步的业务分析，

所有调用都需要提供身份信息，主要是 email 和 key，email 主要是注册和登陆时填写的 email，key 需要用户到个人中心获取 32 位的 hash 值，即为 API KEY。

将上面的两个信息填入 api 接口中，即可获取 json 格式的数据：

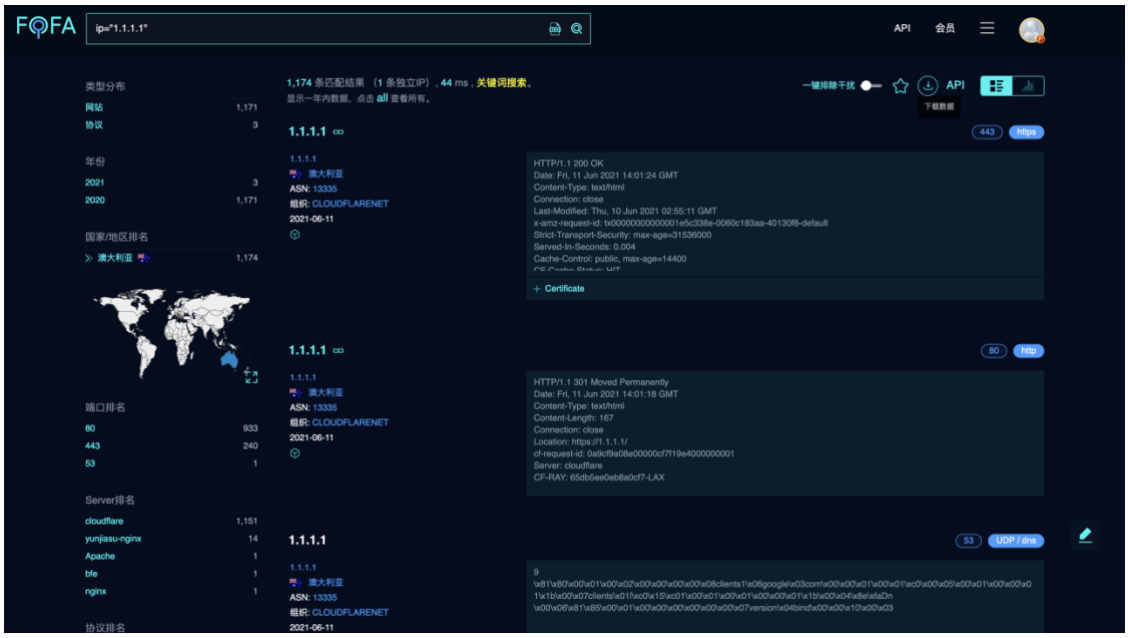
```
echo 'domain="fofa.so"' | base64 - | xargs -I{} curl "https://fofa.so/api/v1/search/all?email=${FOFA_EMAIL}&key=${FOFA_KEY}&qbase
64={}"



# 正确返回结果
{
  "mode": "extended",
  "error": null,
  "query": "domain=\"nosec.org\"\n",
  "page": 1,
  "size": 6,
  "results": [
    [
      "https://i.nosec.org"
    ],
    [
      "https://nosec.org"
    ],
    [
      "down3.nosec.org"
    ],
    [
      "www.nosec.org"
    ],
    [
      "nosec.org"
    ],
    [
      "cdn.nosec.org"
    ]
  ]
}

#错误返回
  #服务器异常
  {"errmsg":"Internal Server Error!","error":true}
  #F币不足
  {"errmsg":"FOFA coin is not enough!","error":true}
  #结果窗口过大
  {"errmsg":"Result window is too large, page must be less than or equal to...","error":true}



{
  "error": true,
  "errmsg": "401 Unauthorized, make sure email and apikey is correct."
}
```

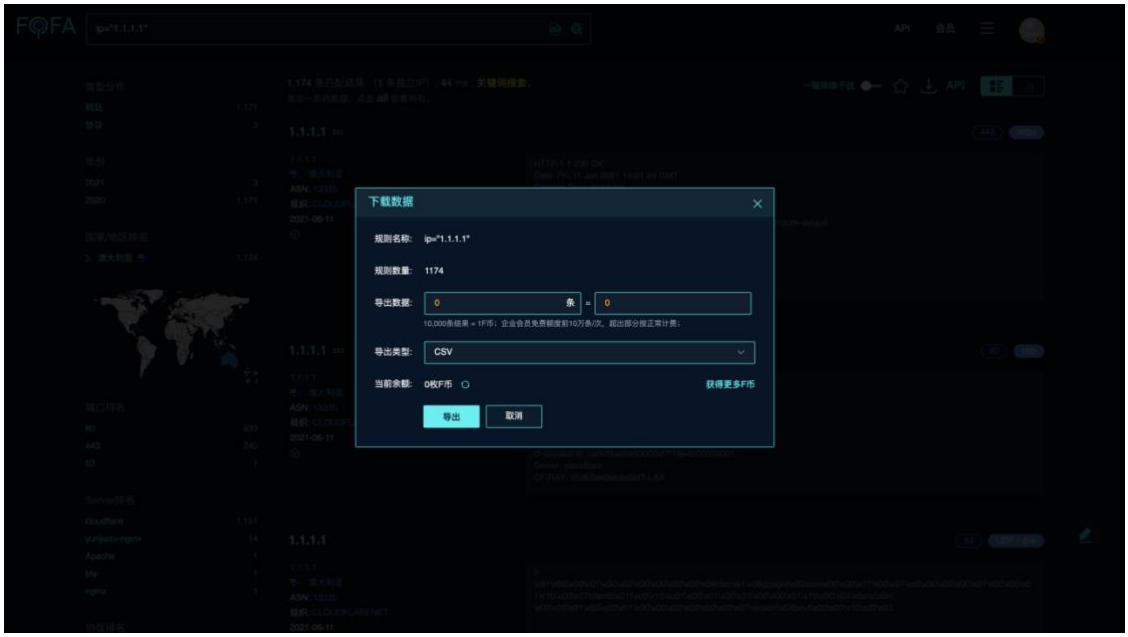
具体的使用如下：

https://fofa.so/staticpages/apihelp

7. 下载功能

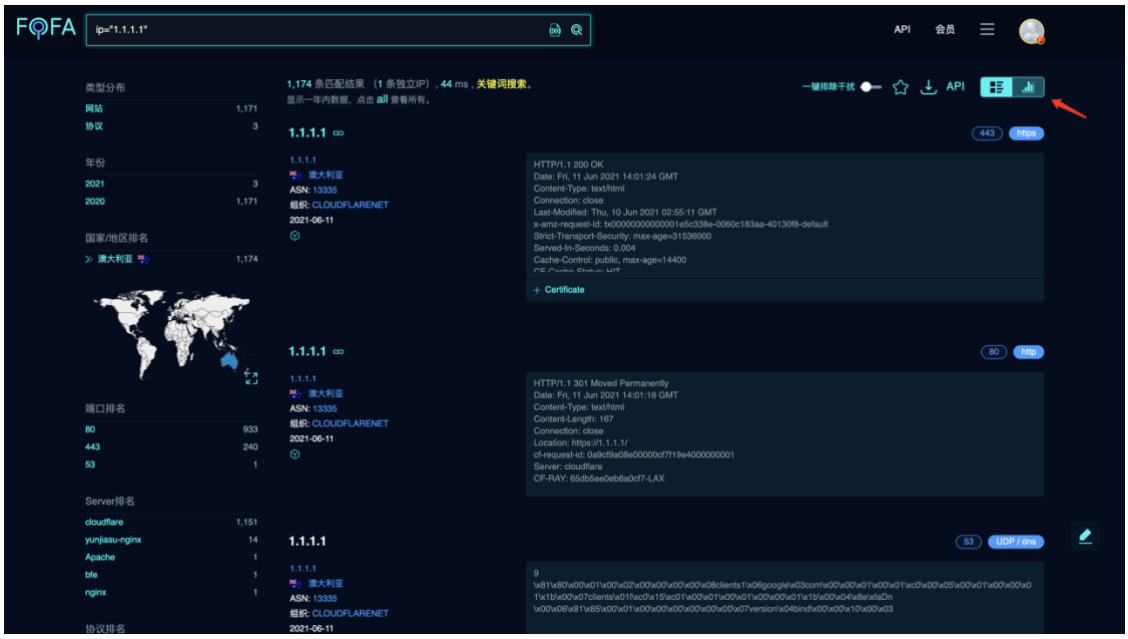
搜索到结果之后可在右侧选择下载功能，可下载搜索到的所有数据，下载的格式支持 CSV，JSON 格式，方便程序调用进行全网扫描。

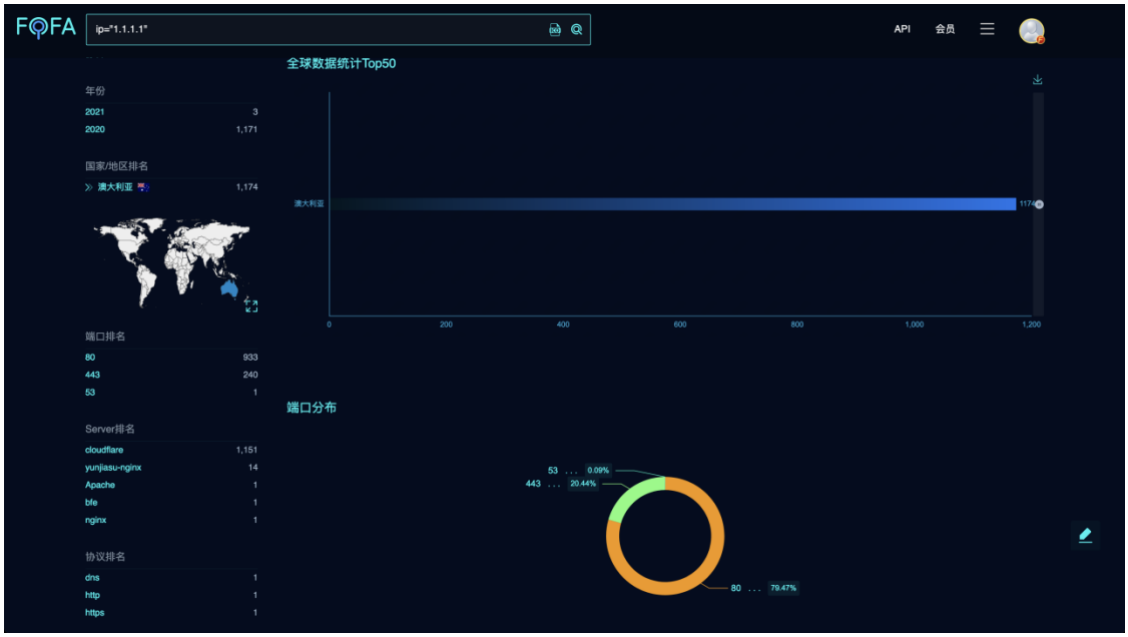




8. 数据统计

查询出的结果可通过图表的形式进行数据统计。





9. 问题列表

9.1. icon_hash 语法怎么使用

使用方法①：已有 icon 文件时，通过在首页搜索框内上传 icon 搜索；

使用方法②：已知 iconhash 时直接使用 iconhash=""语法搜索；

使用方法③：已知域名时，使用 domain=""语法，系统会展示对应的 icon，点击即可进行搜索；

9.2. port_size 语法怎么使用

该语法仅限高级会员、企业会员使用。

通过 port_size=""语法，可以查询开放端口数量等于某数的资产；

通过 portsizegt=""语法，可以查询开放端口数量大于某数的资产；

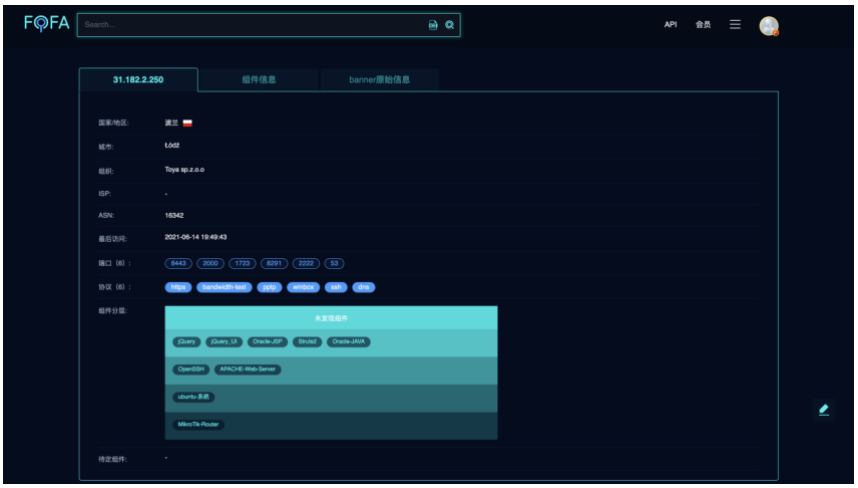
通过 portsizelt=""语法，可以查询开放端口数量小于某数的资产；

9.3. API 可以获取哪些字段？

host, title, ip, domain, port, country, province, city, countryname, header, server, protocol, banner, cert, isp, asnumber, as_organization, latitude, longitude, lastupdatetime 等。

9.4. 能显示独立 ip 吗？

支持，前往该 IP 的聚合页查看。



9.5. 同 IP 数据重复

FOFA 的资产是以 ip 和端口为单位，不是以 ip 为单位。所有存在同 IP 不同端口的数据。

9.6. 同端口数据重复

端口数据分协议数据和网站数据。协议数据有协议等信息，网站数据有网站正文信息。

9.7. 为何有的协议不支持跳转？

只有 https 及 http 协议支持跳转。

9.8. 是否可以识别组件的版本？

公网暴露的信息中若存在版本特征，则可识别。

9.9. API 接口调用查询的时间选项，有很多是以前的信息

搜索语法增加时间限制。

9.10. IP 可以搜索到，Body 中的内容搜索不到？

英文中的. :// _等未做分词，搜索整体才能搜到，搜索一部分搜不到。

9.11. title 支持模糊查询吗？

单等号搜索为包含关系，双等号搜索为绝对相同关系。

10. Fofa 采集工具

10.1. fofa_viewer

https://github.com/wgpsec/fofa_viewer

多标签式查询结果展示

丰富的右键菜单

支持查询结果导出

支持手动修改查询最大条数，方便非高级会员使用(修改 config.properties 中的 maxSize 即可)

支持证书转换 将证书序列填写入启动页框内可转换，再使用 cert="计算出来的值" 语法进行查询

支持输入智能提示

支持 fofa 的一键排除干扰（蜜罐）功能。（注：需要高级会员才能使用，使用时会在 tab 页标记(*)）

知道创宇云安全事业群
解决方案交付中心