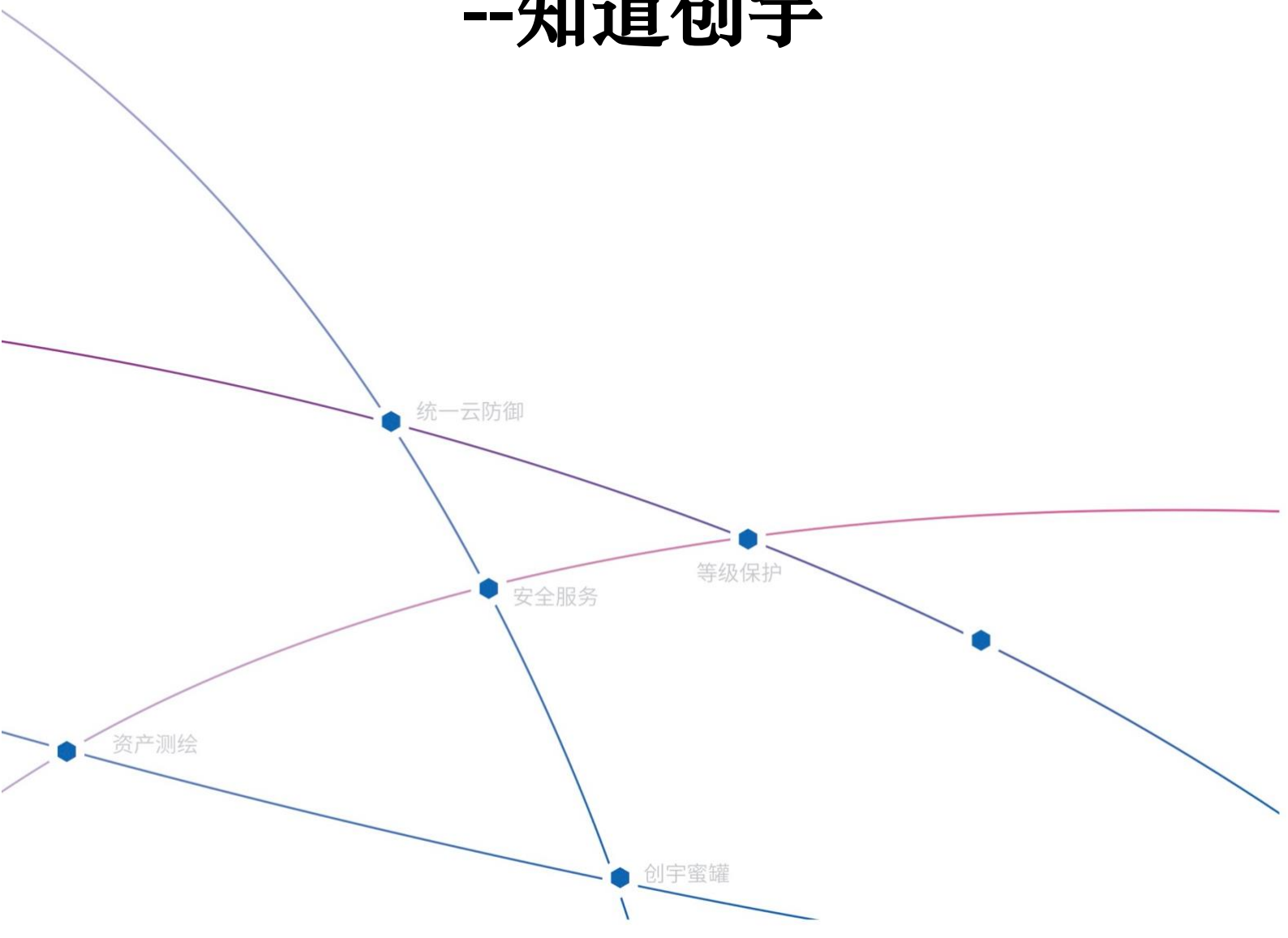
知道创宇

Shodan 使用手册

--知道创宇



文档信息

文档名称	版本号	保密级别
Shodan 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
张宇明	Shodan 使用手册—知道创宇	2021.6.20	1.0	裴文成
裴文成	修订格式	2021.6.21	1.1	马超

版权说明

目录

1. 介绍 1

2. 账户 2

2.1. 账户类型 2

3. Shodan 导航 3

3.1. 搜索页面 3

3.2. Explore 3

3.3. Exposure 4

3.4. Report 5

3.5. Maps 6

3.6. Images 7

3.7. Monitor 8

3.8. 仪表板 9

3.9. 漏洞搜索 9

3.10. 蜜罐验证 11

3.11. 帮助中心 11

4. 元数据 12

4.1. Banner 12

4.2. 设备元数据 13

4.3. SSL 13

4.3.1. SSL banner 14

4.3.2. SSL 检索 14

4.4. Web 组件 15

5. Shodan API 17

5.1. Developer API 17

5.2. API 使用限制 17
5.3. Facets 17
5.4. 安装和初始化 19
5.5. 使用 API 进行搜索 19
5.6. 使用 API 进行主机查询 21
5.7. 使用 API 进行统计 21

6. Shodan CLI 23

6.1. 安装 23
6.2. 初始化密钥 23
6.3. 命令详解 24
6.3.1. alert 命令 24
6.3.2. domain 命令 25
6.3.3. host 命令 26
6.3.4. convert 命令 27
6.3.5. count 命令 28
6.3.6. download 命令 29
6.3.7. honeyscore 命令 29
6.3.8. info 命令 30
6.3.9. myip 命令 30
6.3.10. parse 命令 30
6.3.11. scan 命令 31
6.3.12. stats 命令 33

7. Shodan 外部插件 34

7.1. Maltego 扩展插件 34
7.1.1. Maltego 简介 34
7.1.2. 安装 Shodan 扩展插件 34
7.1.3. 使用 Shodan 扩展插件 35
7.2. 浏览器插件 36

7.2.1. Chrome 扩展插件.....37
7.2.2. Firefox 扩展插件.....38
7.3. MetaSploit 扩展模块.....38
7.3.1. 搜索模块.....38
7.3.2. 蜜罐验证模块.....39
7.3.3. 主机端口收集模块.....39

8. Shodan 搜索指南.....41

8.1. 搜索范围.....41
8.1.1. 默认字符串搜索范围.....41
8.1.2. 默认搜索时间范围.....43
8.2. Shodan 搜索逻辑.....43
8.2.1. 排除符号“-”.....43
8.2.2. 联合查询“,”.....44
8.3. 地理位置搜索.....44
8.3.1. 搜索指定国家的相关设备.....44
8.3.2. 搜索指定城市的相关设备.....45
8.3.3. 搜索指定经纬度的相关设备.....45
8.4. IP、域名及端口信息搜索.....47
8.4.1. 搜索指定 IPv4 的相关设备.....47
8.4.2. 搜索指定 IPv6 的相关设备.....47
8.4.3. 搜索使用 IPv6 的相关设备.....48
8.4.4. 搜索指定 CIDR 格式 IP 地址的相关设备.....48
8.4.5. 搜索指定 ASN 的相关设备.....49
8.4.6. 搜索域名或主机名为“google”的相关设备.....49
8.4.7. 搜索指定组织或公司的相关设备.....50
8.4.8. 搜索指定网络服务提供商的相关设备.....50
8.4.9. 搜索指定端口的相关设备.....51
8.5. 设备指纹搜索.....51
8.5.1. 搜索指定操作系统的相关设备.....51

8.5.2. 搜索指定软件或平台的相关设备.....52
8.5.3. 搜索指定软件版本的相关设备.....53
8.6. 屏幕截图搜索.....54
8.6.1. 搜索被勒索软件攻击的远程桌面.....54
8.6.2. 搜索隐藏在 web 端口下的公共 VNC 服务.....54
8.6.3. 搜索使用机器学习识别到的工业控制系统.....55
8.7. 漏洞搜索.....55
8.7.1. 搜索易受到心脏出血漏洞攻击的设备.....55
8.7.2. 在中国和美国搜索易受到 CVE-2019-19781 攻击的 Citrix 设备.....55
8.8. SSL 相关搜索.....56
8.8.1. 搜索指定证书的相关设备.....56
8.8.2. 搜索支持 TLS1.3 的设备.....56
8.8.3. 搜索支持 HTTP/2 的设备.....57
8.8.4. 搜索支持 SSLv2 但不支持 TLS 的设备.....57
8.8.5. 搜索为*.google.com 颁发证书的设备.....58
8.9. HTTP 相关搜索.....58
8.9.1. 搜索在 HTML 中包含“Apache”的设备.....58
8.9.2. 搜索使用 bootstrap css 框架的设备.....59
8.9.3. 搜索指定 icon_hash 的设备.....59
8.9.4. 搜索指定 HTTP 响应状态码的设备.....60
8.9.5. 搜索指定网站标题的设备.....60
8.9.6. 搜索指定 waf 的相关设备.....61
8.10. 常见网络架构搜索示例.....61
8.10.1. 搜索存在未授权访问的 MongoDB.....61
8.10.2. 搜索存在未授权访问的 Mongo Express 网页界面.....62
8.10.3. 搜索存在未授权访问的 Jenkins 页面.....63
8.10.4. 搜索未受保护的 VNC.....63
8.10.5. 搜索 Windows 远程桌面.....64
8.10.6. 搜索以 Root 身份登录的 telnet.....66

8.10.7. 搜索使用 ADB 的相关设备 66
8.10.8. 搜索可匿名登录的 FTP 服务 67
8.10.9. 搜索存在 Apache 目录遍历的设备 67
8.10.10. 搜索 SMB 文件共享 68
8.10.11. 搜索域控制器 68
8.10.12. 搜索存在密码泄露的 Lantronix 串行以太网适配器 69
8.10.13. 搜索存在错误配置的 Wordpress 69
8.10.14. 搜索 Kubernetes pod 和 Docker 的可视化仪表板 70
8.10.15. 搜索 OctoPrint3D 打印机设备 70
8.10.16. 搜索 Cisco Smart Install 71
8.10.17. 搜索 Outlook 72
8.11. 工业控制系统搜索 72
8.11.1. 工业控制系统简介 72
8.11.2. 搜索工控协议为“XZERES Wind Turbine”的相关设备 73
8.11.3. 搜索工控协议为“Modbus”的相关设备 73
8.11.4. 搜索工控协议为“Niagara Fox”的相关设备 74
8.11.5. 搜索工控协议为“GE-SRTP”的相关设备 74
8.11.6. 搜索工控协议为“MELSEC-Q”的相关设备 75
8.11.7. 搜索工控协议为“CODESYS”的相关设备 76
8.11.8. 搜索工控协议为“S7”的相关设备 76
8.11.9. 搜索工控协议为“BACnet”的相关设备 77
8.11.10. 搜索工控协议为“HART-IP”的相关设备 77
8.11.11. 搜索工控协议为“Omron FINS”的相关设备 78
8.11.12. 搜索工控协议为“IEC 60870-5-104”的相关设备 78
8.11.13. 搜索工控协议为“DNP3”的相关设备 79
8.11.14. 搜索工控协议为“EtherNet/IP”的相关设备 79
8.11.15. 搜索工控协议为“PCWorx”的相关设备 80
8.11.16. 搜索工控协议为“Crimson v3.0”的相关设备 80
8.11.17. 搜索工控协议为“ProConOS”的相关设备 81

8.11.18. 搜索加油站泵控制器.....81
8.11.19. 搜索交通灯控制器、红绿灯摄像头.....82
8.12. 过滤器列表.....83

9. 附录.....84

9.1. 附录 A--Banner 格式.....84
9.1.1. 常用属性.....84
9.1.2. Elastic 属性.....85
9.1.3. HTTP（S）属性.....85
9.1.4. 位置属性.....86
9.1.5. SMB 属性.....86
9.1.6. SSH 属性.....87
9.1.7. SSL 属性.....87
9.1.8. ISAKMP 属性.....88
9.2. 附录 B--过滤器.....89
9.2.1. 常规过滤器.....89
9.2.2. HTTP 过滤器.....90
9.2.3. NTP 过滤器.....90
9.3. 附录 C--Facets.....92
9.3.1. 常用 Facets.....92
9.3.2. HTTP Facets.....92
9.3.3. NTP Facets.....94
9.3.4. SSH Facets.....94

10. Shodan 自动化采集工具.....95

10.1. Shodan_So.....95

1. 介绍

Shodan 是一款功能惊人的所搜引擎。与谷歌不同的是，Shodan 不是在网上搜索网址，而是直接进入互联网的背后通道。Shodan 可以说是一款“黑暗”谷歌，一刻不停的在寻找着所有和互联网关联的服务器、摄像头、打印机、路由器等等。每个月 Shodan 都会在大约 5 亿个服务器上日夜不停地搜集信息。

Shodan 所搜集到的信息是极其惊人的。凡是链接到互联网的红绿灯、安全摄像头、家庭自动化设备以及加热系统等等都会被轻易的搜索到。Shodan 的使用者曾发现过一个水上公园的控制系统，一个加油站，甚至一个酒店的葡萄酒冷却器。而网站的研究者也曾使用 Shodan 定位到了核电站的指挥和控制系统及一个粒子回旋加速器。

Shodan 真正值得注意的能力就是能找到几乎所有和互联网相关联的东西。而 Shodan 真正的可怕之处就是这些设备几乎都没有安装安全防御措施，其可以随意进入。

2. 账户

Shodan 有四种账户类型，分别是：Membership（会员）、Freelancer（自由职业）、Small Business（小企业）、Corporate（公司）。

2.1. 账户类型

四种账户类型，可查询的结果、可扫描 IP 数量、网络监控数量、是否支持漏洞搜索过滤器、是否支持批量 IP 查询等存在查询，具体差异以及资费信息，请参考链接：https://account.shodan.io/billing 获取更多信息。

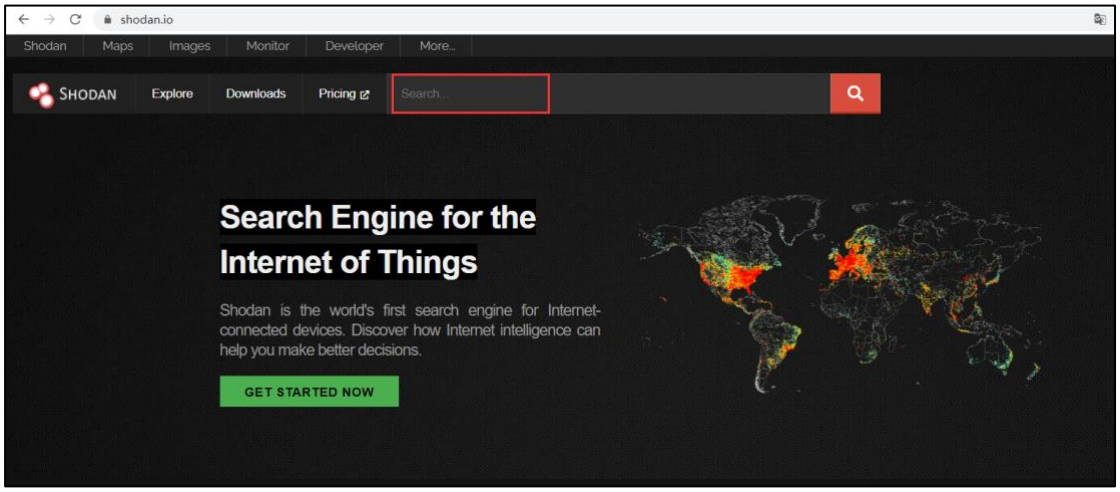
Compare Features

	Membership	Freelancer	Small Business	Corporate	Enterprise
Price	$49 (one-time)	$59/ month	$299/ month	$899/ month	Custom
Query credits (per month)	100	10,000	200,000	Unlimited	Unlimited
Scan credits (per month)	100	5,120	65,536	327,680	Unlimited
Monitored IPs	16	5,120	65,536	327,680	Unlimited
Available search filters	All except `vuln` and `tag`	All except `vuln` and `tag`	All except `tag`	All	All
Number of users	1	1	1	1	Custom
Shodan Search pages	20	20	200	200	200
Shodan Monitor	✓	✓	✓	✓	✓
Private firehose	✓	✓	✓	✓	✓
IP lookups	✓	✓	✓	✓	✓
Batch IP lookups				✓	✓
Bulk Data					✓
InternetDB					✓
Full firehose					✓

3. Shodan 导航

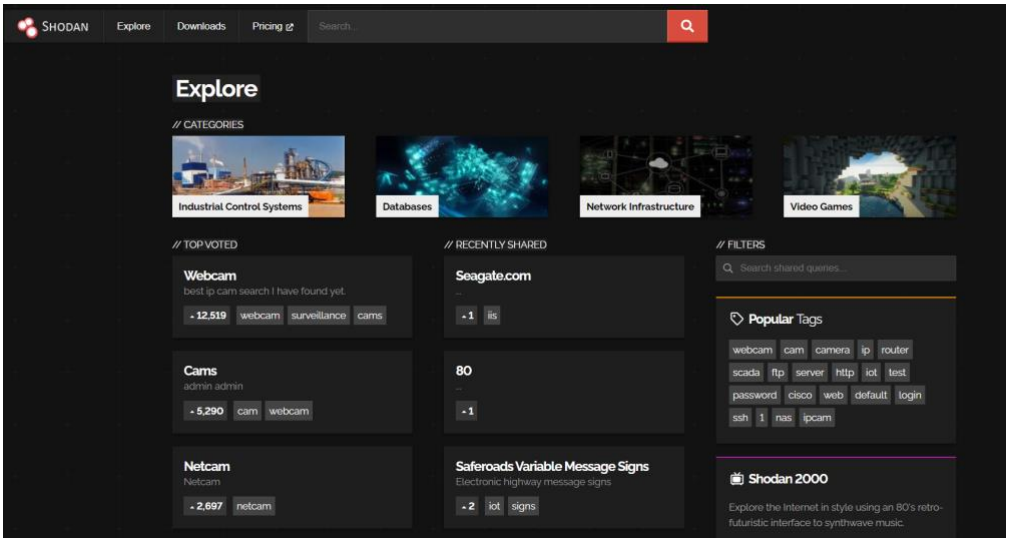
3.1. 搜索页面

Shodan 主要搜索通常在首页的搜索框中完成，输入要查询的内容，即可返回相关的设备信息。



3.2. Explore

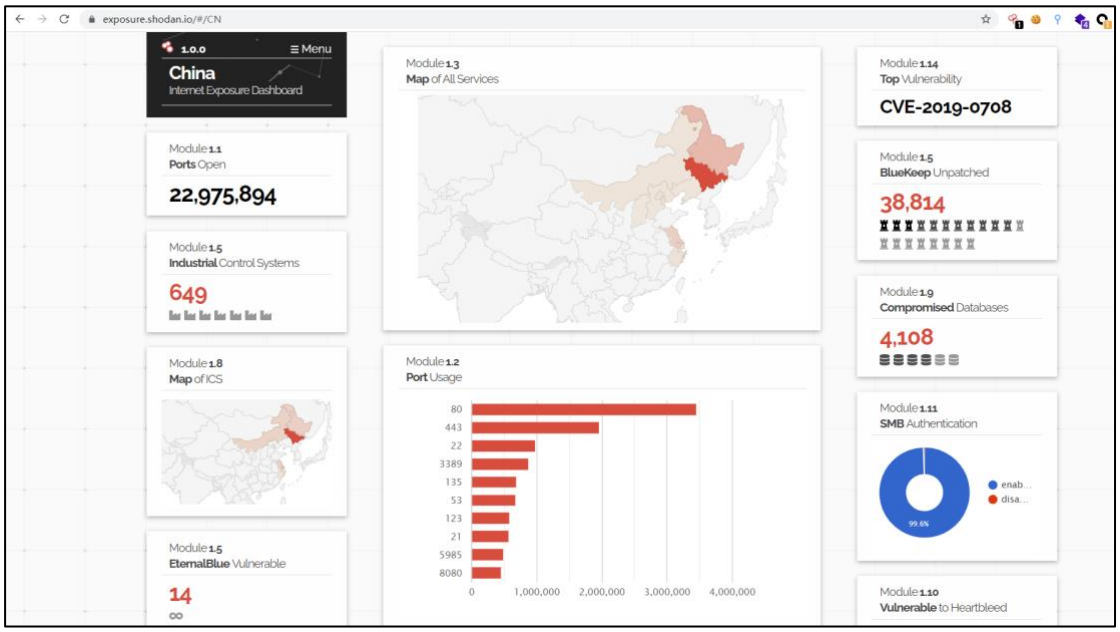
Explore 为用户提供了更多的搜索词条，这些词条由其他用户分享，增强了 Shodan 搜索的功能、精确度以及攻击性。



详情请查阅：https://www.shodan.io/explore 获取更多信息。

3.3. Exposure

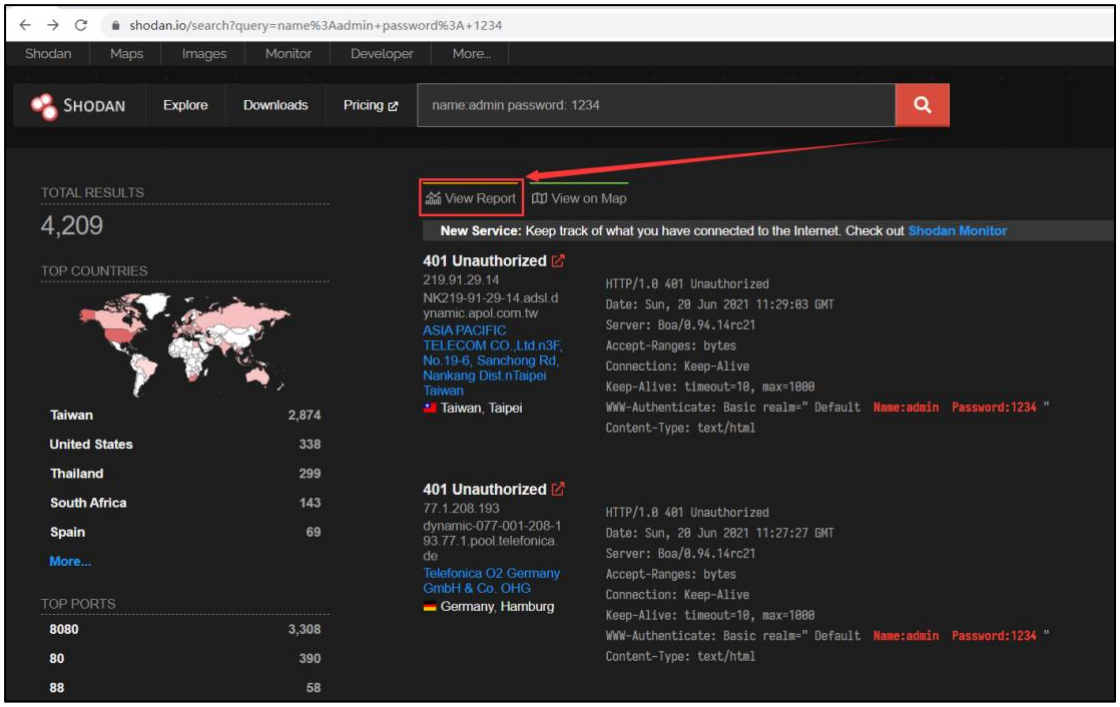
Shodan Exposure 提供了在一个国家/地区公开的服务的高级视图，该视图包含了该地区的开放的端口、最常见漏洞、常见端口 TOP10、危险数据库等资产。

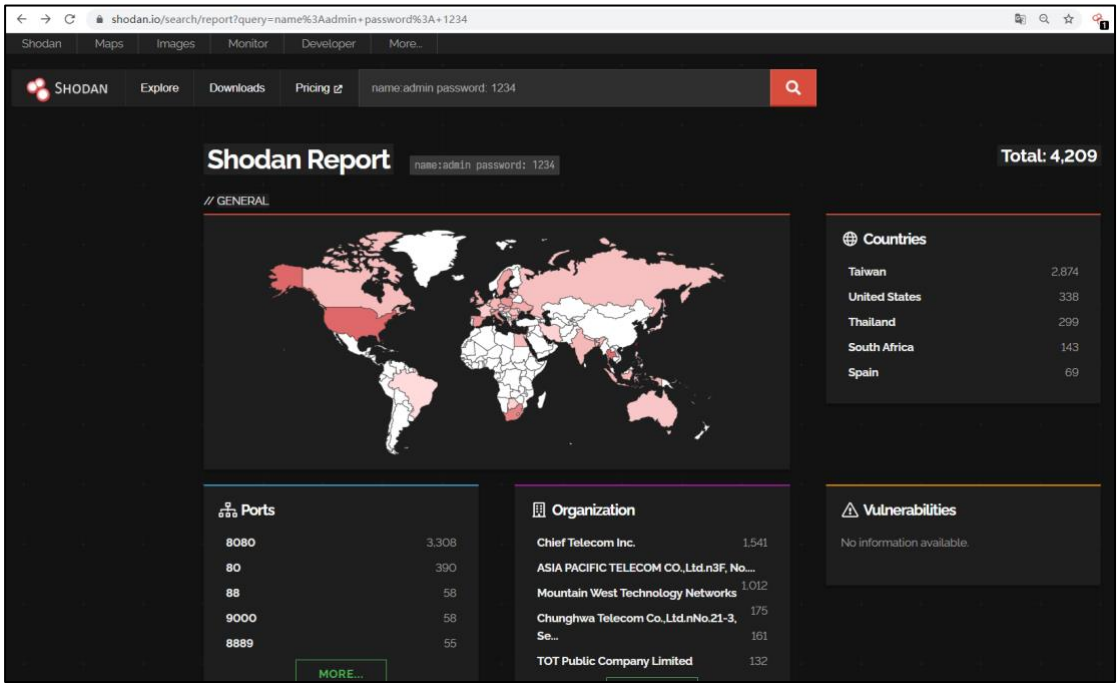


详情请查阅：https://exposure.shodan.io/获取更多信息。

3.4. Report

对于 Shodan 的搜索结果，可以点击 View Report 查看搜索报告，其中包括了搜索结果的数据概览，如国家、端口、漏洞、组织等信息。

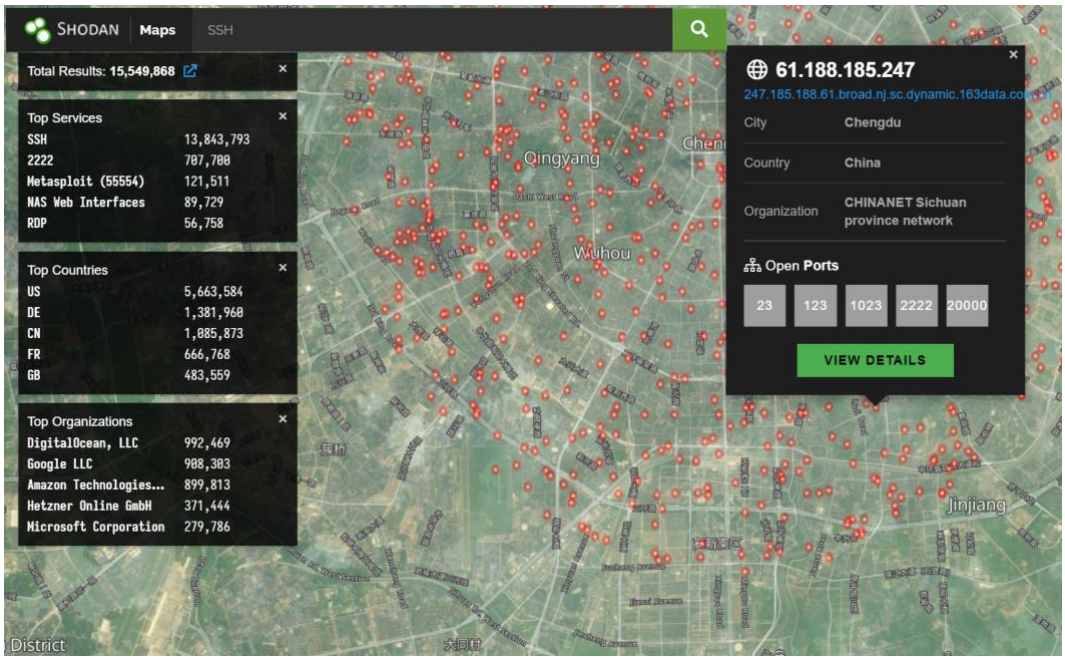


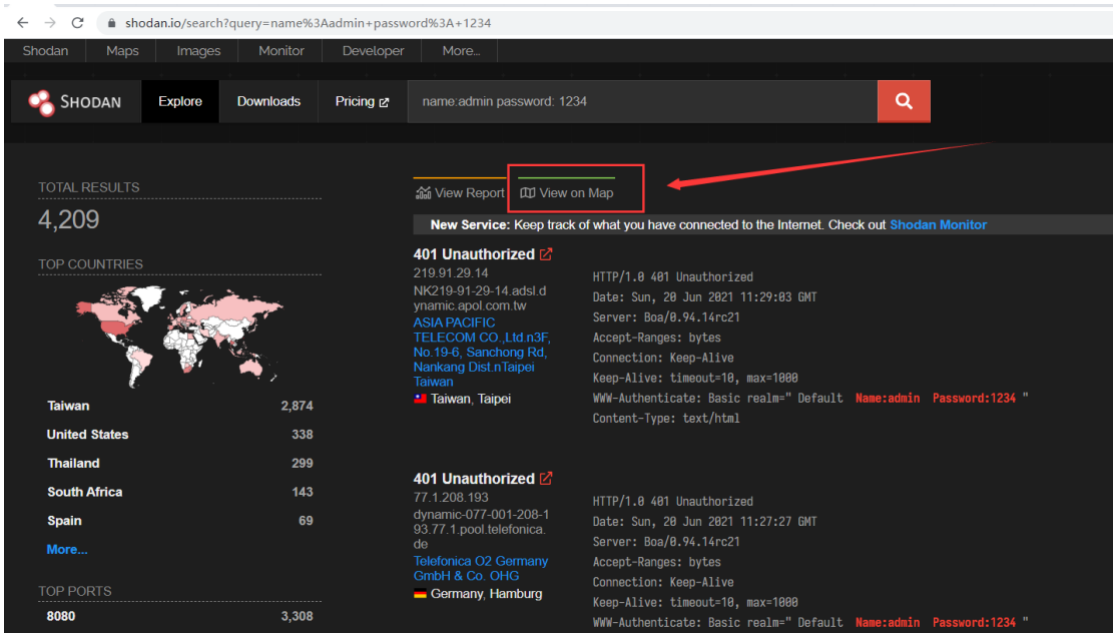


3.5. Maps

Shodan Maps 直观地在地图上展示了对应资产的地理位置，搜索后，点击地图上对应的红点，可以看到该设备的详细信息。

在使用搜索功能完成搜索后，还可以点击 View on Map，将搜索的结果展示在 Map 上。

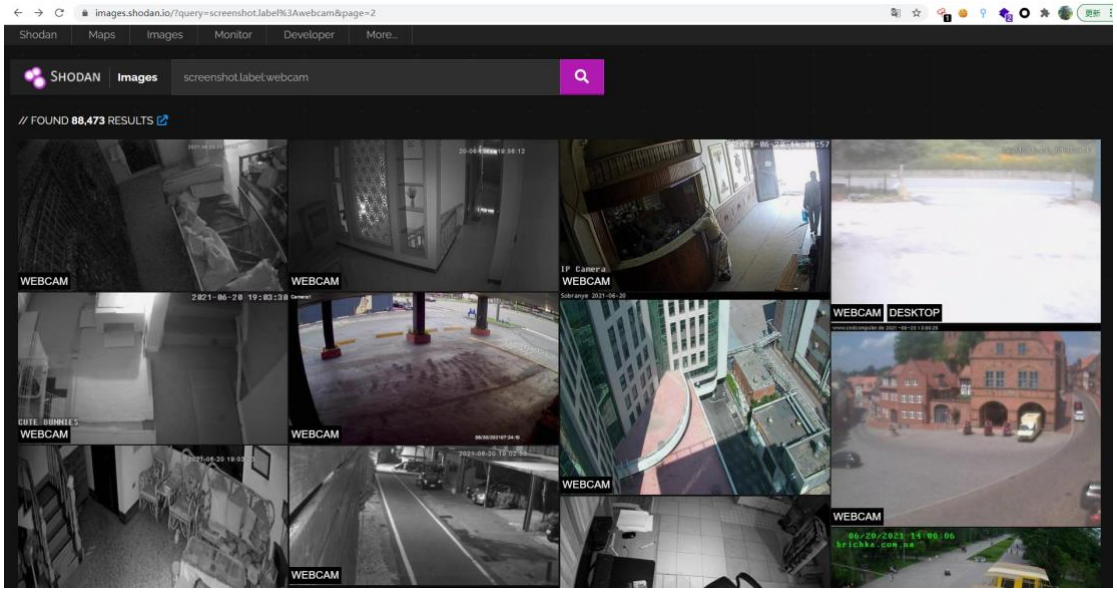


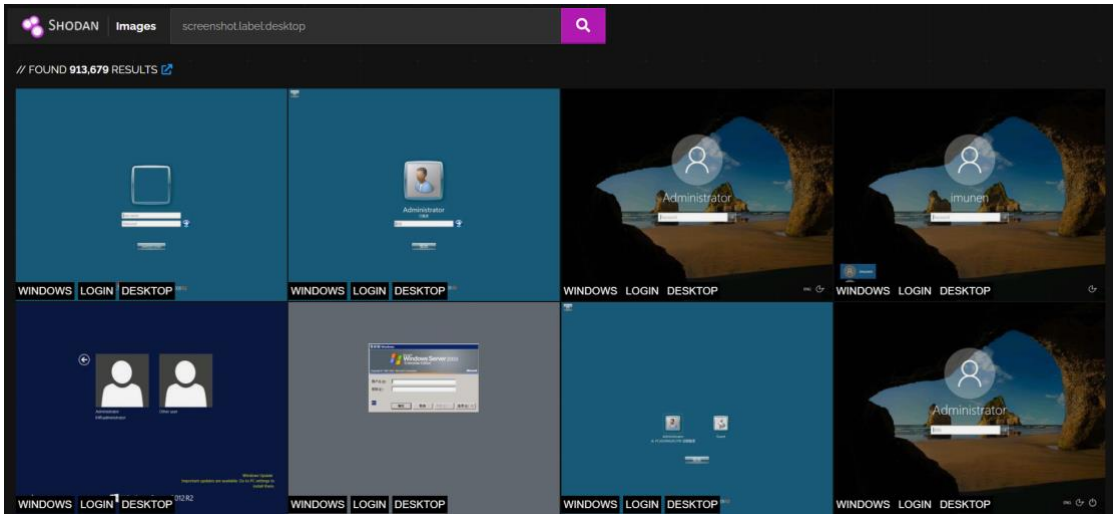


详情请查阅：https://maps.shodan.io/获取更多信息。

3.6. Images

Shodan Images 可以获取当前设备的屏幕截图或摄像头的实时截图。

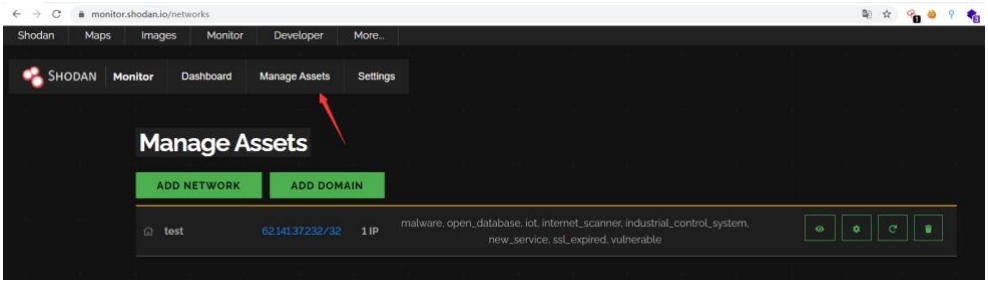


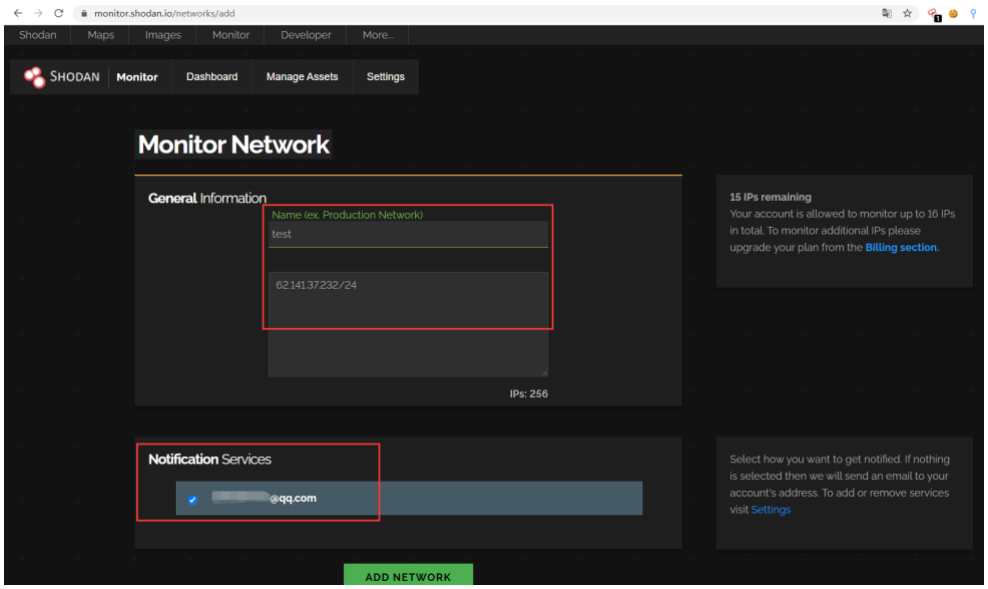


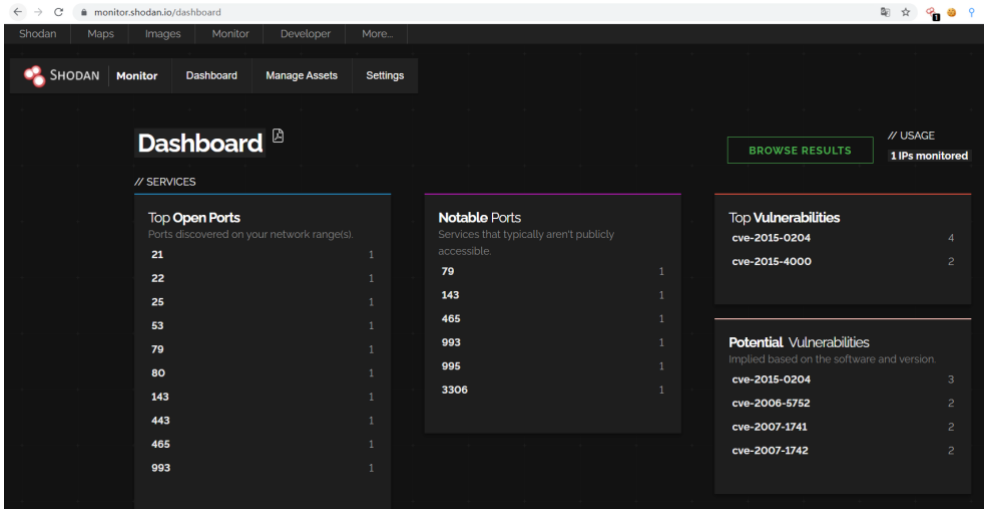
详情请查阅：https://images.shodan.io 获取更多信息。

3.7. Monitor

Shodan 允许用户创建监视器，对指定资产进行监测，当资产更新后，会以指定形式通知给用户。



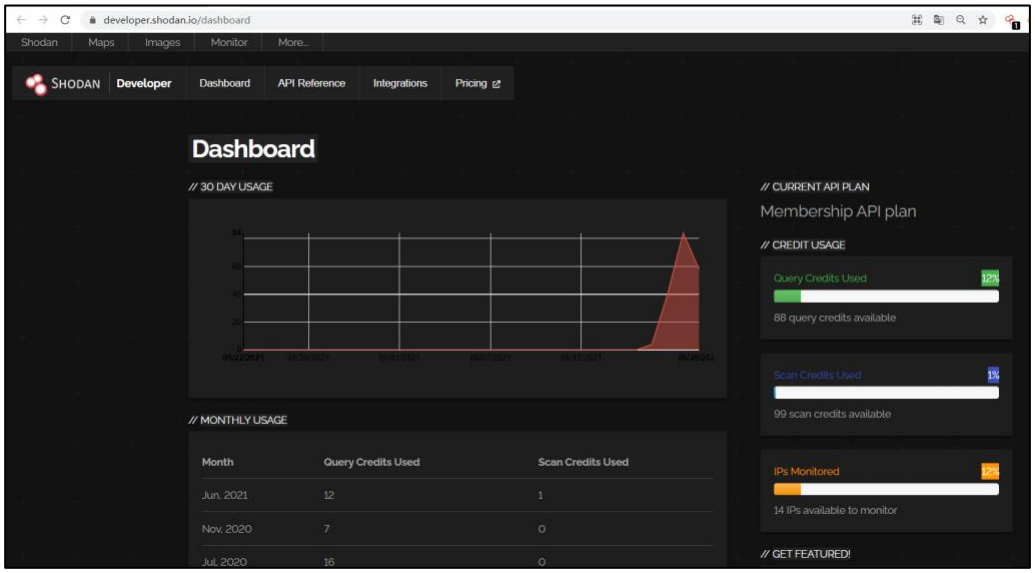




详情请查阅：https://monitor.shodan.io/dashboard 获取更多信息。

3.8. 仪表板

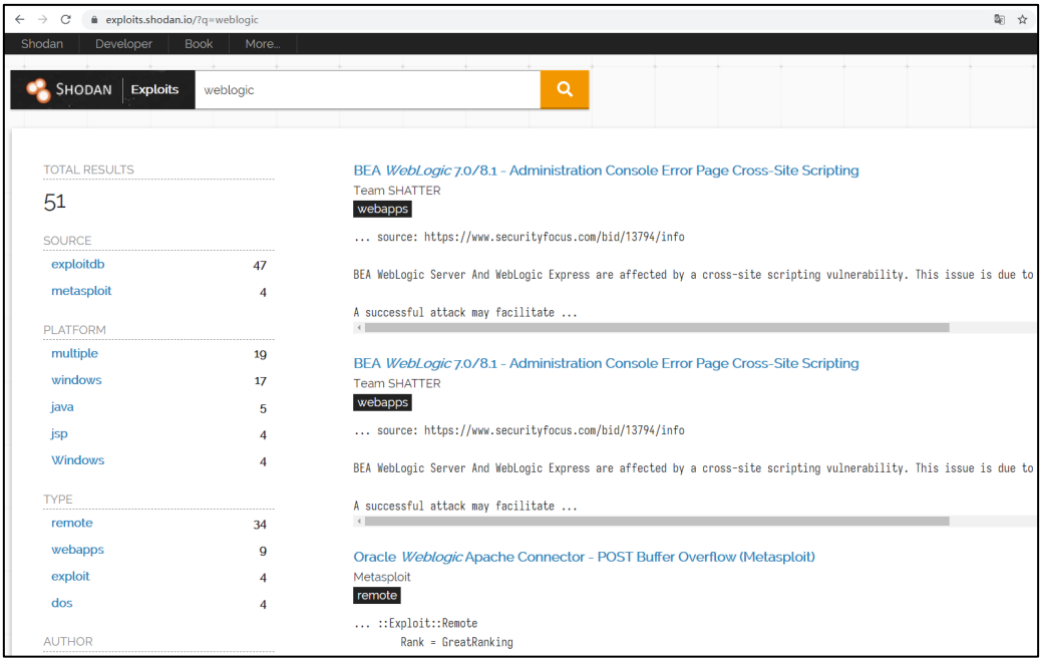
Shodan 的仪表板可以查询用户当前 API 用量，以及各类查询剩余次数。



详情请查阅：https://developer.shodan.io/dashboard 获取更多信息。

3.9. 漏洞搜索

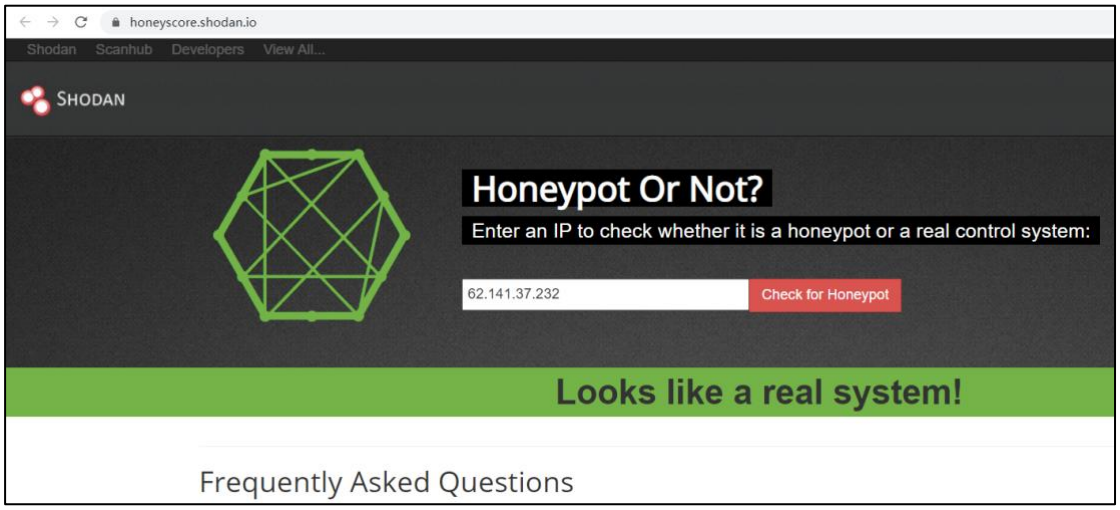
Shodan 的漏洞库集成了 ExploitDB、Metasploit，可以根据搜索内容匹配对的漏洞详情。



详情请查阅：https://exploits.shodan.io/welcome 获取更多信息。

3.10. 蜜罐验证

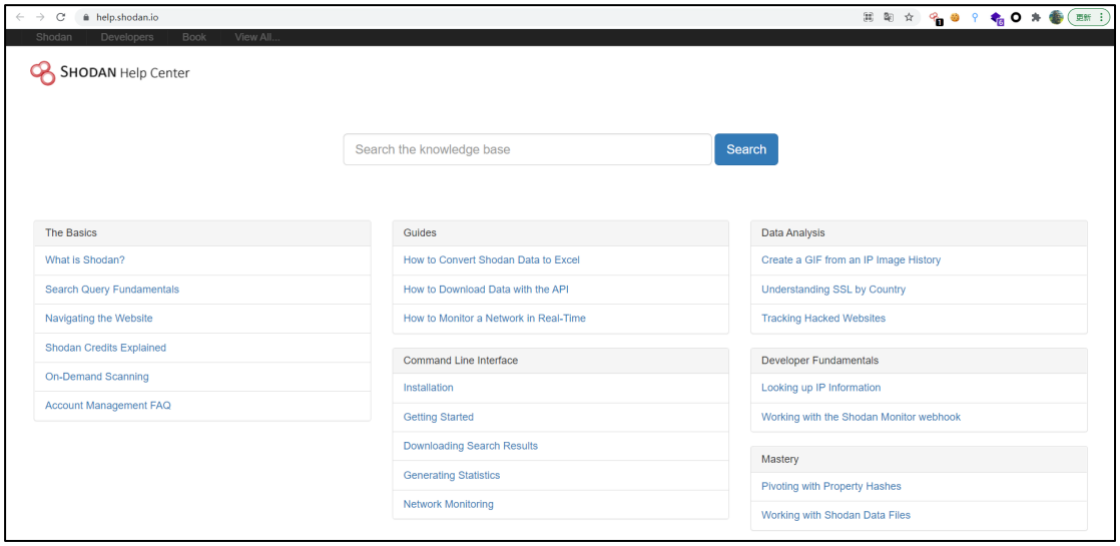
Shodan 蜜罐验证平台可以供用户判断目标设备是否为蜜罐。



详情请查阅： https://honeyscore.shodan.io 获取更多信息。

3.11. 帮助中心

Shodan 帮助中心给用户提供了常见问题查询，包括使用指南、API、命令行的安装入门等。



详情请查阅：https://help.shodan.io 获取更多信息。

4. 元数据

4.1. Banner

Shodan 采集的基本数据单位是 Banner，Banner 是描述设备所运行的服务的标志性文本信息，对于 Web 服务器来说，Banner 会标题或是 telnet 登录界面，Banner 的内容会因服务器类型不同而相异。

下图是一个典型的 Http Banner，该 Banner 还显示了一个正在运行的 nginx 服务器，对应的脚本类型为 PHP：

nginx

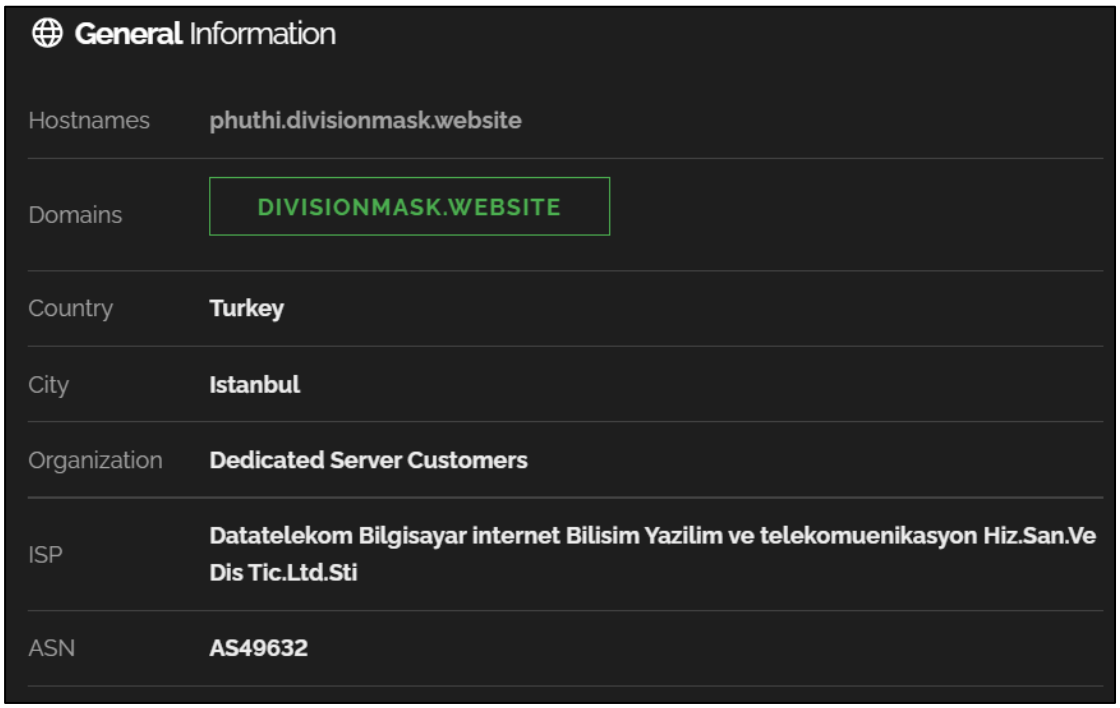
```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 16 Jun 2021 22:00:58 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.45
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=995lnd8f7lqr9bbm9u1b0lla83; path=/
X-Powered-By: PleskLin
```

下图是一个典型的 SSH banner：

4.2. 设备元数据

Shodan 除了获取 banner 外，还可以获取指定设备的元数据，如设备的地址位置、操作系统信息、互联网设备提供商、自治系统编号等。

下图为一个设备的元数据：

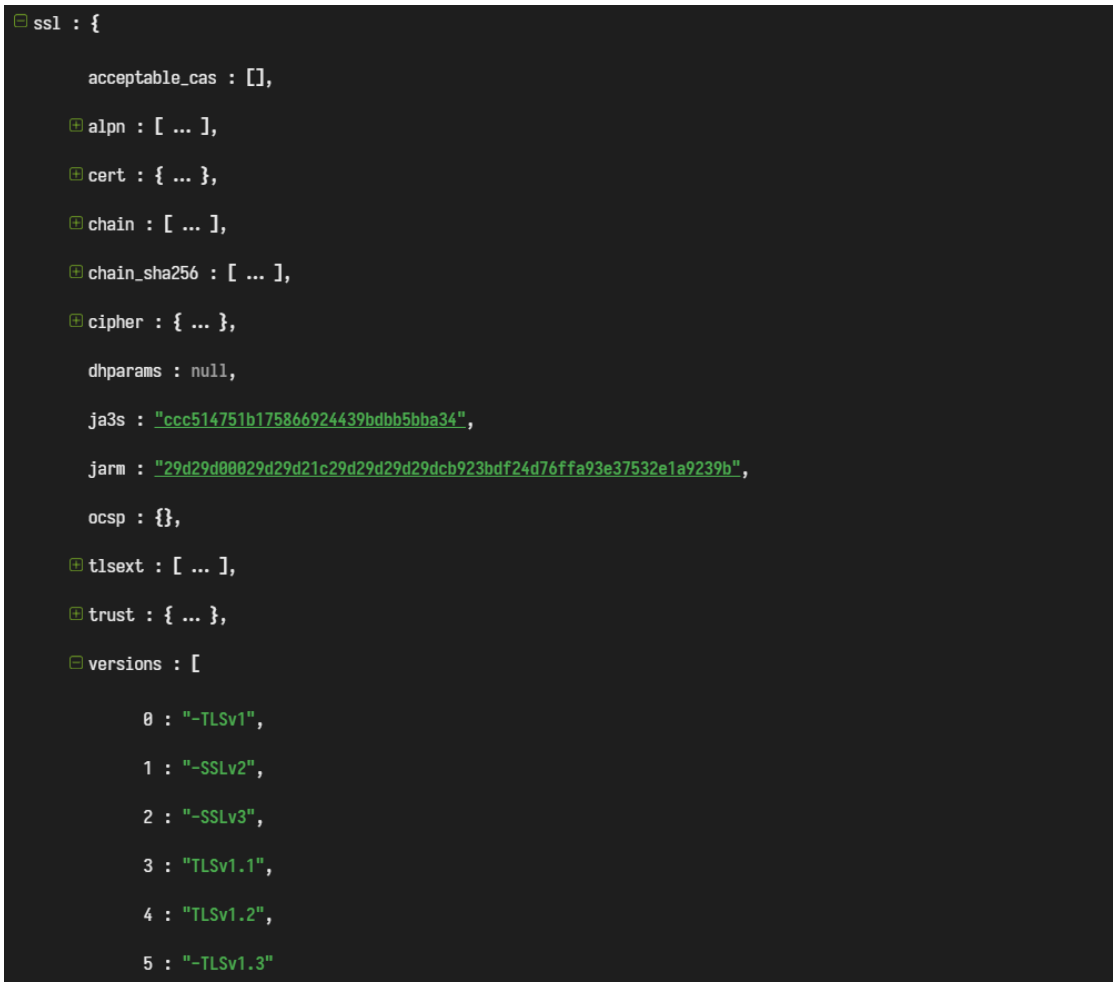


4.3. SSL

SSL 目前是互联网上最为重要的服务，Shodan 也收集其 Banner，包括每个 SSL 的功能服务以及漏洞信息。

4.3.1. SSL banner

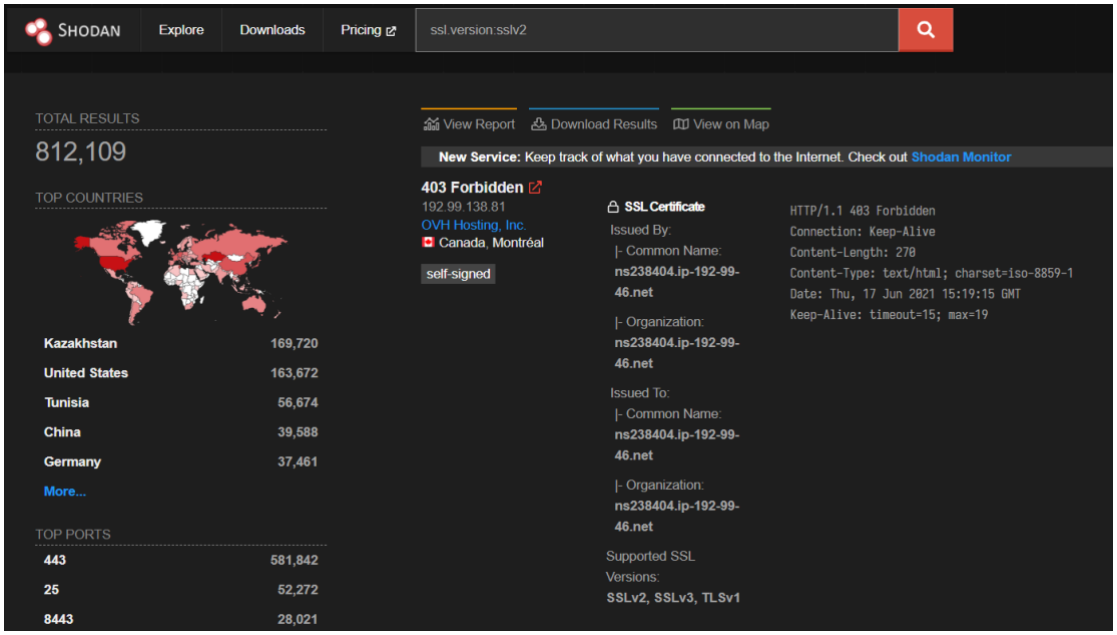
下图为一个标准的 SSL bannner 信息，包括协议、证书、版本等信息。版本信息中，如果存在”-“符号，那么该设备不支持该 SSL 版本，如果版本不以”-”开头，则服务支持给定的 SSL 版本。例如，下图中的服务器，只支持 TLSv1.1、TLSv1.2。



4.3.2. SSL 检索

SSL 版本信息还可以通过 Shodan 网页或者 API 进行检索。例如，输入：

ssl.version:sslv2，将返回允许使用 SSLv2 的所有 SSL 服务，包括 HTTP、SMTP、POP3、IMAP 等。



4.4. Web 组件

Shodan 的爬虫会尝试确定网站的 web 技术，对于 http、https 模块，爬虫将分析 hedaer 与 HTML 来分析判断网站的组件，并将结果存储在 http.components 元数据中，例如：

http.components 表明该网站在运行 Wordpress 内容管理系统，该系统还使用了 PHP、Mysql 等技术。

5. Shodan API

5.1. Developer API

Shodan 提供了一个开发者 API，来编写程序获取所需要的信息。可以通过网站搜索完成的工作，都可以通过 API 来完成。

该 API 分为两部分：REST API、Streaming API。REST API 提供搜索 Shodan 的方法，查找主机，获取关于查询信息的摘要。Streaming API 提供 Shodan 当前收集的数据的原始实时返回。有几个不同的套餐可以获取，该 API 获取的数据不能被搜索或用其他方式进行交互，适用于需要获取大量数据的人。

只有购买开发者 API 计划的人才能获得 Streaming API。

5.2. API 使用限制

根据 API 的套餐不同，API 会有不同的限制：

1. 搜索：每月的搜索次数有不同的限制，且需要使用查询积分。如果直接查询不会消耗查询积分，若进行过滤器或者是超过一页的搜索就需要消耗查询积分。搜索 apache 不需要消耗查询积分，搜索 apache country:"US"将会消耗一个查询积分，就算查询第二页也只会消耗一个查询积分。

2. 扫描：按需获得的 API 也会根据积分限制每月扫描主机的数量。对于每个主机的扫描都需要一个扫描积分才能扫描。

3. 网络提醒：根据不同的 API 的使用次数可以使用提醒功能监视所查询的 IP。只有付费客户才能使用此功能，且无法在账户中创建超过 100 条提醒。

5.3. Facets

类似 Shodan 过滤器，对搜索结果的 Banner 字段进行过滤搜查。

例如，过滤器：port:22 对应的 Facets 为：ssh.fingerprint，详情请查看附录 B 获取。

目前 Facets 只能在 API 和 CLI 上使用。

5.4. 安装和初始化

安装 Shodan API：

pip install shodan / easy_install shodan

初始化：

import shodan

api = shodan.Shodan(API_KEY)

完成安装和 API_KEY 绑定后，便可使用 API 进行搜索。

5.5. 使用 API 进行搜索

Shodan.search()

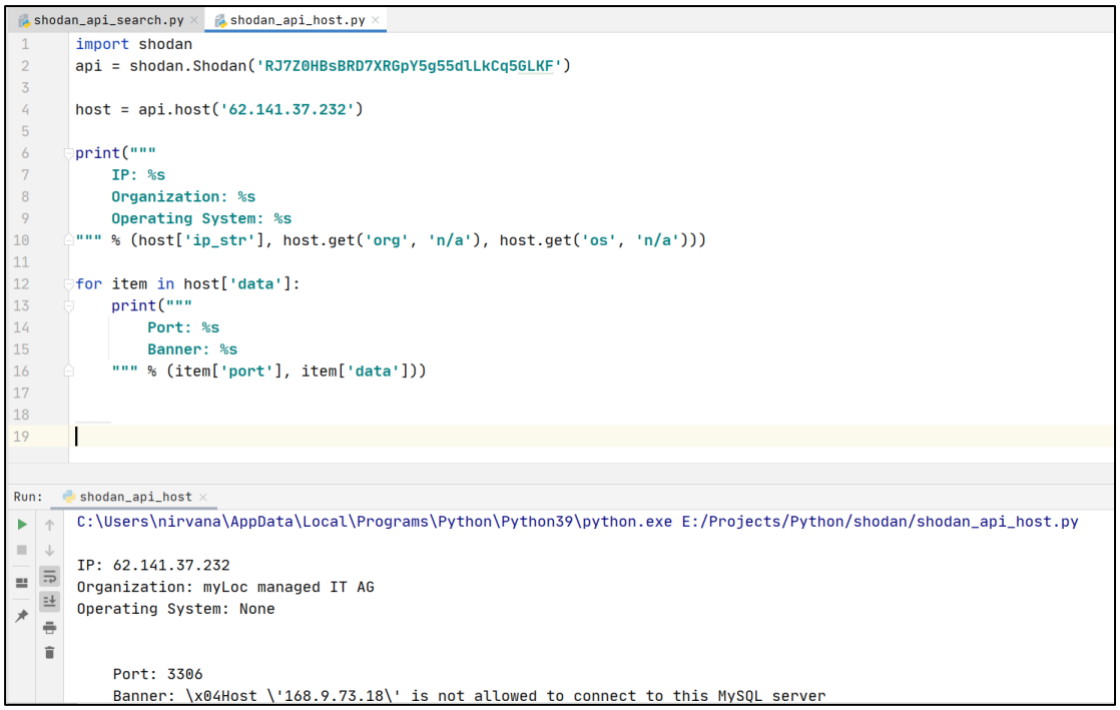
首先调用 api 对象的 Shodan.search( )方法 ,该方法返回的结果放入字典之中。然后，打印出搜索结果数量，最后将返回的结果进行遍历循环，并打印其 IP 和 banner。每一页的搜索结果为 100 个。

默认情况下，Shodan 为了节省带宽使用量，banner 中的一些大的字段会被截断（例如 HTML）。若想要检索所有的信息，需使用 minify=False 禁用概要。

Banner 包含的完整的属性列表请参考附录 A。

5.6. 使用 API 进行主机查询

Shodan.host()



默认情况下，Shodan 只返回最近收集的主机的信息。如果想获取 IP 地址的完整历史记录，需使用 history 参数。

host = api.host('62.141.37.232', history=True)

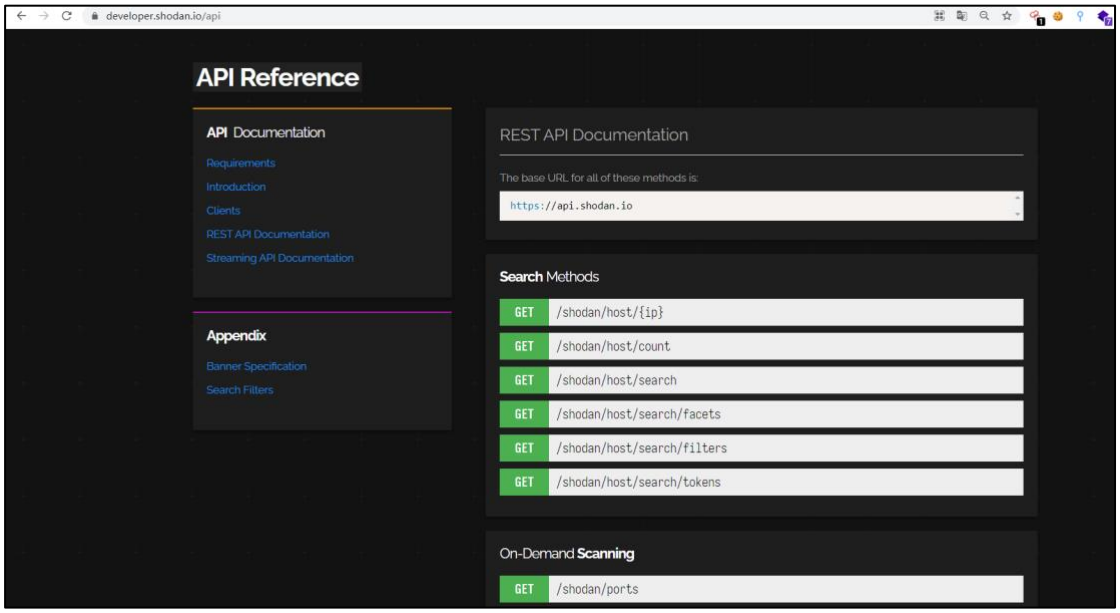
5.7. 使用 API 进行统计

Shodan.count()

```python
shodan_api_scan.py × shodan_api_count.py ×
    query = 'apache 2.4'

    # 计算结果
    result = api.count(query, facets=FACETS)

    print('Shodan Summary Information')
    print('Query: %s' % query)
    print('Total Results: %s\n' % result['total'])

    # 从列表facets中打印摘要信息
    for facet in result['facets']:
        print(FACET_TITLES[facet])

        for term in result['facets'][facet]:
            print('%s: %s' % (term['value'], term['count']))

        # Print an empty line between summary info
        print('')

except shodan.APIError as e:
    print('Error: {}'.format(e))
```

```
try › for facet in result['facets'] › for term in result['facets'][fa…
Run: shodan_api_count ×
C:\Users\nirvana\AppData\Local\Programs\Python\Python39\python.exe E:/Projects/Python/shodan/shodan_api_count.py
Shodan Summary Information
Query: apache 2.4
Total Results: 453662

Top 10 Countries
US: 104945
```

更多 API 接口请参考：https://developer.shodan.io/api 获取



6. Shodan CLI

6.1. 安装

Shodan 有官方 Python 库，项目位于：

https://github.com/achillean/shodan-python ,安装最新的 Shodan 命令行可以通过以下命令安装：

easy_install shodan 或 pip install shodan

要确认是否安装成功，可以运行以下命令，若返回 Shodan 命令行子命令列表，则表明安装成功：

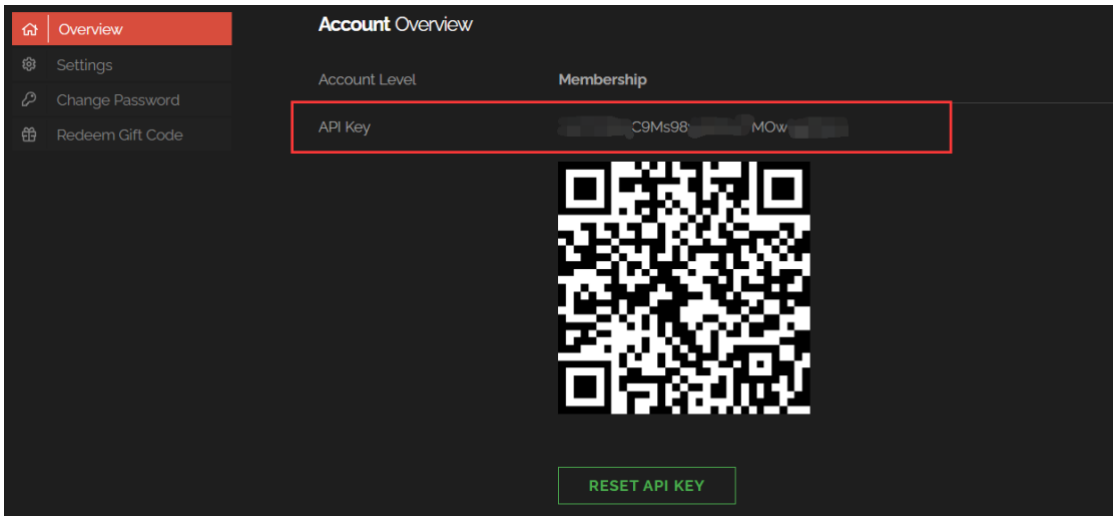
shodan

```
root@VM-0-5-ubuntu:~# shodan
Usage: shodan [OPTIONS] COMMAND [ARGS]...

Options:
  -h, --help  Show this message and exit.

Commands:
  alert       Manage the network alerts for your account
  convert     Convert the given input data file into a different format.
  count       Returns the number of results for a search
  data        Bulk data access to Shodan
  domain      View all available information for a domain
  download    Download search results and save them in a compressed JSON...
  honeyscore  Check whether the IP is a honeypot or not.
  host        View all available information for an IP address
  info        Shows general information about your account
  init        Initialize the Shodan command-line
  myip        Print your external IP address
  org         Manage your organization's access to Shodan
  parse       Extract information out of compressed JSON files.
  radar       Real-Time Map of some results as Shodan finds them.
```

6.2. 初始化密钥

安装好 Shodan 命令行工具后，还需要初始化 API_KEY，才能正常使用，输入以下命令即可绑定 API_KEY，API_KEY 可以在账户概览中查看：

shodan init API_KEY



执行 shodan init 后，命令行回显 Successfully initialized 表示初始化成功。。

```
root@VM-0-5-ubuntu:~# shodan init 2o0T      98ysbiSNJTM
Successfully initialized
root@VM-0-5-ubuntu:~#
```

6.3. 命令详解

Shodan 命令行的每个子命令都可以通过-h 查询命令帮助。

```
root@VM-0-5-ubuntu:~# shodan alert create -h
Usage: shodan alert create [OPTIONS] <name> <netblocks>

  Create a network alert to monitor an external network

Options:
  -h, --help  Show this message and exit.
```

6.3.1. alert 命令

alert 命令提供创建、列表、清楚以及删除网络监视的功能。

6.3.1.1. 创建监视器

shodan alert create 监视器名 IP 或网络范围列表(CIDR 表示法)

如下图，为创建一个名为 test，IP 为 62.141.37.232 的监视器：

```
root@VM-0-5-ubuntu:~# shodan alert create test 62.141.37.232
Successfully created network alert!
Alert ID: AF3WQ821HH4YG56Q
root@VM-0-5-ubuntu:~#
```

6.3.1.2. 查询监视器信息

shodan alert info Alert_ID

```
root@VM-0-5-ubuntu:~# shodan alert info AF3WQ821HH4YG56Q
test
Created: 2021-06-18T02:19:22.290000
Notifications: disabled

Network Range(s):
 > 62.141.37.232
```

6.3.1.3. 删除监视器

shodan alert remove Alert_ID

6.3.2. domain 命令

domain 命令查找与域名有关的所有信息，包括子域名，域名记录类型等。

shodan domain xx.com --type CNAME -H

```
ubuntu@VM-0-5-ubuntu:~$ shodan domain tap4fun.com --type CNAME -H
TAP4FUN.COM

a.portal-platform        CNAME  d29hr3h3hiqnl8.cloudfront.net
a.portal-platform        CNAME  portal-a-tap4fun-1131221457.us-west-2.elb.amazonaws.com
akamai-f.portal-platform  CNAME  akamai-portal-a-tap4fun.tap4fun.com.srip.net
akamai-f.portal-platform  CNAME  portal-a-tap4fun-1131221457.us-west-2.elb.amazonaws.com
akamai.p301              CNAME  tap4fun.edgesuite.net
b                        CNAME  bastion.tap4fun.com
b.portal-platform        CNAME  tokyo-portal-platform-1043349026.ap-northeast-1.elb.amazonaws.com
ba.akamai                CNAME  wildcard-v4.akamai.tap4fun.com.edgekey.net
ba.gateway               CNAME  elb-ba-gateway-1750898565.us-west-2.elb.amazonaws.com
bbs                      CNAME  tap4fun.com
c.portal-platform        CNAME  fk-portal-platform-1-1795622413.eu-central-1.elb.amazonaws.com
campus                   CNAME  customapply.mokahr.com
cn                       CNAME  elb-web-tap4fun-1820861536.us-west-2.elb.amazonaws.com
cndl.gl                  CNAME  cndl.gl.tap4fun.com.w.alikunlun.com
e                        CNAME  email.secureserver.net
e.portal-platform        CNAME  portal-a-tap4fun-1131221457.us-west-2.elb.amazonaws.com
email                    CNAME  email.secureserver.net
gateway.pf               CNAME  PF-gateway-1397015035.us-west-2.elb.amazonaws.com
gateway.pf               CNAME  portal-a-tap4fun-1131221457.us-west-2.elb.amazonaws.com
gateway2.pf              CNAME  pf-gold.portal-platform.tap4fun.com
guide.pf                 CNAME  d1ekuex9v90jlu.cloudfront.net
images                   CNAME  elb-web-tap4fun-1820861536.us-west-2.elb.amazonaws.com
images.web               CNAME  d2p2fa87jazjha.cloudfront.net
imap                     CNAME  imap.secureserver.net
invasion                 CNAME  tf-lb-20190506033533268900000001-181456960.us-west-2.elb.amazonaws.com
```

6.3.3. host 命令

host 命令查找主机相关的信息，包括主机名、地理位置、漏洞、开放端口以及条目更新时间。

6.3.3.1. 查询完整历史信息

shodan host –history IP

```
root@VM-0-5-ubuntu:~/workspace# shodan host --save --history 62.141.37.232
62.141.37.232
Hostnames:              root-space.eu
City:                   Düsseldorf
Country:                Germany
Organization:           myLoc managed IT AG
Updated:                2021-06-18T01:14:51.421184
Number of open ports:   15
Vulnerabilities:        CVE-2008-2939  CVE-2012-0027  CVE-2017-7679  CVE-2007-4465  CVE-2007-4995  CVE-2006-5752
52      CVE-2012-2687   CVE-2007-4752  CVE-2017-3167  CVE-2011-4327  CVE-2012-0053  CVE-2012-0883  CVE-2017-3169
17      CVE-2006-3738   CVE-2014-0195  CVE-2011-3348  CVE-2007-1741  CVE-2006-7250  CVE-2011-5000  CVE-2011-3210
15      CVE-2007-1742   CVE-2007-1743  CVE-2010-5107  CVE-2010-0433  CVE-2009-1891  CVE-2013-2249  CVE-2010-0434
43      CVE-2008-2384   CVE-2011-0419  CVE-2014-0231  CVE-2010-4180  CVE-2014-3510  CVE-2009-4355  CVE-2008-3259
25      CVE-2011-1945   CVE-2018-1312  CVE-2011-3368  CVE-2009-0590  CVE-2014-0221  CVE-2014-3506  CVE-2014-3507
40      CVE-2008-1483   CVE-2007-5000  CVE-2008-5077  CVE-2016-10708 CVE-2013-0166  CVE-2014-3470  CVE-2013-0169
20      CVE-2007-6421   CVE-2007-5135  CVE-2007-6423  CVE-2008-4109  CVE-2012-1165  CVE-2010-0408  CVE-2014-0076
66      CVE-2016-8612   CVE-2017-3735  CVE-2012-2333  CVE-2007-3102  CVE-2012-3499  CVE-2012-0031  CVE-2008-0456
87      CVE-2011-4619   CVE-2008-7270  CVE-2009-0789

Ports:
    21/tcp              (2021-06-12)
    21/tcp              (2021-05-16)
    21/tcp              (2021-04-10)
    22/tcp OpenSSH (4.3p2 Debian 9etch2)            (2021-06-09)
    22/tcp OpenSSH (4.3p2 Debian 9etch2)            (2021-05-31)
```

6.3.3.2. 保存搜索信息

shodan host –save IP

```
root@VM-0-5-ubuntu:~/workspace# shodan host --save 62.141.37.231
62.141.37.231
Hostnames:              qweeky.de;vps2055036.fastwebserver.de
City:                   Düsseldorf
Country:                Germany
Organization:           myLoc managed IT AG
Updated:                2021-06-17T17:07:38.690172
Number of open ports:   6
Vulnerabilities:        CVE-2015-0204  CVE-2015-4000

Ports:
     22/tcp OpenSSH (8.0)
     25/tcp
     80/tcp
    111/tcp
    443/tcp
   8181/tcp
        |-- SSL Versions: -SSLv2, -TLSv1.1, -TLSv1.2, SSLv3, TLSv1
        |-- Diffie-Hellman Parameters:
```

6.3.4. convert 命令

convert 命令可导出 Shodan 搜索结果为指定文件 ,支持的文件格式包括 :kml, csv, geo.json, images, xlsx。

例如，将默认保存的 json.gz 格式的文件转换成 geo.json 文件格式：

shodan convert xx.xx.xx.xx.json.gz geo.json

```
Successfully created new file: 62.141.37.231.geo.json.37.231.json.gz geo.json
root@VM-0-5-ubuntu:~/workspace# ls
62.141.37.231.geo.json  62.141.37.231.json.gz
root@VM-0-5-ubuntu:~/workspace# cat 62.141.37.231.geo.json
{
           "type": "FeatureCollection",
           "features": [
       {"type": "Feature", "id": "62.141.37.231", "properties": {"name": "62.141.37.231", "lat": 51.22172, "lon": 6.77616},
untu:~/workspace#
```

6.3.5. count 命令

count 命令可以统计查询结果的数量 ,例如查询连网设备中 Windows 2012 的总数，以及 microsoft iis 6.5 的总数。

6.3.5.1. 查询指定设备类型的数量

shodan count Windows 2012

shodan count microsoft iis 6.5

```
root@VM-0-5-ubuntu:~/workspace# shodan count Windows 2012
278914
root@VM-0-5-ubuntu:~/workspace# shodan count microsoft iis 6.5
55
root@VM-0-5-ubuntu:~/workspace#
```

6.3.5.2. 查询指定网段在互联网上暴露的设备数量

shodan count net:78.13/16

shodan count net:78.13.16/24

```
root@VM-0-5-ubuntu:~/workspace# shodan count net:78.13/16
5829
root@VM-0-5-ubuntu:~/workspace# shodan count net:78.13.16/24
41
root@VM-0-5-ubuntu:~/workspace#
```

6.3.6. download 命令

download 命令可以搜索 Shodan 并将结果保存到本地，默认情况下 download 命令会下载 1000 条结果，如果想要到处更多数据，需要使用—limit 子命令。download 可以保存搜索结果到本地，随时使用 parse 命令处理分析结果，当再次导出相同搜索结果的时候，不会花费积分。

6.3.6.1. 导出 Shodan 搜索结果

下载 5 条 microsoft iis 6.5 的数据：

shodan download microsoft iis 6.5 --limit 5

```
root@VM-0-5-ubuntu:~/workspace# shodan download microsoft iis 6.5 --limit 5
Search query:                   iis 6.5
Total number of results:        65
Query credits left:             100
Output file:                    microsoft.json.gz
  [################################--------]   80%  00:00:05
Saved 5 results into file microsoft.json.gz
root@VM-0-5-ubuntu:~/workspace#
```

6.3.6.2. 分析导出的搜索结果

shodan parse microsoft.json.gz

```
Saved 5 results into file microsoft.json.gz
root@VM-0-5-ubuntu:~/workspace# ls
62.141.37.231.geo.json  62.141.37.231.json.gz  microsoft.json.gz
root@VM-0-5-ubuntu:~/workspace# shodan parse microsoft.json.gz
202.105.240.141 443             HTTP/1.1 302 Found\r\nconnection: close\r\nset-cookie: JSESSIONID=AA861A911
861A91136CA06D344A56A00D37A200\r\ncontent-length: 0\r\ndate: Sat, 19 Jun 2021 04:02:32 GMT\r\nserver: Micro
67.230.162.32   80      us.gutx.org     HTTP/1.1 200 OK\r\nDate: Sat, 19 Jun 2021 03:19:19 GMT\r\nServer: M
34.123.154.47   443     47.154.123.34.bc.googleusercontent.com  HTTP/1.1 200 OK\r\nDate: Thu, 17 Jun 2021 0
F-8\r\nX-Varnish-Url: /\r\nhost: www.staging.betabrand.io\r\nX-Varnish-Generated-By: b0\r\nX-Varnish-Cachea
ice-User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.
.1 varnish (Varnish/6.5)\r\nX-Varnish-Cache: HIT 38\r\nX-Varnish-Frontend-Cookie: No Frontend Cookie\r\nX-V
r\nContent-Length: 9712\r\nX-HAProxy-Server: staging-haproxy-7b6f444d4b-f5plw\r\nX-Unique-Id: 47068783:BC60
31536000; includeSubDomains\r\nX-Robots-Tag: none\r\n\r\n
162.220.63.198  80              HTTP/1.1 200 OK\r\nDate: Fri, 18 Jun 2021 22:51:08 GMT\r\nServer: Micorsoft
Encoding: chunked\r\nContent-Type: text/html; charset=GB2312\r\n\r\n
47.241.66.63    443             HTTP/1.1 404 Not Found\r\nContent-Length: 0\r\nDate: Fri, 18 Jun 2021 22:42
root@VM-0-5-ubuntu:~/workspace#
```

6.3.7. honeyscore 命令

honeyscore 命令可以用来检测设备是否是蜜罐，返回的 score 值表示该设备是蜜罐的可能性。

shodan honeyscore xx.xx.xx.xx

```
root@VM-0-5-ubuntu:~/workspace# shodan honeyscore 62.141.37.1
Not a honeypot
Score: 0.0
root@VM-0-5-ubuntu:~/workspace# shodan honeyscore 62.141.37.232
Not a honeypot
Score: 0.3
root@VM-0-5-ubuntu:~/workspace#
```

6.3.8. info 命令

info 命令主要用于查询绑定的 API_KEY 对应账号的账户信息、剩余查询次数、扫描积分等。

```
root@VM-0-5-ubuntu:~/workspace# shodan info
Query credits available: 100
Scan credits available: 100

root@VM-0-5-ubuntu:~/workspace#
```

6.3.9. myip 命令

myip 命令用于查询本机的出口 IP，功能类似于 curl ip.sb

shodan myip

```
root@VM-0-5-ubuntu:~/workspace# shodan myip
1.117.19.218
root@VM-0-5-ubuntu:~/workspace# curl ip.sb
1.117.19.218
root@VM-0-5-ubuntu:~/workspace# curl http://ip-api.com/json/?lang-zh-CN
```

6.3.10. parse 命令

parse 命令可以分析 Shodan 导出的搜索结果，并允许对结果进行过滤，也可以将 json 格式转换为 CSV。

例如，只查看搜索结果中的 ip、port、org

shodan parse --fields ip_str,port,org xx.xx.xx.xx.json.gz

```
root@VM-0-5-ubuntu:~/workspace# shodan parse --fields ip_str,port,org 62.141.37.231.json.gz
62.141.37.231   22      myLoc managed IT AG
62.141.37.231   25      myLoc managed IT AG
62.141.37.231   80      myLoc managed IT AG
62.141.37.231   111     myLoc managed IT AG
62.141.37.231   443     myLoc managed IT AG
62.141.37.231   8181    myLoc managed IT AG
62.141.37.231   22      myLoc managed IT AG
62.141.37.231   25      myLoc managed IT AG
62.141.37.231   80      myLoc managed IT AG
62.141.37.231   111     myLoc managed IT AG
62.141.37.231   443     myLoc managed IT AG
62.141.37.231   8181    myLoc managed IT AG
```

6.3.11. scan 命令

6.3.11.1. 查询所有可以扫描的协议

shodan scan protocols

```
root@VM-0-5-ubuntu:~/workspace# shodan scan protocols
afp                         AFP server information grabbing module
ajp                         Check whether the Tomcat server running AJP protocol
amqp                        Grab information from an AMQP service
andromouse                  Checks whether the device is running the remote mouse AndroMouse service.
apple-airport-admin         Check whether the device is an Apple AirPort administrative interface.
ard                         Query the Apple Remote Desktop service for information about the device
auto                        Detect the type of service that runs on the port and send the appropriate request.
automated-tank-gauge        Get the tank inventory for a gasoline station.
bacnet                      Gets various information from a BACnet device.
beanstalk                   Get general information about the Beanstalk daemon
bgp                         Checks whether the device is running BGP.
```

6.3.11.2. 对目标发起扫描结果并存储扫描结果

shodan scan submit --filename xx.xxx.xx.xx_scan.json.gz xx.xx.xx.xx

```
root@VM-0-5-ubuntu:~/workspace# shodan scan submit --filename 1.117.19.218_scan.json.gz 1.117.19.218

Starting Shodan scan at 2021-06-19 13:02 - 100 scan credits left
o open ports found or the host has been recently crawled and cant get scanned again so soon.
root@VM-0-5-ubuntu:~/workspace# s
```

6.3.11.3. 查询扫描历史

shodan scan list

```
root@VM-0-5-ubuntu:~/workspace# shodan scan list
# 1 Scans Total - Showing 10 most recent scans:
# Scan ID               Status          Size       Timestamp
BrJLliV5lgBNmq1a        DONE            1          2021-06-19T05:02:55.618000
```

6.3.12. stats 命令

status 命令提供了搜索结果的摘要信息，可以统计搜索结果，例如，显示 Apache Web 服务器所在的最常用的国家。

shodan stats --facets country apache

```
root@VM-0-5-ubuntu:~/workspace# shodan stats --facets country apache
Top 10 Results for Facet: country
US                            6,558,817
DE                            1,721,915
JP                            1,575,501
CN                            1,291,401
FR                            1,005,912
GB                              648,871
NL                              551,257
CA                              517,972
HK                              497,495
BR                              363,059
```

7. Shodan 外部插件

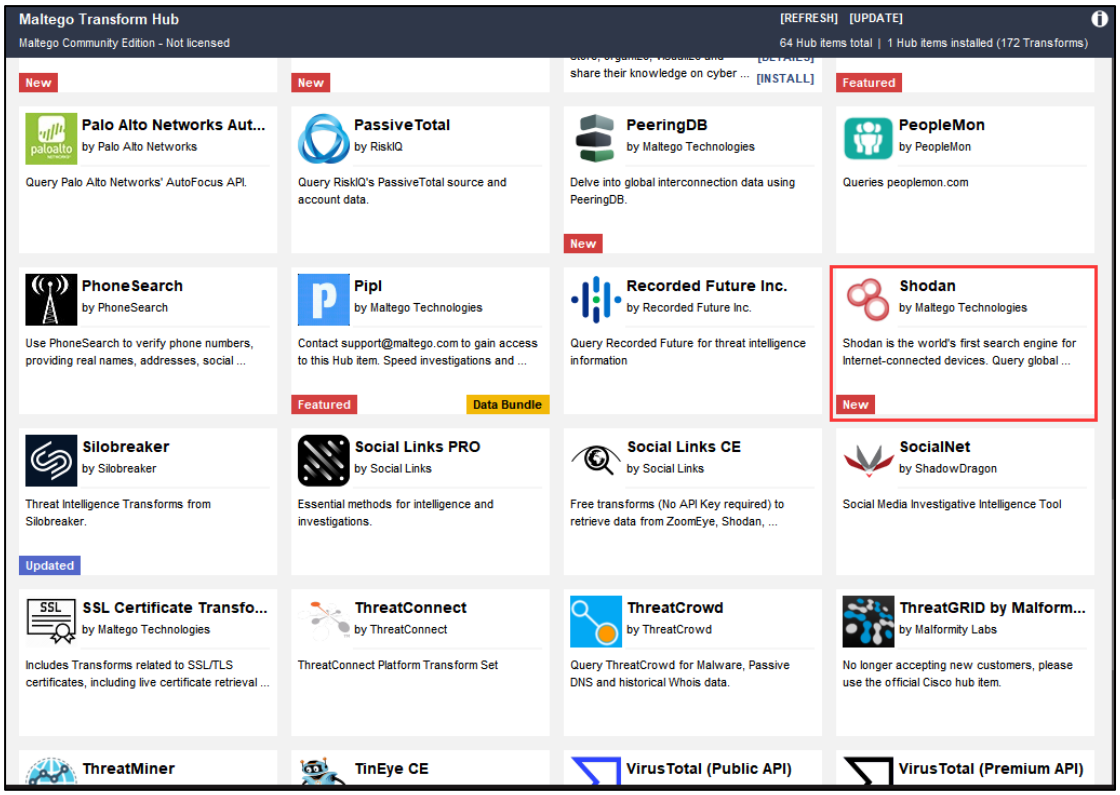
7.1. Maltego 扩展插件

7.1.1. Maltego 简介

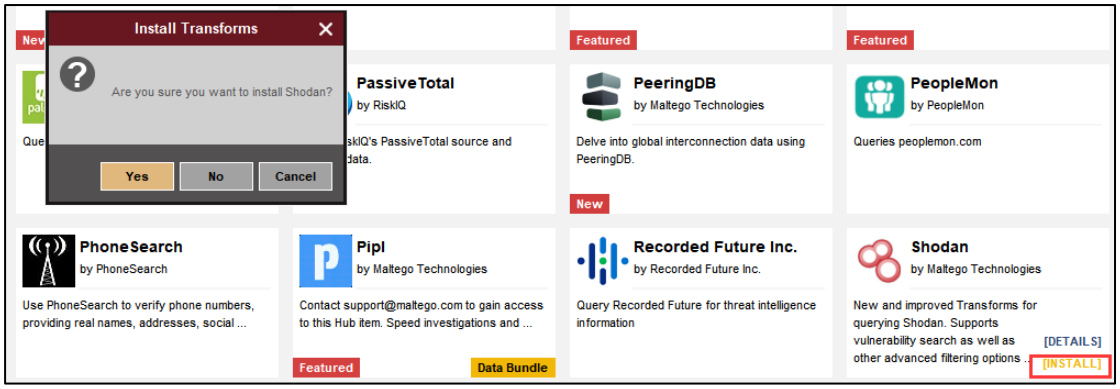
Maltego 是一个跨平台的信息搜集工具，可以安装在 Windows，Linux，MacOS 上。当然它在 Kali Linux 上是默认安装的，只需要一个域名，便可对互联网上的资源自上而下的搜集。它可以枚举网络和域的信息，包括 whois,nds，IP 地址；可以搜集 Person 的信息，电子邮件，网站，电话号码，组织，公司等。

7.1.2. 安装 Shodan 扩展插件

在 Maltego Home 界面-->Transform 选项卡中，找到 Shodan 插件

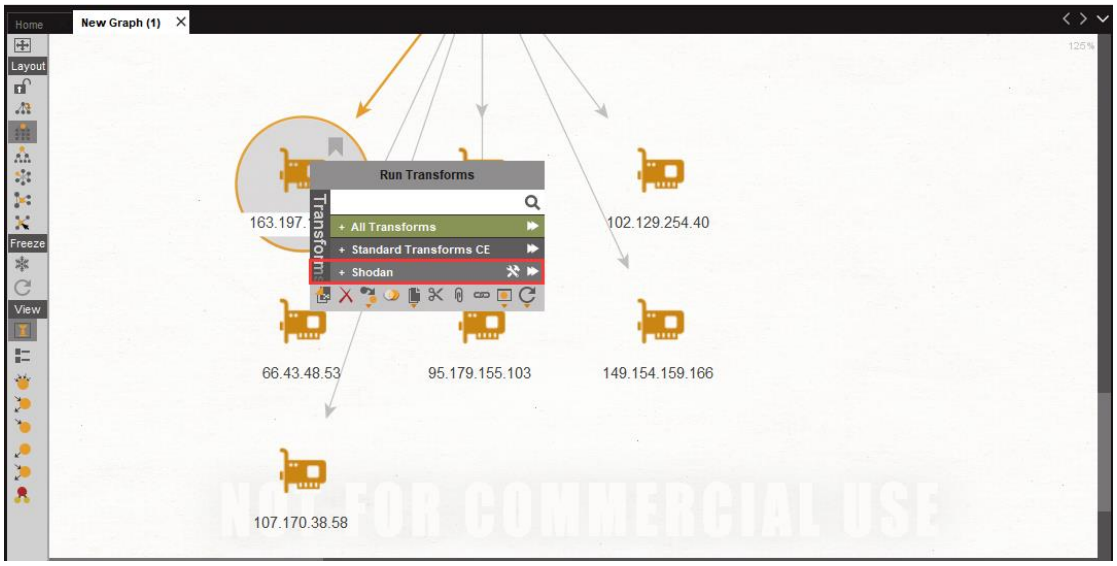


选择 install，并输入 API_KEY 完成安装。

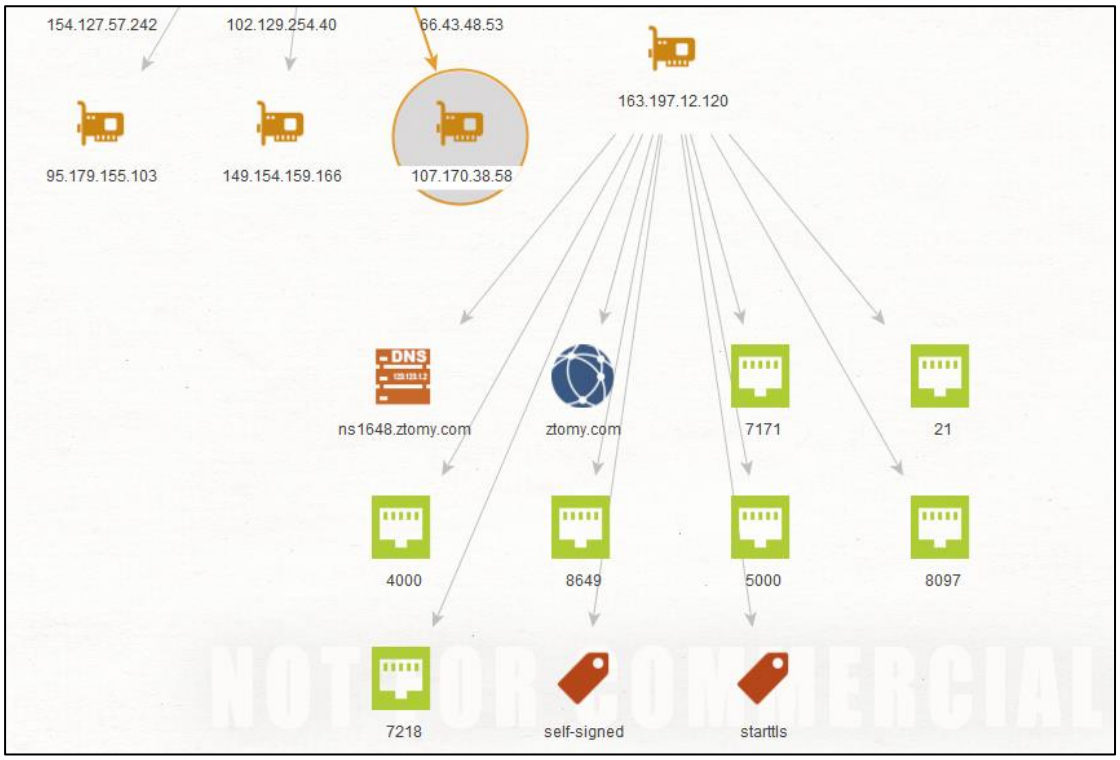


7.1.3. 使用 Shodan 扩展插件

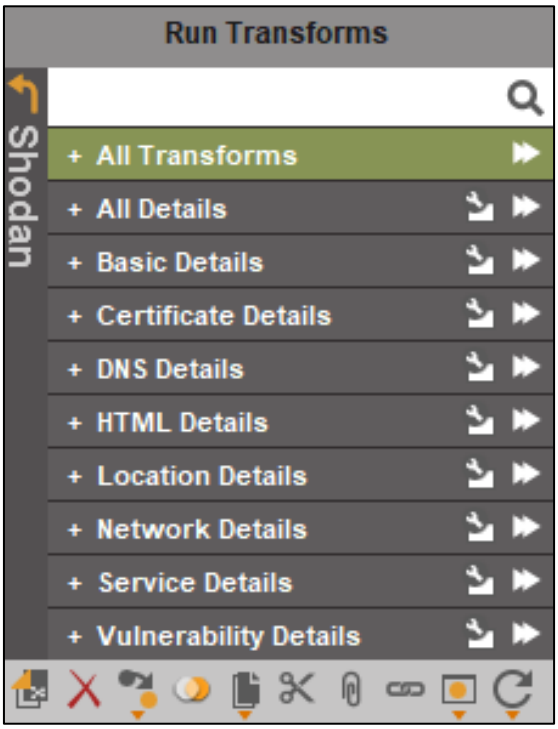
新建一个页面，创建相应的资产后，右键指定资产，便可对其使用 Shodan 进行资产收集分析。



下图为使用 Shodan 对目标资产 163.197.12.120 进行”All Details”信息收集的结果。



Shodan 扩展组件为 Maltego 提供的所有功能如下：



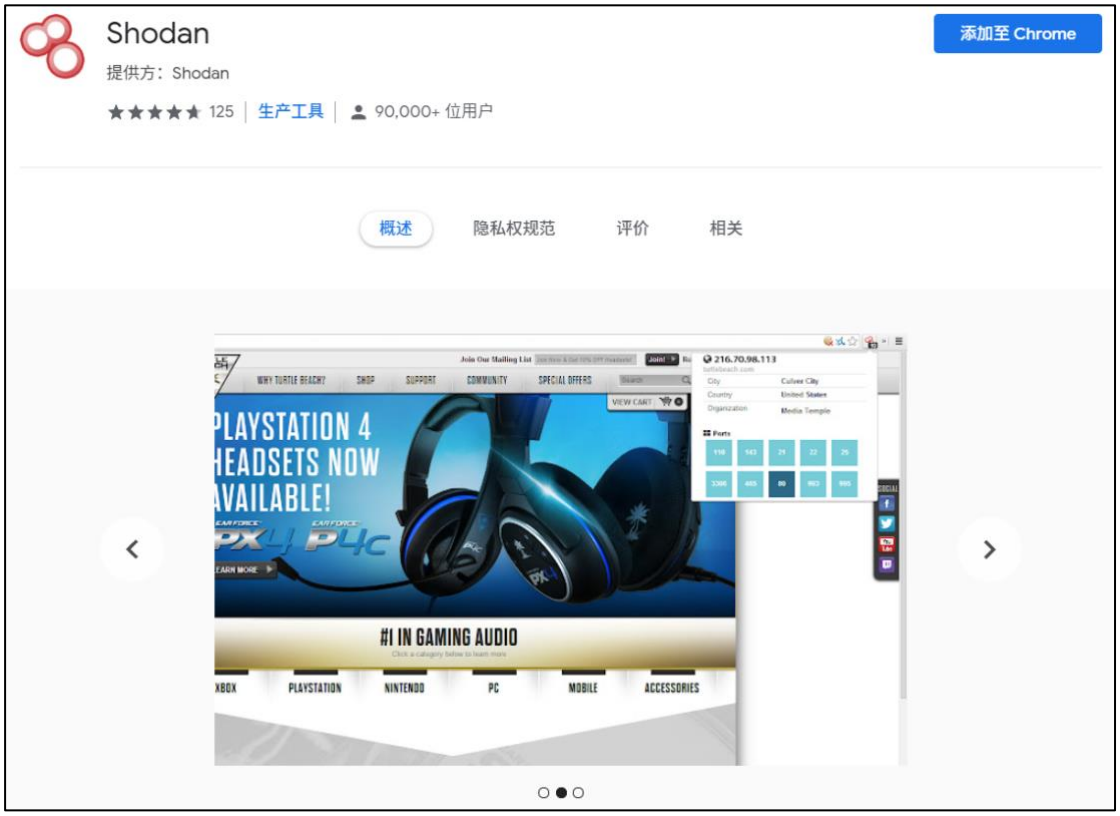
7.2. 浏览器插件

Shodan 为 Chrome 和 Firefox 都提供了扩展插件。

7.2.1. Chrome 扩展插件

应用商店链接：

https://chrome.google.com/webstore/detail/shodan/jjalcfnidlmpjhdfepjhjbhnhkbgleap



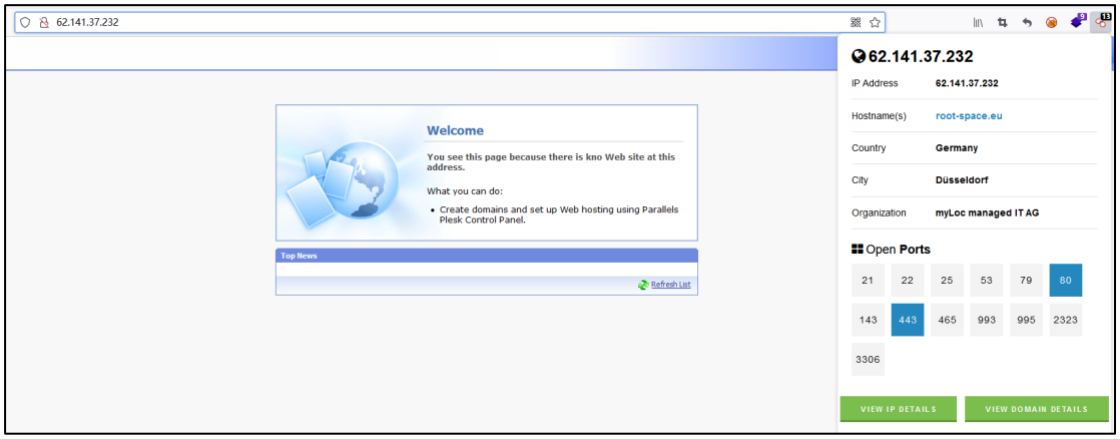
使用方法于 Wappalyzer 类似，在目标站点点击插件图片，即可看到站点相关信息，包括开放的端口等，点击下方”VIEW DETAILS”，可以查询更多站点相关信息。

7.2.2. Firefox 扩展插件

应用商店链接：

https://addons.mozilla.org/zh-CN/firefox/addon/shodan-addon/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

使用方法与 Chrome 插件相同：



7.3. MetaSploit 扩展模块

7.3.1. 搜索模块

模块位于：auxiliary/gather/shodan_search

set SHODAN_APIKEY API_KET

set QUERY “search query”

run

```
msf6 > use auxiliary/gather/shodan_search
msf6 auxiliary(gather/shodan_search) > show options

Module options (auxiliary/gather/shodan_search):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   DATABASE       false            no        Add search results to the database
   MAXPAGE        1                yes       Max amount of pages to collect
   OUTFILE                         no        A filename to store the list of IPs
   QUERY                           yes       Keywords you want to search for
   REGEX          .*               yes       Regex search for a specific IP/City/Country/Hostname
   SHODAN_APIKEY                   yes       The SHODAN API key

msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY 2
SHODAN_APIKEY => 2
msf6 auxiliary(gather/shodan_search) > set QUERY weblogic
QUERY => weblogic
msf6 auxiliary(gather/shodan_search) > run

[*] Total: 382485 on 3825 pages. Showing: 1 page(s)
[*] Collecting data, please wait...

Search Results
==============

 IP:Port              City             Country          Hostname
 -------              ----             -------          --------
 13.208.165.103:3557  Osaka            Japan            ec2-13-208-165-103.ap-northeast-3.compute.amazonaws.com
 13.208.211.232:9991  Osaka            Japan            ec2-13-208-211-232.ap-northeast-3.compute.amazonaws.com
 13.212.18.141:119    Singapore        Singapore        ec2-13-212-18-141.ap-southeast-1.compute.amazonaws.com
 13.229.148.6:79      Singapore        Singapore        ec2-13-229-148-6.ap-southeast-1.compute.amazonaws.com
 13.229.157.235:9006  Singapore        Singapore        ec2-13-229-157-235.ap-southeast-1.compute.amazonaws.com
 13.230.72.192:2761   Tokyo            Japan            ec2-13-230-72-192.ap-northeast-1.compute.amazonaws.com
 13.230.72.192:83     Tokyo            Japan            ec2-13-230-72-192.ap-northeast-1.compute.amazonaws.com
 13.231.56.206:2443   Tokyo            Japan            ec2-13-231-56-206.ap-northeast-1.compute.amazonaws.com
 13.233.119.24:8126   Mumbai           India            ec2-13-233-119-24.ap-south-1.compute.amazonaws.com
 13.236.184.246:491   Sydney           Australia        ec2-13-236-184-246.ap-southeast-2.compute.amazonaws.com
```

7.3.2. 蜜罐验证模块

模块位于：use auxiliary/gather/shodan_honeyscore

set SHODAN_APIKEY API_KET

set target IP

run

```
msf6 auxiliary(gather/shodan_honeyscore) > set target 62.141.37.232
target => 62.141.37.232
msf6 auxiliary(gather/shodan_honeyscore) > run

[*] Scanning 62.141.37.232
[-] 62.141.37.232 is probably not a honeypot
[*] 62.141.37.232 honeyscore: 0.3/1.0
[*] Auxiliary module execution completed
msf6 auxiliary(gather/shodan_honeyscore) >
```

7.3.3. 主机端口收集模块

模块位于：auxiliary/gather/shodan_search

set SHODAN_APIKEY API_KET

set RHOSTS ip/ips

run

```
msf6 auxiliary(gather/shodan_host) > set RHOSTS 62.141.37.232-62.141.37.254
RHOSTS => 62.141.37.232-62.141.37.254
msf6 auxiliary(gather/shodan_host) > run
[*] Running module against 62.141.37.232

[+] 62.141.37.232:993
[+] 62.141.37.232:995
[+] 62.141.37.232:79
[+] 62.141.37.232:143
[+] 62.141.37.232:80
[+] 62.141.37.232:465
[+] 62.141.37.232:2323
[+] 62.141.37.232:53
[+] 62.141.37.232:22
[+] 62.141.37.232:25
[+] 62.141.37.232:443
[+] 62.141.37.232:3306
[+] 62.141.37.232:21
[*] Running module against 62.141.37.233
[+] 62.141.37.233:80
[+] 62.141.37.233:22
[*] Running module against 62.141.37.234
[+] 62.141.37.234:80
[+] 62.141.37.234:22
[+] 62.141.37.234:111
[*] Running module against 62.141.37.235
[+] 62.141.37.235:8880
[+] 62.141.37.235:995
[+] 62.141.37.235:993
[+] 62.141.37.235:7080
```

8. Shodan 搜索指南

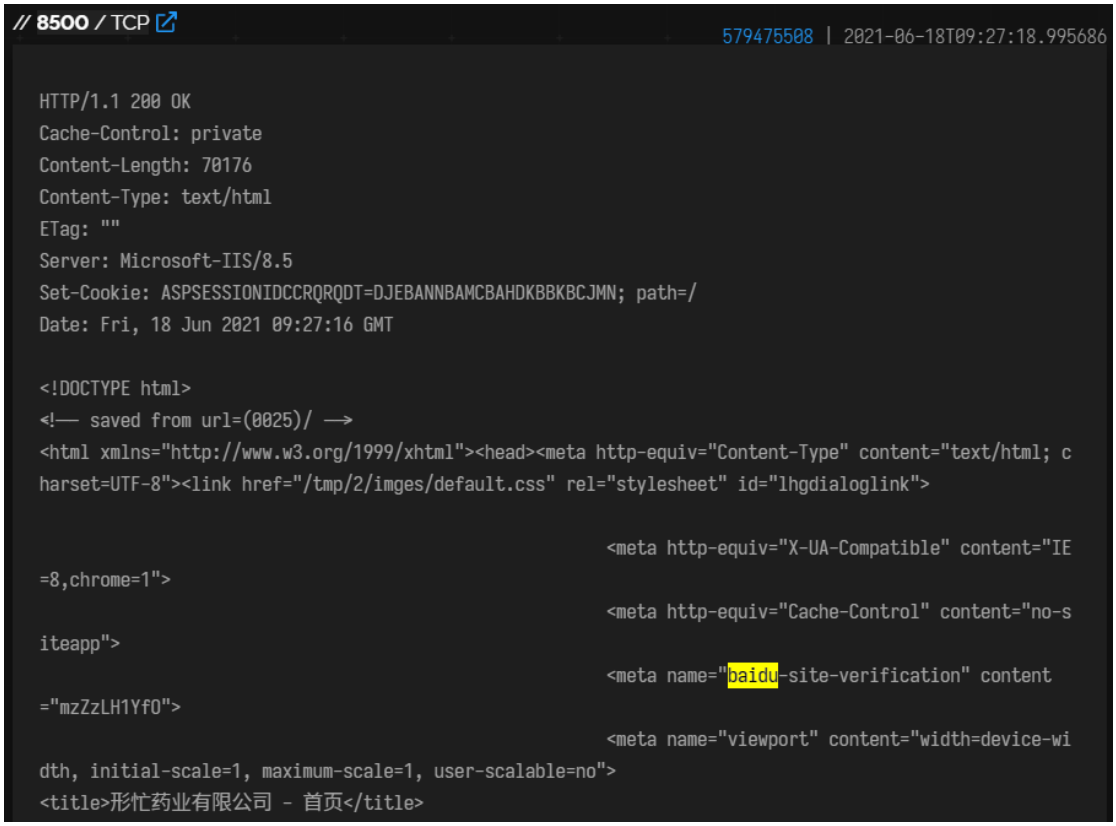
Shodan 作为一个搜索引擎，我们要熟悉它的查询语法，类似 google 语法，Shodan 的语法也是简单易懂，主要以键值对的形式进行查询。

8.1. 搜索范围

8.1.1. 默认字符串搜索范围

Shodan 默认情况下，搜索内容不区分大小写，并且只会从 Banner 中查询搜索内容，不对元数据进行搜索。例如，搜索”Google”，搜索结果只包含 Banner 中存在”Google”的设备，不一定会返回 Google 资产范围的结果。

例如，查找”baidu”，返回许多 Banner 中含有标签<meta name="baidu-site-verification">的设备，该标签为百度站长平台验证网站归属权的验证代码，并不属于百度相关的设备。


// 8500 / TCP
579475508 | 2021-06-18T09:27:18.995686
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 70176
Content-Type: text/html
ETag: ""
Server: Microsoft-IIS/8.5
Set-Cookie: ASPSESSIONIDCCRQRQDT=DJEBANNBAMCBAHDKBBKBCJMN; path=/
Date: Fri, 18 Jun 2021 09:27:16 GMT
<!DOCTYPE html>
<!— saved from url=(0025)/ —>
<html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; c
harset=UTF-8"><link href="/tmp/2/imges/default.css" rel="stylesheet" id="lhgdialoglink">
<meta http-equiv="X-UA-Compatible" content="IE
=8,chrome=1">
<meta http-equiv="Cache-Control" content="no-s
iteapp">
<meta name="baidu-site-verification" content
="mzZzLH1YfO">
<meta name="viewport" content="width=device-wi
dth, initial-scale=1, maximum-scale=1, user-scalable=no">
<title>形忙药业有限公司 - 首页</title>

8.1.2. 默认搜索时间范围

默认情况下，Shodan 将搜索过去 30 天内的数据。

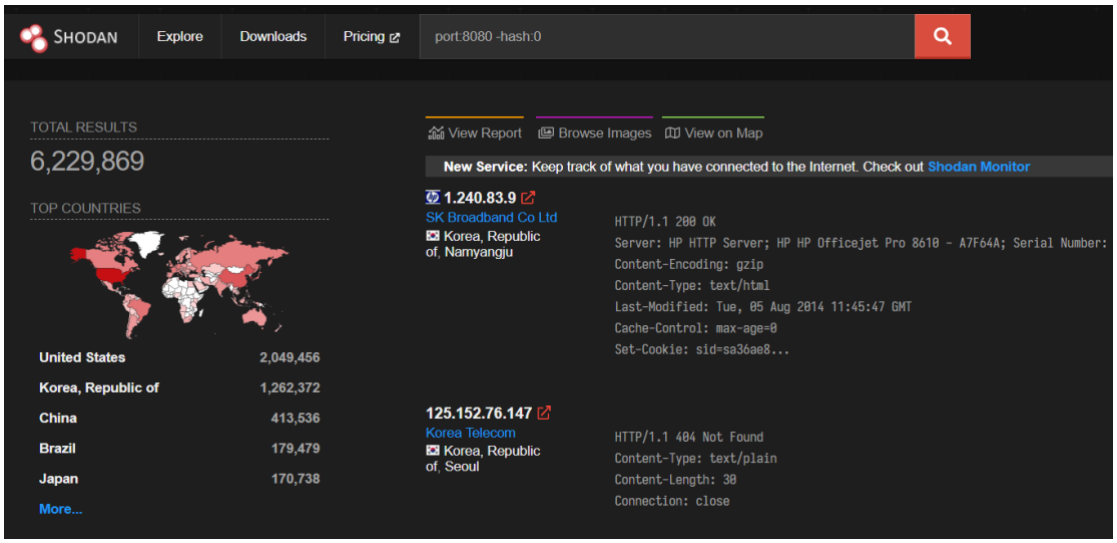
8.2. Shodan 搜索逻辑

Shodan 将尝试找到所有搜索项的结果，这意味着在每个搜索项之间隐含地存在+或 AND 连接符号。例如，搜索“Apache 2.4.9”，相当于搜索“Apache”+ "2.4.9"。

8.2.1. 排除符号“-”

例如，搜索开放 8080 端口，但 Banner 不为空的设备：

port:8080 -hash:0

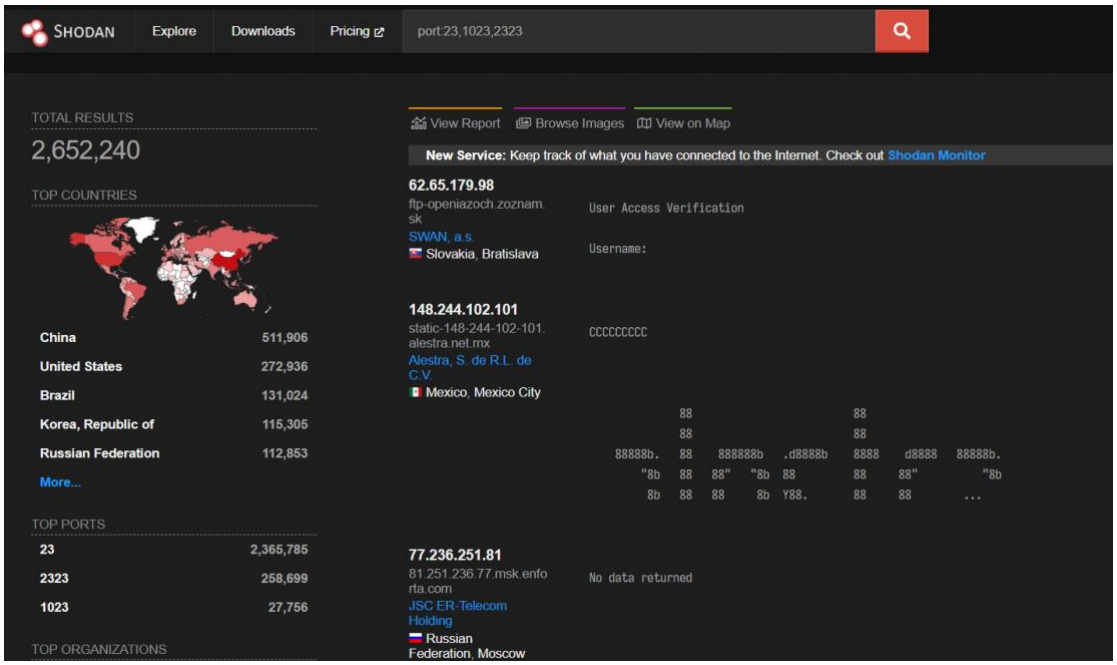


8.2.2. 联合查询“,”

例如，查询开放 23 或 1023 或 2323 端口的设备：

port:23,1023,2323

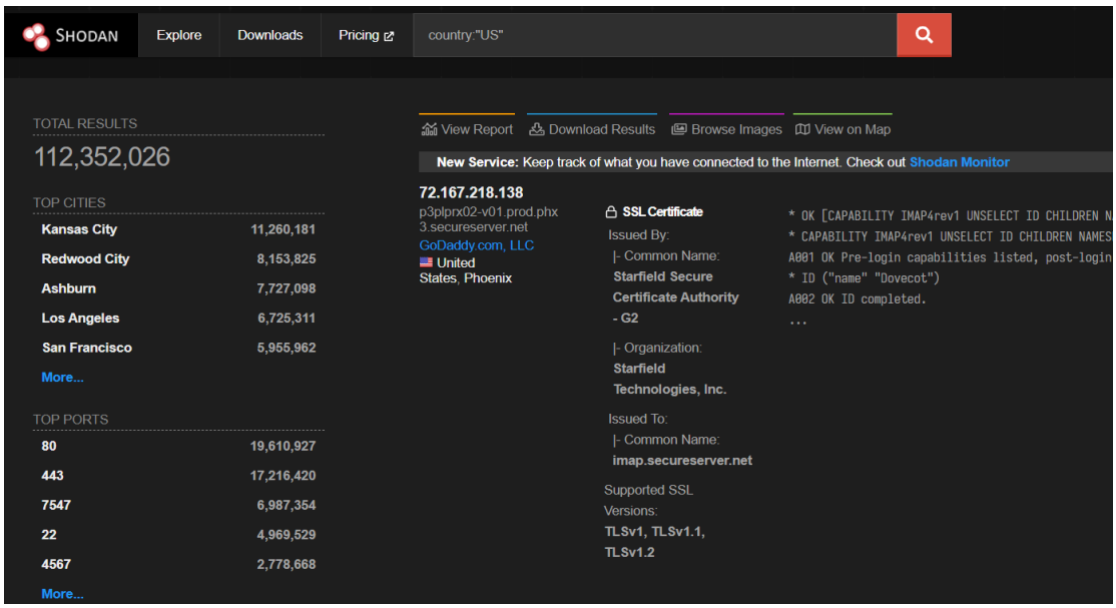
它们之间的关系是“或”



8.3. 地理位置搜索

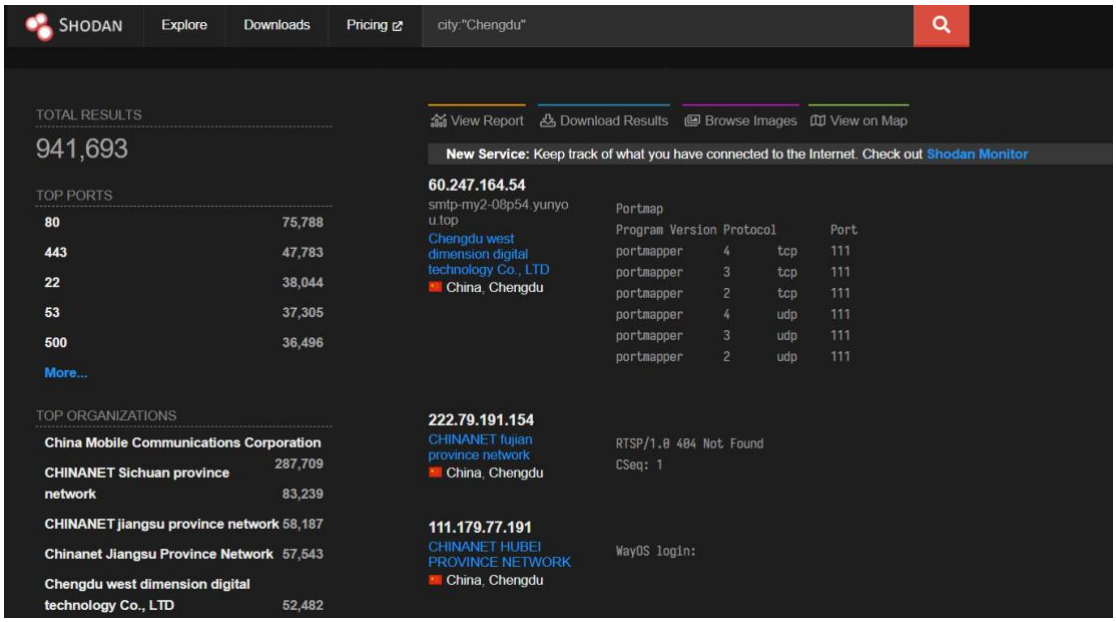
8.3.1. 搜索指定国家的相关设备

country:"US"



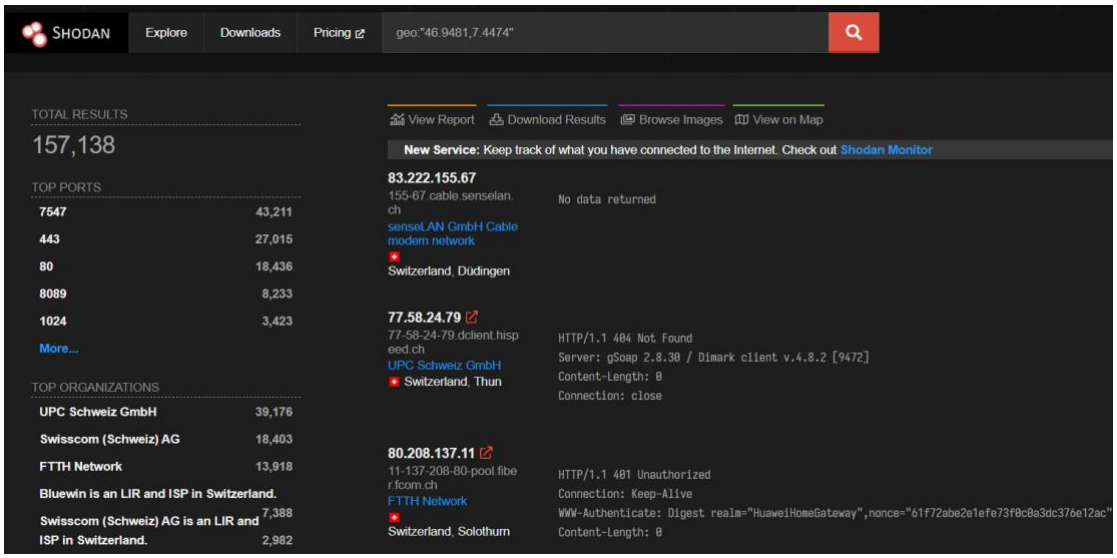
8.3.2. 搜索指定城市的相关设备

city:"Chengdu"



8.3.3. 搜索指定经纬度的相关设备

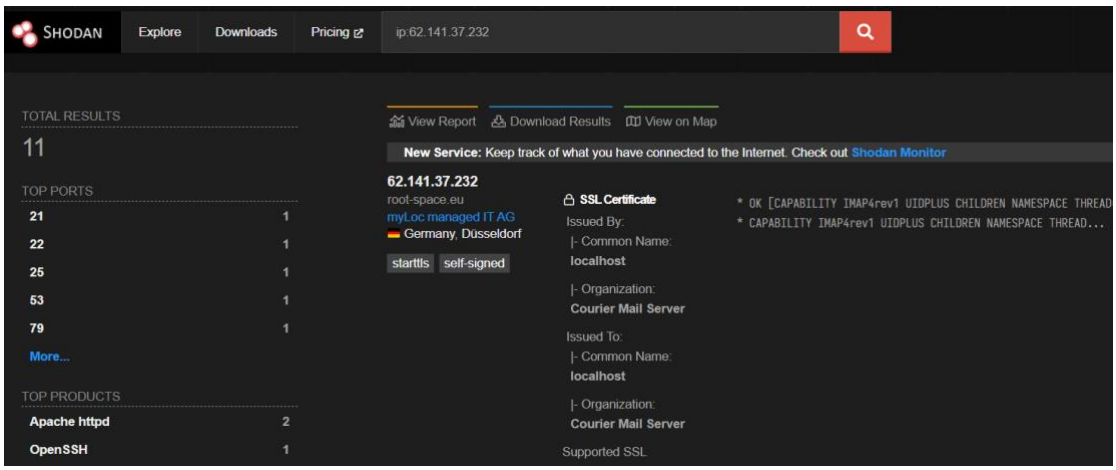
geo:"46.9481,7.4474"


SHODAN
Explore
Downloads
Pricing
geo:"46.9481,7.4474"
TOTAL RESULTS
157,138
TOP PORTS
7547 43,211
443 27,015
80 18,436
8089 8,233
1024 3,423
More...
TOP ORGANIZATIONS
UPC Schweiz GmbH 39,176
Swisscom (Schweiz) AG 18,403
FTTH Network 13,918
Bluewin is an LIR and ISP in Switzerland. 7,388
Swisscom (Schweiz) AG is an LIR and ISP in Switzerland. 2,982
View Report
Download Results
Browse Images
View on Map
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
83.222.155.67
155-67.cable.senselan.ch
senseLAN GmbH Cable modem network
Switzerland, Düdingen
No data returned
77.58.24.79
77-58-24-79.dclient.hispeed.ch
UPC Schweiz GmbH
Switzerland, Thun
HTTP/1.1 404 Not Found
Server: gSoap 2.8.30 / Dimark client v.4.8.2 [9472]
Content-Length: 0
Connection: close
80.208.137.11
11-137-208-80-pool.fiber.fcom.ch
FTTH Network
Switzerland, Solothurn
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="61f72abe2e1efe73f0c0a3dc376e12ac"
Content-Length: 0

8.4. IP、域名及端口信息搜索

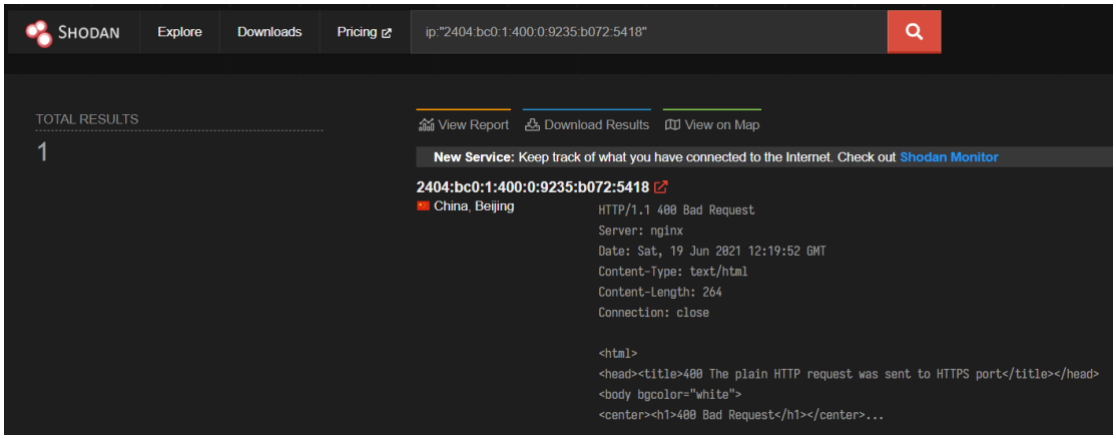
8.4.1. 搜索指定 IPv4 的相关设备

ip:62.141.37.232



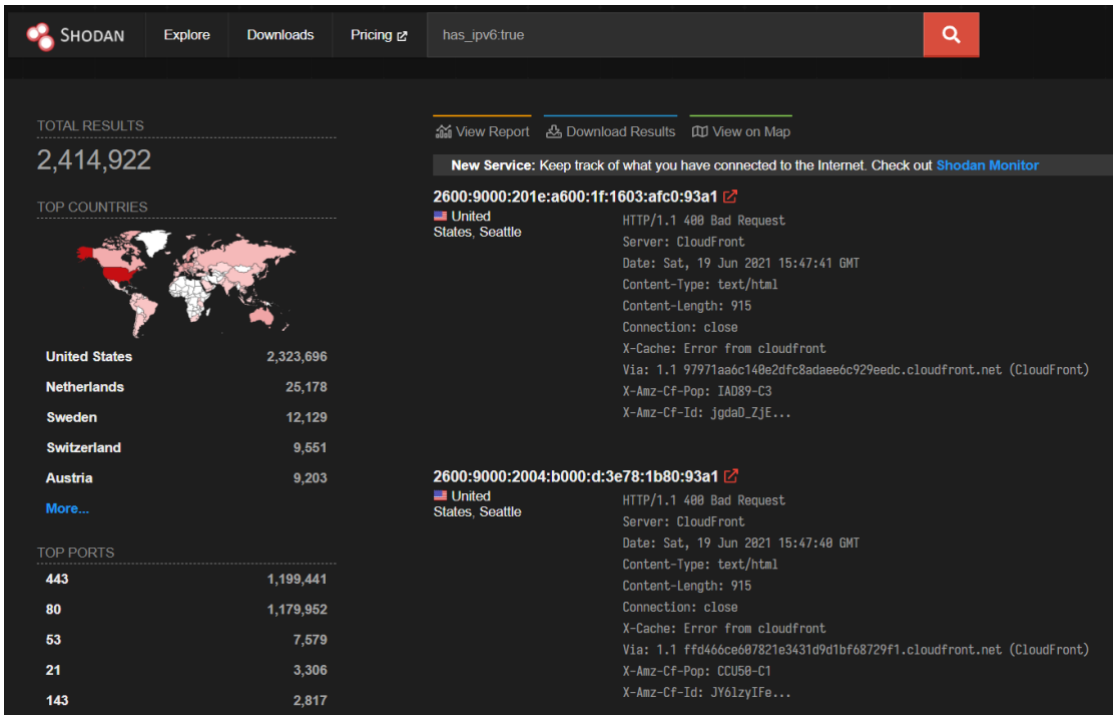
8.4.2. 搜索指定 IPv6 的相关设备

ip:"2404:bc0:1:400:0:9235:b072:5418"



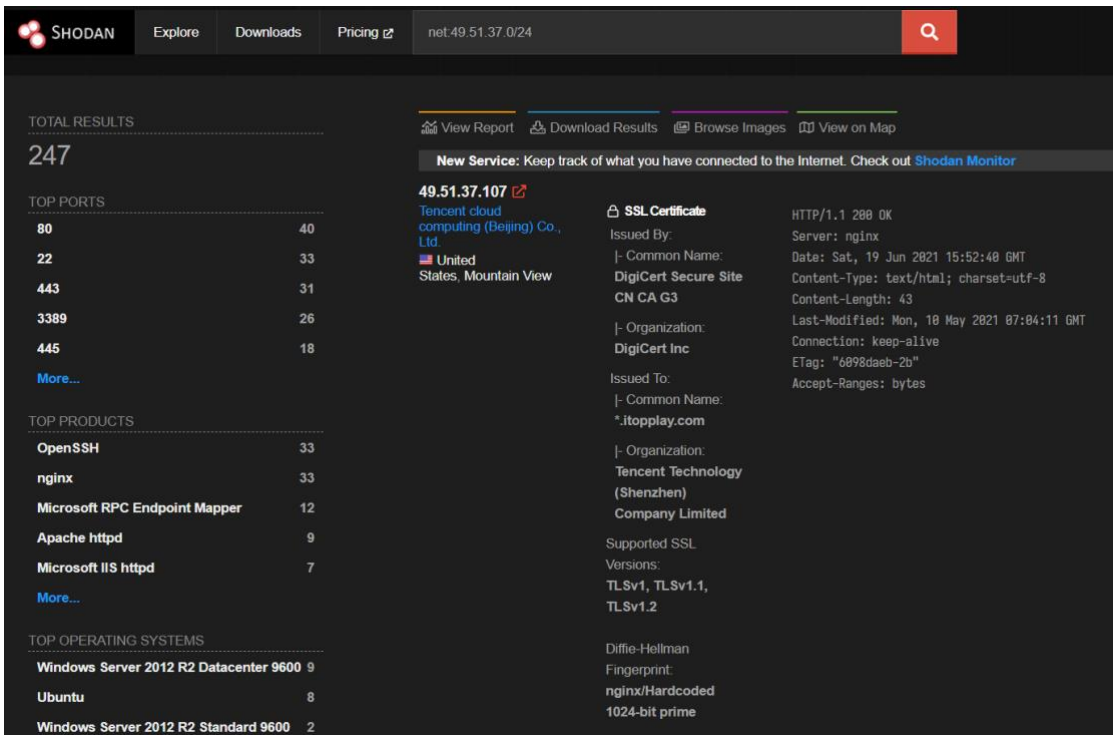
8.4.3. 搜索使用 IPv6 的相关设备

has_ipv6:true



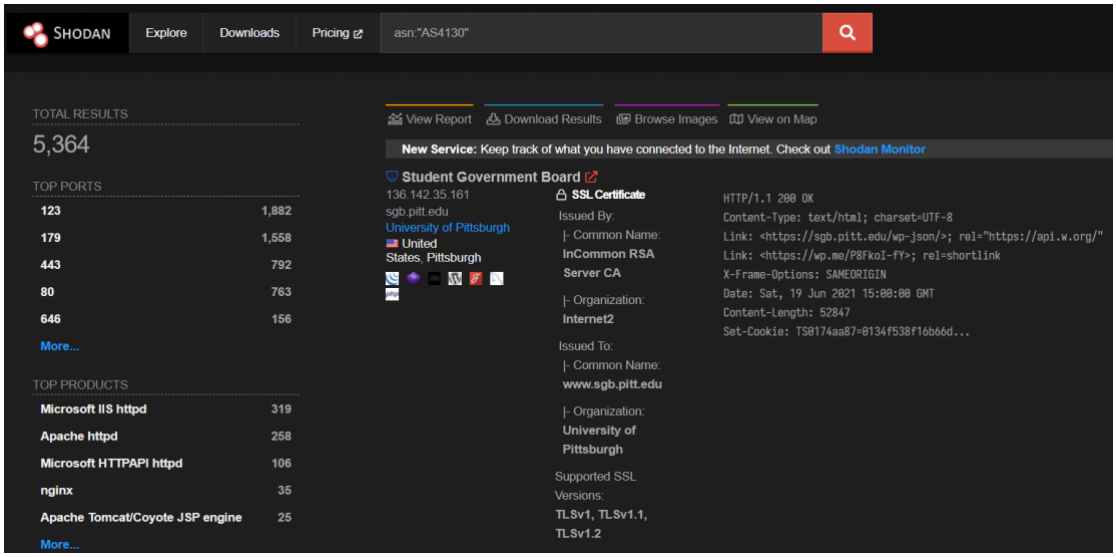
8.4.4. 搜索指定 CIDR 格式 IP 地址的相关设备

net:49.51.37.0/24



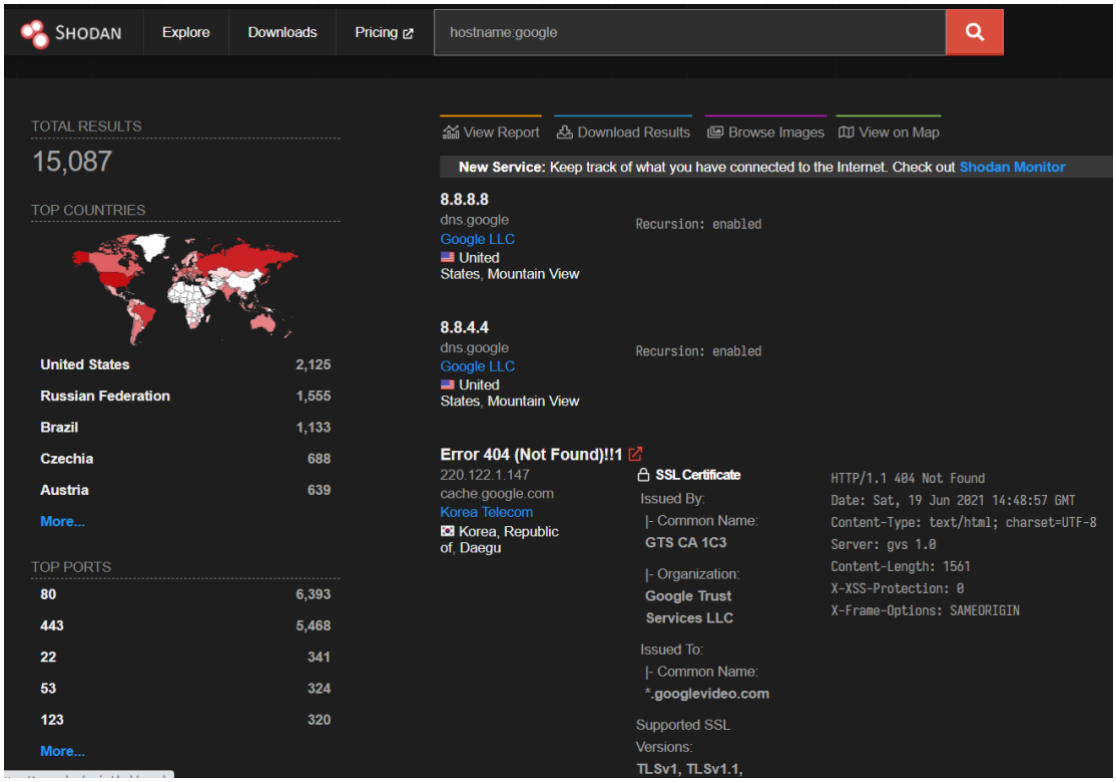
8.4.5. 搜索指定 ASN 的相关设备

asn:"AS4130"



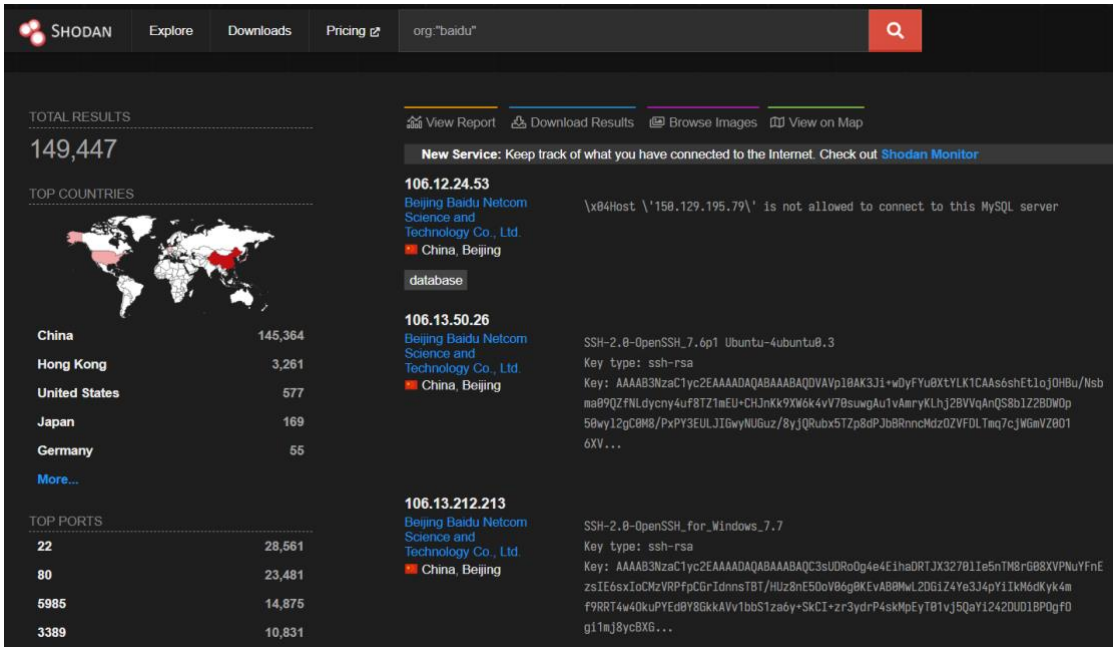
8.4.6. 搜索域名或主机名为“google”的相关设备

hostname:google



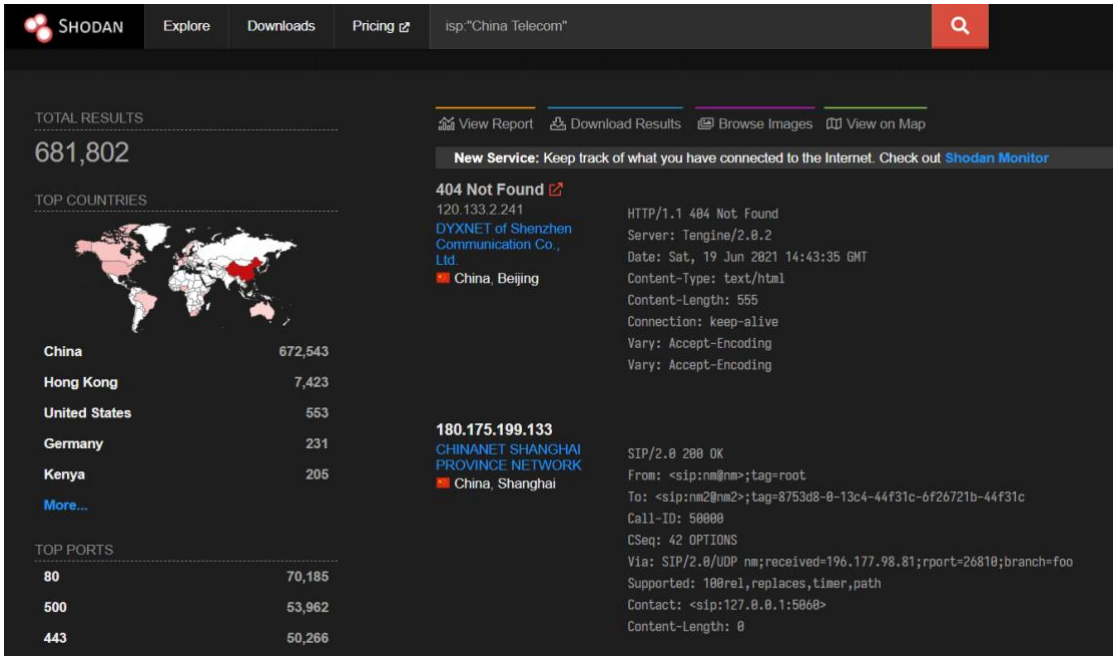
8.4.7. 搜索指定组织或公司的相关设备

org:"baidu"



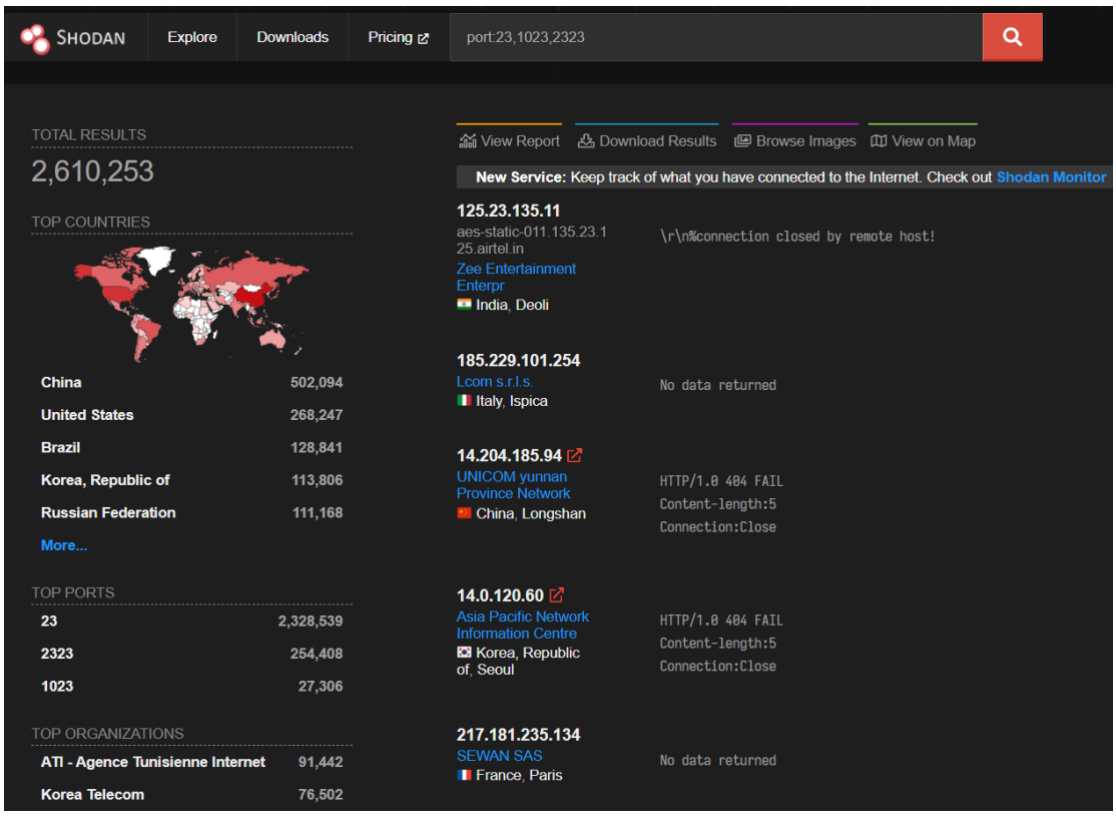
8.4.8. 搜索指定网络服务提供商的相关设备

isp: "China Telecom"



8.4.9. 搜索指定端口的相关设备

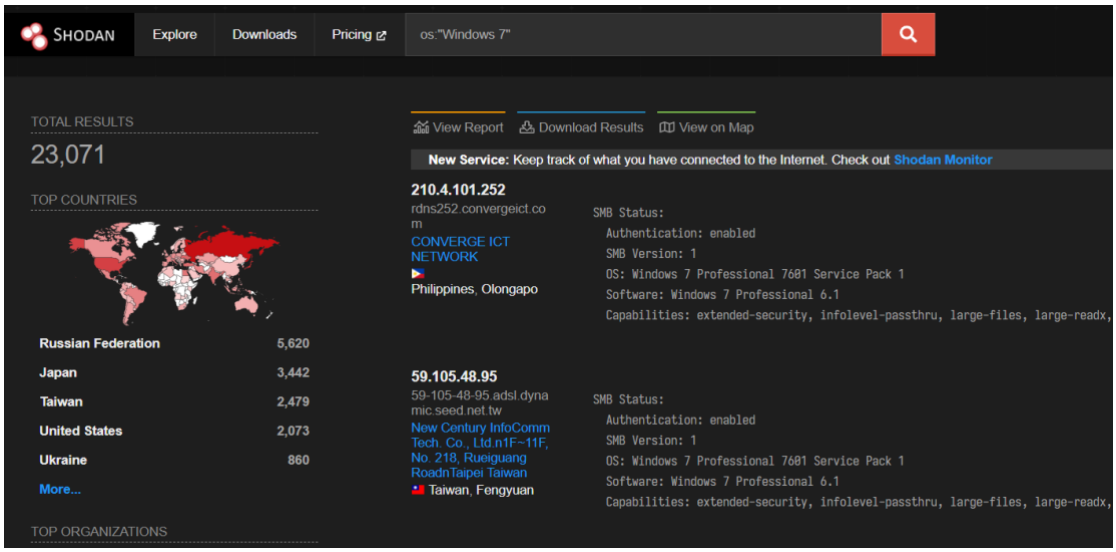
port:23,1023,2323



8.5. 设备指纹搜索

8.5.1. 搜索指定操作系统的相关设备

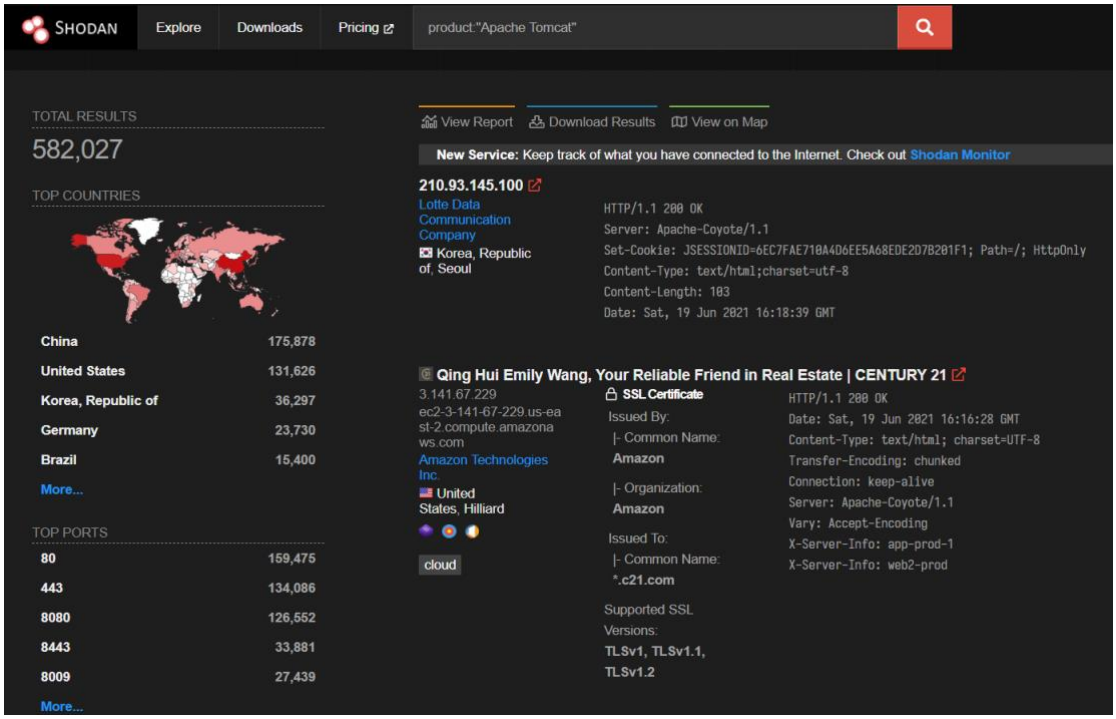
os:"Windows 7"



8.5.2. 搜索指定软件或平台的相关设备

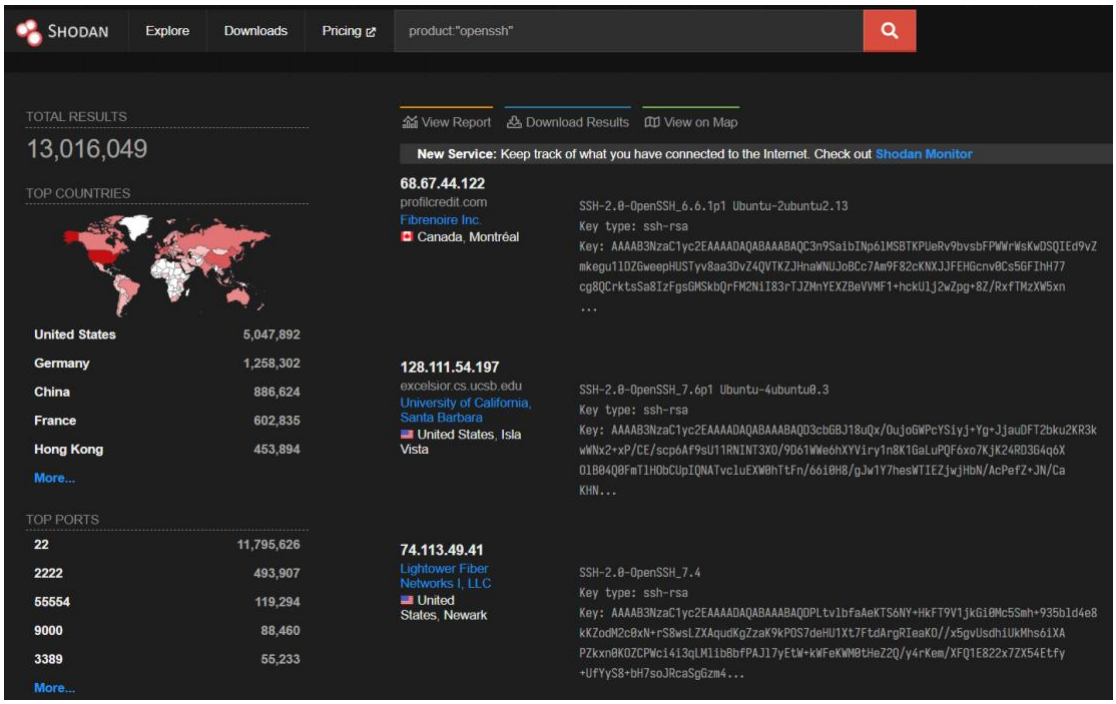
搜索 Tomcat 相关设备

product:"Apache Tomcat"



搜索 Openssh

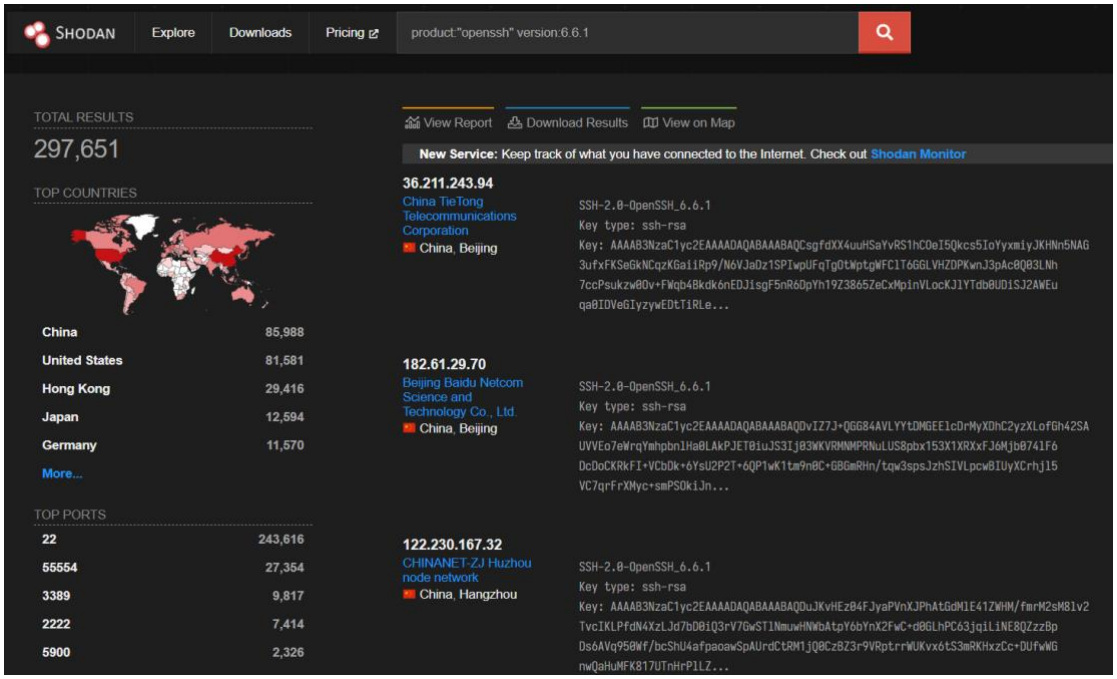
product:"openssh"



8.5.3. 搜索指定软件版本的相关设备

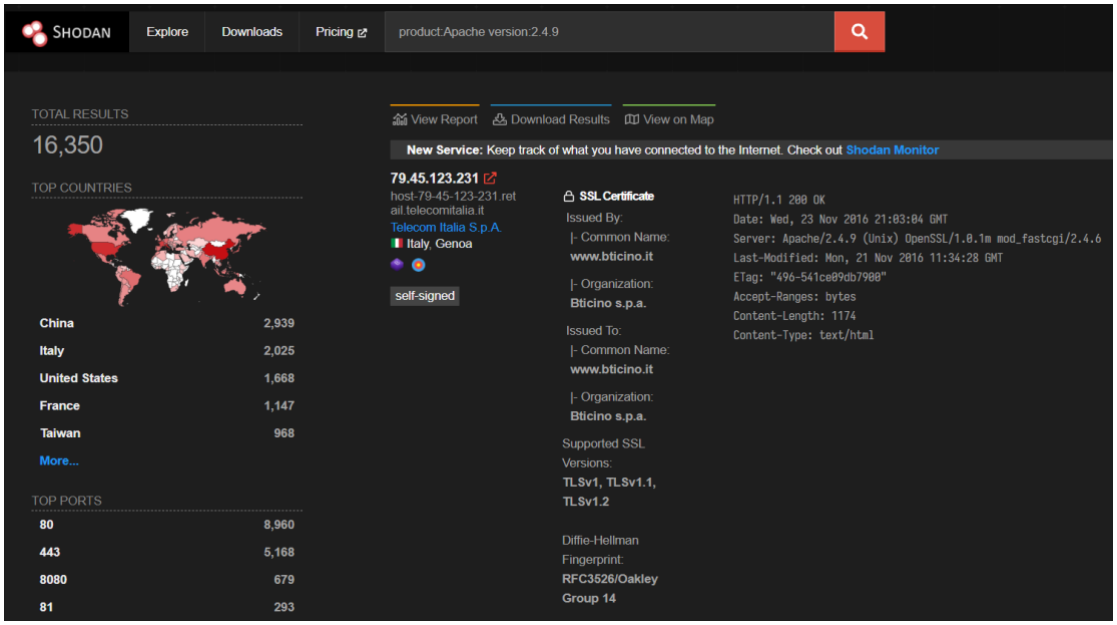
搜索指定版本的 Openssh 的设备

product:"openssh" version:6.6.1



搜索指定版本的 Apache 的设备

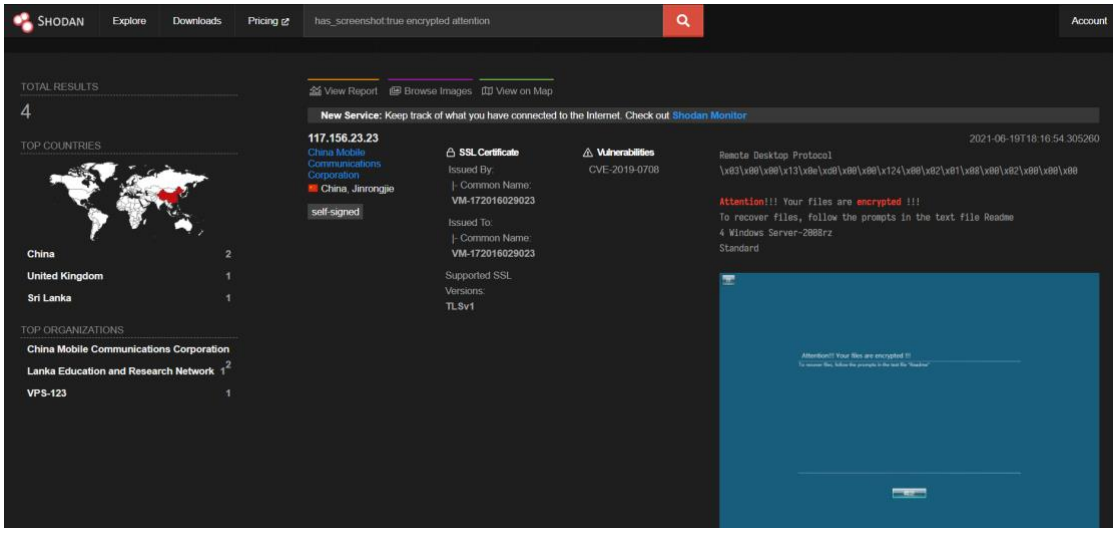
product:Apache version:2.4.9



8.6. 屏幕截图搜索

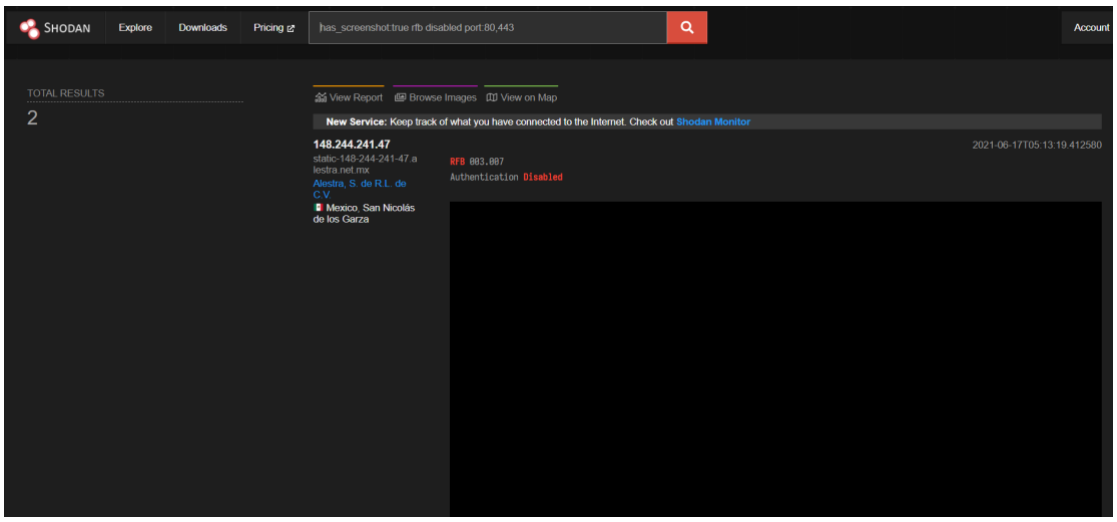
8.6.1. 搜索被勒索软件攻击的远程桌面

has_screenshot:true encrypted attention



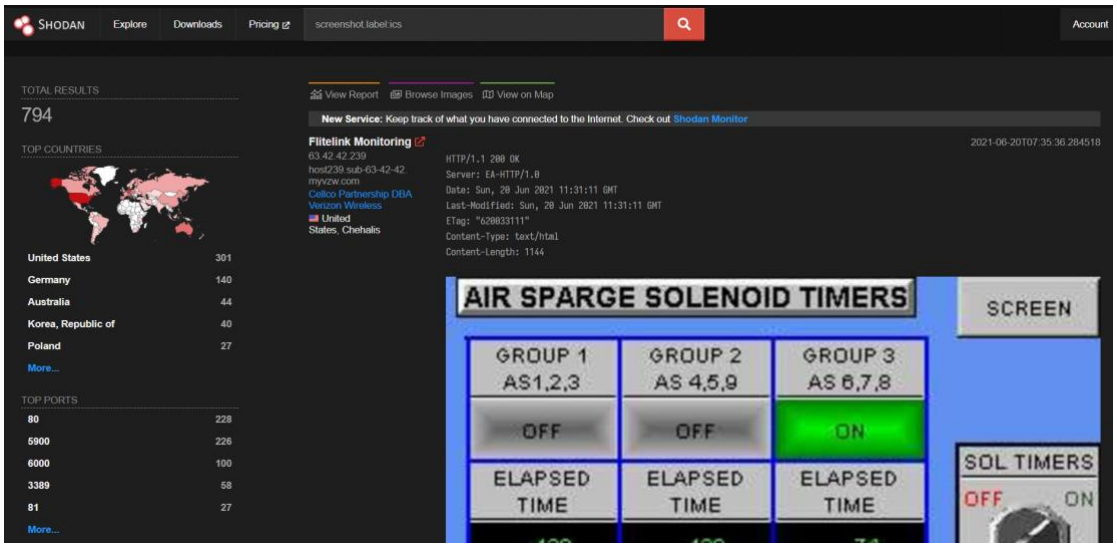
8.6.2. 搜索隐藏在 web 端口下的公共 VNC 服务

has_screenshot:true rfb disabled port:80,443



8.6.3. 搜索使用机器学习识别到的工业控制系统

screenshot.label:ics



8.7. 漏洞搜索

8.7.1. 搜索易受到心脏出血漏洞攻击的设备

vuln:CVE-2014-0160

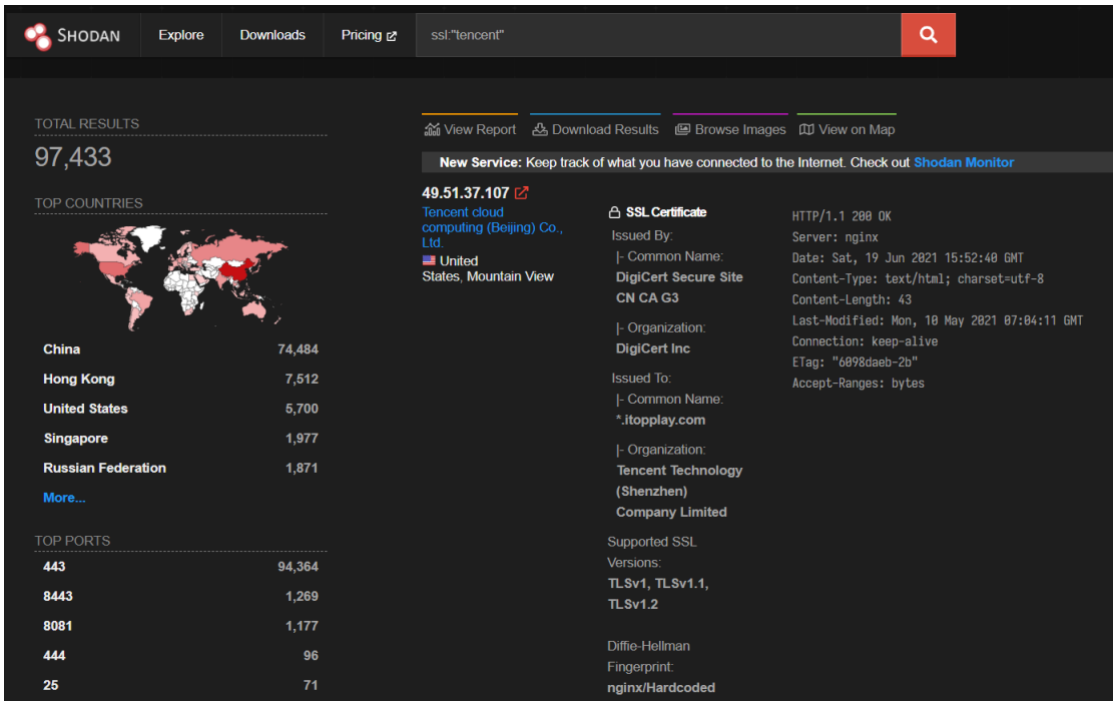
8.7.2. 在中国和美国搜索易受到 CVE-2019-19781 攻击的 Citrix 设备

vuln:CVE-2019-19781 country:US,CN

8.8. SSL 相关搜索

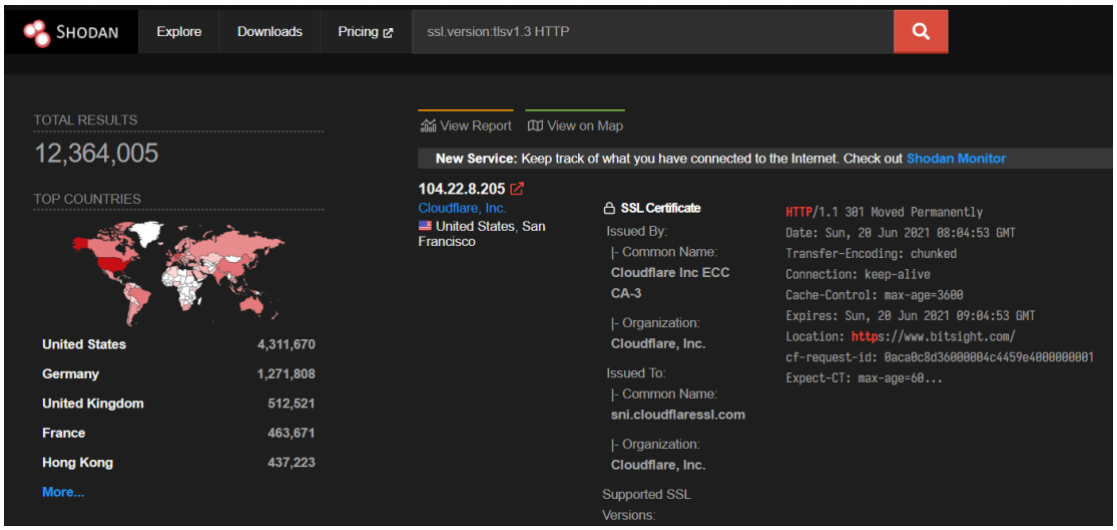
8.8.1. 搜索指定证书的相关设备

ssl:"tencent"



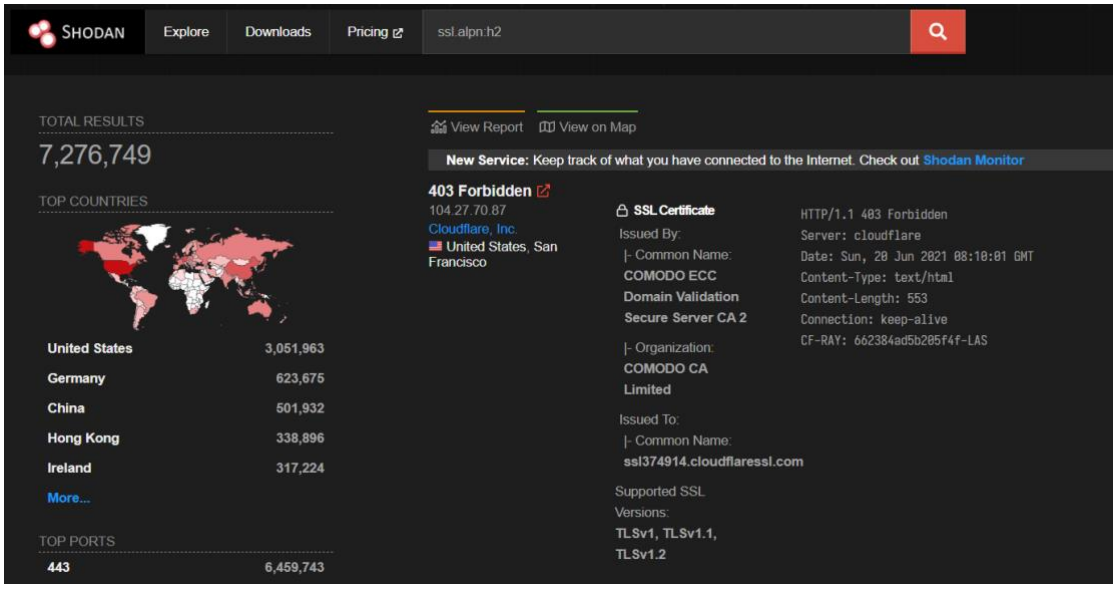
8.8.2. 搜索支持 TLS1.3 的设备

ssl.version:tlsv1.3 HTTP



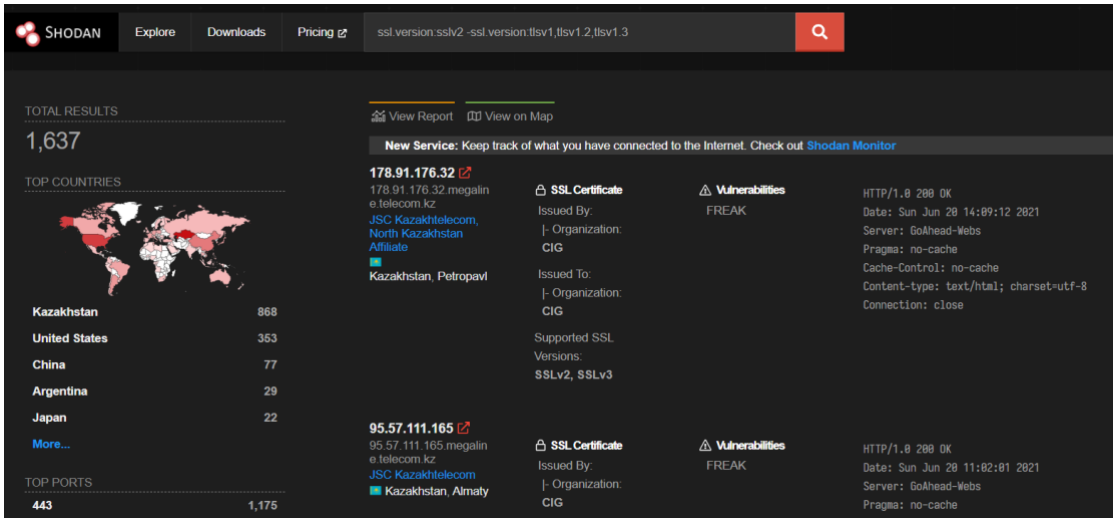
8.8.3. 搜索支持 HTTP/2 的设备

ssl.alpn:h2



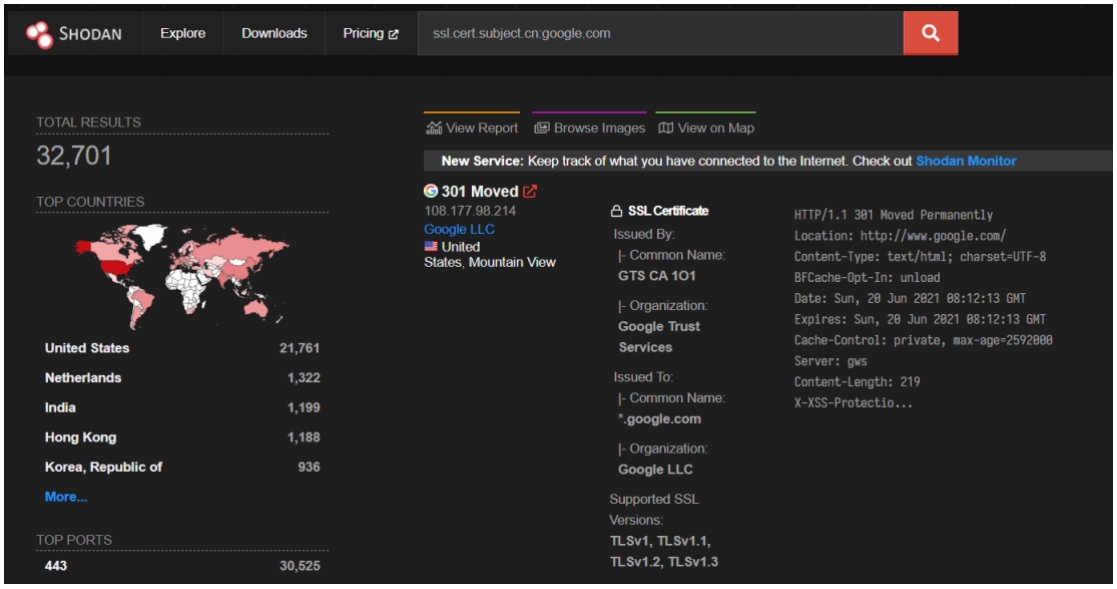
8.8.4. 搜索支持 SSLv2 但不支持 TLS 的设备

ssl.version:sslv2 -ssl.version:tlsv1,tlsv1.2,tlsv1.3



8.8.5. 搜索为*.google.com 颁发证书的设备

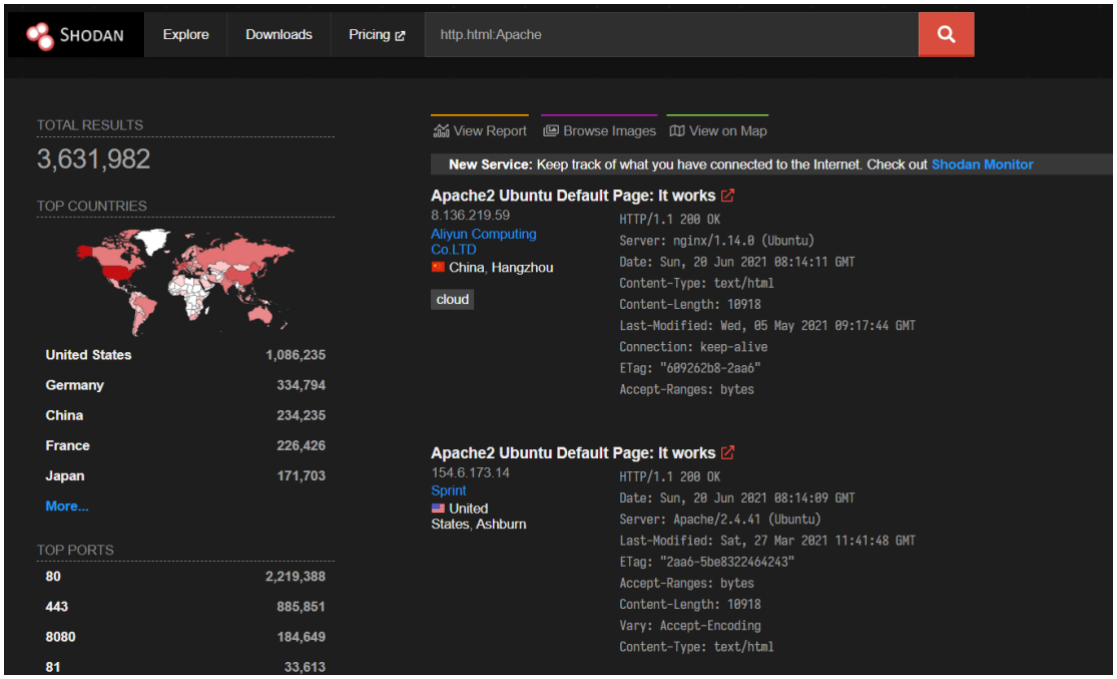
ssl.cert.subject.cn:google.com



8.9. HTTP 相关搜索

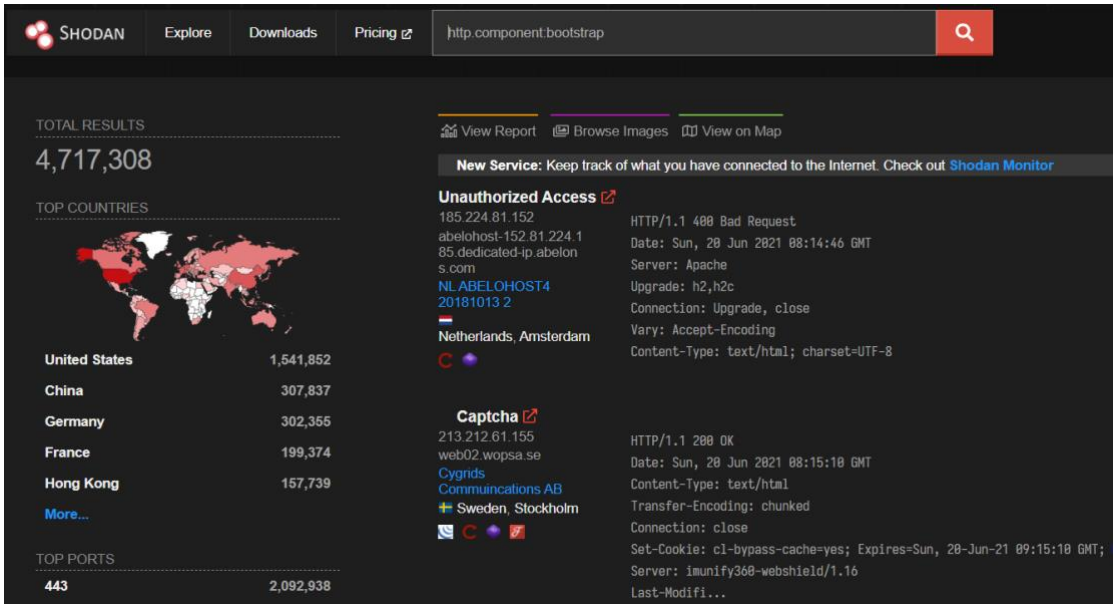
8.9.1. 搜索在 HTML 中包含“Apache”的设备

http.html:Apache



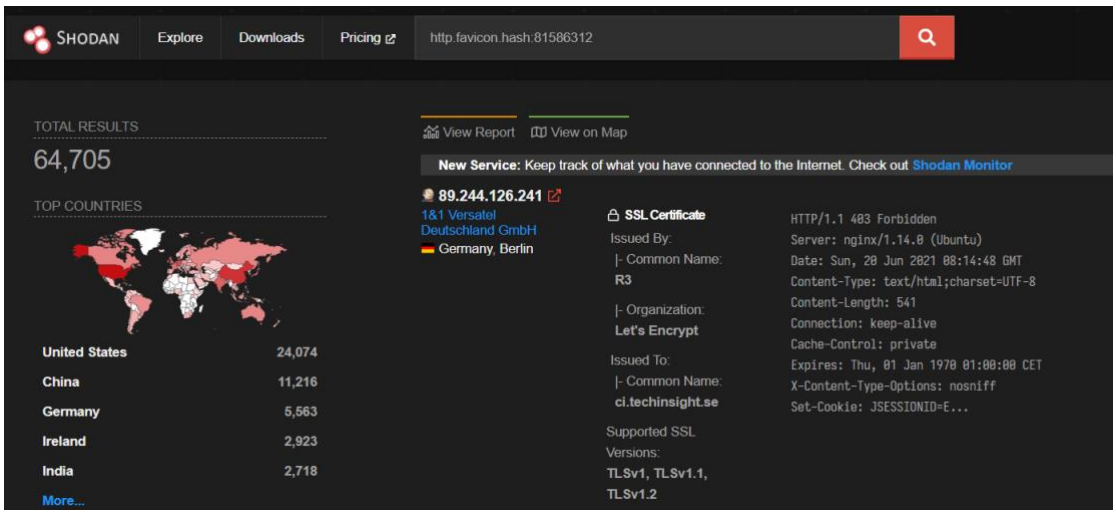
8.9.2. 搜索使用 bootstrap css 框架的设备

http.component:bootstrap



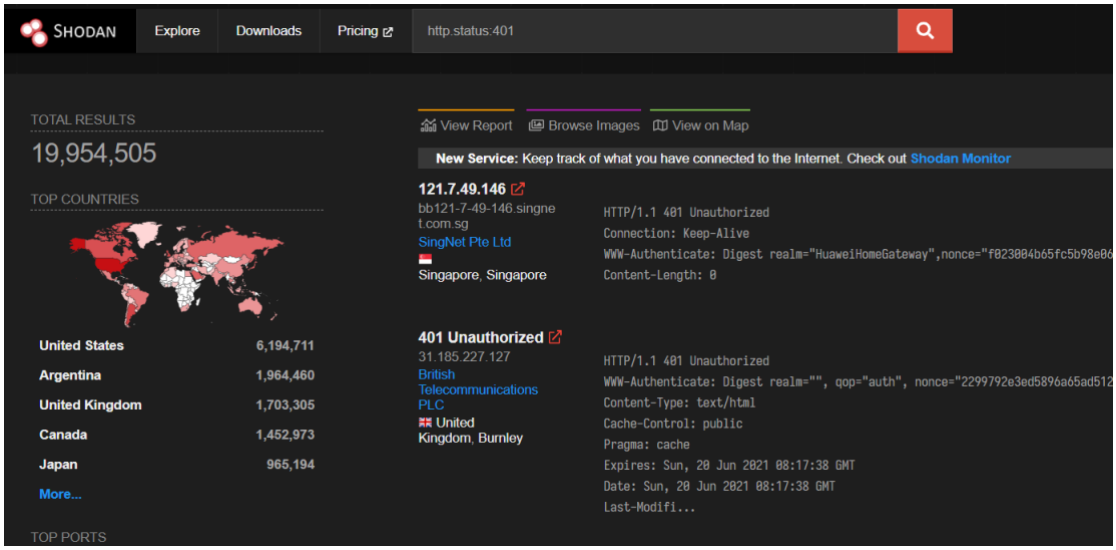
8.9.3. 搜索指定 icon_hash 的设备

http.favicon.hash:81586312



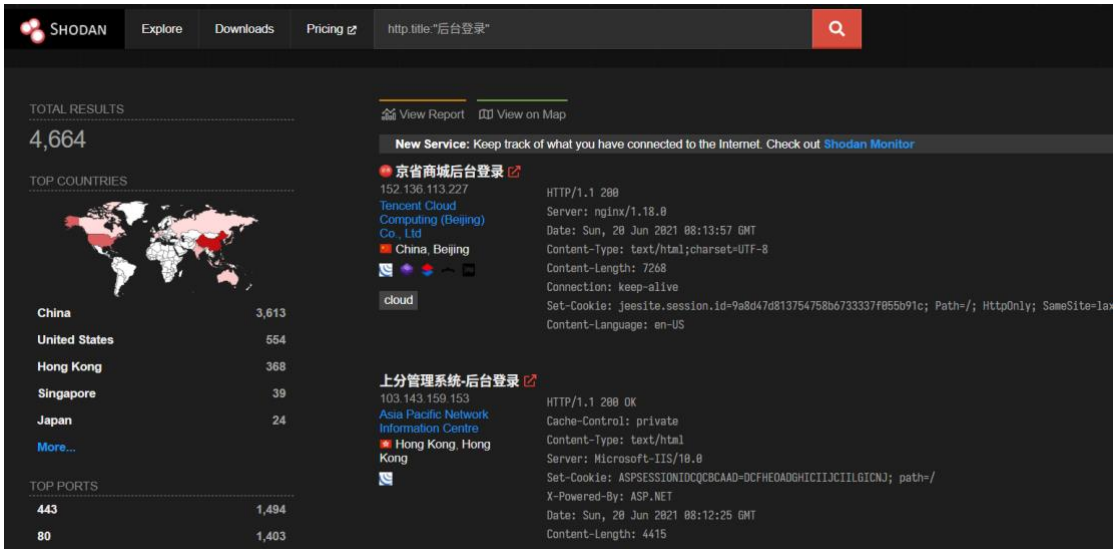
8.9.4. 搜索指定 HTTP 响应状态码的设备

http.status:401



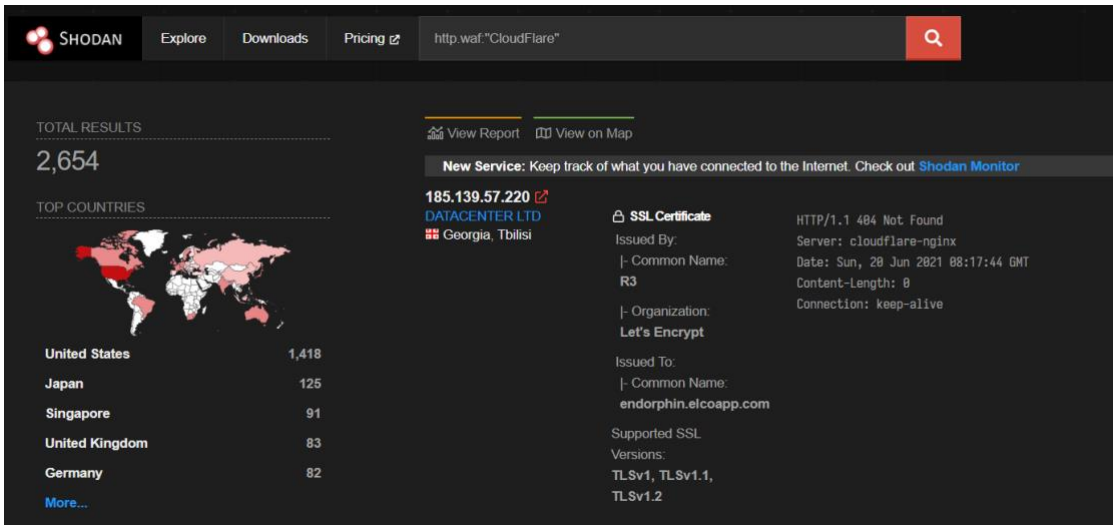
8.9.5. 搜索指定网站标题的设备

http.title:"后台登录"



8.9.6. 搜索指定 waf 的相关设备

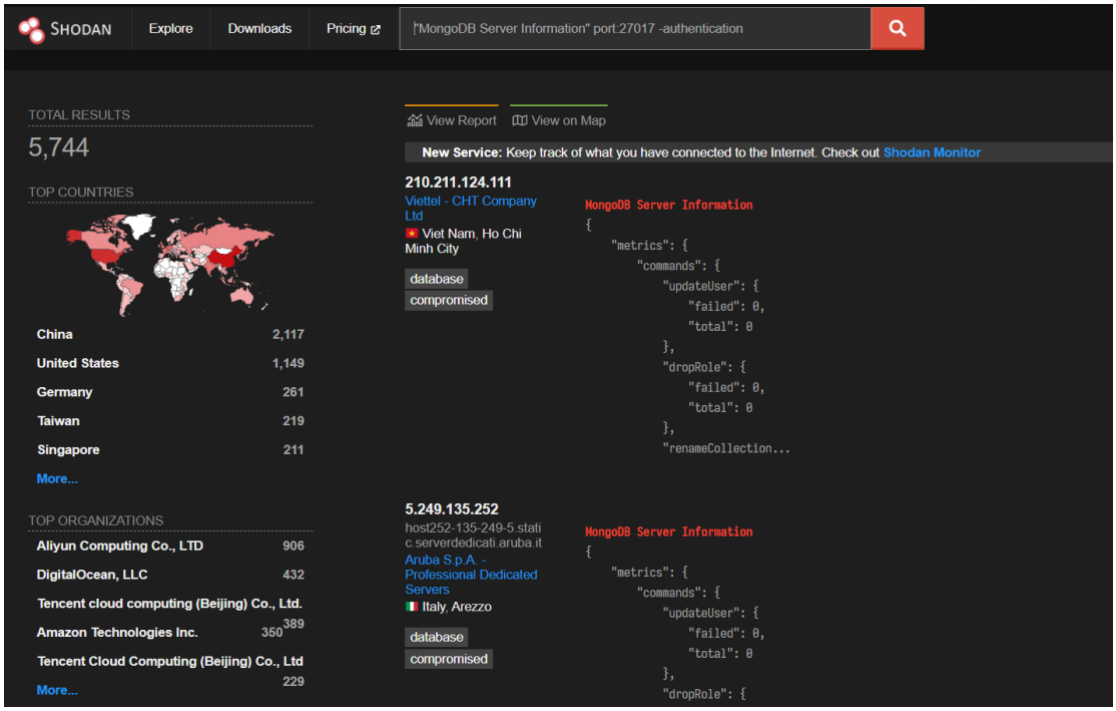
http.waf:"CloudFlare"



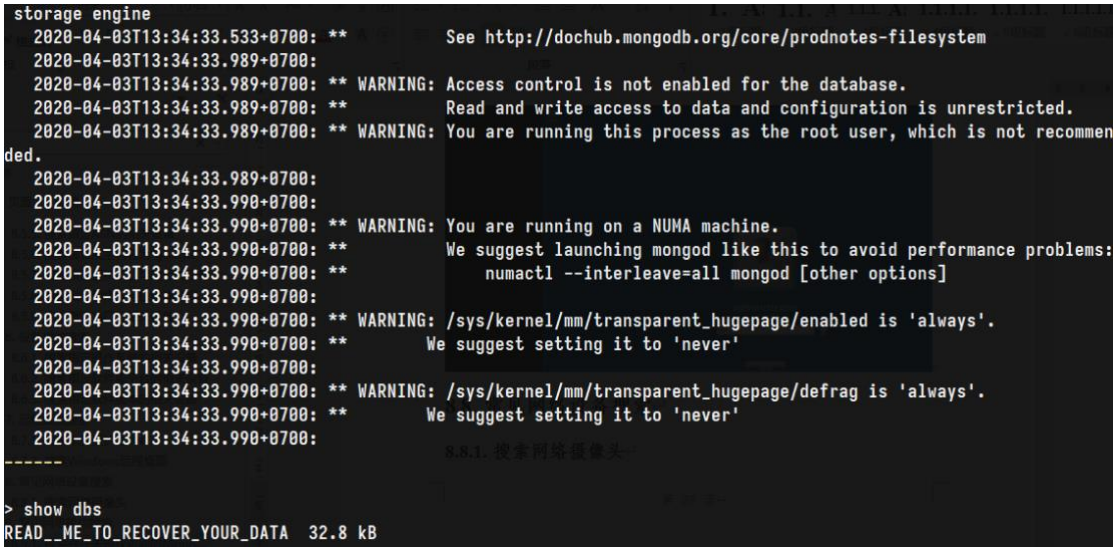
8.10. 常见网络架构搜索示例

8.10.1. 搜索存在未授权访问的 MongoDB

"MongoDB Server Information" port:27017 -authentication

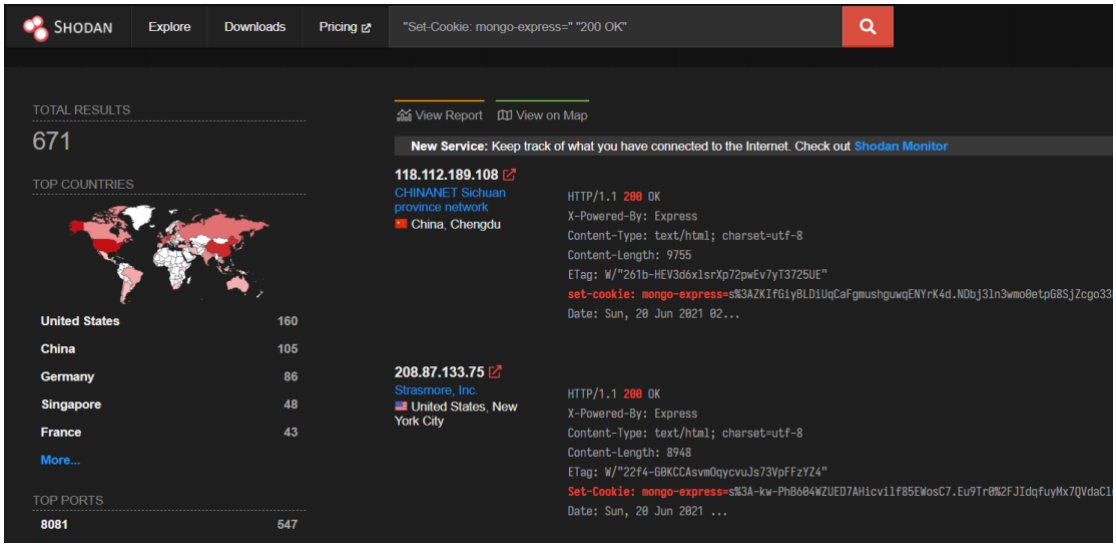


使用 mongodb shell 连接，验证未授权访问漏洞：



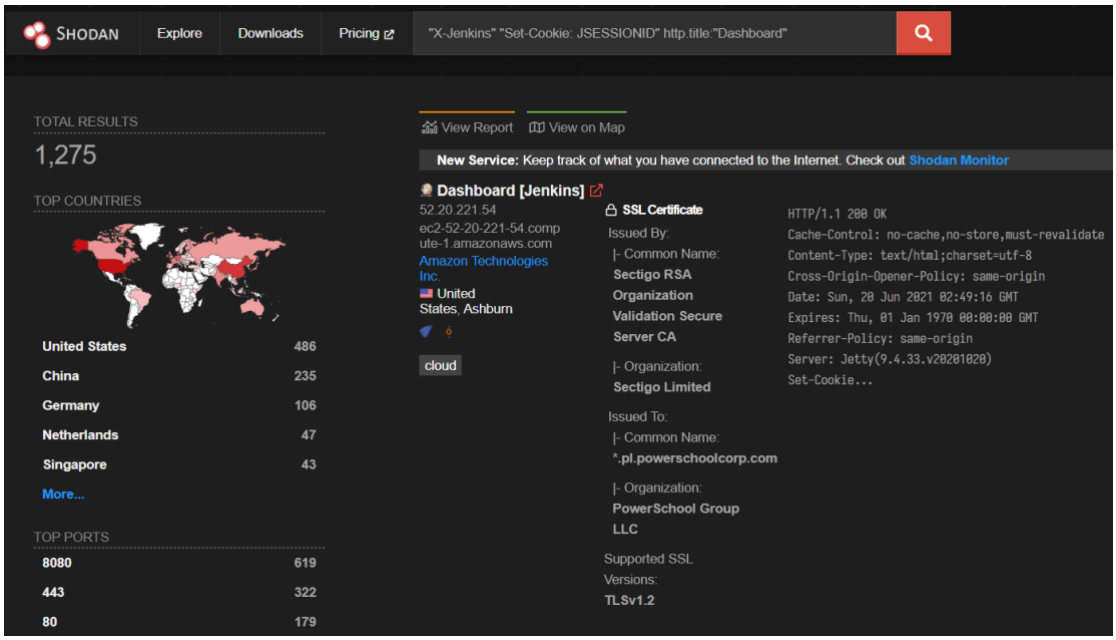
8.10.2. 搜索存在未授权访问的 Mongo Express 网页界面

"Set-Cookie: mongo-express=" "200 OK"



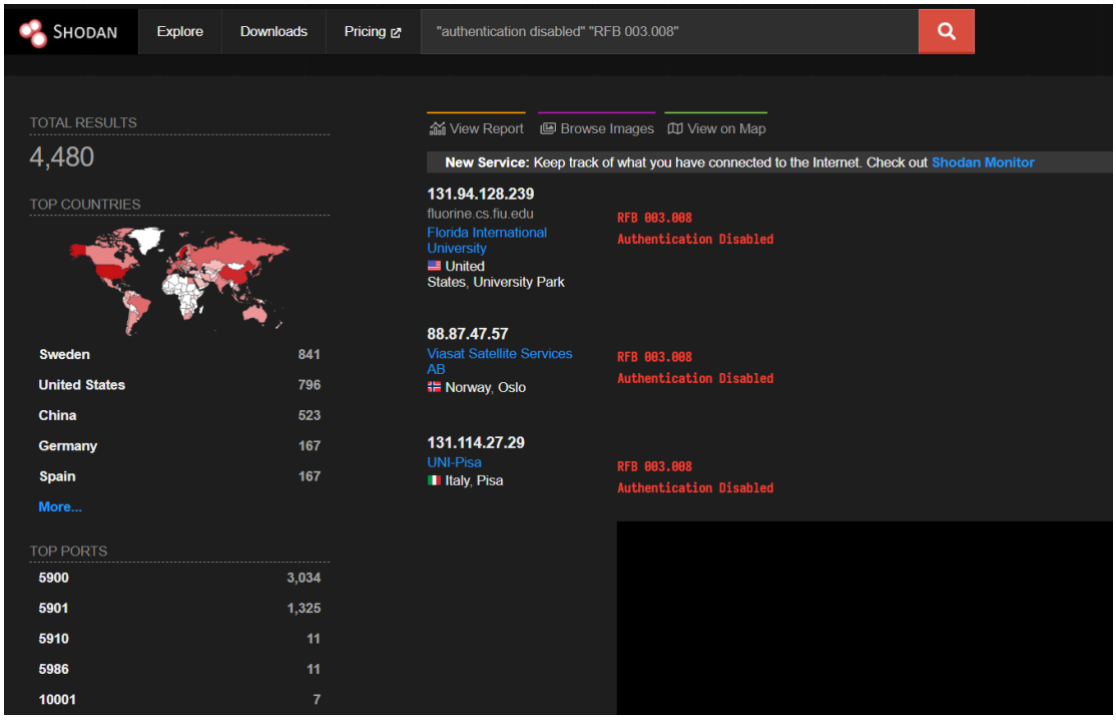
8.10.3. 搜索存在未授权访问的 Jenkins 页面

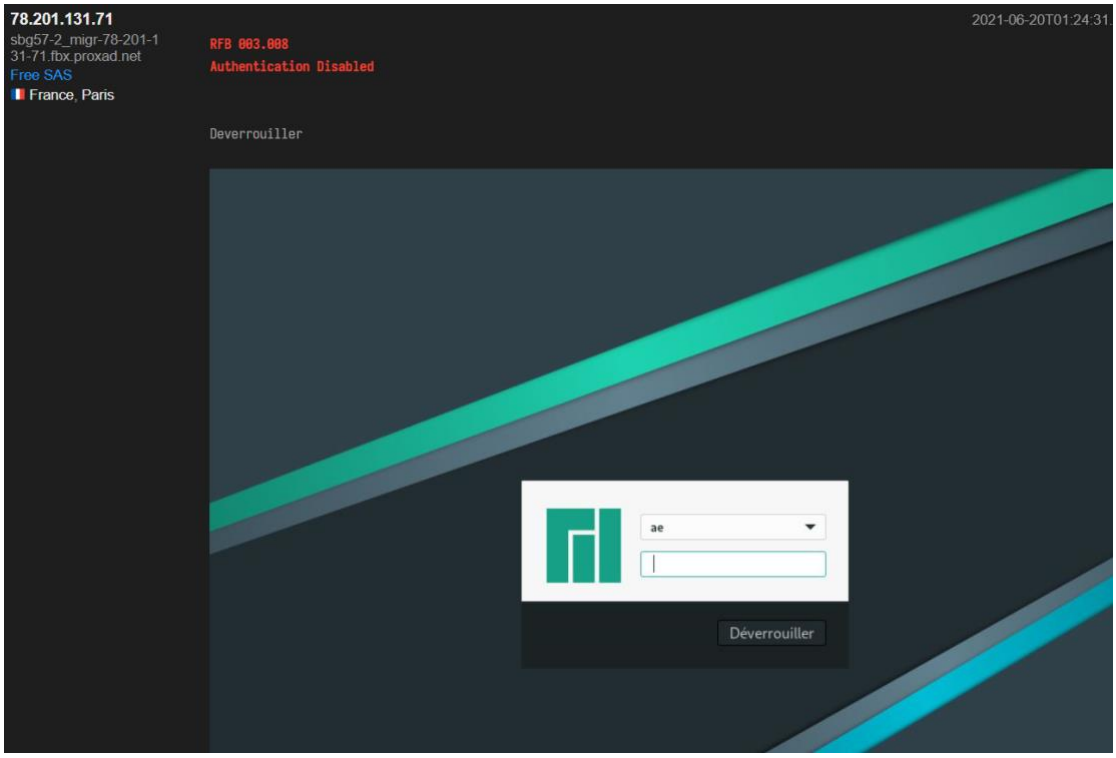
"X-Jenkins" "Set-Cookie: JSESSIONID" http.title:"Dashboard"



8.10.4. 搜索未受保护的 VNC

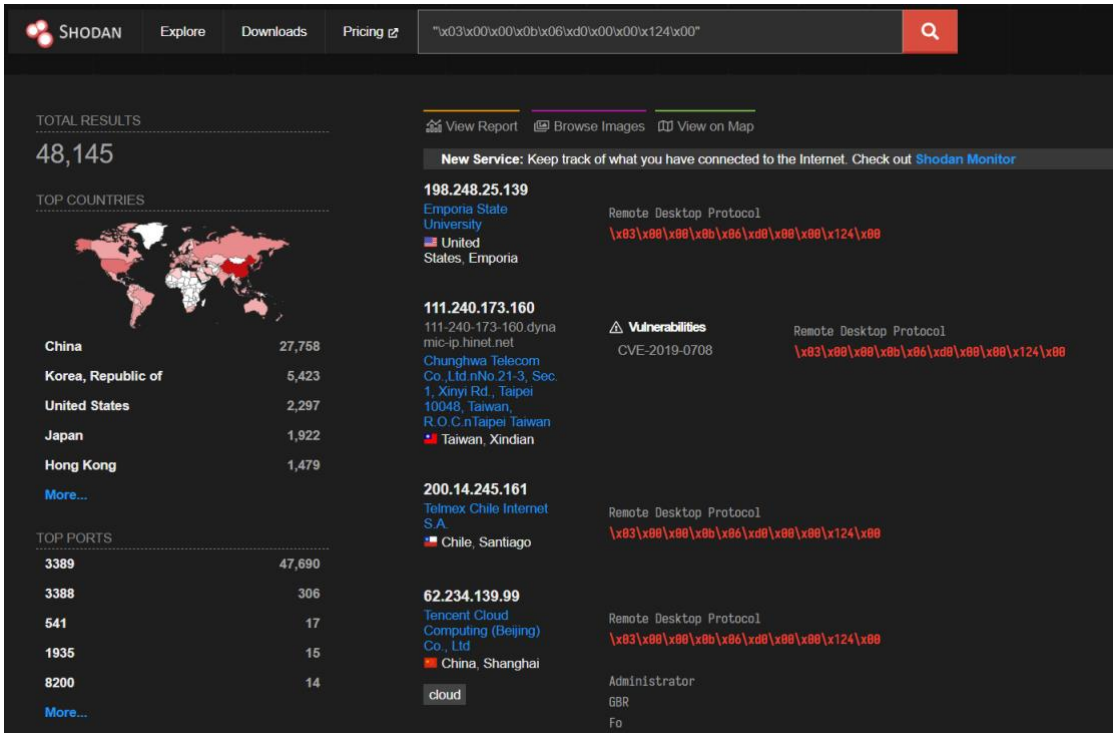
"authentication disabled" "RFB 003.008"

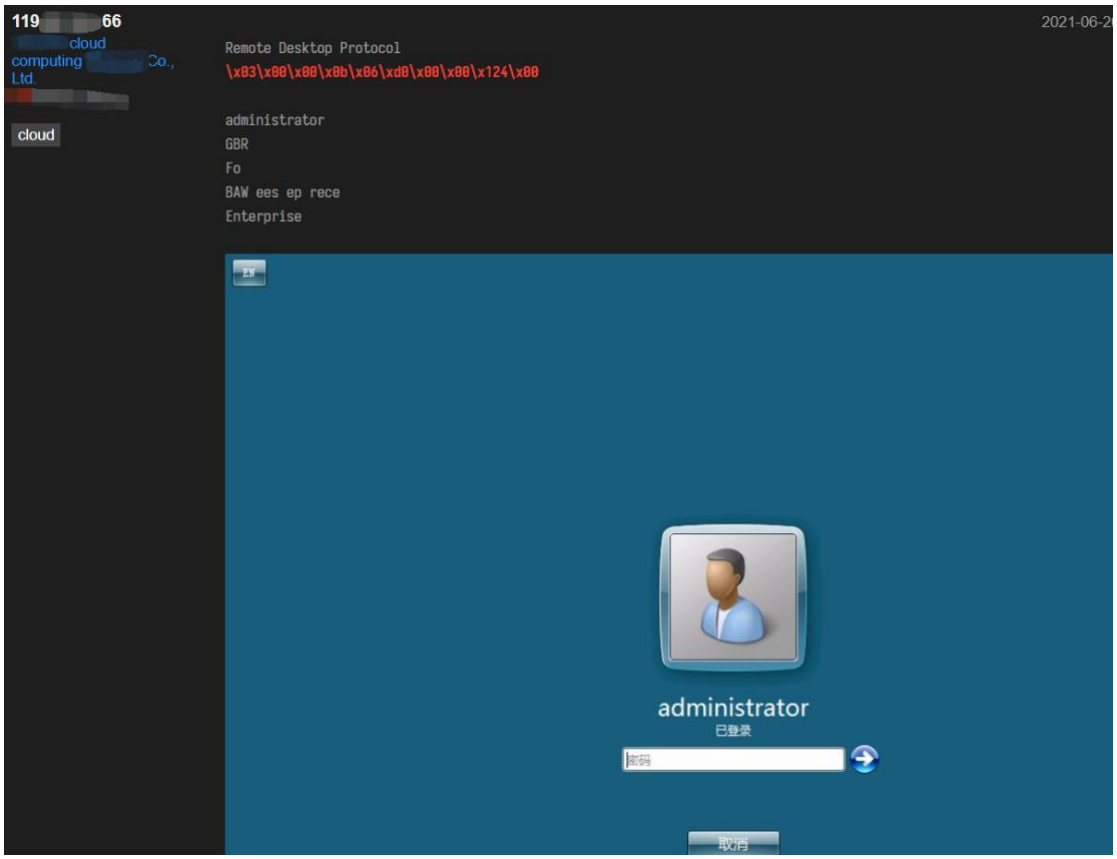




8.10.5. 搜索 Windows 远程桌面

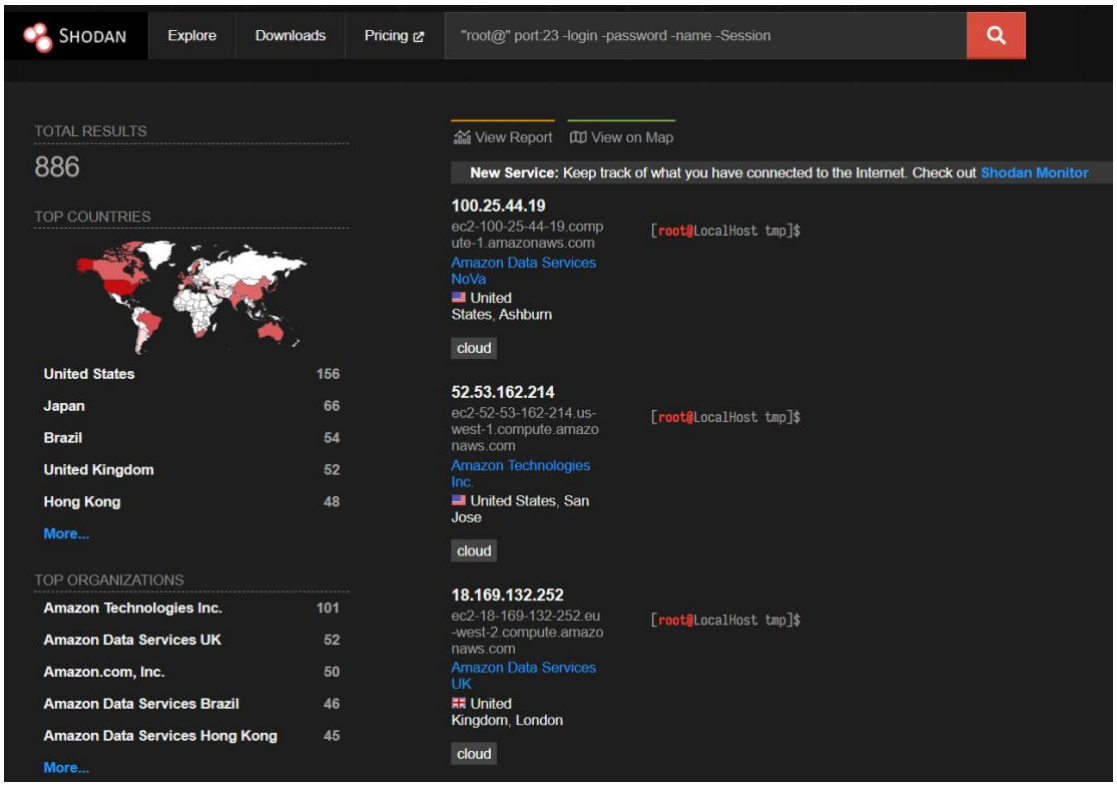
"\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00"




119 66
cloud
computing Co.,
Ltd.
cloud
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x00\x124\x00
administrator
GBR
Fo
BAW ees ep rece
Enterprise
administrator
已登录
密码
取消

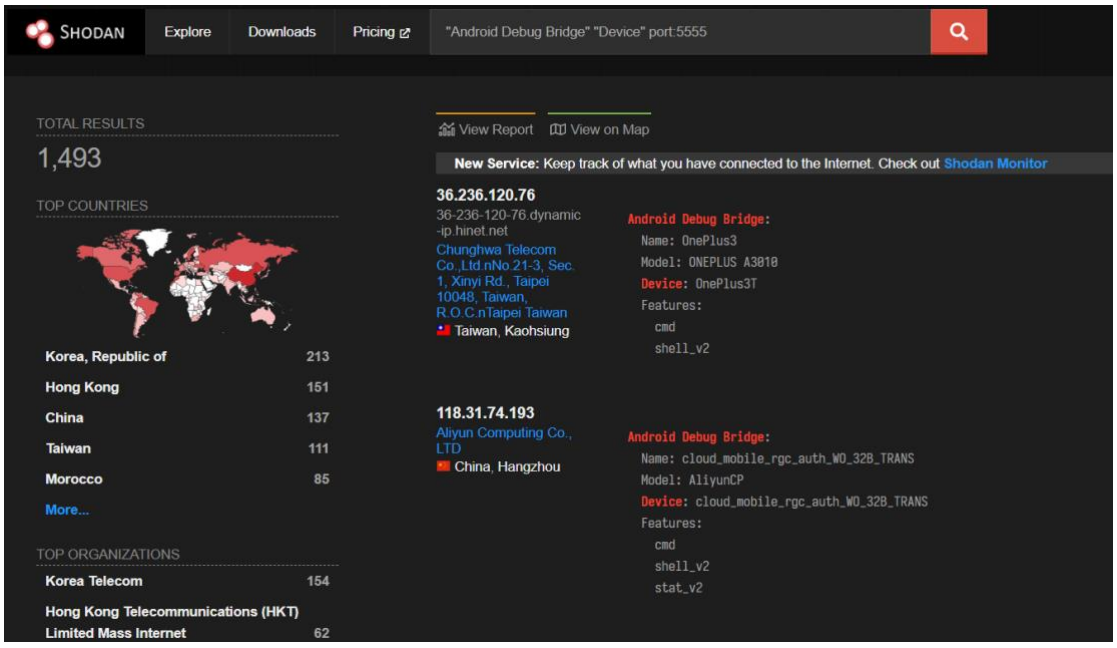
8.10.6. 搜索以 Root 身份登录的 telnet

"root@" port:23 -login -password -name -Session



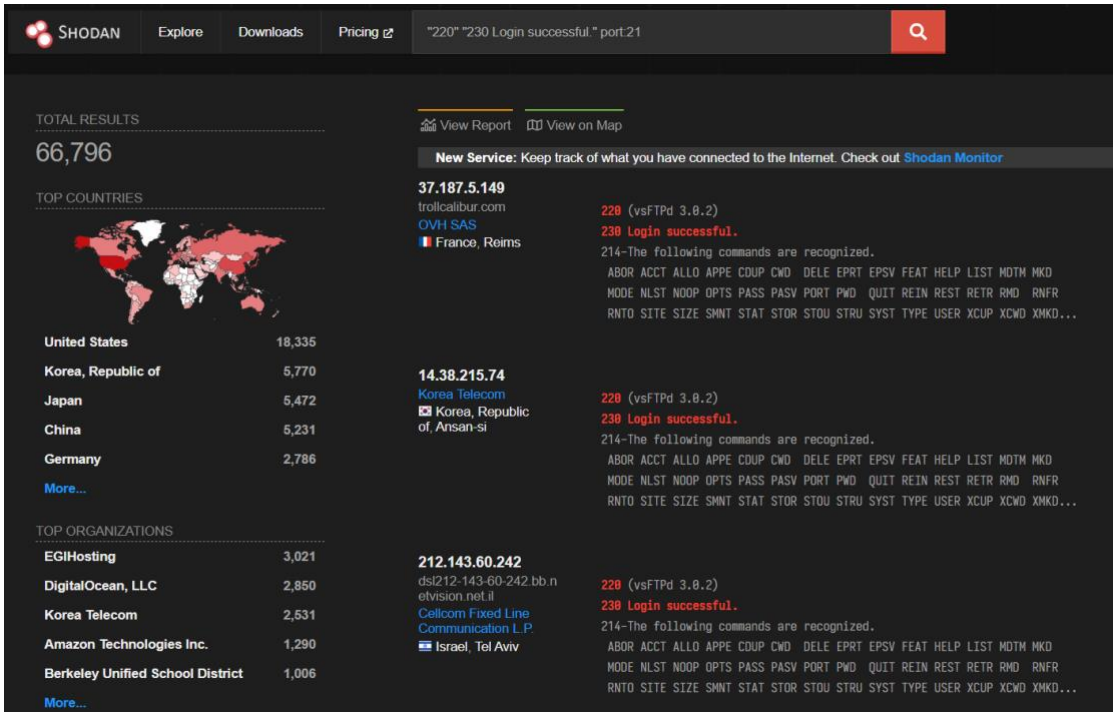
8.10.7. 搜索使用 ADB 的相关设备

"Android Debug Bridge" "Device" port:5555



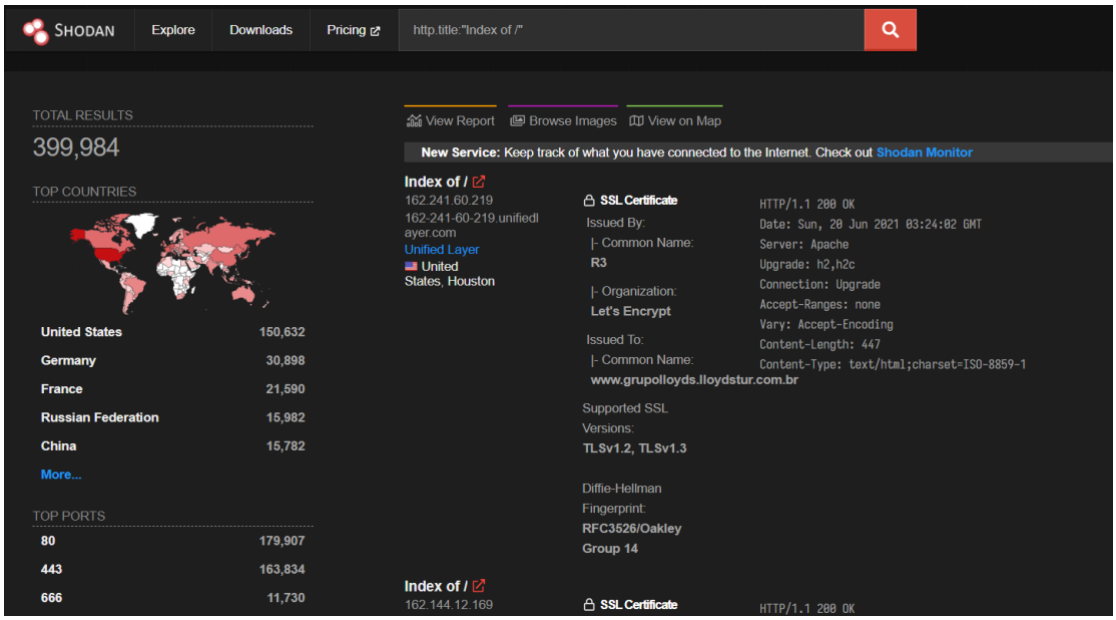
8.10.8. 搜索可匿名登录的 FTP 服务

"220" "230 Login successful." port:21



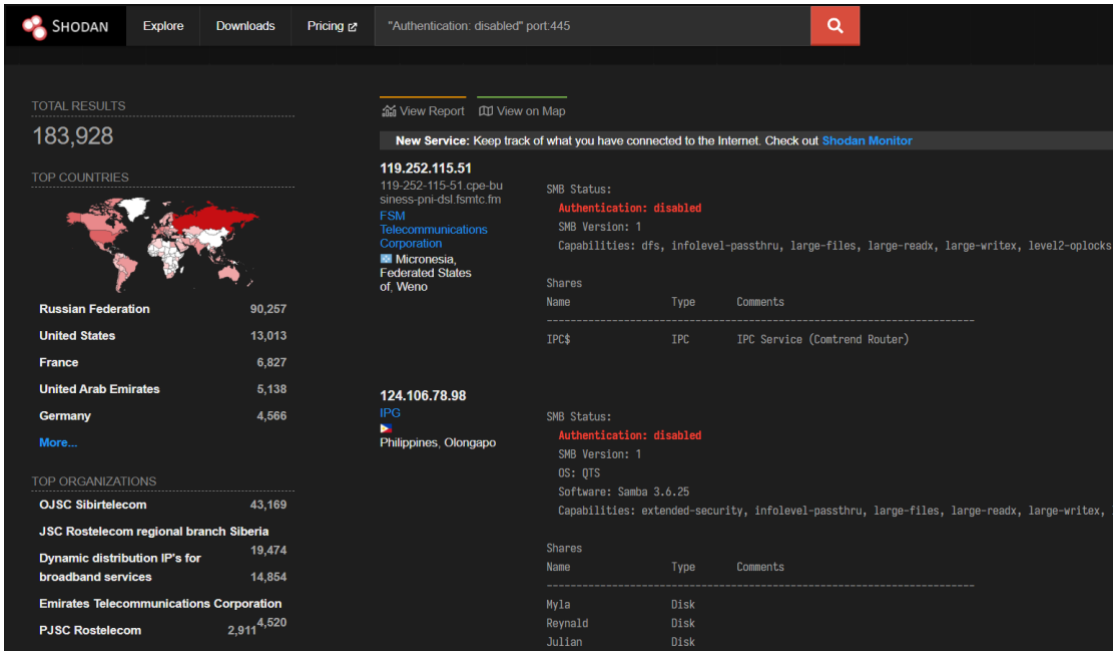
8.10.9. 搜索存在 Apache 目录遍历的设备

http.title:"Index of /"



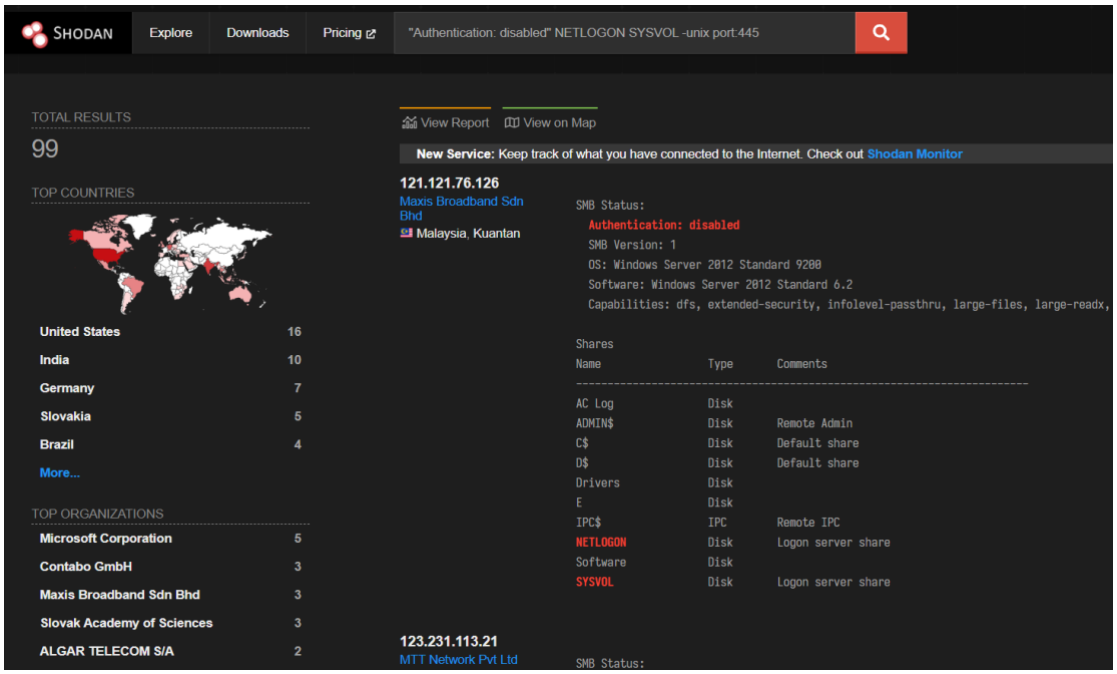
8.10.10. 搜索 SMB 文件共享

"Authentication: disabled" port:445



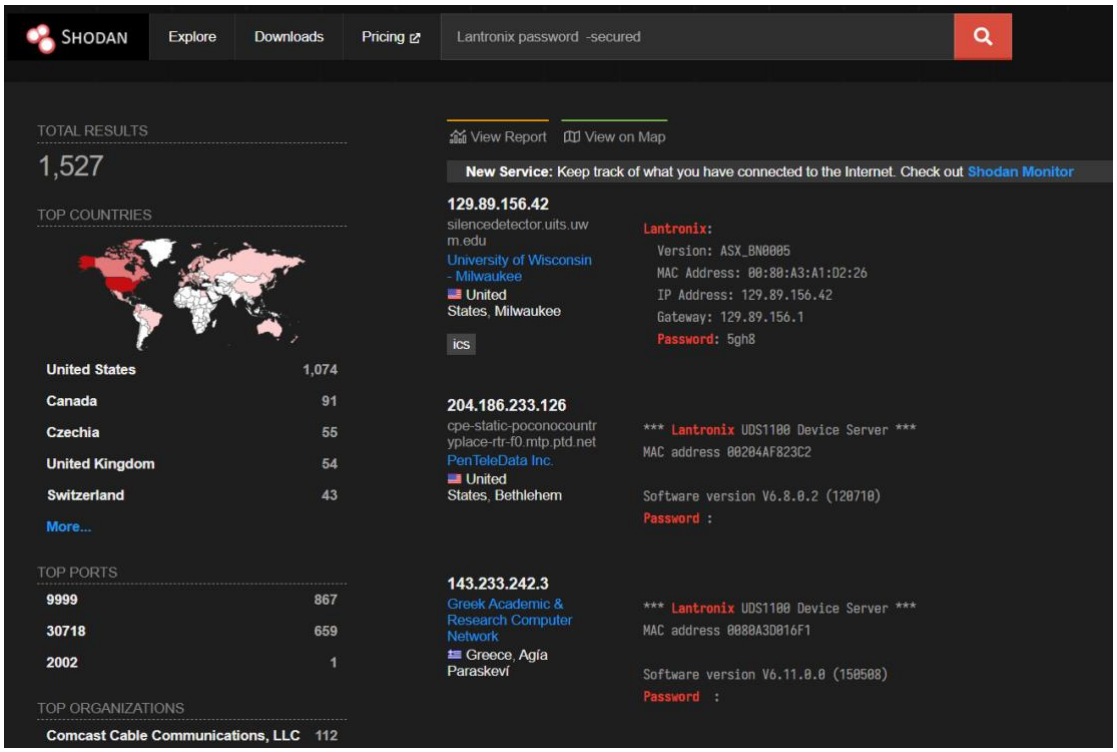
8.10.11. 搜索域控制器

"Authentication: disabled" NETLOGON SYSVOL -unix port:445



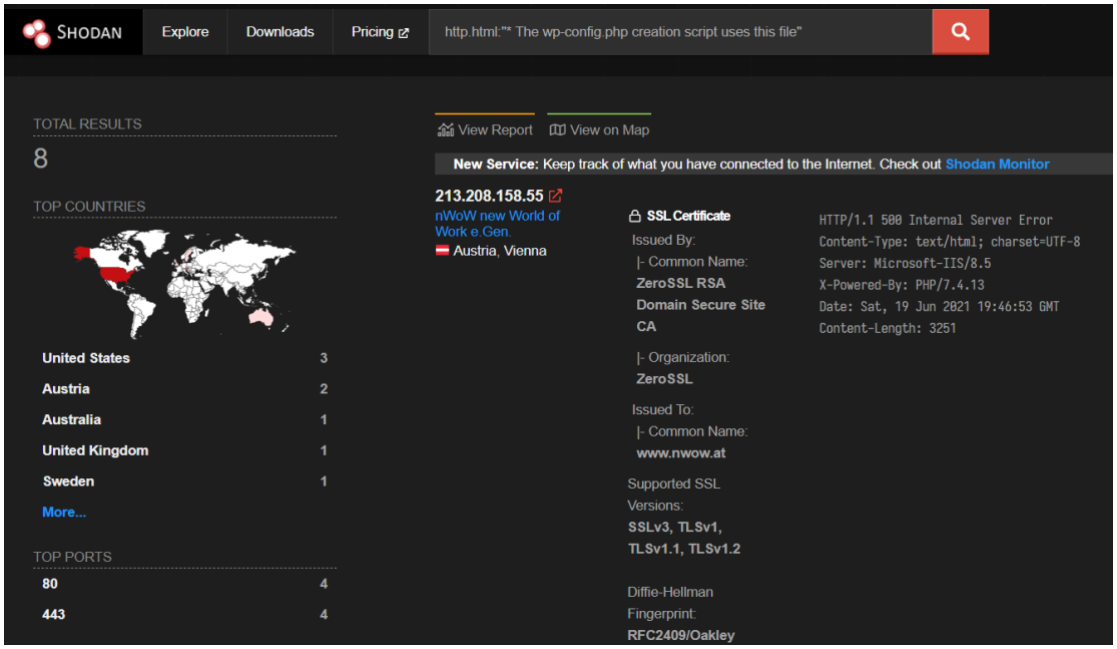
8.10.12. 搜索存在密码泄露的 Lantronix 串行以太网适配器

Lantronix password -secured



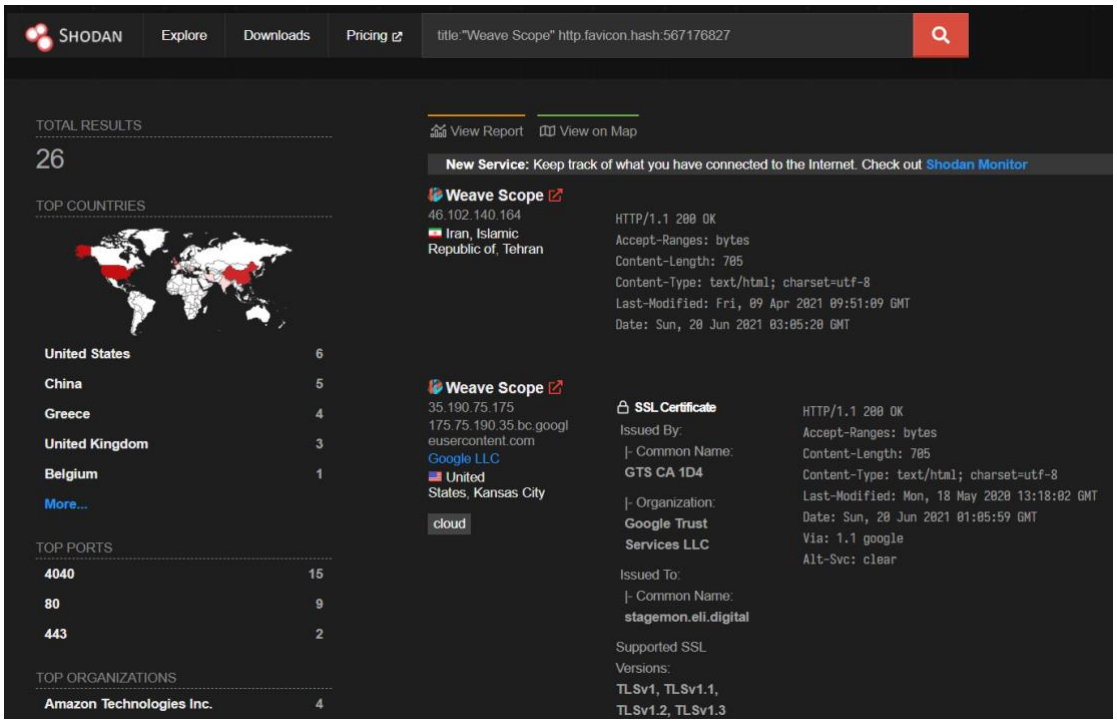
8.10.13. 搜索存在错误配置的 Wordpress

http.html:"* The wp-config.php creation script uses this file"



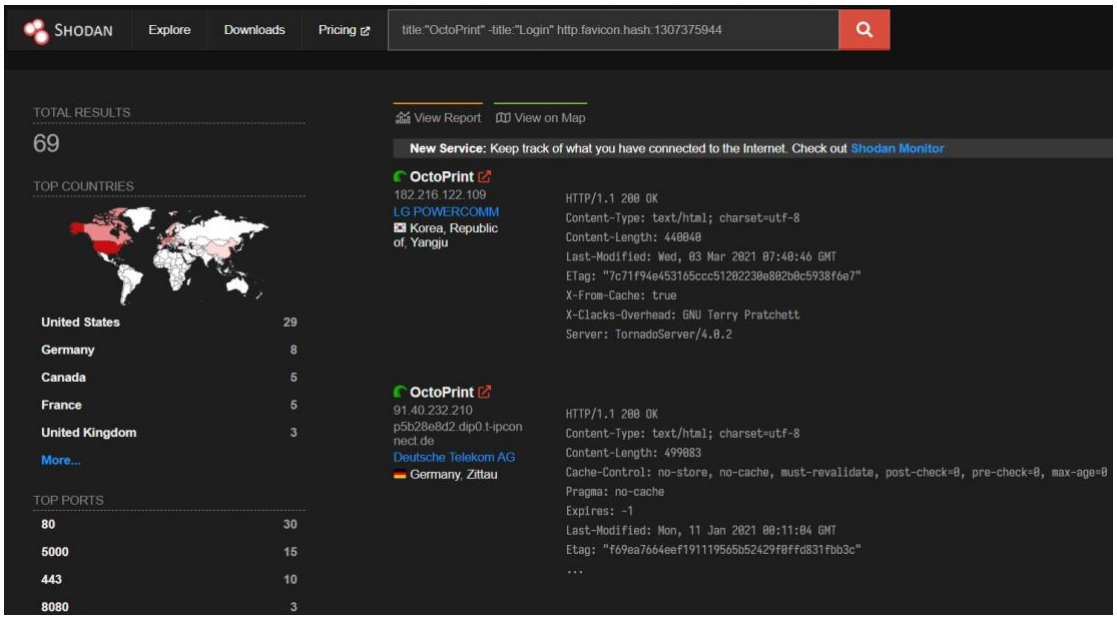
8.10.14. 搜索 Kubernetes pod 和 Docker 的可视化仪表板

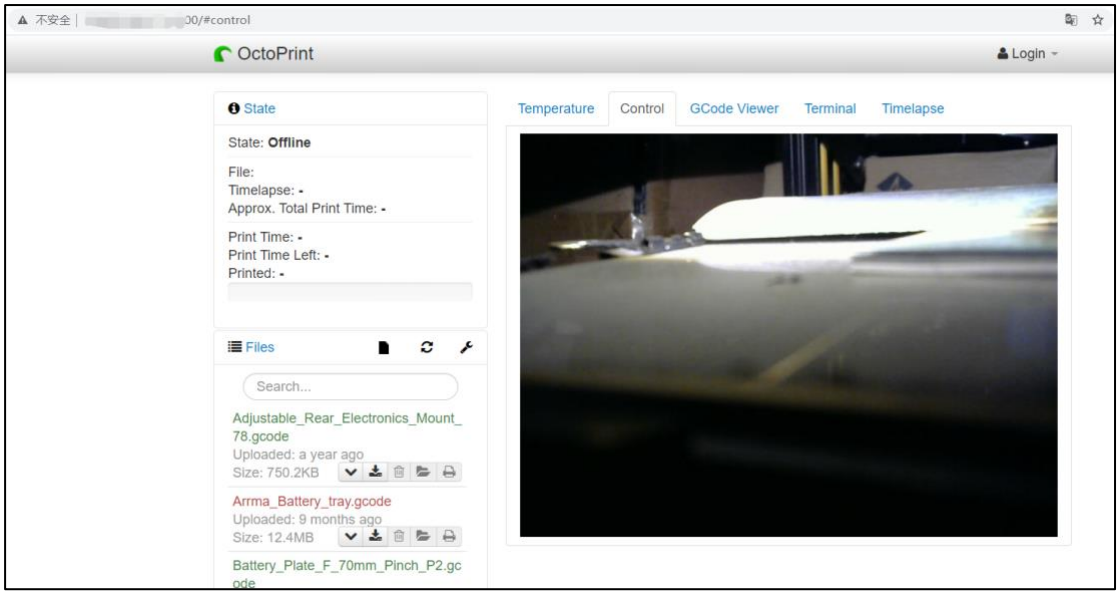
title:"Weave Scope" http.favicon.hash:567176827



8.10.15. 搜索 OctoPrint3D 打印机设备

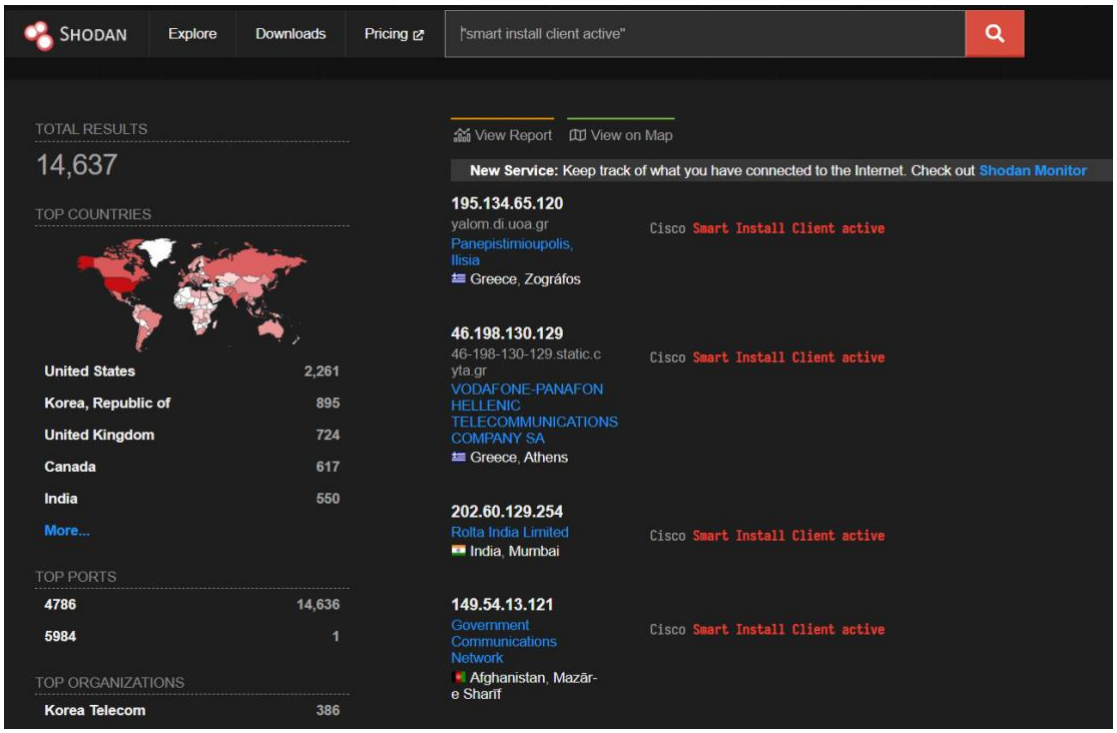
title:"OctoPrint" -title:"Login" http.favicon.hash:1307375944





8.10.16. 搜索 Cisco Smart Install

"smart install client active"

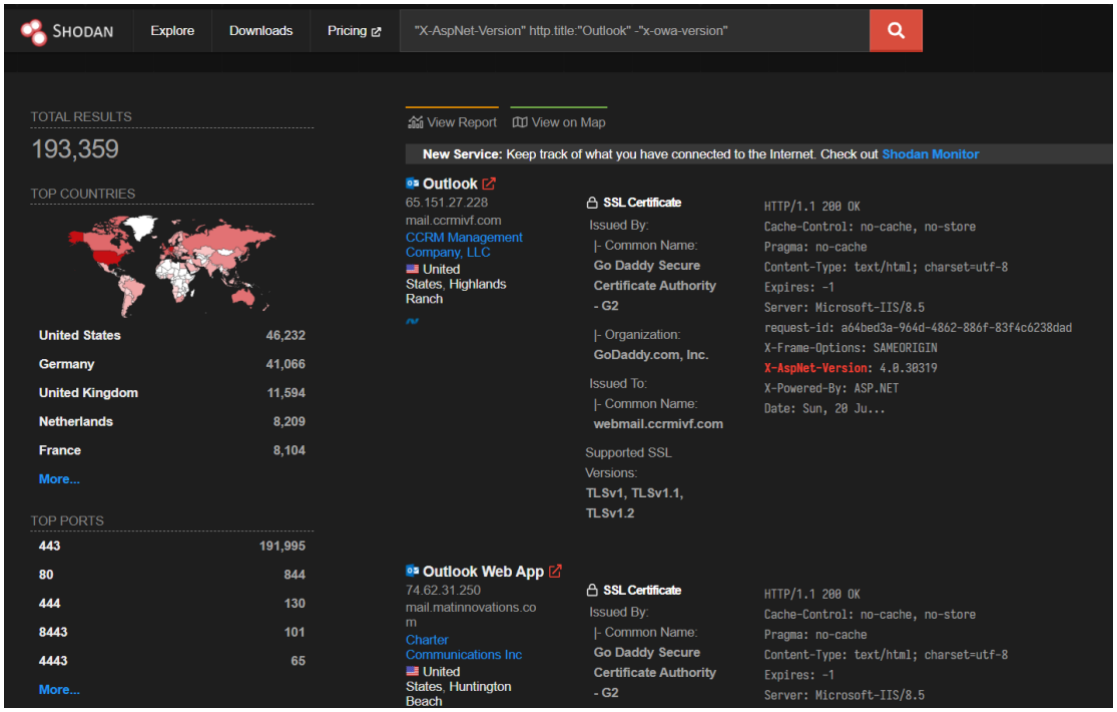


8.10.17. 搜索 Outlook

"X-AspNet-Version" http.title:"Outlook" -"x-owa-version"

"x-owa-version" "IE=EmulateIE7" "Server: Microsoft-IIS/7.0"

"x-owa-version" "IE=EmulateIE7" http.favicon.hash:442749392



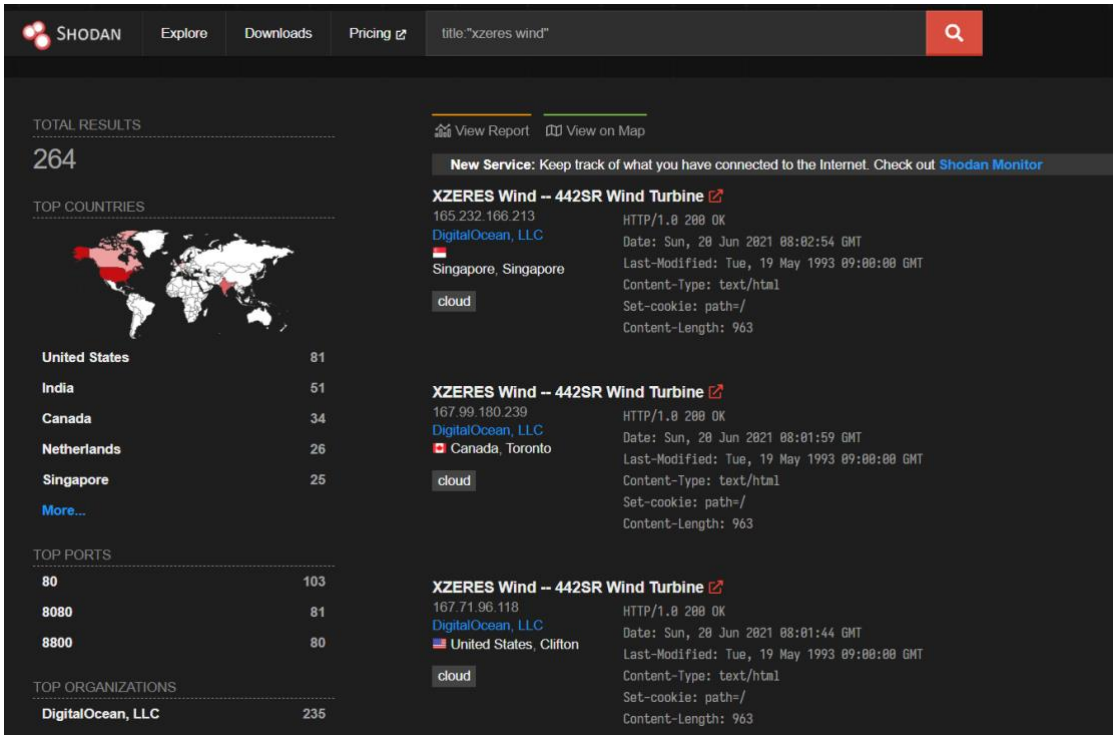
8.11. 工业控制系统搜索

8.11.1. 工业控制系统简介

工控指的是工业自动化控制，主要利用电子电气、机械、软件组合实现。工业控制系统(ICS)是控制周围世界的计算机。它们负责管理办公室的空调、发电厂的涡轮机、剧院的照明设备或者工厂的机器人。

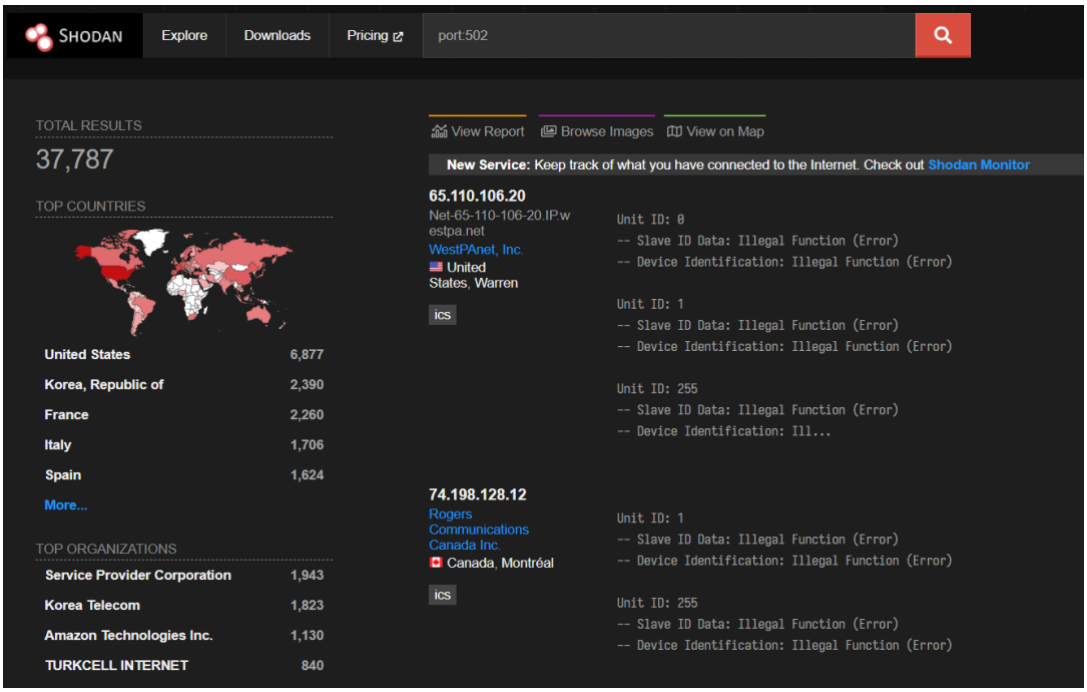
8.11.2. 搜索工控协议为“XZERES Wind Turbine”的相关设备

title:"xzeres wind"



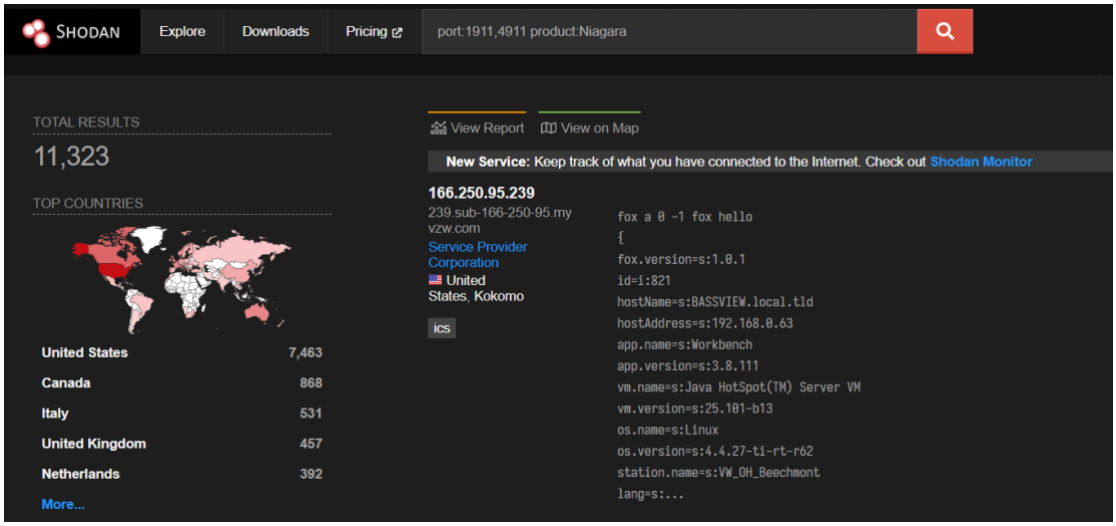
8.11.3. 搜索工控协议为“Modbus”的相关设备

port:502



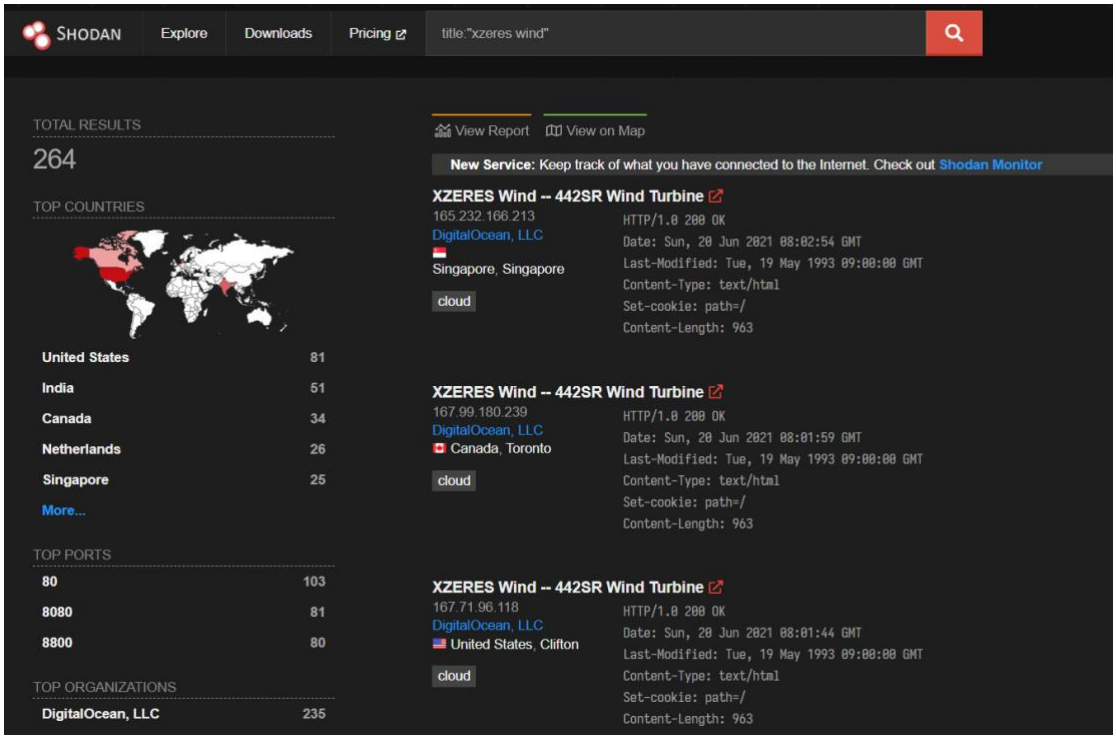
8.11.4. 搜索工控协议为“Niagara Fox”的相关设备

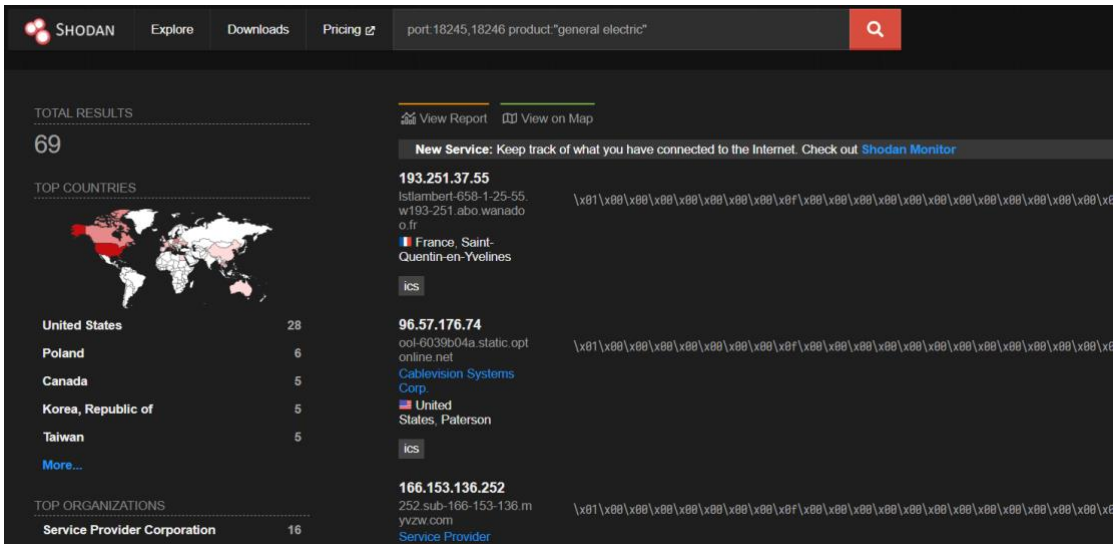
port:1911,4911 product:Niagara



8.11.5. 搜索工控协议为“GE-SRTP”的相关设备

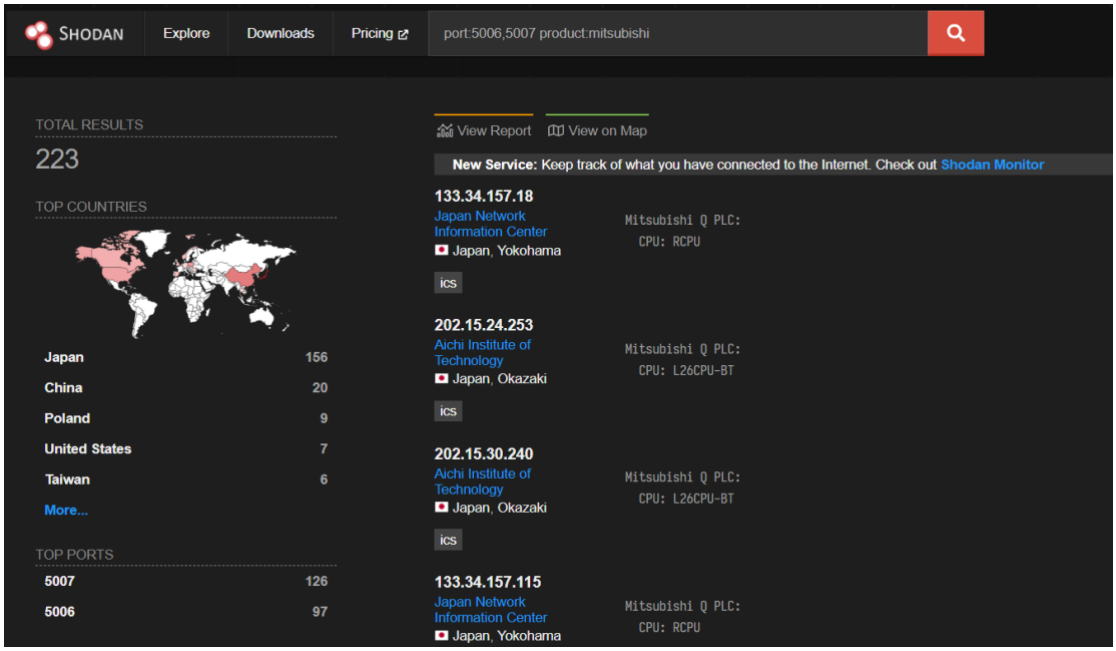
port:18245,18246 product:"general electric"





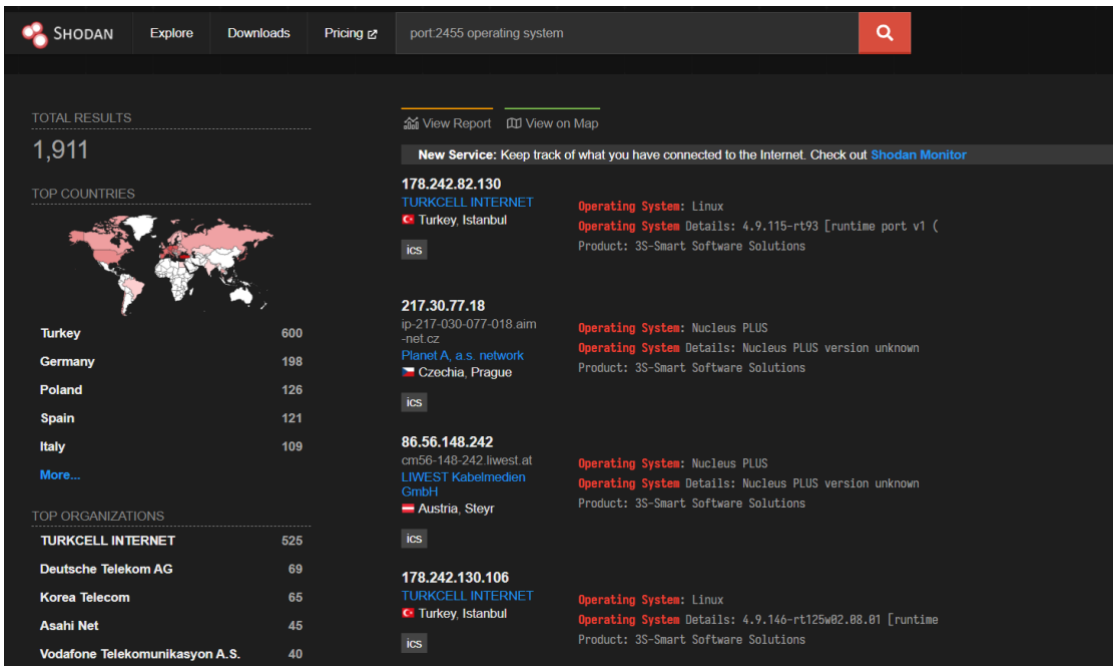
8.11.6. 搜索工控协议为“MELSEC-Q”的相关设备

port:5006,5007 product:mitsubishi



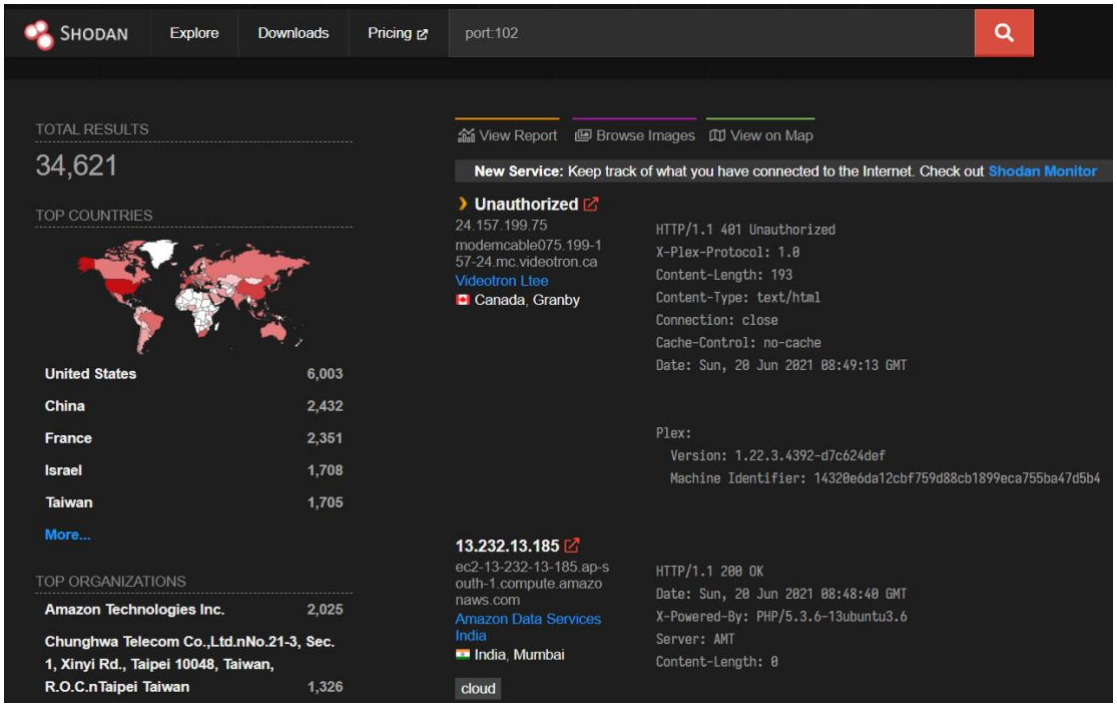
8.11.7. 搜索工控协议为“CODESYS”的相关设备

port:2455 operating system



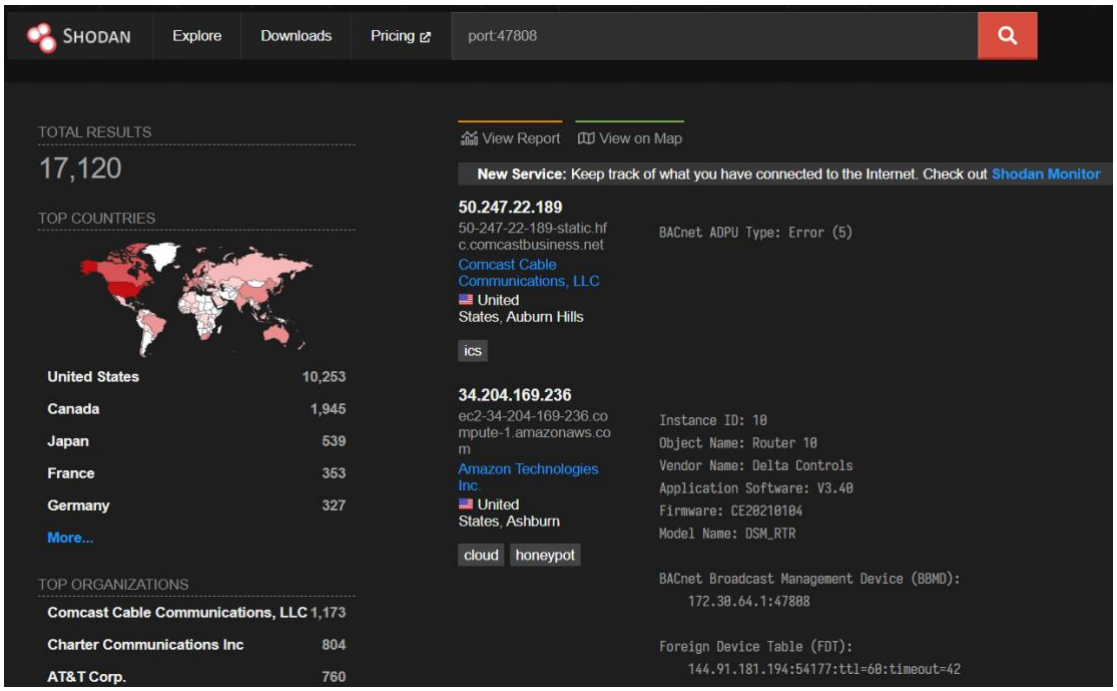
8.11.8. 搜索工控协议为“S7”的相关设备

port:102



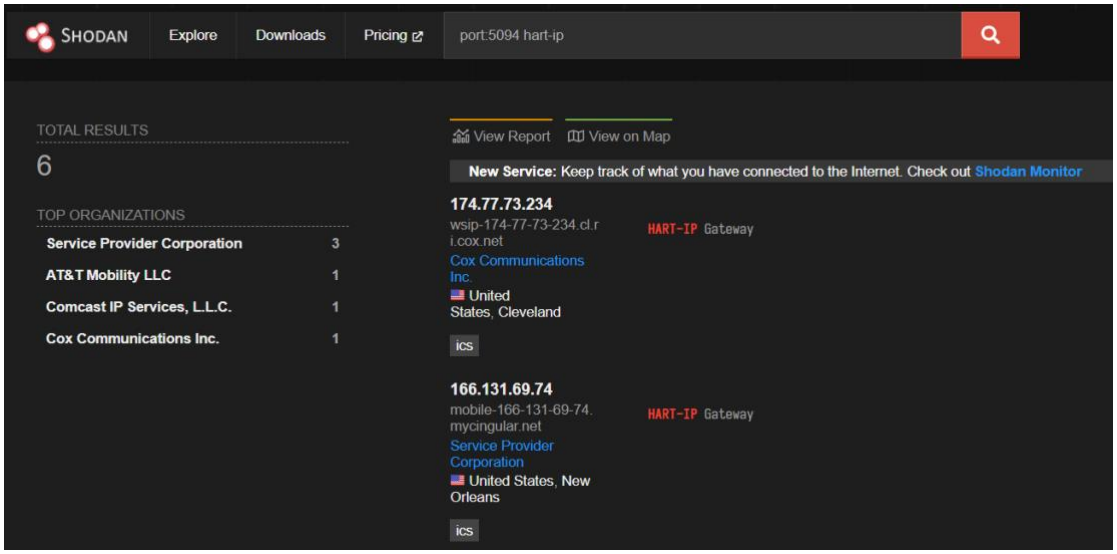
8.11.9. 搜索工控协议为“BACnet”的相关设备

port:47808



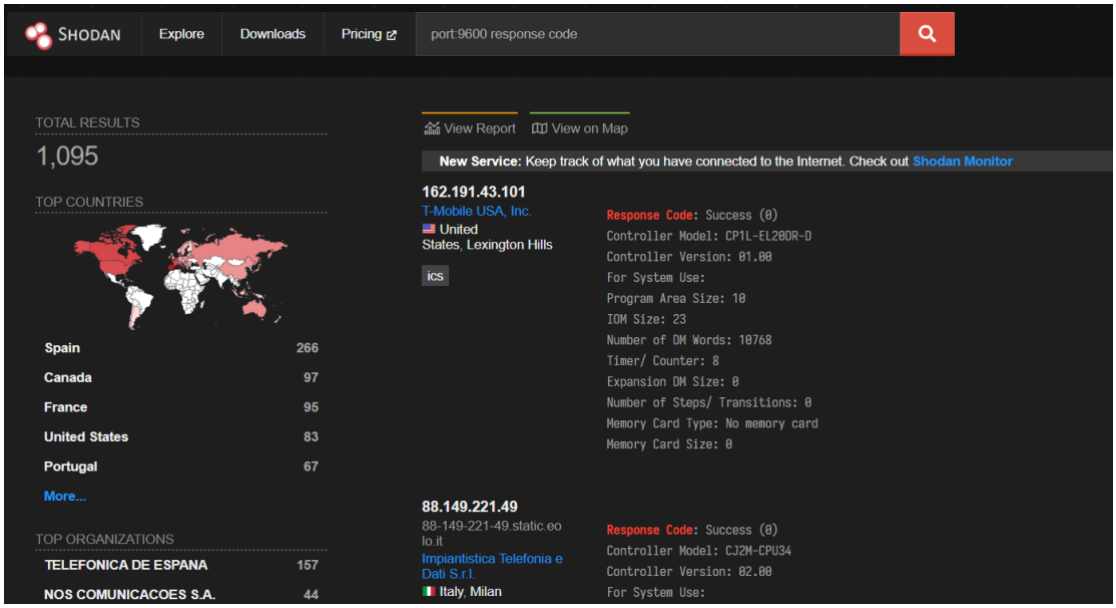
8.11.10. 搜索工控协议为“HART-IP”的相关设备

port:5094 hart-ip



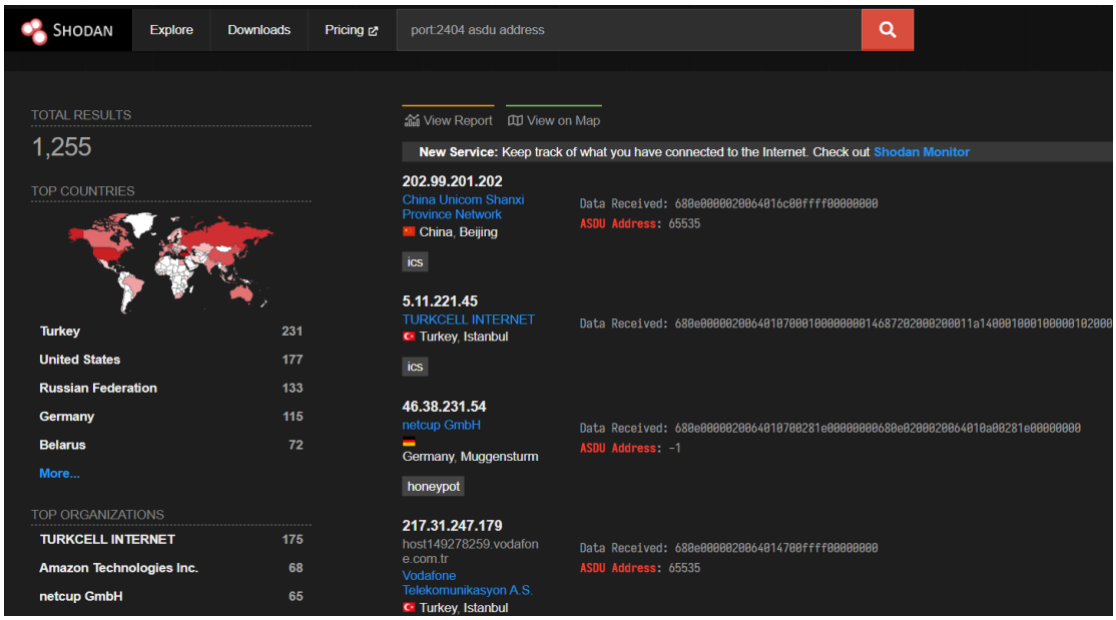
8.11.11. 搜索工控协议为“Omron FINS”的相关设备

port:9600 response code



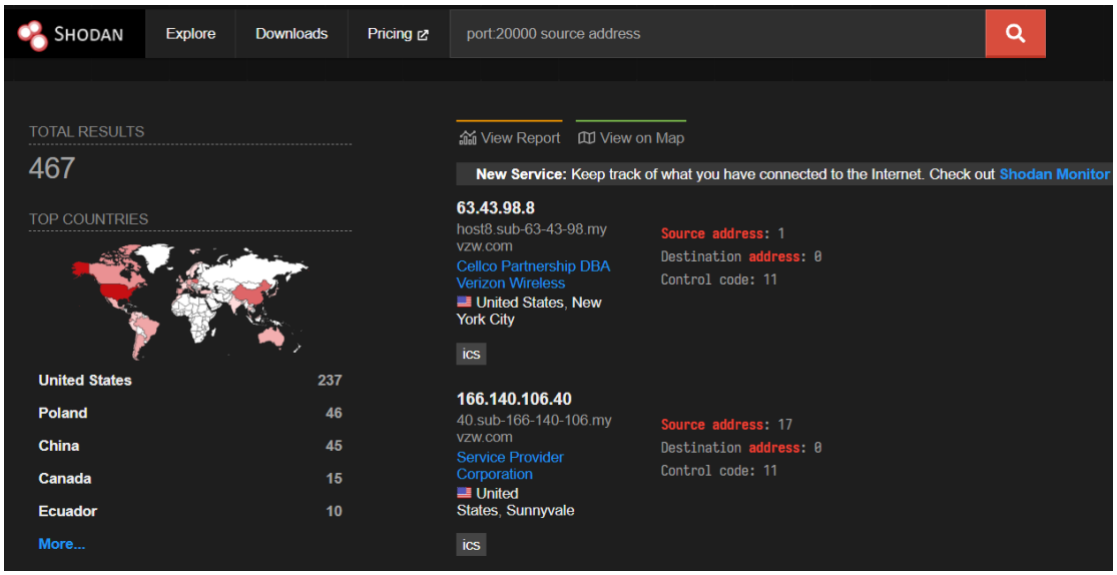
8.11.12. 搜索工控协议为“IEC 60870-5-104”的相关设备

port:2404 asdu address



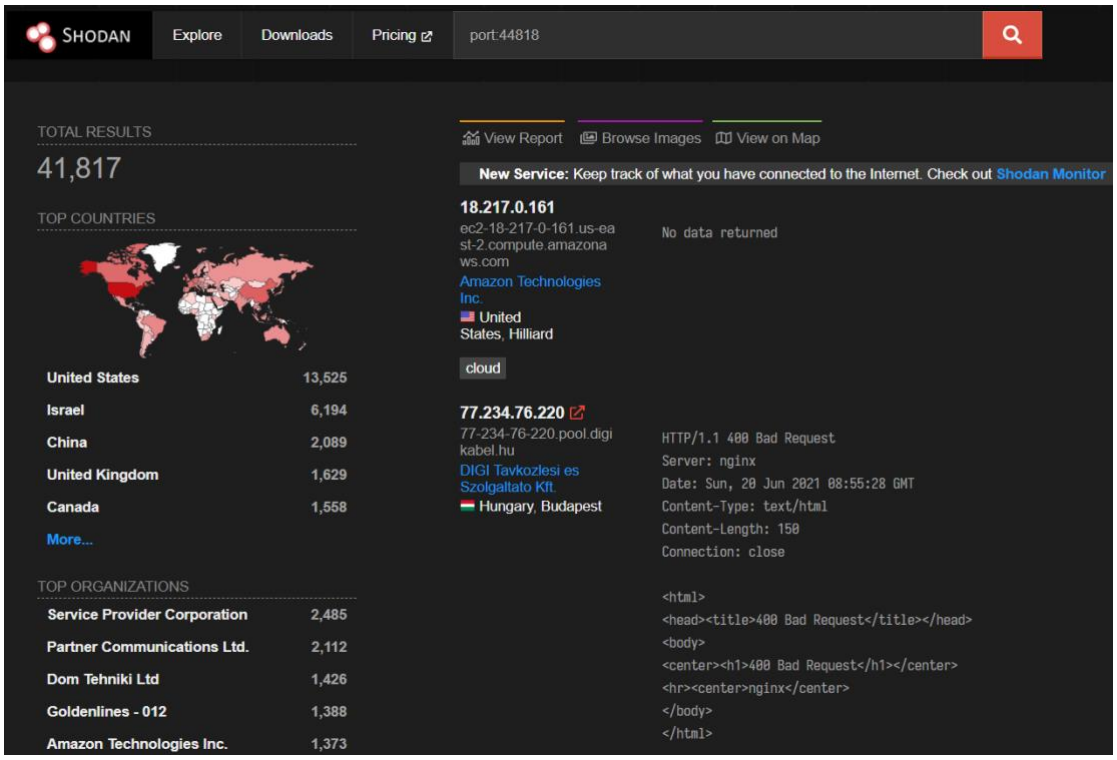
8.11.13. 搜索工控协议为“DNP3”的相关设备

port:20000 source address



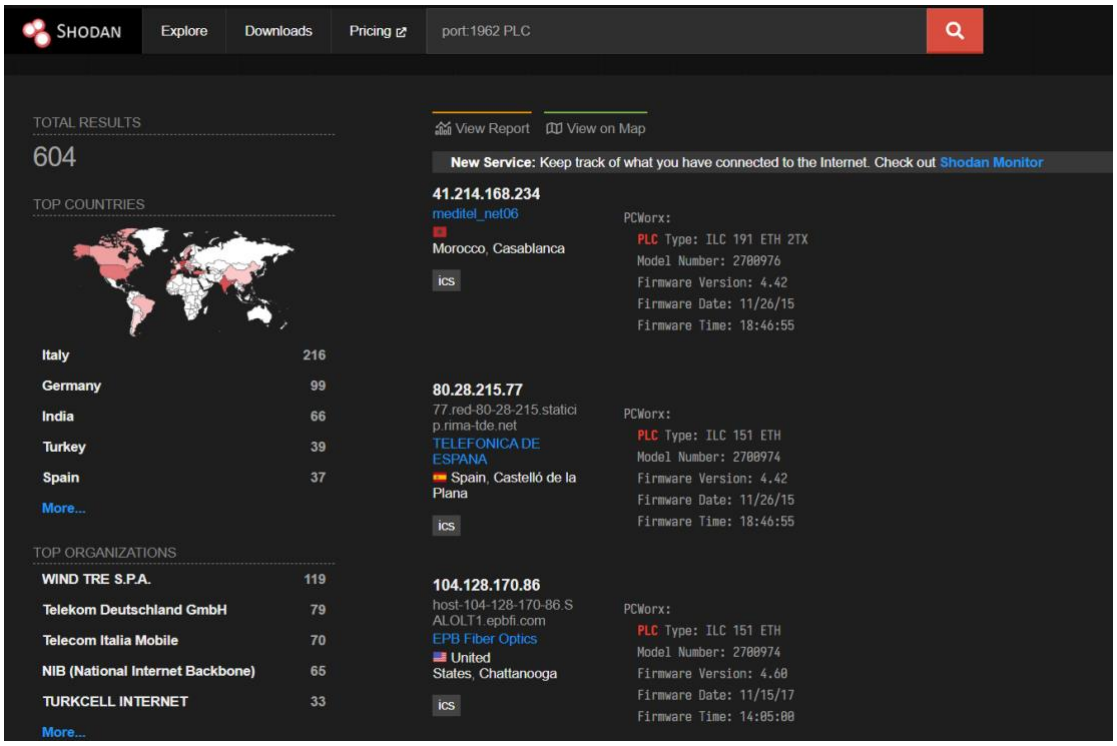
8.11.14. 搜索工控协议为“EtherNet/IP”的相关设备

port:44818



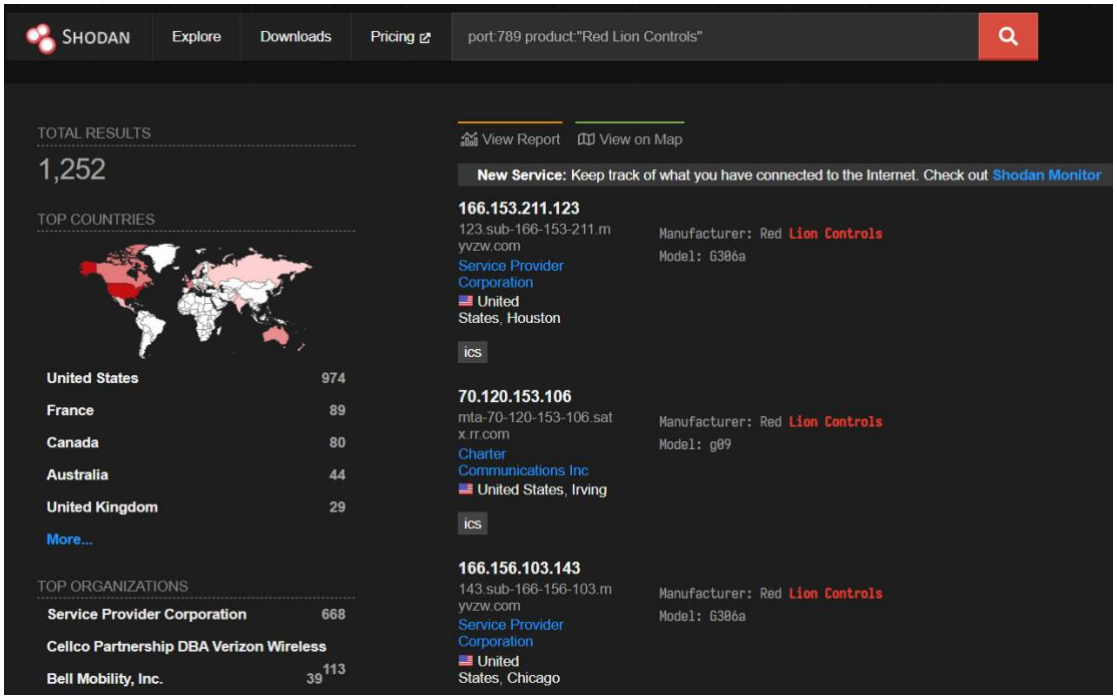
8.11.15. 搜索工控协议为“PCWorx”的相关设备

port:1962 PLC



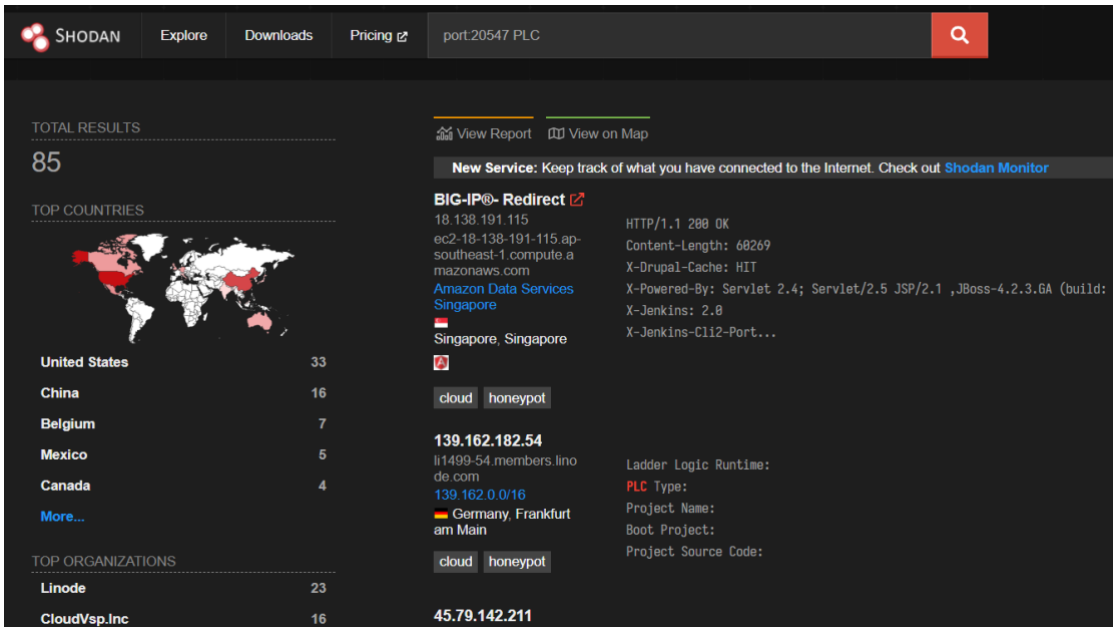
8.11.16. 搜索工控协议为“Crimson v3.0”的相关设备

port:789 product:"Red Lion Controls"



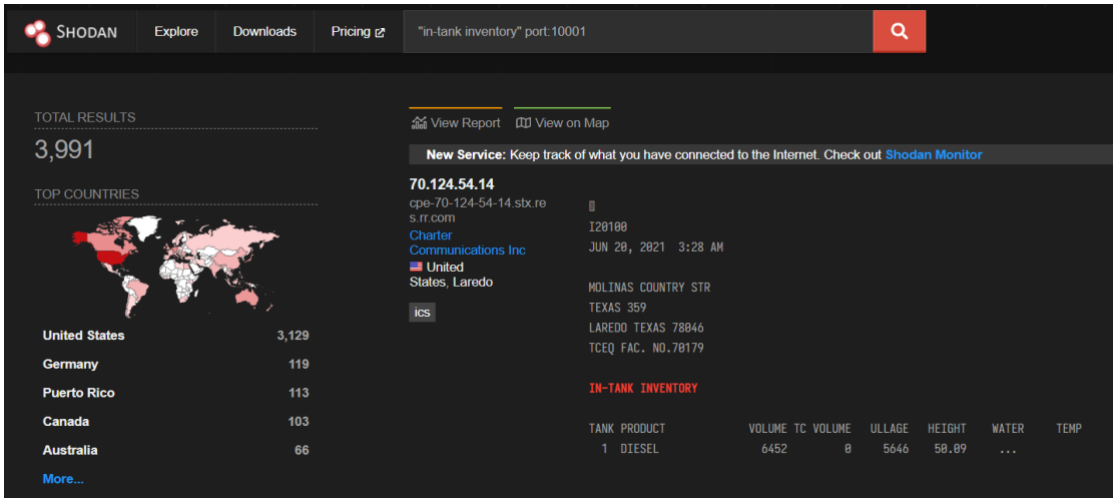
8.11.17. 搜索工控协议为“ProConOS”的相关设备

port:20547 PLC



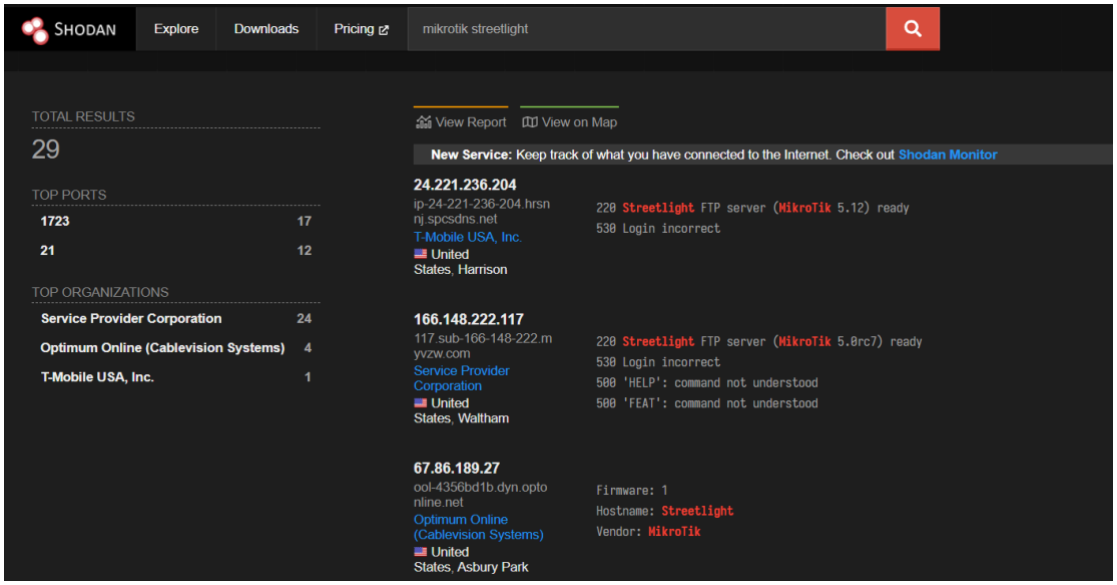
8.11.18. 搜索加油站泵控制器

"in-tank inventory" port:10001



8.11.19. 搜索交通灯控制器、红绿灯摄像头

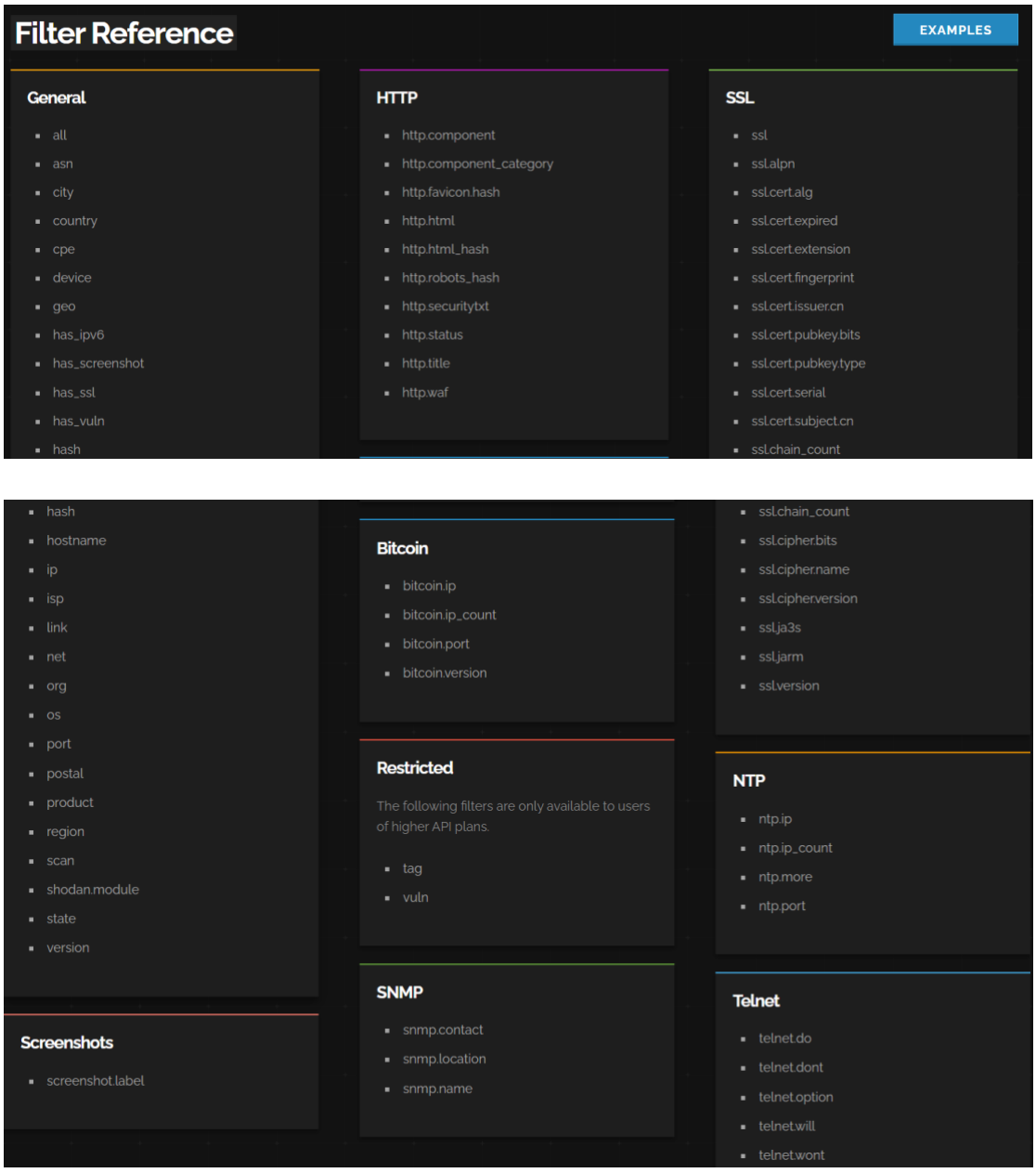
mikrotik streetlight



8.12. 过滤器列表

Shodan 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 Shodan 支持了多个网络组件的指纹识别，包括 SSL、HTTP、Bitcoin、NTP、SNMP、Telnet、Screenshots 等。

详情请查看：https://beta.shodan.io/search/filters 获取。



9. 附录

9.1. 附录 A--Banner 格式

9.1.1. 常用属性

名称	描述	举例
asn	自治系统号	AS4837
data	服务的主要 banner	HTTP/1.1200…
ip	整数型的 IP 地址格式	493427495
ip_str	字符串型 IP	199.30.15.20
ipv6	字符串型 IPv6	2001:4860:4860::8888
port	服务的端口号	80
timestamp	收集信息的日期	2014-01-15T05:49:56.283713
hash	数据属性的散列值	Numerichashofthedataproperty
hostnames	目标 IP 的主机名	[“shodan.io”,“www.shodan.io”]
domains	目标 IP 的所有域名	[“shodan.io”]
link	网络连接类型	以太网/调制解调器
location	设备的物理地址	
opts	补充或者实验数据不包含在主要的 banner 中	
org	分配 IP 的组织	GoogleInc.
isp	负责 IP 空间的 ISP	VerizonWireless
os	操作系统	Linux
uptime	IP 上线时间	50
tags	描述设备用途的标签列表(仅供企业型账号使用)	["ics","vpn"]
transport	用于收集 banner 的传输协议(UDP 或者是 TCP)	tcp

9.1.2. Elastic 属性

名称	描述
elastic.cluster	有关集群的一般信息集群上可用的索引列表
elastic.indices	
elastic.nodes	

9.1.3. HTTP（S）属性

名称	描述
http.components	用于创建网站的网站技术
http.host	发送主机名来抓取网站的 HTML
http.html	网站的 HTML 内容
http.html_hash	html 散列值
http.location	最终的 HTML 响应位置
http.redirects	遵循的重定向列表。每个重定向项目有三个属性：主机、数据和位置
http.robots	robots.txt 文件的网站
http.server	HTTP 响应的服务器头
http.sitemap	网站的 Sitemap XML
http.title	网站的标题

9.1.4. 位置属性

名称	描述
area_code	设备位置的区号
city	城市名称
country_code	2 个字母组成的国家代码
country_code3	3 个字母组成的国家代码
country_name	国家的全名
dma_code	指定市场区号（仅限美国）
latitude	维度
longitude	经度
postal_code	邮政编码
region_code	地区代码

9.1.5. SMB 属性

名称	描述
smb.anonymous	服务器是否允许匿名连接
smb.capabilities	服务支持的功能列表
smb.shares	可用的网络共享列表
smb. smb_version	用于收集信息的协议版本
smb.software	提供服务的软件
smb.raw	服务器发送的十六进制编码数据包列表

9.1.6. SSH 属性

名称	描述
ssh.cipher	协商期间使用的密码
ssh.fingerprint	设备的指纹
ssh.kex	服务器支持的密钥交换算法列表
ssh.key	服务器 SSH 密钥
ssh.mac	消息认证码算法

9.1.7. SSL 属性

如果服务使用 SSL 进行包装，则 Shodan 将执行附加测试，并在以下属性中提供结果：

名称	描述
ssl.acceptable_cas	服务器接受的证书颁发机构列表
ssl.cert	可解析的 SSL 证书
ssl.cipher	SSL 连接的首选密码
ssl.chain	从用户证书到根证书的 SSL 证书列表
ssl.dhparams	Diffie-Hellman 参数
ssl.tlsext	服务器支持的 TLS 扩展列表
ssl.version	支持的 SSL 版本

9.1.8. ISAKMP 属性

以下为使用 ISAKMP 协议的 VPN 收集的属性：

名称	描述
isakmp.initiator_spi	初始化器的 hex 编码的安全参数索引
isakmp.responder_spi	用于响应器的 hex 编码的安全参数索引
isakmp.next_payload	启动发送的下一个 payload
isakmp.version	协商版本
isakmp.exchange_type	交换类型
isakmp.flags.encryption	加入设置
isakmp.flags.commit	提交设置
isakmp.flags.authentication	认证设置
isakmp.msg_id	消息的十六进制编码标识
isakmp.length	ISAKMP 数据包的大小

9.2. 附录 B--过滤器

9.2.1. 常规过滤器

过滤器名	描述	类型	举例
after	只显示给出日期之后的结果 (dd/mm/yyyy)	string	after:"04/02/2017"
asn	自治系统号码	string	asn:"AS4130"
before	只显示给出日期之前的结果 (dd/mm/yyyy)	string	before:"04/02/2017"
category	现有的分类：ics,malware	string	category:"malware"
city	城市的名字	string	city:"SanDiego"
country	国家简写	string	country:"ES"country:"CN"
geo	经纬度	string	geo:"46.9481,7.4474"
hash	数据的 hash 值	int	-hash:0
has_ipv6	是否是 IPv6	boolean	has_ipv6:true
has_screenshot	是否有截图	boolean	has_screenshot:true
hostname	主机名或域名	string	hostname:"google"
ip	ip 地址	string	ip:"54.67.82.248"
isp	ISP 供应商	string	isp:"ChinaTelecom"
org	组织或公司	string	org:"google"
os	操作系统	string	os:"Windows7or8"
port	端口号	int	port:21

postal	邮政编码(仅限于美国)	string	postal:"98221"
product	软件、平台	string	product:"Apachehttpd"product:"openssh"
region	地区或国家别名	string	-
state		string	-
net	CIDR 格式的 IP 地址	string	net:190.30.40.0/24
version	软件版本	string	version:"2.6.1"
vuln	漏洞的 CVEID	string	vuln:CVE-2014-0723

9.2.2. HTTP 过滤器

过滤器名	描述	类型
http.component	网站上所使用的网络技术名称	string
http.component_category	网站上使用的网络组件的类别	string
http.html	Webbanner	string
http.html_hash	网站 HTML 的哈希值	int
http.status	响应状态码	int
http.title	网站 title 的 banner	string

9.2.3. NTP 过滤器

名称	描述	类型
ntp.ip	查找在其 monlist 中 NTP 服务器的 IP	
ntp.ip_count	初始 monlist 返回的 IP 数量	int
ntp.more	真/假;monlist 集是否有更多的 IP 地址	boolean
ntp.port	monlist 中的 IP 地址使用的端口	int

9.3. 附录 C--Facets

9.3.1. 常用 Facets

名称	描述
asn	自治系统号码
city	城市的全名
country	国家的全名
domain	设备的域名
hash_screenshot	有无可用的截图
isp	ISP 管理网络块
link	网络连接的类型
org	拥有该网快的组织
os	操作系统
port	服务的端口号
postal	邮政编码
product	软件/产品名称
region	地区/国家名称
state	区域的别名
uptime	主机启动的时间
vuln	漏洞的 CVE ID

9.3.2. HTTP Facets

名称	描述	类型

http.conponents	网站上使用的网络技术的名称	string
http.component_category	网站上使用的网络组件的类别	string
http.html_hash	HTML 网站的哈希值	int
http.status	响应状态码	int

9.3.3. NTP Facets

名称	描述
ntp.ip	monlist 返回的 IP 地址
ntp.ip_count	初始 monlist 返回的 IP 数量
ntp.more	monlist 收集的是否有更多的 IP 地址
mtp.port	monlist 中的 IP 地址使用的端口

9.3.4. SSH Facets

名称	描述
ssh.cipher	密码的名称
ssh.fingerprint	设备的指纹
ssh.mac	使用的 MAC 算法名称
ssh.type	密钥认证的类型

10. Shodan 自动化采集工具

10.1. Shodan_So

https://github.com/zev3n/Shodan_So

查看使用帮助：

./Shodan_So.py -h

```
root@VM-0-5-ubuntu:~/tools/Shodan_So# python Shodan_So.py -h
usage: Shodan_So.py [-f ips.txt] [--ip 217.140.75.46-217.140.75.56] [--search Apache] [--hostnameonly] [--history] [--page 1] [--list_ip] [--list_ip_port]

Shodan_So - Search Assistant: Searching shodan via API. --By: Zev3n

optional arguments:
  -f ips.txt            Using THe Ips List - File containing IPs to search shodan for.
  --ip 217.140.75.46-217.140.75.56
                        Shodan Host Search against IP/IP range & return results from Shodan about a it/them.
  --search Apache       when searching Shodan for a string.
  --hostnameonly        Only provide results with a Shodan stored hostname.
  --history             Return all historical banners.
  --page 1              Page number of results to return (default 1 (first page)).
  --list_ip             Singled out IP address from query results.
  --list_ip_port        Singled out IP address with port from query results.
root@VM-0-5-ubuntu:~/tools/Shodan_So#
```

搜索内容：

./Shodan_So.py –search “query”

```
*** RESULT 99***
IP Address: 52.220.10.176
Last updated: 2021-06-20T11:26:22.676936
Port: 80
Data: HTTP/1.1 302 Found
Date: Sun, 20 Jun 2021 11:26:14 GMT
Server: Apache/2.4.9 (Win64) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
location: https://52.220.10.176
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8



*** RESULT 100***
IP Address: 202.29.149.198
Last updated: 2021-06-20T11:26:05.287430
Port: 80
Data: HTTP/1.1 200 OK
Date: Sun, 20 Jun 2021 11:26:03 GMT
Server: Apache/2.4.9 (Unix) OpenSSL/1.0.1g PHP/5.5.11 mod_perl/2.0.8-dev Perl/v5.16.3
Content-Length: 7237
Content-Type: text/html;charset=ISO-8859-1
```

提取搜索结果中的 IP 并输出的文本中：

./Shodan_So.py --search "apache" --list_ip >> ip.txt

--list_ip_port 参数是返回 IP 地址:端口形式的结果，以供后续不同场景的利用：

./Shodan_So.py -search “apache” --list_ip >> ip.txt --list_ip_port

-iprg 参数接受的则是 CIDR 地址块，可实现指定子网范围内主机的查询。-f 参数接受的是一个 ip 地址的文本文档，不同地址用换行隔开，本工具会依次读取文档内的 ip 地址并依次查询。

知道创宇云安全事业群
解决方案交付中心