Shodan S.O.P.

By: Cpl Jimenez

3rd PLT DCO-IDM

LU: 20240228

This document will serve as the guide to Shodan setup and usage for operations.

Shodan Overview

Shodan.io is a search engine for the Internet of Things. It functions similar to Google and Bing in that it searches and indexes information, but whereas the latter two search engines crawl the web, Shodan crawls the entire Internet. It gathers information about all devices directly connected to the Internet, by banner grabbing. The types of devices that can be indexed vary tremendously, from small desktops to nuclear power plants, and everything in between.

Usage/Legality

Occasionally, when searching for IP addresses in Shodan, it will say “No information available for that IP”. Keep in mind that Shodan queries *publicly*

available information, so if devices are behind a firewall or otherwise not directly connected to the Internet, Shodan will not be able to query them.
This could be due to various reasons, and does not imply anything about the security of a target machine. The absence of information on Shodan doesn't necessarily imply that a system is secure or insecure. Security depends on various factors, including the configuration of services, software updates, firewall settings, and other security measures in place on the target machine.

Shodan is an OSINT tool and is generally considered legal and ethical for passive reconnaissance during a penetration test because it is a search engine that gathers publicly available information about a target.
However, improper interaction with a target system without proper authorization can lead to illegal activities like exploiting vulnerabilities, attempting to access systems, or launching attacks.

These activities are illegal under the Computer Fraud and Abuse Act (CFAA) in the US, the Police and Justice Act in the UK, section 342.1(1) of the Criminal Code of Canada (Unauthorized Use of Computer), and similar laws in other countries.

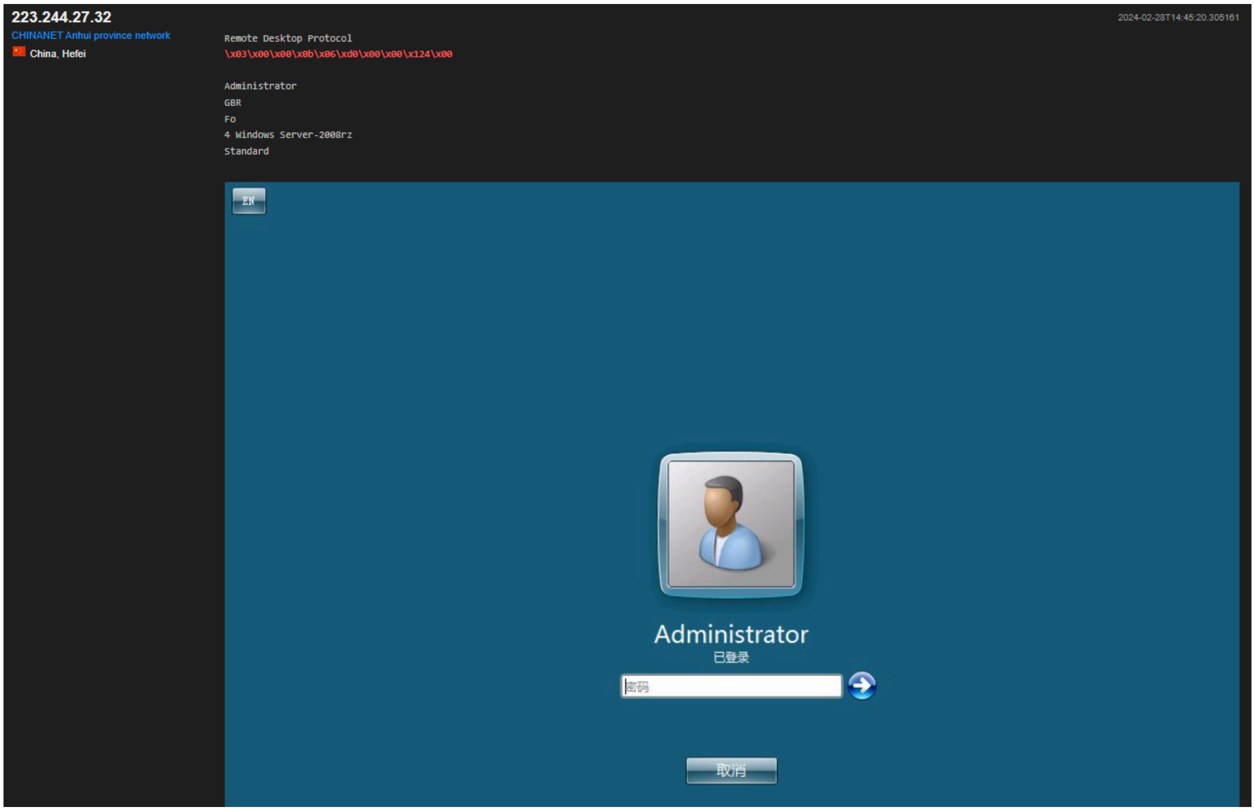
For example, you can use the query

"\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00" has_screenshot:true

If we break it down, we can see that the first part of the query is a hex string, which is a response typically associated with an open Windows Remote Desktop Protocol (RDP) connection. This means that port 3389 is open on the target machine, and that it has been configured to allow remote connections.

The second part of the query is ‘has_screenshot:true’. This tells Shodan to only show results that have a screenshot. Putting both of these queries together will show us machines that have port 3389 open (if not more ports) and show a screenshot. Viewing the screenshot will likely show the login screen of a vulnerable machine, which also shows a username. However, the screenshot may also be something from a webcam or a CCTV camera, which can lead to other avenues of reconnaissance. Thus with a single query, you have obtained much of the information you need to do further reconnaissance or stage an attack.

Pictured below is a vulnerable Chinese server. From this query, we already know a lot of information: IP address, open ports, ISP, organization, geolocation, OS version, username, and the autonomous system number (look it up on search.arin.net).

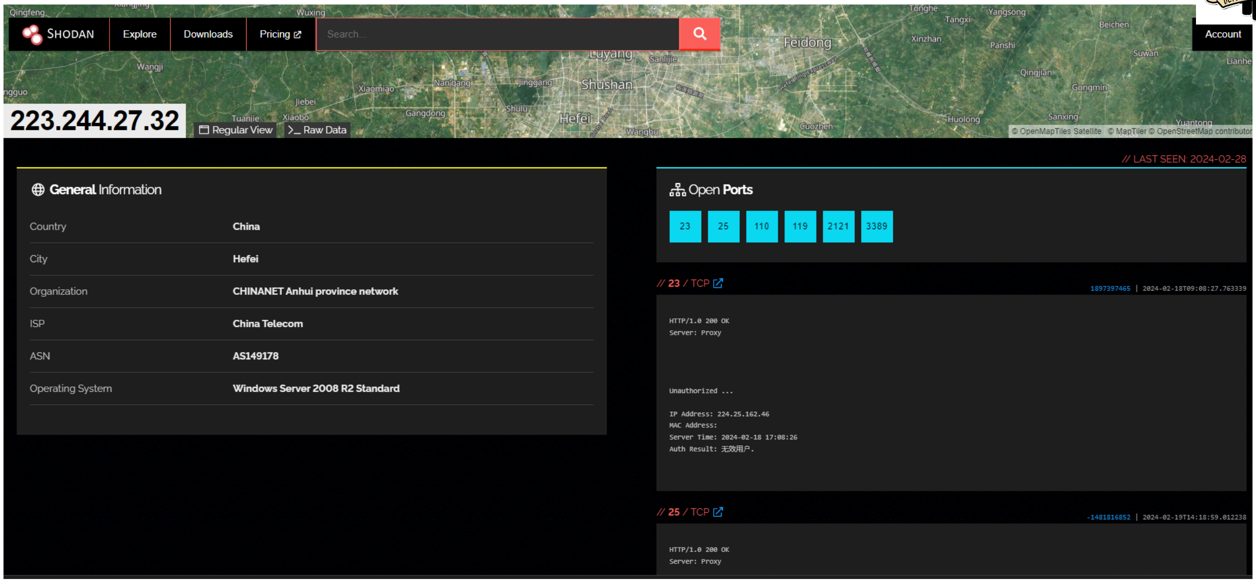


223.244.27.32
CHINANET Anhui province network
China, Hefei

2024-02-28T14:45:20.305161

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

Administrator
GBR
Fo
4 Windows Server-2008rz
Standard
```



223.244.27.32

// LAST SEEN: 2024-02-28

General Information

Country	China
City	Hefei
Organization	CHINANET Anhui province network
ISP	China Telecom
ASN	AS149178
Operating System	Windows Server 2008 R2 Standard

Open **Ports**

23 25 110 119 2121 3389

// 23 / TCP   1897397465 | 2024-02-18T09:08:27.763339

```
HTTP/1.0 200 OK
Server: Proxy




Unauthorized ...

IP Address: 224.25.162.46
MAC Address:
Server Time: 2024-02-18 17:08:26
Auth Result: 无效用户.
```

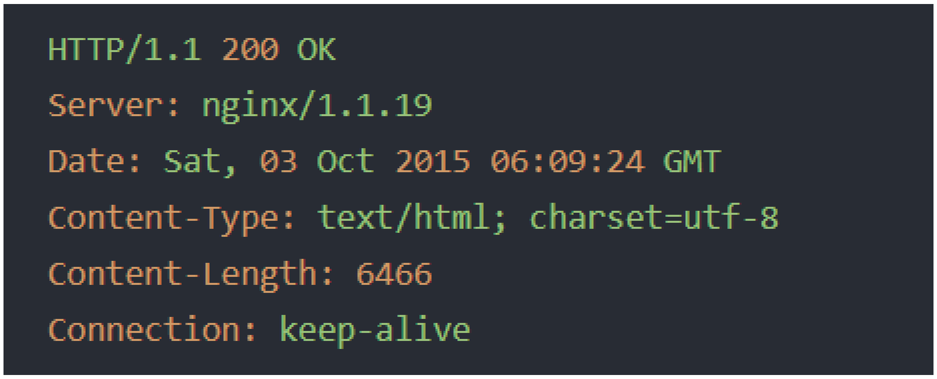
// 25 / TCP   -1481816852 | 2024-02-19T14:18:59.012238

```
HTTP/1.0 200 OK
Server: Proxy
```

Up until this point, it is perfectly legal to do this kind of reconnaissance, but taking it any further, such as launching an attack against the system, would run you afoul of the law. **Do not attempt to exploit machines or launch attacks without proper authorization to do so!**

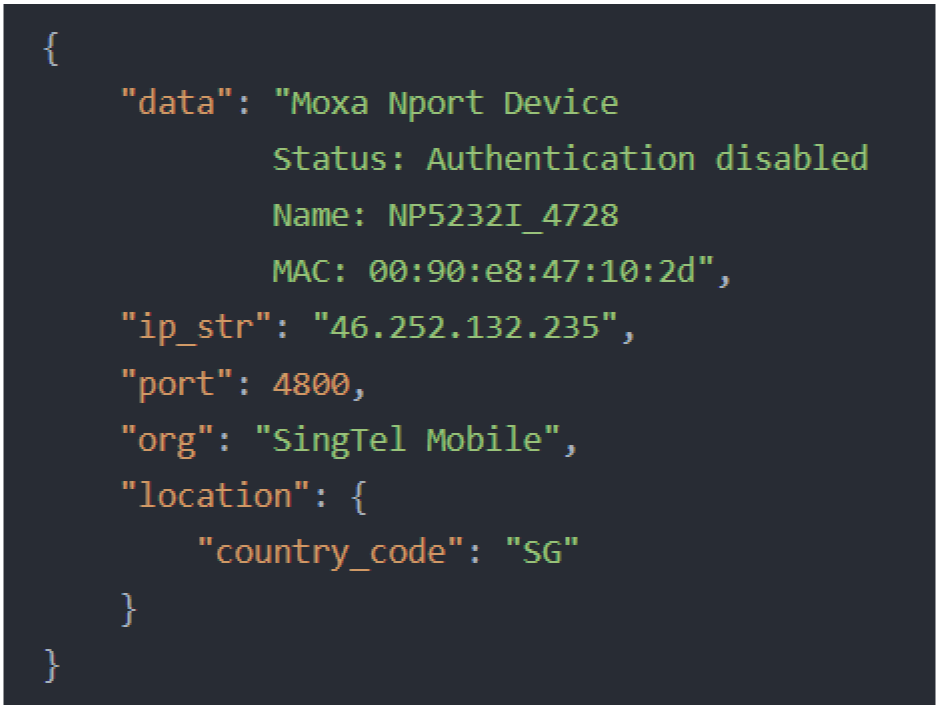
Search Query Fundamentals

Shodan queries devices by using a technique called banner grabbing. Banners are a common instance on machines. When attempting to connect to a server, a banner is typically one of the first things that you will see. If not configured correctly, banners can give away a lot of information, such as server names, versions and timestamps. Below is a typical example of a banner grabbed from an HTTP server:



```
HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Sat, 03 Oct 2015 06:09:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 6466
Connection: keep-alive
```

Each banner has several properties which describe different pieces of information about the machine you're trying to reach. Here is an example of a different banner's raw information:



```
{
    "data": "Moxa Nport Device
            Status: Authentication disabled
            Name: NP5232I_4728
            MAC: 00:90:e8:47:10:2d",
    "ip_str": "46.252.132.235",
    "port": 4800,
    "org": "SingTel Mobile",
    "location": {
        "country_code": "SG"
    }
}
```

This banner has five different properties: "data", "ip_str", "port", "org", and "country_code".

data - This is the main response from the service itself and the default property searched by Shodan if you don't indicate anything else. This is a Moxa Nport device
ip_str - This stands for "IP string" and shows the machine's IP address, 46.252.132.235
port - This shows all open ports. This particular device has a singular open port, 4800
org - org is short for "Organization". This identifies the device as being a SingTel Mobile device
country_code - Country code is a two letter country code that identifies what country the device is located in, in this case Singapore.

Again, by default, Shodan will query only the “data” property, so if you wanted to do a search to find all SingTel devices, it wouldn’t work because that falls under the “org” property. In order to search for different properties, you need to use the following format:

filtername:value

Therefore, if you wanted to search for SingleTel devices, you would have to search for org:SingTel. You can also string queries together to narrow your search results. If you wanted to search for all SingTel devices in the city of Singapore, you would search “org:SingTel city:Singapore” (no quotes).

Shodan has a filter cheat sheet that you can use at https://www.shodan.io/search/filters

Shodan CLI

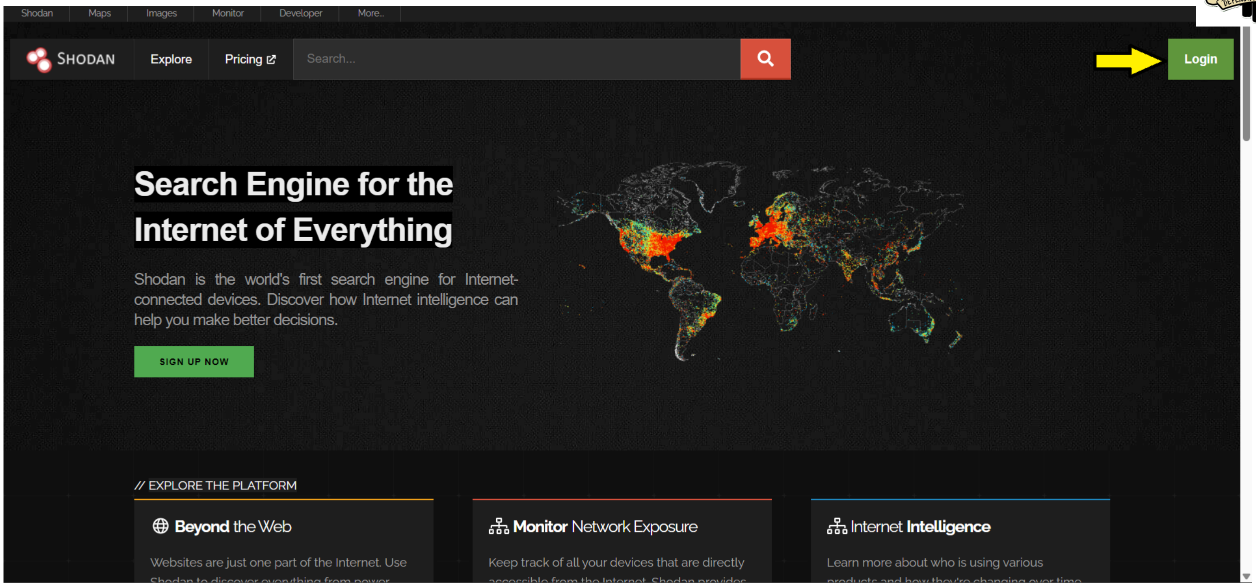
Shodan has a CLI capability that is built into Python as a library. Therefore if you do not have python installed on your machine, you will not be able to use the CLI version. Installation is easy, requiring only two commands:

`pip install -U --user shodan` This command will install the shodan library in your pythonXY\Scripts\ directory, where XY is the version of python that you are using

`shodan init YOUR_API_KEY` This command initializes shodan and connects your shodan account to the .exe so that you can use more advanced commands.

You can find your API under the Account Tab in Shodan:

Start by going to the main page and logging in:



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

// EXPLORE THE PLATFORM

Beyond the Web

Websites are just one part of the Internet. Use

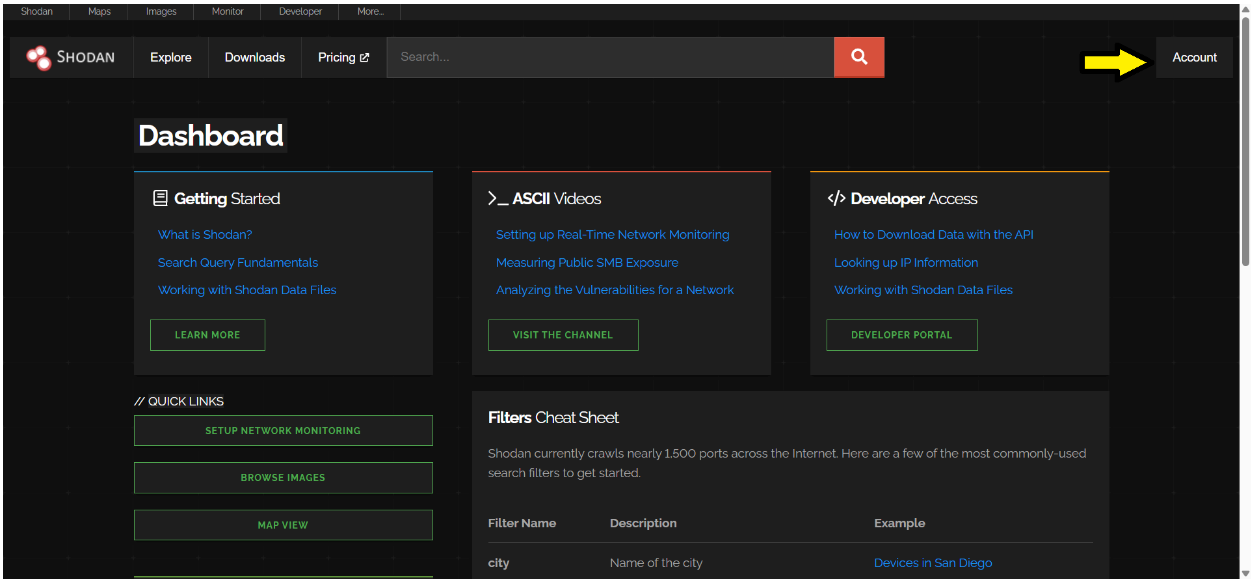
Monitor Network Exposure

Keep track of all your devices that are directly

Internet **Intelligence**

Learn more about who is using various

Next, click on the Account tab:



Dashboard

Getting Started

What is Shodan?
Search Query Fundamentals
Working with Shodan Data Files

>_ **ASCII** Videos

Setting up Real-Time Network Monitoring
Measuring Public SMB Exposure
Analyzing the Vulnerabilities for a Network

</> **Developer** Access

How to Download Data with the API
Looking up IP Information
Working with Shodan Data Files

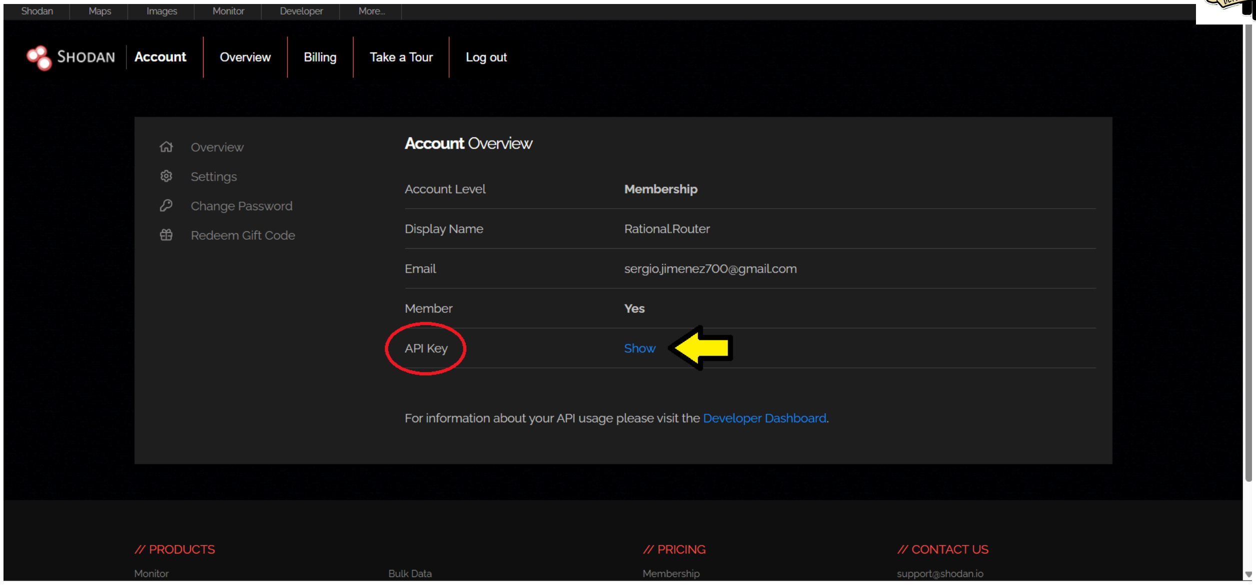
// QUICK LINKS

Filters Cheat Sheet

Shodan currently crawls nearly 1,500 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

Filter Name	Description	Example
city	Name of the city	Devices in San Diego

Next to API Key, click Show:

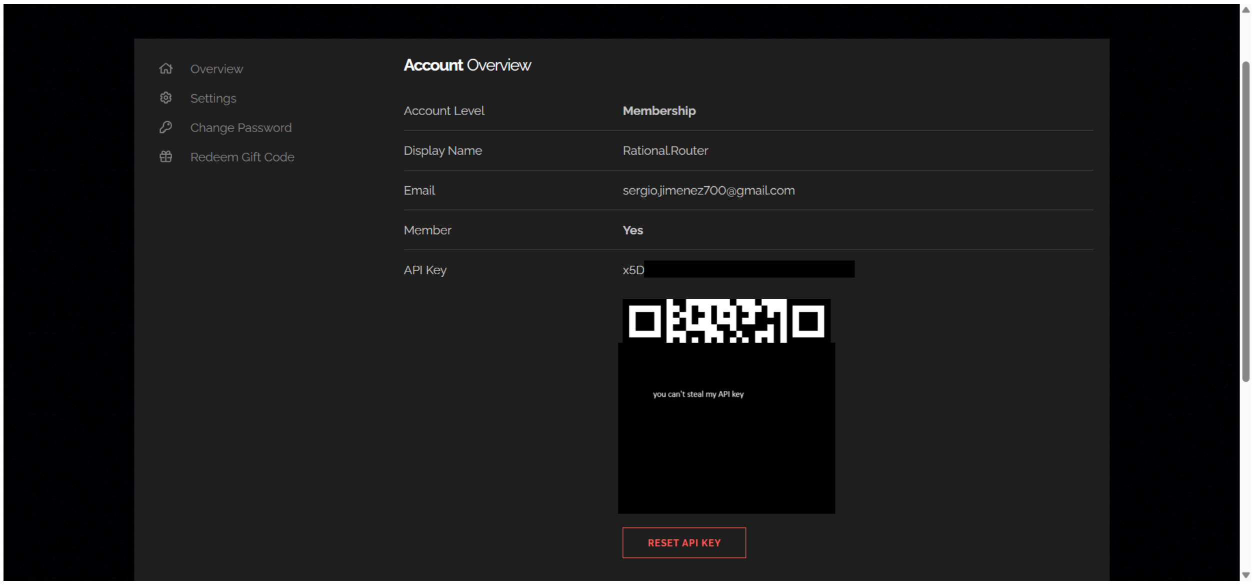


Account Overview

Account Level	**Membership**
Display Name	RationalRouter
Email	sergio.jimenez700@gmail.com
Member	**Yes**
API Key	Show

For information about your API usage please visit the Developer Dashboard.

It will then show you your API key, as well as giving you a QR code version of the key:



Account Overview

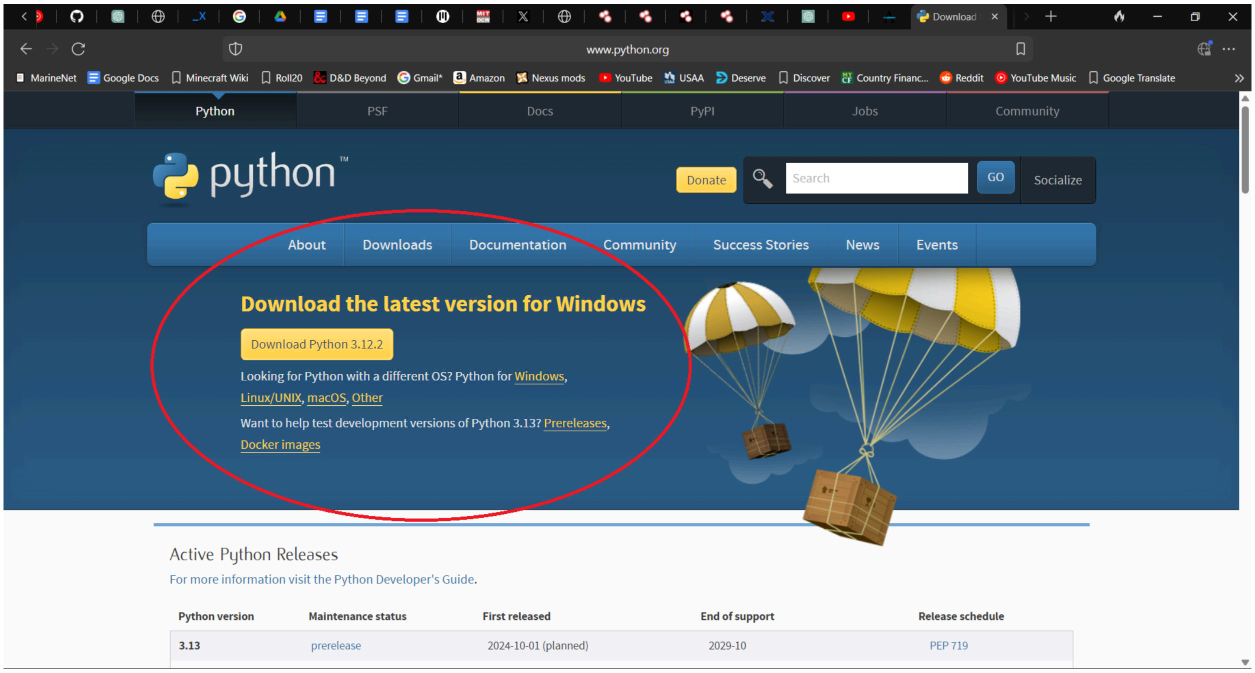
Account Level	**Membership**
Display Name	RationalRouter
Email	sergio.jimenez700@gmail.com
Member	**Yes**
API Key	x5D[redacted]

[redacted]

you can't steal my API key

Python Installation

In case you do not have Python installed on your system, I will outline the steps for that as well. These instructions will go over how to download Python onto a Windows machine. First, navigate to https://www.python.org/downloads/. There should be a big yellow download button that you need to click.



Download the latest version for Windows

Looking for Python with a different OS? Python for Windows, Linux/UNIX, macOS, Other

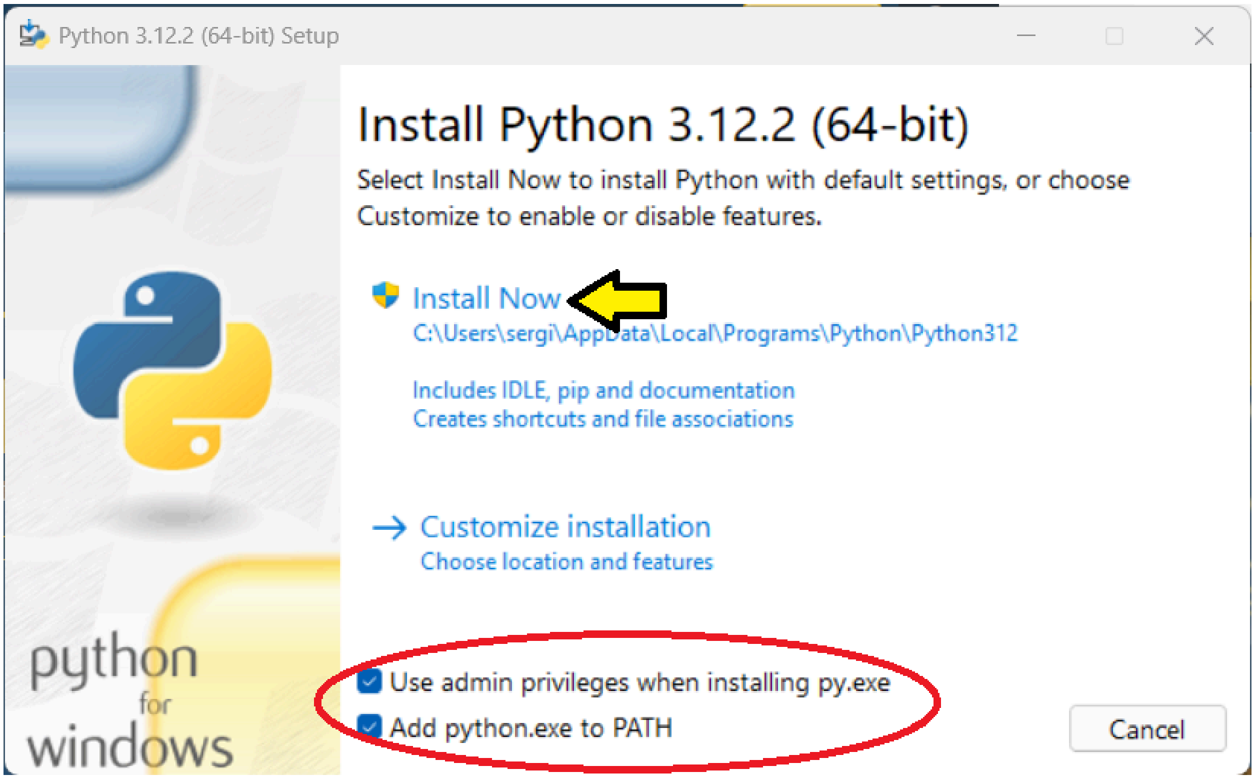
Want to help test development versions of Python 3.13? Prereleases, Docker images

Active Python Releases

For more information visit the Python Developer's Guide.

Python version	Maintenance status	First released	End of support	Release schedule
3.13	prerelease	2024-10-01 (planned)	2029-10	PEP 719

Once the .exe is downloaded, bring up the installation wizard and select ‘Install Now’. Make sure to check the boxes to install python with admin privileges and to add python.exe to PATH. If you do not add Python to your PATH, then commands and libraries will not work as intended.



Python 3.12.2 (64-bit) Setup

Install Python 3.12.2 (64-bit)

Select Install Now to install Python with default settings, or choose Customize to enable or disable features.

Install Now
C:\Users\sergi\AppData\Local\Programs\Python\Python312

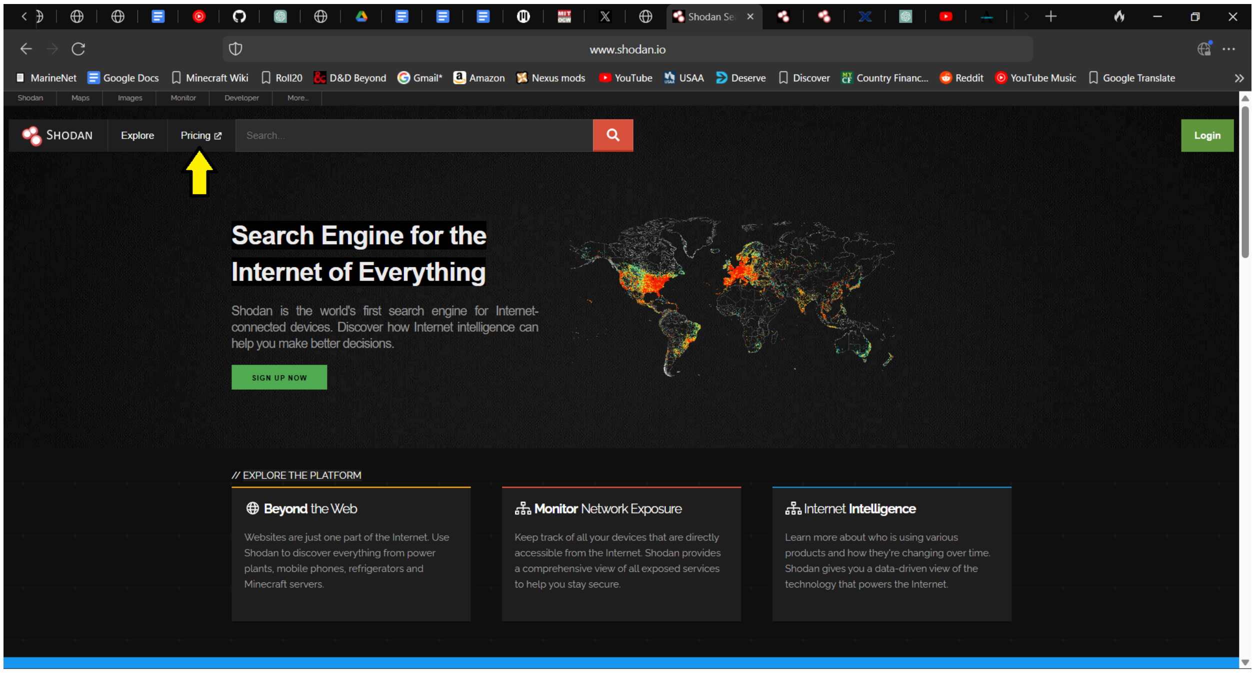
Includes IDLE, pip and documentation
Creates shortcuts and file associations

→ Customize installation
Choose location and features

☑ Use admin privileges when installing py.exe
☑ Add python.exe to PATH

Pricing and Membership Types

Shodan is a free tool, but there are also paid options if you wish to expand your toolset. Membership, Freelancer, Small Business, Corporate, or Enterprise level plans are available for purchase. Start at the home page, and then click the Pricing button:



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

Beyond the Web

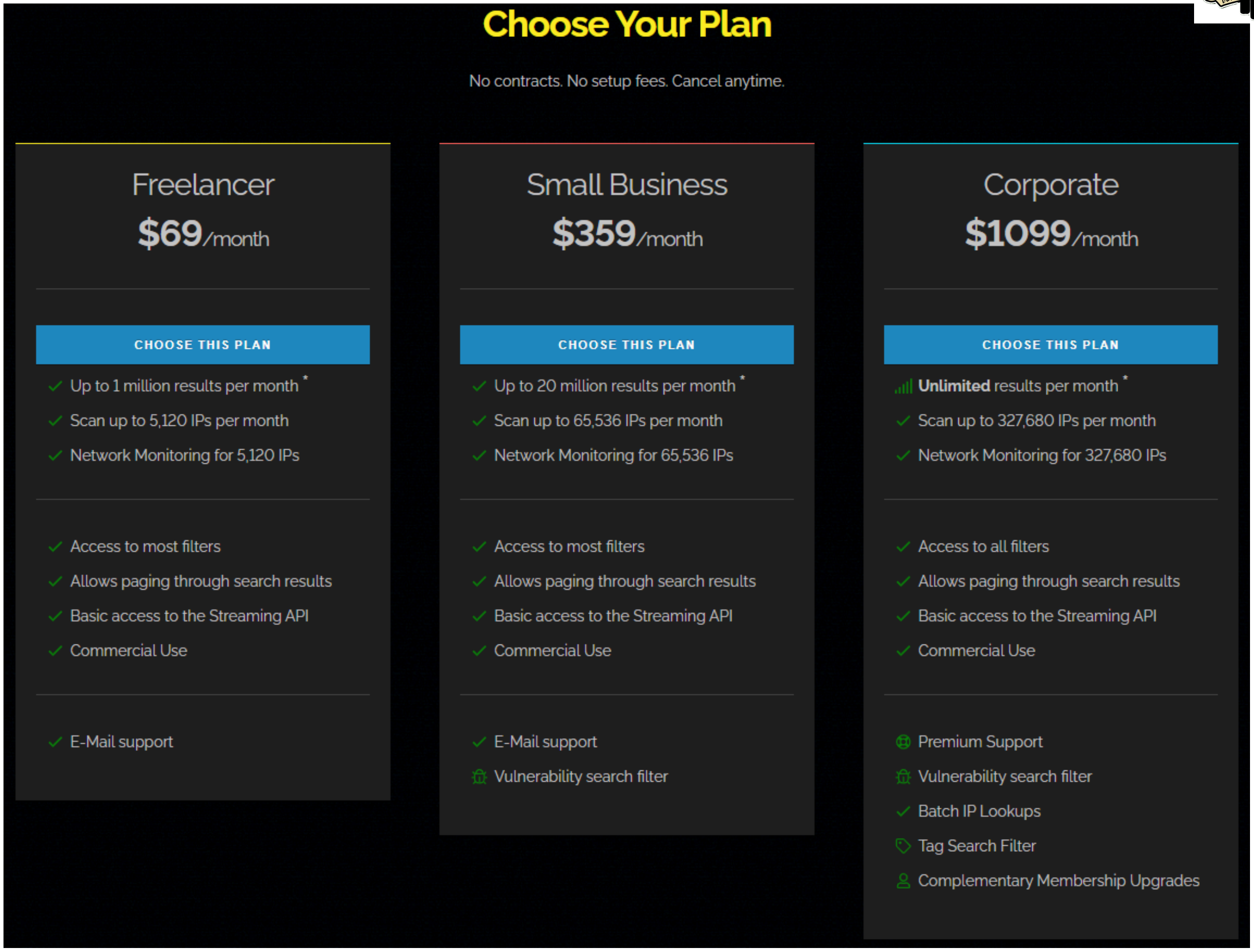
Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Monitor Network Exposure

Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

Internet **Intelligence**

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.



Choose Your Plan

No contracts. No setup fees. Cancel anytime.

Freelancer

$69/month

CHOOSE THIS PLAN

- ✓ Up to 1 million results per month *
- ✓ Scan up to 5,120 IPs per month
- ✓ Network Monitoring for 5,120 IPs

- ✓ Access to most filters
- ✓ Allows paging through search results
- ✓ Basic access to the Streaming API
- ✓ Commercial Use

- ✓ E-Mail support

Small Business

$359/month

CHOOSE THIS PLAN

- ✓ Up to 20 million results per month *
- ✓ Scan up to 65,536 IPs per month
- ✓ Network Monitoring for 65,536 IPs

- ✓ Access to most filters
- ✓ Allows paging through search results
- ✓ Basic access to the Streaming API
- ✓ Commercial Use

- ✓ E-Mail support
- Vulnerability search filter

Corporate

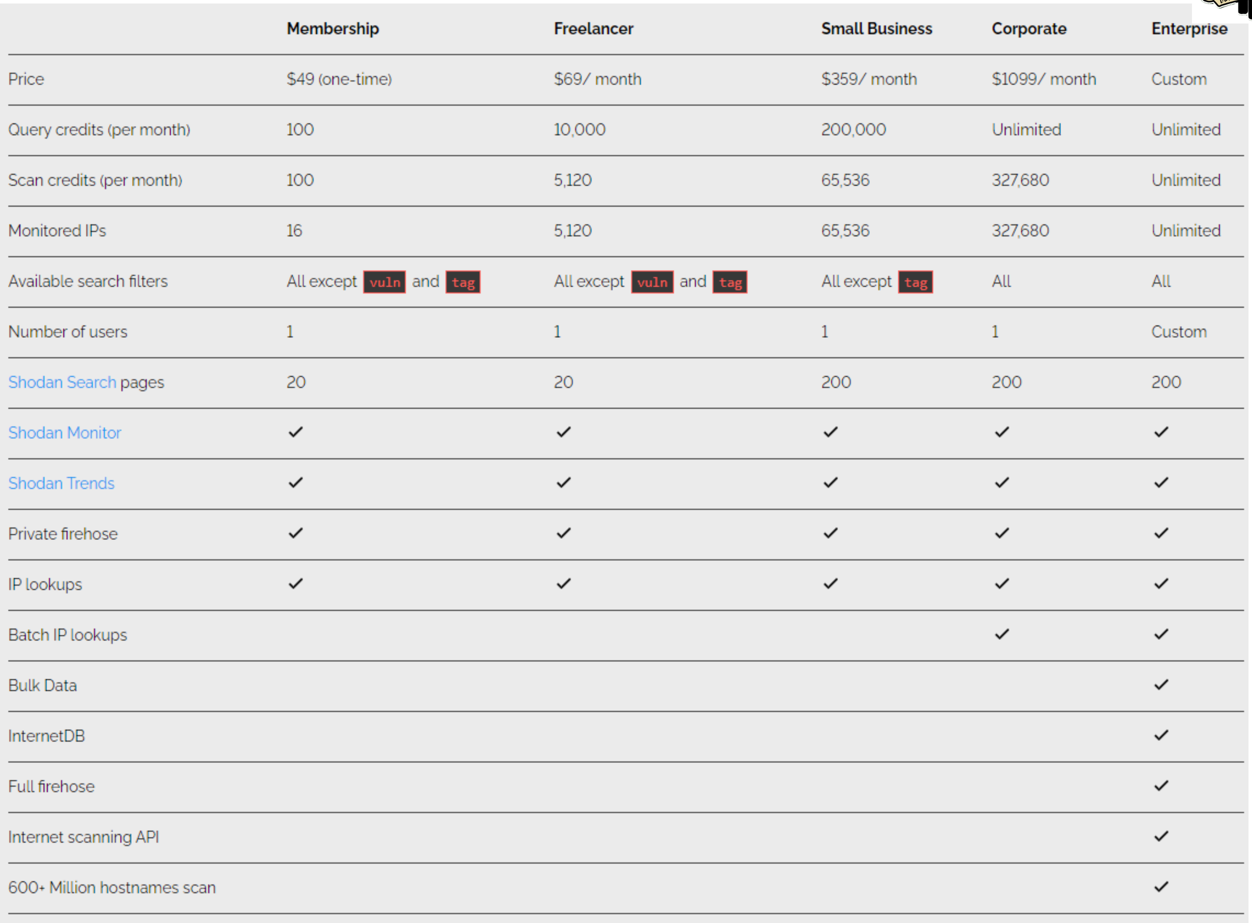
$1099/month

CHOOSE THIS PLAN

- **Unlimited** results per month *
- ✓ Scan up to 327,680 IPs per month
- ✓ Network Monitoring for 327,680 IPs

- ✓ Access to all filters
- ✓ Allows paging through search results
- ✓ Basic access to the Streaming API
- ✓ Commercial Use

- Premium Support
- Vulnerability search filter
- ✓ Batch IP Lookups
- Tag Search Filter
- Complementary Membership Upgrades

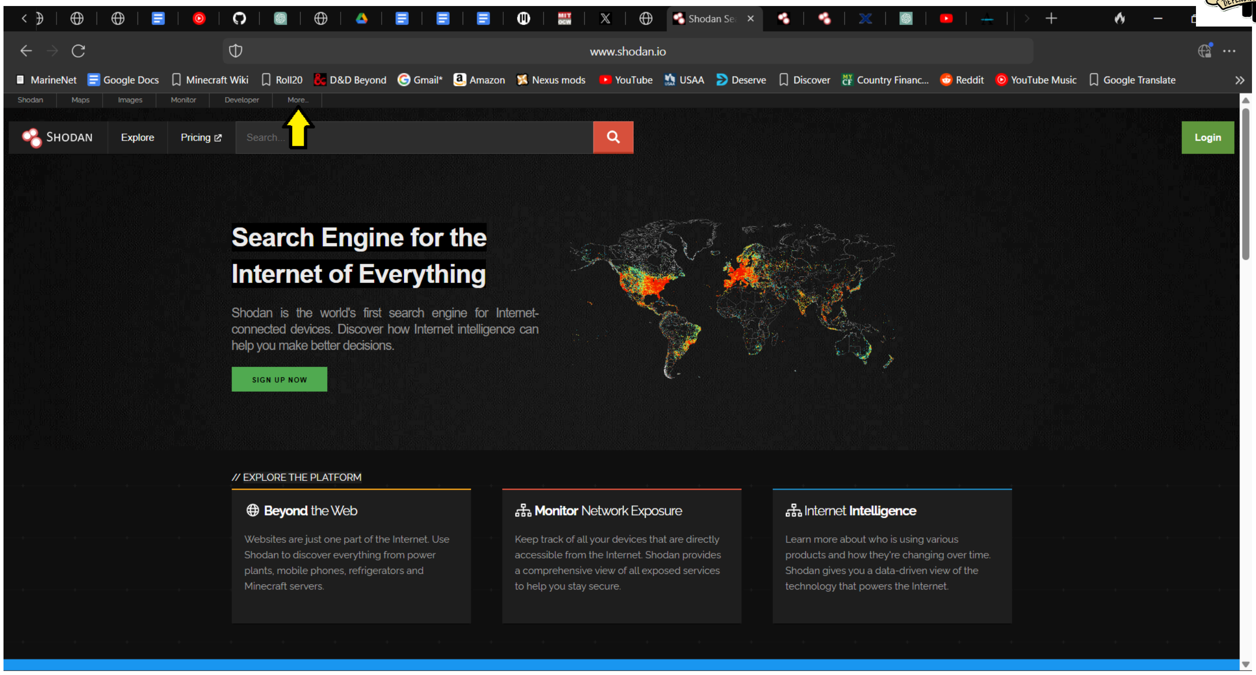


	Membership	Freelancer	Small Business	Corporate	Enterprise
Price	$49 (one-time)	$69/ month	$359/ month	$1099/ month	Custom
Query credits (per month)	100	10,000	200,000	Unlimited	Unlimited
Scan credits (per month)	100	5,120	65,536	327,680	Unlimited
Monitored IPs	16	5,120	65,536	327,680	Unlimited
Available 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	✓	✓	✓	✓	✓
Shodan Trends	✓	✓	✓	✓	✓
Private firehose	✓	✓	✓	✓	✓
IP lookups	✓	✓	✓	✓	✓
Batch IP lookups				✓	✓
Bulk Data					✓
InternetDB					✓
Full firehose					✓
Internet scanning API					✓
600+ Million hostnames scan					✓

For a one-time fee of $49, you can get a membership that includes a couple of extra tools, like Shodan Monitor, Shodan Trends, and IP lookups, as detailed below in the Shodan Products section.

Shodan Products

Shodan offers several products and capabilities depending on what you are looking to do and what type of account/membership you have. First, go to the More tab to see the list of products.



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

SIGN UP NOW

// EXPLORE THE PLATFORM

Beyond the Web

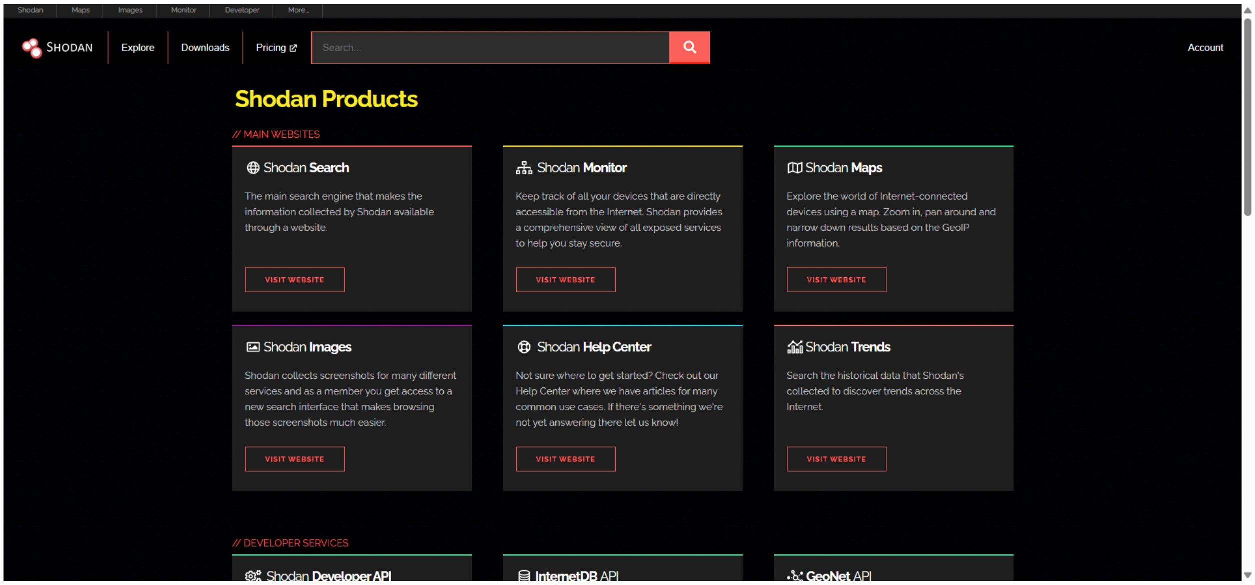
Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Monitor Network Exposure

Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

Internet **Intelligence**

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.



Shodan Products

// MAIN WEBSITES

Shodan **Search**

The main search engine that makes the information collected by Shodan available through a website.

VISIT WEBSITE

Shodan **Monitor**

Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

VISIT WEBSITE

Shodan **Maps**

Explore the world of Internet-connected devices using a map. Zoom in, pan around and narrow down results based on the GeoIP information.

VISIT WEBSITE

Shodan **Images**

Shodan collects screenshots for many different services and as a member you get access to a new search interface that makes browsing those screenshots much easier.

VISIT WEBSITE

Shodan **Help Center**

Not sure where to get started? Check out our Help Center where we have articles for many common use cases. If there's something we're not yet answering there let us know!

VISIT WEBSITE

Shodan **Trends**

Search the historical data that Shodan's collected to discover trends across the Internet.

VISIT WEBSITE

// DEVELOPER SERVICES

Shodan **Developer API**

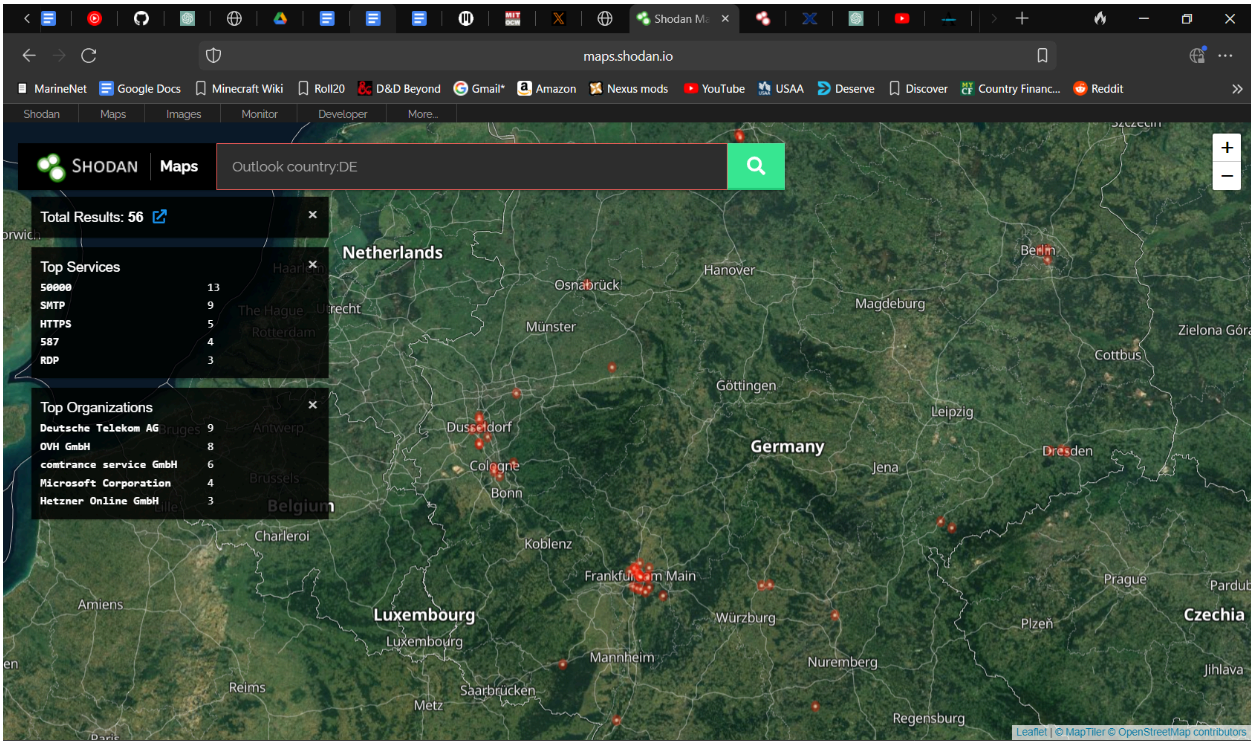
InternetDB API

GeoNet API

Shodan Search - This is the main search engine that makes the information collected by Shodan available through a website.

Shodan Monitor - This is a specialized tool available only to those users who have some kind of paid membership. Once configured, Shodan will monitor the network you specify and send you alerts. Depending on which plan you have, you are allowed to monitor an increasing amount of IPs. For example, a paid Membership will allow you to monitor a small network of 16 devices, whereas a Corporate plan will allow you to scan and monitor up to 327,680 IPs.

Shodan Maps - Shodan Maps gives you a visualization of where devices are located in the world. If for example, you wanted to search for Outlook servers in Germany, Maps will show you the location of every single Outlook server in the country. As you can see from the picture, most of the servers are concentrated in Frankfurt and Dusseldorf, with a couple sprinkled in Berlin and a few other cities.



Outlook country:DE

Total Results: 56

Top Services

50000	13
SMTP	9
HTTPS	5
587	4
RDP	3

Top Organizations

Deutsche Telekom AG	9
OVH GmbH	8
comtrance service GmbH	6
Microsoft Corporation	4
Hetzner Online GmbH	3

Shodan Images - This tool will pull screenshots and live feeds from various IoT devices around the globe, including but not limited to webcams, CCTV cameras, and smart doorbells. As with other types of queries, clicking on one of the results will show you the IP address of the device, where it is located, and ASN number, along with a lot of other information. Unlike other queries, depending on the device, you can also directly interact with these devices live, for example CCTV cameras. (50.75.137.2)

Shodan Help Center - This is the section of the site that functions as a FAQ. If you have a question about what something is or how it works, it's a good idea to start here first before moving on to other troubleshooting steps or methods.

Shodan Trends - Shodan Trends allows you to search the historical data that Shodan has collected to discover trends across the Internet. At the time of this writing, Trends is still in a beta phase and is subject to change. Historical data goes back as far as 2017, and you can even export data into .csv files for further analysis/dissemination.

InternetDB API - Provides port scanning capability for an IP address. Customizing the script you embed it into will allow you to see more information about the queried IP address/device.