What is Shodan?

According to GitHub, Shodan is “the world’s largest search engine for internet-connected devices”. But what exactly does this mean?

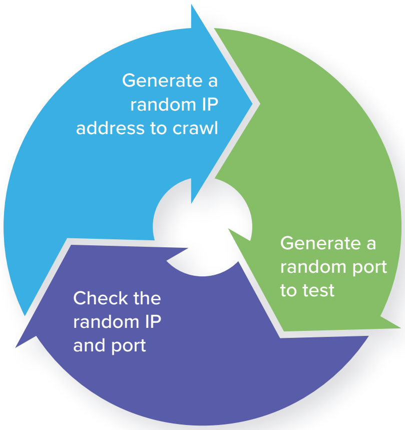
Most search engines are text indexes, meaning they allow search for content based on keywords. However, the task of scanning, indexing the ports and services running, and then searching for internet-connected devices at the scope and scale of the internet has been largely impossible to do.

With Shodan, it is now possible to identify nearly any internet-connected device, such as industrial control systems running specific software, internet-of-things devices like smart TVs, FTP servers with sensitive information and even very small aperture terminals (VSATs) on naval vessels.

How Shodan works

Shodan maintains servers across the globe that scan the internet-connected devices and harvest the banner of whatever is running on the server.

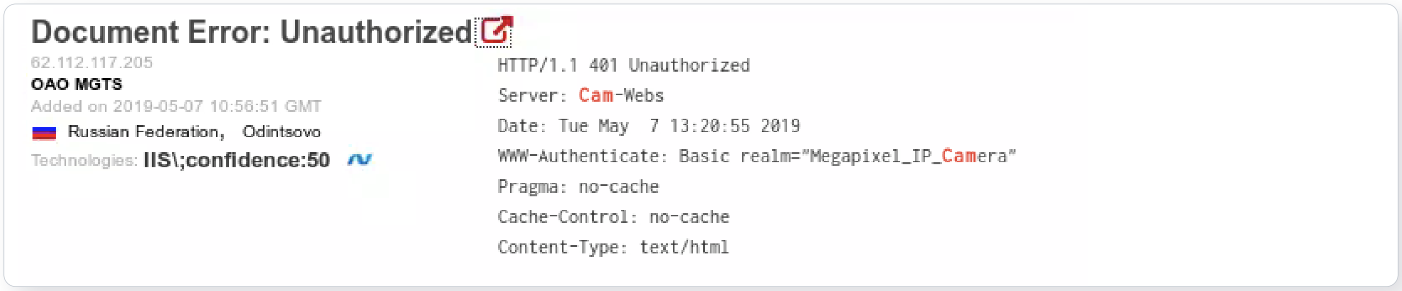
The diagram at right shows how these servers crawl.


Generate a random IP address to crawl
Generate a random port to test
Check the random IP and port

These internet-connected devices return different banners depending on the different service running on it.

Example search returns

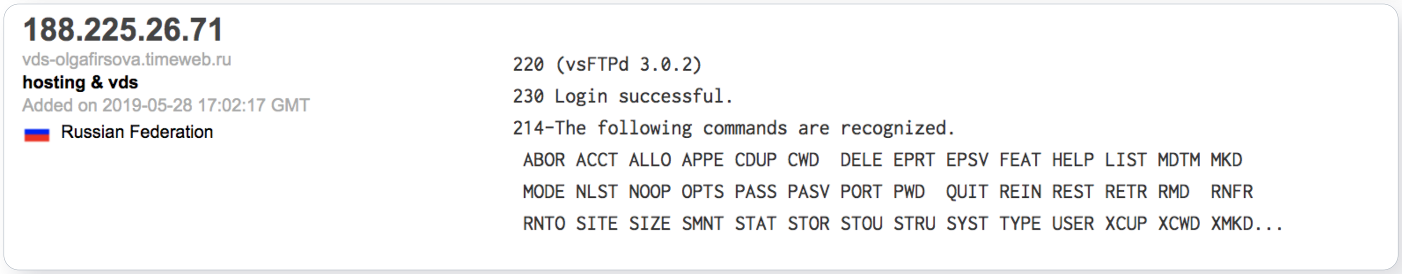
Two examples are below, one for an IP camera and one for an FTP server (FTP runs on port 21):



Document Error: Unauthorized

62.112.117.205
OAO MGTS
Added on 2019-05-07 10:56:51 GMT
Russian Federation, Odintsovo
Technologies: IIS\;confidence:50

```
HTTP/1.1 401 Unauthorized
Server: Cam-Webs
Date: Tue May  7 13:20:55 2019
WWW-Authenticate: Basic realm="Megapixel_IP_Camera"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
```



188.225.26.71

vds-olgafirsova.timeweb.ru
hosting & vds
Added on 2019-05-28 17:02:17 GMT
Russian Federation

```
220 (vsFTPd 3.0.2)
230 Login successful.
214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD...
```

Basic Shodan searches and filters

Shodan allows for advanced search using filters. Filters are entered in a simple format: a filter, a colon and the search value, with no spaces between these three components.

Filter format	`filtername:value`
Filter example	`City:Moscow`

If searching a value that includes a space, double quotes must be used.

Filter example	`City:”Saint Petersburg”`

Examples of Shodan’s most useful geographic filters

Country using two-letter geocode	`country:XX`
City using city name	`city:cityname`

Geographic coordinates in a bounding box	`geo:top-left-lat,top-left-long,`
	`top-right-lat,top-right-long`

Region	`region:region-name-or-state`

These filters are useful when attempting to identify something of interest in a specific AOR.

For example, a search for webcam `City:Incirlik` would find webcams, with some hopefully located near Incirlik Air Base.

Examples of software-focused filters

Firewall port	`port:XX`
Product name	`product:XX`
Product version	`version:XX`
Product vulnerability CVE	`vuln:XX`

These filters are useful when searching for a particular technology, like a database, a file server or vulnerable software.

For example, a search for `port:21 country:”RU” “login successful”` would find file transfer protocol (FTP) servers in Russia that do not require logins. This could yield valuable unsecured information if found in a location of interest, or can be used as a non-attributable temporary data transfer point.

Examples of organization-focused filters

Device hostname	`hostnames:XX`
Organization assignment	`org:XX`
Network CIDR range	`net:XX`

Examples of Shodan’s temporal filters

Results before a given date	`before:00/00/0000`
Results after a given date	`after:00/00/0000`

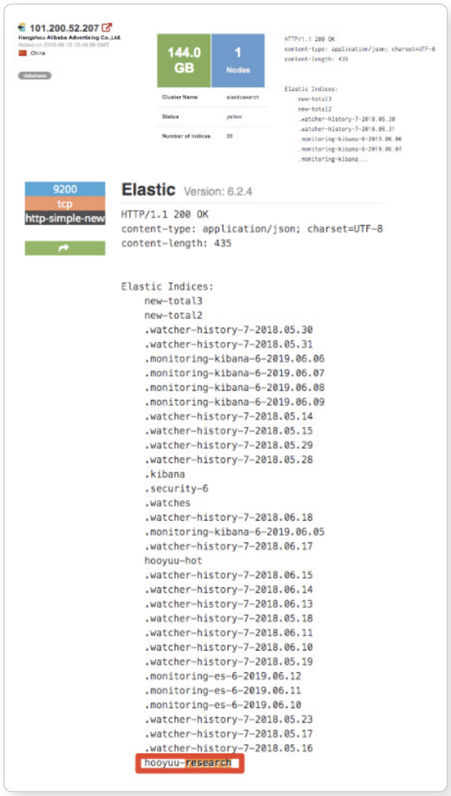
Finding open databases

A few databases openly list their indices: MongoDB, ElasticSearch and CouchDB.

Below are the baseline searches that allow you to quickly identify open databases with potentially valuable information sources.

Example database searches

Elasticsearch databases	`product:elastic port:9200`
MongoDB databases	`product:MongoDB`
CouchDB databases	`product:couchdb`
Kibana visualization of Elasticsearch	`kibana content-length: 217`
Gitlab software repos	`http.favicon.hash:1278323681`
Rsync utilities	`product:rsyncd`
Jenkins software automation	`jenkins 200 ok`



101.200.52.207
Hangzhou Alibaba Advertising Co.,Ltd.
Added on 2019-06-12 12:40:38 GMT
China

Cluster Name	elasticsearch
Status	yellow
Number of Indices	33

```
HTTP/1.1 200 OK
content-type: application/json; charset=UTF-8
content-length: 435

Elastic Indices:
    new-total3
    new-total2
    .watcher-history-7-2018.05.30
    .watcher-history-7-2018.05.31
    .monitoring-kibana-6-2019.06.06
    .monitoring-kibana-6-2019.06.07
    .monitoring-kibana...
```

Elastic Version: 6.2.4

```
HTTP/1.1 200 OK
content-type: application/json; charset=UTF-8
content-length: 435


Elastic Indices:
    new-total3
    new-total2
    .watcher-history-7-2018.05.30
    .watcher-history-7-2018.05.31
    .monitoring-kibana-6-2019.06.06
    .monitoring-kibana-6-2019.06.07
    .monitoring-kibana-6-2019.06.08
    .monitoring-kibana-6-2019.06.09
    .watcher-history-7-2018.05.14
    .watcher-history-7-2018.05.15
    .watcher-history-7-2018.05.29
    .watcher-history-7-2018.05.28
    .kibana
    .security-6
    .watches
    .watcher-history-7-2018.06.18
    .monitoring-kibana-6-2019.06.05
    .watcher-history-7-2018.06.17
    hooyuu-hot
    .watcher-history-7-2018.06.15
    .watcher-history-7-2018.06.14
    .watcher-history-7-2018.06.13
    .watcher-history-7-2018.05.18
    .watcher-history-7-2018.06.11
    .watcher-history-7-2018.06.10
    .watcher-history-7-2018.05.19
    .monitoring-es-6-2019.06.12
    .monitoring-es-6-2019.06.11
    .monitoring-es-6-2019.06.10
    .watcher-history-7-2018.05.23
    .watcher-history-7-2018.05.17
    .watcher-history-7-2018.05.16
    hooyuu-research
```

Combining these search filters and other key phrases allows analysts to identify high value and unsecured information.

Example search for Elasticsearch databases in China mentioning “research”:

```
product:elastic port:9200 country:cn research
```

This results in identifying an IP address hosting an open elasticsearch index with mentions of research. In this case, the research is about “Hooyuu,” a Chinese social media site.

The others range from what looks like security research, notifications and some form of alerting.

For more information please contact osint@authentic8.com.

Silo
BY AUTHENTIC8

Silo for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It's built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

+1 877-659-6535
www.authentic8.com