

Forum:[Hack Forums](#)

Thread: [shodan dork \(Find Vulnerable Devices On The Internet With Shodan\)](#)

st3v3n - February 21, 2021, 6:30 pm

Basic Shodan Filters

city:

Find devices in a particular city.

`city:"Bangalore"``

country:

Find devices in a particular country.

`country:"IN"``

geo:

Find devices by giving geographical coordinates.

`geo:"56.913055,118.250862"``

Location

`country:us`

`country:ru country:de city:chicago`

hostname:

Find devices matching the hostname.

`server: "gws" hostname:"google"``

`hostname:example.com -hostname:subdomain.example.com`

`hostname:example.com,example.org`

net:

Find devices based on an IP address or /x CIDR.

`net:210.214.0.0/16`

Organization

`org:microsoft`

`org:"United States Department"``

Autonomous System Number (ASN)

`asn:ASxxxx`

os:

Find devices based on operating system.

`os:"windows 7"``

port:

Find devices based on open ports.

`proftpd port:21`

before/after:

Find devices before or after between a given time.

`apache after:22/02/2009 before:14/3/2010`

SSL/TLS Certificates

Self signed certificates

`ssl.cert.issuer.cn:example.com ssl.cert.subject.cn:example.com`

Expired certificates

`ssl.cert.expired:true`

`ssl.cert.subject.cn:example.com`

Device Type

`device:firewall`

`device:router`

`device:wap`

`device:webcam`

`device:media`

`device:"broadband router"`

`device:pbx`

`device:printer`

`device:switch`

`device:storage`

`device:specialized`

`device:phone`

`device:"voip phone"`

`device:"voip adaptor"`

`device:"load balancer"`

`device:"print server"`

`device:terminal`

`device:remote`

`device:telecom`

`device:power`

`device:proxy`

`device:pda`

`device:bridge`

Operating System

`os:"windows 7"`

`os:"windows server 2012"`

`os:"linux 3.x"`

Product

`product:apache`

`product:nginx`

`product:android`

`product:chromecast`

Customer Premises Equipment (CPE)

`cpe:apple`

`cpe:microsoft`

`cpe:nginx`

`cpe:cisco`

Server

`server: nginx`
`server: apache`
`server: microsoft`
`server: cisco-ios`

ssh fingerprints

`dc:14:de:8e:d7:c1:15:43:23:82:25:81:d2:59:e8:c0`

Web

Pulse Secure

`http.html:/dana-na`

PEM Certificates

`http.title:"Index of /" http.html:".pem`

Databases

MySQL

`"product:MySQL"`

MongoDB

`"product:MongoDB"`

elastic

`port:9200 json`

Memcached

`"product:Memcached"`

CouchDB

`"product:CouchDB"`

PostgreSQL

`"port:5432 PostgreSQL"`

Riak

`"port:8087 Riak"`

Redis

`"product:Redis"`

Cassandra

`"product:Cassandra"`

Industrial Control Systems

Samsung Electronic Billboards

`"Server: Prismview Player"`

Gas Station Pump Controllers

`"in-tank inventory" port:10001`

Fuel Pumps connected to internet:

No auth required to access CLI terminal.</br>
`"privileged command" GET`

Automatic License Plate Readers

`P372 "ANPR enabled"`

Traffic Light Controllers / Red Light Cameras

`mikrotik streetlight`

Voting Machines in the United States

"voter system serial" country:US

Open ATM:
May allow for ATM Access availability
`NCR Port:"161"`

Telcos Running Cisco Lawful Intercept Wiretaps

`"Cisco IOS" "ADVIPSERVICESK9\_LI-M"`

Prison Pay Phones

`"[2J[H Encartele Confidential]"`

Tesla PowerPack Charging Status

`http.title:"Tesla PowerPack System" http.component:"d3" -ga3ca4f2`

Electric Vehicle Chargers

`"Server: gSOAP/2.8" "Content-Length: 583"`

Maritime Satellites

Shodan made a pretty sweet Ship Tracker that maps ship locations in real time, too!

`"Cobham SATCOM" OR ("Sailor" "VSAT")`

Submarine Mission Control Dashboards

`title:"Slocum Fleet Mission Control"`

CAREL PlantVisor Refrigeration Units

`"Server: CarelDataServer" "200 Document follows"`

Nordex Wind Turbine Farms

`http.title:"Nordex Control" "Windows 2000 5.0 x86" "Jetty/3.1 (JSP 1.1; Servlet 2.2; java 1.6.0\_14)"`

C4 Max Commercial Vehicle GPS Trackers

`"[1m[35mWelcome on console"``

DICOM Medical X-Ray Machines

Secured by default, thankfully, but these 1,700+ machines still have no business being on the internet.

`"DICOM Server Response" port:104`

GaugeTech Electricity Meters

`"Server: EIG Embedded Web Server" "200 Document follows"``

Siemens Industrial Automation

`"Siemens, SIMATIC" port:161`

Siemens HVAC Controllers

`"Server: Microsoft-WinCE" "Content-Length: 12581"``

Door / Lock Access Controllers

`"HID VertX" port:4070`

Railroad Management

`"log off" "select the appropriate"``

Tesla Powerpack charging Status:

Helps to find the charging status of tesla powerpack.

`http.title:"Tesla PowerPack System" http.component:"d3" -ga3ca4f2`

XZERES Wind Turbine

`title:"xzeres wind"``

PIPS Automated License Plate Reader

`"html:"PIPS Technology ALPR Processors"````

Modbus

`"port:502"``

Niagara Fox

`"port:1911,4911 product:Niagara"``

GE-SRTP

`"port:18245,18246 product:"general electric"````

MELSEC-Q

`"port:5006,5007 product:mitsubishi"``

CODESYS

`"port:2455 operating system"``

S7

`"port:102"``

BACnet

`"port:47808"``

HART-IP

`"port:5094 hart-ip"``

Omron FINS

`"port:9600 response code"``

IEC 60870-5-104

`"port:2404 asdu address"``

DNP3

`"port:20000 source address"``

EtherNet/IP

`"port:44818"``

PCWorx

`"port:1962 PLC"``

Crimson v3.0

`"port:789 product:"Red Lion Controls"``

ProConOS

`"port:20547 PLC"``

Remote Desktop

Unprotected VNC

`"authentication disabled" port:5900,5901`

`"authentication disabled" "RFB 003.008"``

Windows RDP

99.99% are secured by a secondary Windows login screen.

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

Network Infrastructure

Hacked routers:

Routers which got compromised </br>

`hacked-router-help-sos`

Redis open instances

`product:"Redis key-value store"``

Citrix:

Find Citrix Gateway.

`title:"citrix gateway"`

Weave Scope Dashboards

Command-line access inside Kubernetes pods and Docker containers, and real-time visualization/monitoring of the entire infrastructure.

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

MongoDB

Older versions were insecure by default. Very scary.

`"MongoDB Server Information" port:27017 -authentication`