

Module:- SECURITY CONCEPT (SHODON)

Name:- Prithviraj Nikam

Lab Assignments:

SHODAN:- Shodan is a search engine that lets users search for various types of servers connected to the internet using a variety of filters.

- First of all create a account on shodan
- Then type shodan keyword in search box to find out the data and information about target

2. Execute following keywords in shodan

----->org:"Amazon" ssl:"target"

It is sho

The screenshot displays the Shodan search engine interface. At the top, the search bar contains the query 'org:Amazon ssl:target'. Below the search bar, the interface is divided into several sections:

- TOTAL RESULTS:** 584
- TOP COUNTRIES:** A world map showing the distribution of results by country. The United States is the most prominent.
- TOP PORTS:** A table showing the most common ports used by the search results.
- Partner Spotlight:** A banner for Gravwell, suggesting it as a place to store Shodan data.
- Search Results:** Two detailed results are shown, each including an IP address, domain, organization, and SSL certificate information.

Port	Count
443	530
5432	30
4443	7
8081	7
25	2

IP Address	Domain	Organization	SSL Certificate
ec2-18-213-225-182.compute-1.amazonaws.com	Amazon Technologies Inc.	United States, Ashburn	Issued By: Amazon Issued To: target-ams.com Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2
52.3.99.168	axa-custdashdev.tolunainights-internal.com	United States, Ashburn	Issued By: GlobalSign RSA OV SSL CA 2018 Issued To: *tolunainights-internal.com Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

52.71.197.138

Regular View

> Raw Data

History

52.71.197.138

cloud

General Information

Hostnames

ec2-52-71-197-138.compute-1.amazonaws.com

Domains

AMAZONAWS.COM

Cloud Provider

Amazon

Cloud Region

us-east-1

Cloud Service

EC2

Country

United States

City

Ashburn

Organization

Amazon Technologies Inc.

ISP

Amazon.com, Inc.

Open Ports

80

443

// 80 / TCP

1965132531

2022-12-19T09:11:20.518634

HTTP/1.1 403 Forbidden

Date: Mon, 19 Dec 2022 09:11:20 GMT

Content-Type: text/html

Content-Length: 564

Connection: keep-alive

Server: nginx

// 443 / TCP

1965132531

2022-12-27T19:06:46.271924

HTTP/1.1 403 Forbidden

Date: Tue, 27 Dec 2022 19:06:45 GMT

Content-Type: text/html

Content-Length: 564

LAST SEEN: 2022-12-27

----->ssl:"target"

It show the result on secure socket layer about the target

SHODAN

Explore

Downloads

Pricing

ssl:"target"

Q

TOTAL RESULTS

9,255

TOP COUNTRIES

United States

4,205

Germany

445

India

351

United Kingdom

340

Australia

301

More...

TOP PORTS

443

8,649

3389

61

8443

52

5432

48

993

41

More...

View Report

Browse Images

View on Map

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Gravwell](#)

Target : Expect More. Pay Less.

151.101.130.187

ios.studioconnect.live

apollo-metrics.target.com

pid.partnersonline.com

lgt-files.target.com

factorial.partnersonline.com

Fastly, Inc.

United States, San Francisco

cdn

SSL Certificate

Issued By:

GlobalSign Atlas R3 OV TLS CA 2022 Q3

Organization:

GlobalSign nv-sa

Issued To:

sites.target.com

Organization:

Target Corporation

Supported SSL Versions:

TLSv1.2

HTTP/1.1 200 OK

Connection: keep-alive

Content-Length: 314187

Content-Type: text/html; charset=utf-8

cache-control: no-cache

ETag: "14r2ejerrhi6qd2"

Accept-Ranges: bytes

Age: 440

Set-Cookie: TealeafAkaSid=JA75DpgxxqH8NSht0tE7fMk8Cvvhycil; b

18.213.225.182

ec2-18-213-225-182.compute-1.amazonaws.com

Amazon Technologies Inc.

United States, Ashburn

cloud

SSL Certificate

Issued By:

Amazon

Organization:

Amazon

Issued To:

*.target-ams.com

Supported SSL Versions:

TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 404 Not Found

Content-Type: application/json; charset=utf-8

Date: Tue, 27 Dec 2022 11:01:39 GMT

Server: kong/0.11.2

Content-Length: 45

Connection: keep-alive

shodan.io/host/106.75.48.134

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2022-0778

The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: -

1741	1883	1911	1925	1926	1935	1962	2000	2002	2006
2008	2018	2050	2066	2067	2081	2082	2083	2086	2087
2100	2121	2150	2154	2181	2211	2225	2332	2345	2375
2376	2379	2404	2455	2480	2550	2553	2566	2570	2628
2761	2762	2985	3000	3001	3002	3048	3049	3050	3054
3060	3070	3075	3080	3081	3083	3084	3085	3090	3092
3094	3095	3099	3114	3116	3119	3121	3128	3129	3200
3221	3260	3268	3269	3299	3301	3310	3311	3388	3400
3401	3405	3406	3407	3479	3541	3542	3548	3551	3555

// 80 / TCP

1995972035 | 2022-12-26T23:44:03.120141

```

HTTP/1.1 200 OK
Server: BigIP Docker/1.13.1 (linux), docker 1.20,Jboss, Intel(R) Active Manage
nt Technology 9.1.34, jetty(winstone-2.9), Apache-Coyote/1.1, WildFly/10,
WebLogic Server 6.0, WebLogic Server 7.0 SP4, phpstudy,struts,jenkins,gSOAP,
lighttpd,Servlet,IBM_HTTP_Server/6.0.2, Apache/2.0.47 (Unix),Raptor Simple, Secu
re Web Server 1.0,28ZE,300Mbps Wireless N ADSL2+ Modem Router TD-W8960N, ::: Login :::,AD
SL2 PLUS,AGS GmbH Webserver Setup,AIROS,AN550602B, Apache Tomcat,AsicMiner,BaseDashboard,
Braunschweiger Seven Stammtisch, CBT Routers,CRM - Welcome,Center of Inspiration,Channel
management, Chaparral Wireless,Costume Designers Guild | IATSE local 892,D-LINK SYSTEMS,
INC. | WIRELESS ROUTER | HOME,DIR600 1,DIR-615 DLINK,DLINK DIR-905L, DSL Router,
DSL Router - GKM 1220,DVR Components Download,Dlink DIR-610, Dlink DIR-611,ELSYS CPE-2N,F
609,FiberHome AN5506-02-B, hardware: GJ-2.134.321B7G, firmware: RP2520,FiberLink101,GOTH
AN,GPON Home Gateway,GREATEK,GWR-120, Game of Life,Gial Plast,GoAhead-Boa,GoAhead-Webs,Go
Ahead-Webs Routers, GoAhed 302,HD,Home - B52,Home - International Club Winterthur,
HtmlAnvView:D7B039C1-5929-49B3-913E-EB62C8866FC4,IIS7, IIS Windows Server,IP Camera,IPCam
Client,IPOX,Infipix,Intelbras,KP8696X, Link One,Linksys Smart Wi-Fi,Login,Mini_httpd,Mult
ilaser Router,NAS, NETSurveillance WEB,NETSuveillance WEB,Net Systems Research,Network Vi
deo Recorder Login, OIWTECH,PLC Wireless Router,PROVERLINK TELECOM,PayNet,PellesWeb,Proqu
alit Router, Realtek Semiconductor,Realtek Semiconductor [Title],Roteador ADSL, R
oteador Wireless KLR 300N,Roteador Wireless N 150 Mbps,Roteador Wireless N 150Mbps, Rotea
dor Wireless N 300 Mbps,Roteador Wireless N 300 Mbps [ LinkOne ], Roteador Wireless N 300
Mbps [Link One],Roteador Wireless N ( Multilaser ), Roteador Wireless N [ Multilaser ],Ro
uterOS router configuration page, Server&nbsp;-&nbsp;Synology&nbsp;RackStation,Siceteleco

```

----->http.component:"jenkins"

It is shows the content about the jenkins

[Explore](#)
[Downloads](#)
[Pricing](#)

TOTAL RESULTS
3,463

TOP COUNTRIES

United States	1,446
India	386
Germany	333
Japan	186
Singapore	174
More...	

TOP PORTS

8080	206
------	-----

[View Report](#)
[View on Map](#)

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Gravwell](#)

45.79.132.133

#1231-133.members.linode.com
Linode
United States, Morris Plains

cloud honeypot

```

HTTP/1.1 200 OK
content-type: text/html; charset=UTF-8
content-length: 1
server: Cisco-CcspCompTcpCR/1.0 WildFly/8 OpenCms/11.0.2 waitress Ruljle Server Easy-html RomPager/4.07 UPnP/1.0 In

```

107.20.223.41

ec2-107-20-223-41.compute-1.amazonaws.com
Amazon.com, Inc.
United States, Ashburn

cloud

```

HTTP/1.1 403 Forbidden
date: Tue, 27 Dec 2022 10:45:24 GMT
x-content-type-options: nosniff
set-cookie: JSESSIONID.5d1a9172-node016fuaK7bgrneprrr2e9q8fnjfj290177.node0; Path=/; HttpOnly
expires: Thu, 01 Jan 1970 00:00:00 GMT
content-type: text/html; charset=utf-8
x-hudson: 1.395
x-jenkins: 2.28...

```

Web Technologies

AMAZON EC2
AMAZON WEB SERVICES
APACHE

APACHE HTTP SERVER
APACHE TOMCAT

APACHE TRAFFIC SERVER
BOOTSTRAP
CHERRYVPY

COUCHDB
DRUPAL
EMBEDTHIS APPWEB

ERLANG
FLASK
GLASSFISH

GOAHEAD
GOOGLE WEB SERVER
GUNICORN

HP ILO
IBM HTTP SERVER
INDY

INTEL ACTIVE MANAGEMENT TECHNOLOGY
JAVA

JENKINS
JETTY
JQUERY
LIGHTTPD

MICROSOFT HTTPAPI
MINI_HTTPD
MINISERV

1741	1830	1883	1925	1926	1935	1947	1950	1990	2000
2008	2022	2053	2054	2056	2058	2061	2062	2065	2067
2069	2079	2081	2083	2087	2095	2096	2121	2150	2181
2200	2201	2202	2220	2222	2323	2332	2345	2351	2375
2376	2404	2443	2455	2550	2559	2561	2570	2572	2601
2628	2650	2761	2762	3000	3001	3050	3051	3052	3056
3057	3062	3066	3068	3069	3074	3075	3079	3082	3084
3087	3092	3097	3098	3105	3107	3111	3116	3128	3211
3260	3268	3269	3270	3299	3301	3306	3310	3333	3337
3388	3389	3401	3404	3405	3408	3460	3498	3521	3524
3541	3542	3548	3551	3556	3558	3560	3561	3562	3566

---->http.title:302 Found

[Explore](#)
[Downloads](#)
[Pricing](#)

TOTAL RESULTS

1,035,926

TOP COUNTRIES

United States	295,160
Germany	96,784
Japan	52,553
France	41,485
Ireland	37,814

[View Report](#) [View on Map](#)

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Gravwell](#)

302 Found

3.143.183.66
ec2-3-143-183-66.us-east-2.compute.amazonaws.com
Amazon Technologies Inc.
United States, Hilliard

cloud

HTTP/1.1 302 Found
Content-Type: text/html; charset=iso-8859-1
Date: Tue, 27 Dec 2022 19:07:51 GMT
Location: https://3.143.183.66/
Server: Apache/2.4.41 (Amazon) mod_wsgi/3.5 Python/3.6.10
Content-Length: 205
Connection: keep-alive

302 Found

204.136.101.14
ite.mypepsico.com
vcs.fm.ite.mypepsico.com
nafglmippqa2.ite.mypepsico.com
Pensi Cola Company

SSL Certificate

Issued By:
Common Name:
Entrust Certification Authority - L1K

HTTP/1.1 302 Found
Date: Tue, 27 Dec 2022 19:07:51 GMT
Server: Apache
Cache-Control: no-store
Location: https://sso.ite.mypepsico.com/login/2login.jsp?TYPE=3355443&RE

General Information

Hostnames: api-stage.oculartechnologies.net, ec2-3-143-183-66.us-east-2.compute.amazonaws.com

Domains: OCULARTECHNOLOGIES.NET, AMAZONAWS.COM

Cloud Provider: Amazon

Cloud Region: us-east-2

Cloud Service: EC2

Country: United States

Open Ports

80 443

// 80 / TCP

Apache httpd 2.4.41

HTTP/1.1 302 Found
Content-Type: text/html; charset=iso-8859-1
Date: Tue, 27 Dec 2022 19:07:51 GMT
Location: https://3.143.183.66/
Server: Apache/2.4.41 (Amazon) mod_wsgi/3.5 Python/3.6.10
Content-Length: 205
Connection: keep-alive


---->http.component:"java"

It is shows the information about java

SHODAN Explore Downloads Pricing

TOTAL RESULTS
114,051

TOP COUNTRIES



Country	Count
United States	42,055
China	13,294
Germany	9,779
France	4,459
United Kingdom	3,068

More...

TOP PORTS

Port	Count
443	64,737
80	16,338
8080	7,757
8090	7,338
9000	3,559

More...

View Report View on Map

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Gravwell](#)

Autohaus Jensen Wittstock

23.67.33.42
www.krammes-schoenberg.audi
www.huff-krosdorf.audi
www.henzel-krankenhal.audi
www.jutz-oberhausen.audi
www.kutz-donzdorf.audi
[Akamai Technologies, Inc.](#)
United States, Santa Clara

cdn

SSL Certificate

Issued By:
Common Name: R3
Organization: Let's Encrypt

Issued To:
Common Name: cert.audi-iph-handel12.audi

Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
X-LBLID: ivnb4821-231
Content-Type: text/html; charset=UTF-8
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Tue, 27 Dec 2022 11:59:42 GMT
Date: Tue, 27 Dec 2022 10:59:4...

Spring Education Group

104.16.75.30
discountschoolsupply.com
sni.cloudflaressl.com
[Cloudflare, Inc.](#)
United States, San Francisco

cdn

SSL Certificate

Issued By:
Common Name: Cloudflare Inc ECC CA-3
Organization: Cloudflare, Inc.

Issued To:
Common Name: sni.cloudflaressl.com
Organization: Cloudflare, Inc.

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

HTTP/1.1 200 OK
Date: Tue, 27 Dec 2022 10:59:16 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Strict-Transport-Security: max-age=31536...


—>ssl.cert.subject.cn:"target"

Shows the SSL Certificate of target and its all certificate details

SHODAN Explore Downloads Pricing

TOTAL RESULTS
2,537

TOP COUNTRIES



Country	Count
United States	1,405
Germany	97
United Kingdom	80
Japan	77
Poland	73

More...

TOP PORTS

Port	Count
443	2,209
5432	37
993	27
995	25
3389	25

More...

View Report Browse Images View on Map

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Gravwell](#)

Target : Expect More. Pay Less.

151.101.130.187
ios.studioconnect.live
apollo-melica.target.com
pid.partnersonline.com
tgt-files.target.com
factorial.partnersonline.com
[Fastly, Inc.](#)
United States, San Francisco

cdn

SSL Certificate

Issued By:
Common Name: GlobalSign Atlas R3 OV TLS CA 2022 Q3
Organization: GlobalSign nv-sa

Issued To:
Common Name: sites.target.com
Organization: Target Corporation

Supported SSL Versions: TLSv1.2

HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 314187
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
ETag: "14c2ejerrh1s0dz"
Accept-Ranges: bytes
Age: 448
Set-Cookie: TealeafAkaSid=JA750poxqH9MSHT8TE7fakScvvhcIL; Expires=Th

18.213.225.182

ec2-18-213-225-182.compute-1.amazonaws.com
[Amazon Technologies Inc.](#)
United States, Ashburn

cloud

SSL Certificate

Issued By:
Common Name: Amazon
Organization: Amazon

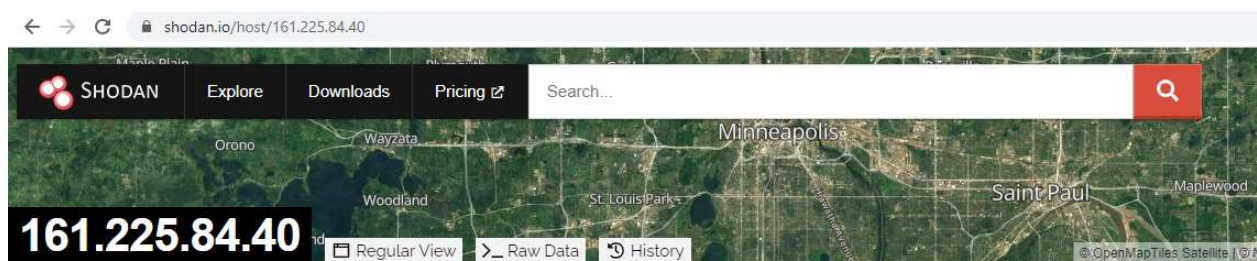
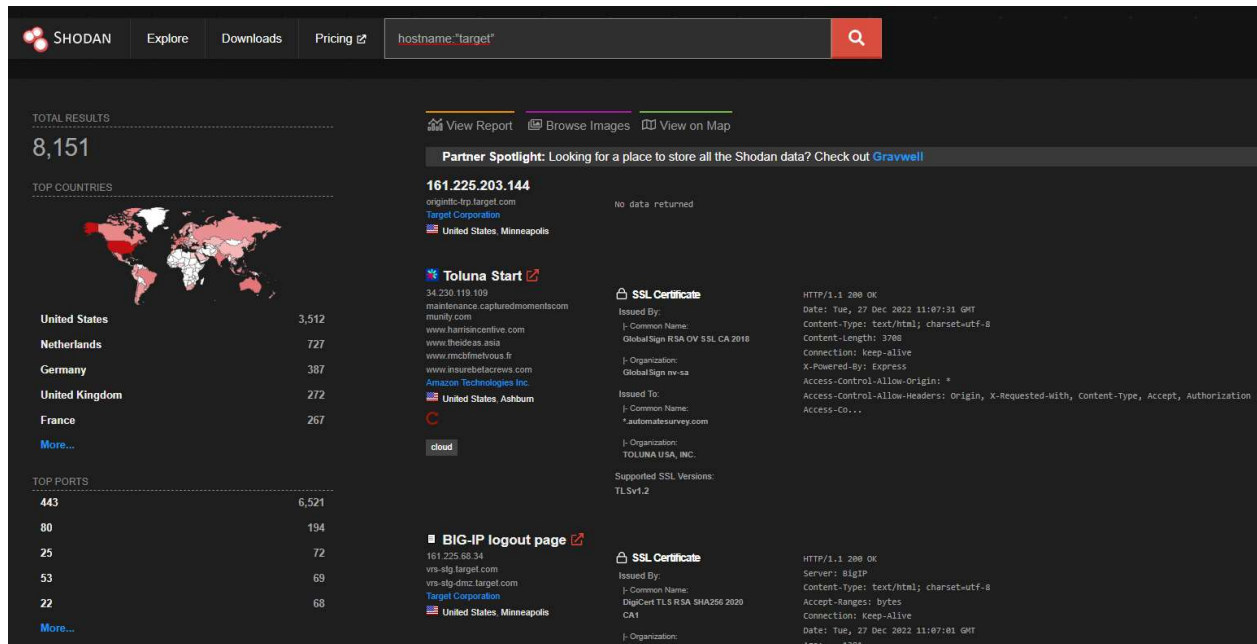
Issued To:
Common Name: *target-ams.com

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 404 Not Found
Content-Type: application/json; charset=utf-8
Date: Tue, 27 Dec 2022 11:01:39 GMT
Server: kong/0.11.2
Content-Length: 45
Connection: keep-alive

----->hostname:"target"

It is shows the target hostname related information



General Information	
Hostnames	cevagoodsissue.target.com
Domains	TARGET.COM
Country	United States
City	Minneapolis
Organization	Target Corporation
ISP	Target Corporation

Open Ports	
80	443
// 80 / TCP	
BigIP	
HTTP/1.0 302 Moved Temporarily Location: https://161.225.84.40:443/ Server: BigIP Connection: Keep-Alive Content-Length: 0	

---->html:"© 2020 target"

It shows the web data that is copyright in year 2020


---->http.favicon.hash:-335242539

It shows the hash information

SHODAN Explore Downloads Pricing

TOTAL RESULTS
1,701

TOP COUNTRIES



Country	Count
United States	509
China	200
Korea, Republic of	145
Hong Kong	86
Taiwan	62

More...

TOP PORTS

Port	Count
443	1,524
8443	158
80	3
10443	3
4443	2

More...

View Report View on Map

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Grawwell](#)

BIG-IP®- Redirect
210.122.97.116
[Sejong Telecom](#)
Korea, Republic of, Seoul
self-signed

SSL Certificate
Issued By: j- Common Name: dhcp-209
Organization: MyCompany
Issued To: j- Common Name: dhcp-209
Organization: MyCompany
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK
Date: Tue, 27 Dec 2022 10:59:50 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=16070400; includeSubDomains
Last-Modified: Mon, 28 Nov 2022 04:14:27 GMT
ETag: "96ade4d-f97-5ee01b70ddf1"
Accept-Ranges: bytes
Content-Length: 3991
X-Content...

BIG-IP®- Redirect
201.230.120.6
client-201.230.120.6.speedy.net.pe
PE-TDP-GRS
Peru, Iquitos
self-signed

SSL Certificate
Issued By: j- Common Name: localhost.localdomain
Organization: MyCompany
Issued To: j- Common Name: localhost.localdomain
Organization: MyCompany

Vulnerabilities
CVE-2020-5902

HTTP/1.1 200 OK
Date: Tue, 27 Dec 2022 10:47:30 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=16070400
Last-Modified: Tue, 27 Sep 2022 18:42:39 GMT
ETag: "27eab22-f97-5e9ad023c717c"
Accept-Ranges: bytes
Content-Length: 3991
X-Content...

```

CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
2d:d1:a8:69:20:d0:08:c5:8b:73:67:82:d7:a8:9a:23:01:41:
52:7c:a7:26:57:7c:38:24:72:87:6c:86:53:41:81:9f:11:19:
42:67:99:45:64:4e:e9:b3:89:da:74:47:0d:49:a9:5c:b9:b4:
36:94:d6:63:d3:63:be:33:2d:74:46:ba:a8:e5:ce:0c:38:df:
98:4a:ef:09:6d:66:2a:a3:81:f1:45:03:6a:f9:5d:86:2d:e4:
1f:14:71:45:c5:5a:0c:4b:4e:90:fa:6f:75:dc:ad:4e:cf:5e:
1b:03:44:5d:af:e0:e6:46:c2:26:80:10:e9:3c:01:0d:56:5e:
8d:af:c7:f9:f8:dd:ab:ed:4e:1d:6c:05:85:3f:8b:0d:36:10:
ab:cf:90:5e:17:cd:00:46:95:8c:c7:50:2a:61:96:a1:14:ba:
bf:b4:84:85:be:b0:cb:d6:13:ab:a0:2d:6a:0b:6d:1a:b5:ef:
82:be:65:26:24:ca:2e:2e:9d:96:5f:2a:b9:f4:5e:55:fa:b6:
eb:48:3e:d7:d2:0e:bb:43:86:03:ca:1e:6e:b2:fe:59:c1:21:
84:9e:8c:ba:b8:25:59:c8:78:cf:ce:fa:a3:b1:a3:28:3c:8b:
0f:4b:2a:17:46:2f:e8:ce:c2:36:84:8d:2d:05:3c:4c:6a:8e:
a4:49:17:ec

```

----->product:elastic port:9200
Shows the open Port

[SHODAN](#)
[Explore](#)
[Downloads](#)
[Pricing](#)

TOTAL RESULTS

27,529

TOP COUNTRIES

China	13,564
United States	3,653
Germany	1,611
Hong Kong	1,089
France	848
More...	

TOP ORGANIZATIONS

Allyun Computing Co., LTD	5,924
Tencent cloud computing (Beijing) Co., Ltd.	2,312
Tencent Cloud Computing (Beijing) Co., Ltd	1,858
Huawei Public Cloud Service (Huawei Software T...	1,082
Amazon Technologies Inc.	966
More...	

[View Report](#)
[View on Map](#)

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Grawwell](#)

43.143.239.165

Tencent Cloud Computing (Beijing) Co., Ltd

China, Beijing

cloud database

HTTP/1.1 200 OK

content-type: application/json; charset=UTF-8

content-length: 540

Elastic:

Total Size: 44.45 KB

Total Docs: 7

Indices:

.apm-agent-configuration (283.0 B)

.kibana_1 (22.41 KB)

.kibana_task_manager_1 (21.76 KB)

210.89.178.65

NAVER Cloud Corp

Korea, Republic of, Seoul

database

HTTP/1.1 200 OK

content-type: application/json; charset=UTF-8

content-length: 491

118.31.76.105

Allyun Computing Co., LTD

China, Hangzhou

database

HTTP/1.1 200 OK

content-type: application/json; charset=UTF-8

content-length: 540

Elastic:

Total Size: 4.07 KB

Total Docs: 1

// 9200 / TCP

584638057 | 2022-12-27T19:00:08.319194

Elastic 23.1

```

HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 322
  
```