

Now You TCP Me, Now You Don't

The Strengths and Weaknesses of Various Internet Scanning Services

Adi Ben-Israel



Whoami - Adi Ben-Israel

- Former internet security researcher
- Current developer at Weka
- Home network specialist

 adlda_adAstra



#20-talk

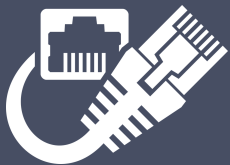


Why Scan the Internet?



Scanning is Hard

Bandwidth



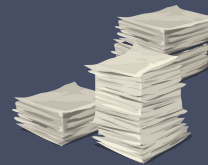
ISP Blocks



DB



Versioning



What does an internet scanning service do?

- Scans the internet

What does an internet scanning service do?

- Scans the internet
- Displays data

The screenshot displays the results of an internet scan for the IP address 59.127.169.181. The interface is divided into two main sections: a table of general information on the left and a 'Ports' section on the right.

General Information Table:

City	Kaohsiung City
Country	Taiwan
Organization	HiNet
ISP	HiNet
Last Update	2020-06-30T07:21:28.722205
Hostnames	59-127-169-181.HINET-IP.hinet.net
ASN	AS3462

Ports Section:

The 'Ports' section shows two open ports: 80 and 554. Each port entry includes a status bar with the port number, protocol, and a green checkmark, followed by detailed service information.

Port 80:

- Protocol: http
- Status: 80/tcp http
- Service: HTTP/1.1 401 Unauthorized
- Server: d15a7d5d-2623-ee47-cf83-c38204c1e34
- Date: Sun, 28 Jun 2020 22:05:25 GMT
- Cache-Control: no-cache, no-store
- WWW-Authenticate: Basic realm=""
- Content-Type: text/html; charset=%s
- Connection: close

Port 554:

- Protocol: rtsp-tcp
- Status: 554/tcp rtsp-tcp
- Service: RTSP/1.0 200 OK
- CSeq: 1
- Public: OPTIONS, GET_PARAMETER, DESCRIBE, SETUP, TEARDOWN, PLAY

What does an internet scanning service do?

- Scans the internet
- Displays data
- Democratizes access to internet-scale data sets

The screenshot displays a web interface for an IP scanning service. At the top, the IP address **59.127.169.181** is shown, along with its associated domain **59-127-169-181.HINET-IP.hinet.net** and a link to **View Raw Data**.

Below this, a table provides detailed information about the IP:

City	Kaohsiung City
Country	Taiwan
Organization	HiNet
ISP	HiNet
Last Update	2020-06-30T07:21:28.722205
Hostnames	59-127-169-181.HINET-IP.hinet.net
ASN	AS3462

To the right of the table, a **Ports** section shows two active ports: **80** and **554**.

Below the ports, a **Services** section lists the detected services and their details:

- 80** (tcp/http): HTTP/1.1 401 Unauthorized. Server: d15a7d5d-2623-ee47-cf83-c38204c1e34. Date: Sun, 28 Jun 2020 22:05:25 GMT. Cache-Control: no-cache, no-store. WWW-Authenticate: Basic realm="". Content-Type: text/html; charset=%s. Connection: close.
- 554** (tcp/rtsp-tcp): RTSP/1.0 200 OK. CSeq: 1. Public: OPTIONS, GET_PARAMETER, DESCRIBE, SETUP, TEARDOWN, PLAY.

Scanning Services



https://www.shodan.io/search?query=asus

ShodanDevelopersMonitorView All...

Try out the new beta website!Help Center

SHODAN

asus

ExplorePricingEnterprise Access


New to Shodan?Login or Register

ExploitsMapsImages

TOTAL RESULTS

69,114

TOP COUNTRIES



China	11,568
United States	10,724
Russian Federation	5,942
Taiwan	4,555
Korea, Republic of	4,034

TOP SERVICES

FTP	65,680
8081	864
NetBIOS	487
HTTP (8080)	367
HTTP	174

TOP ORGANIZATIONS

China Telecom	6,729
HiNet	3,976
Comcast Cable	3,215
Spectrum	2,881
China Unicom Liaoning	2,756

TOP OPERATING SYSTEMS

Linux 2.6.x	27
Windows 6.1	15

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

RELATED TAGS:1

122.139.179.71

71.179.139.122.adsl-pool.jlccptt.net.cn

China Unicom Liaoning

Added on 2020-06-17 16:15:12 GMT

China

220 Welcome to **ASUS** RT-AC86U FTP service.

530 This FTP server does not allow anonymous logins.

331 Please specify the password.

530 Please login with USER and PASS.

183.179.32.136

183179032136.ctinets.com

Hong Kong Broadband Network

Added on 2020-06-17 16:14:55 GMT

Hong Kong, Ngau Chi Wan

220 Welcome to **ASUS** RT-N18U FTP service.

530 This FTP server does not allow anonymous logins.

331 Please specify the password.

530 Please login with USER and PASS.

1.163.197.253

1-163-197-253.dynamic-ip.hinet.net

HiNet

Added on 2020-06-17 16:14:04 GMT

Taiwan, Taoyuan District

220 Welcome to **ASUS** RT-AC66U FTP service.

530 This FTP server does not allow anonymous logins.

331 Please specify the password.

530 Please login with USER and PASS.

112.80.70.6

China Unicom Liaoning

Added on 2020-06-17 16:17:28 GMT

China, Nanjing

220 Welcome to **ASUS** WS880 FTP service.

530 Login incorrect.

530 Please login with USER and PASS.

211-Features:

EPRT

EPSV

MDTM

PASV

ICNV

REST STREAM

SIZE

Quick Filters

For all fields, see [Data Definitions](#)

Autonomous System:

- 3,782 COMCAST-7922
- 2,471 HINET Data Communication Business Group
- 2,339 CHINANET-BACKBONE No.31,Jin-rong Street
- 1,981 KIXS-AS-KR Korea Telecom
- 1,349 SKB-AS SK Broadband Co Ltd

☒ More

Protocol:

- 50.35K 21/ftp
- 34.45K 443/https
- 15.0K 80/http
- 6,997 22/ssh
- 4,755 8080/http

☒ More

Tag:

- 50.35K ftp
- 46.33K soho router
- 41.38K http

IPv4 Hosts

Page: 1/2,633 Results: 65,810 Time: 123ms

[140.116.92.211 \(pcnw1.ee.ncku.edu.tw\)](#)

- ERX-TANET-ASN1 Taiwan Academic Network (TANet) Information Center (1659) Kaohsiung City, Kaohsiung, Taiwan
- 465/smtp, 995/pop3s

[163.15.168.183 \(c183.psy.kmu.edu.tw\)](#)

- ERX-TANET-ASN1 Taiwan Academic Network (TANet) Information Center (1659) Kaohsiung City, Kaohsiung, Taiwan
- 465/smtp, 995/pop3s

[140.127.37.85](#)

- Unknown Network Unknown
- 3389/rdp, 465/smtp, 995/pop3s

RDP

REMOTE_DISPLAY

[210.209.189.241 \(210-209-189-241.veetime.com\)](#)

- VEETIME-TW-AP VEE TIME CORP. (17809) Taipei, Taipei City, Taiwan
- 465/smtp, 995/pop3s
- 465.smtp.tls.tls.certificate.parsed.issuer.organization: ASUS

[140.119.143.122 \(ASUS.dormA.nccu.edu.tw\)](#)

- ERX-TANET-ASN1 Taiwan Academic Network (TANet) Information Center (1659) Taipei, Taipei City, Taiwan
- 465/smtp, 995/pop3s
- 465.smtp.tls.tls.certificate.parsed.issuer.organization: ASUS

[205.185.122.187](#)

How do we Compare the Two?



Shodan

- More focused search
- More ports (about 1230)



Censys

- Index all the things!
- Known tools

Enter GreyNoise





GREYNOISE

Enter GNQL query...

Today's Top Anomalies: `!!^? / ^*+ | <7` unique IPs `^ ()<*&%`

[> Explore Trends](#)





GREYNOISE

shodan.io

Today's Top Anomalies: 32346 / TCP | 83 unique IPs

▲ 1418%

> Explore Trends





Top Countries

United States 35

Netherlands 10

Vietnam 3

Iceland 2

Romania 2

Classification

Benign 56

Spoofable

False 40

True 1

> Benign

ISP

> View IP Detail

Organization:

IP Volume inc

Actor:

Shodan.io

ADB Worm

Bitcoin Node Scanner

Cassandra Scanner

Cisco Smart Install Endpoint Scanner

Cobalt Strike Scanner

+57 tags

> IP: 93.174.95.106 Country: Netherlands Last Seen: 2020-06-30

> rDNS: battery.census.shodan.io

> Benign

Hosting

> View IP Detail

Organization:

SingleHop LLC

Actor:

Shodan.io

CPanel Scanner

Printer Scanner

Privoxy Proxy Scanner

SOCKS Proxy Scanner

ZMap Client

> IP: 198.20.99.130 Country: United States Last Seen: 2020-06-30

> rDNS: census4.shodan.io

> Benign

ISP

> View IP Detail

Organization:

IP Volume inc

Actor:

Shodan.io

> Benign

ISP

93.174.95.106

Organization: IP Volume inc

Actor: Shodan.io

This IP address has been opportunistically scanning the Internet, and has completed a full TCP connection. Reported activity could not be spoofed.

> First Seen: 2017-09-20 Last Seen: 2020-06-30

> OS: Linux 3.11+ ASN: AS202425

> Country: Netherlands City: Amsterdam

> rDNS: battery.census.shodan.io

ADB Worm

Bitcoin Node Scanner

Cassandra Scanner

Cisco Smart Install Endpoint Scanner

Cobalt Strike Scanner

CounterStrike Server Scanner

CPanel Scanner

Cryptocurrency Node Scanner

Dahua DVR Auth Bypass

Digi RealPort Scanner

DNS Scanner

Dockerd Scanner

Elasticsearch Scanner

Ethereum Node Scanner

FTP Scanner

HID Door Controller Scanner

HTTP Alt Scanner

IMAP Scanner

IOT MQTT Scanner

IPSec VPN Scanner

IRC Scanner

JRMI Scanner

Kubernetes Crawler

LDAP Scanner

Memcached Scanner

Minecraft Scanner

MongoDB Scanner

MSSQL Scanner

MySQL Scanner

NETBIOS Scanner

Netis Router Admin Scanner

NTP Scanner

Oracle SQL Scanner

Phoenix Contact PLC Scanner

POP3 Scanner

Postgres Scanner

Printer Crawler

Printer Scanner

RabbitMQ Scanner

RDP Alternative Port Crawler

RDP Scanner

Redis Scanner

Router RPC Scanner

SAProuter Scanner

Siemens PLC Scanner

SMB Protocol Interrogation

SMB Scanner

SMTP Scanner

SNMP Scanner

Squid Proxy Scanner

SSDP/UPNP Scanner

SSH Alternative Port Crawler

SSH Scanner

Telnet Scanner

TFTP Scanner

TLS/SSL Crawler

VNC Scanner

VOIP Scanner

Web Crawler

Web Scanner

WinRM Scanner

X Server Connection Attempt

This IP address has been observed by GreyNoise scanning the Internet on the following ports:

▼ Scan Port / Protocol

7 / UDP

11 / TCP

13 / TCP

15 / TCP

17 / TCP

19 / UDP

21 / TCP

22 / TCP

23 / TCP

25 / TCP

26 / TCP

37 / TCP

43 / TCP

49 / TCP

53 / UDP

69 / UDP

70 / TCP

79 / TCP

80 / UDP

81 / TCP

82 / TCP

83 / TCP

84 / TCP

88 / TCP

102 / TCP

104 / TCP

110 / TCP

111 / TCP

113 / TCP

119 / TCP

123 / UDP

129 / UDP

137 / UDP

143 / TCP

164 / UDP

This device has been observed probing the Internet for, or exploiting, the following CVEs

> CVE-1999-0526

> CVE-2013-6117

Tags

🔗 ADB Worm

Category: Worm

This IP address has been observed exploiting the Android Debug Bridge vulnerability.

References:

<https://doublepulsar.com/root-bridge-ho>

W...

<https://blog.trendmicro.com/trendlabs-s>

e...

🔗 Bitcoin Node Scanner

Category: Activity

This IP address has been seen scanning the Internet for ports commonly used by Bitcoin nodes.

🔗 Cassandra Scanner

Category: Activity

This IP address has been seen scanning the Internet for Cassandra nodes.

Greynoise Classification

Malicious

Brute-forces
passwords or scans
for recognizable
exploits



Unknown

Doesn't do anything
malicious, but scans
without a known
“who”



Benign

The scans come from
a source Greynoise
recognizes



Other Scanning Services



Other Scanning Services

- ONYPHE
- Rapid7

BinaryEdge

- Look at organizations

35.235.124.140

reverseUnknown (Unknown)

domainUnknown

geoloc *

Nothing known (yet)

inetnum

Nothing known (yet)

pastries

key - [TrxE17nH](#) (2020-06-16)

title - Unknown

user - Unknown

syntax - [bash](#)

size - 2004

source - [pastebin](#)

[Query full result\(s\)](#)

key - [KVGqV21a](#) (2020-06-11)

title - [fas](#)

user - Unknown

syntax - [bash](#)

size - 30956

source - [pastebin](#)

[Query full result\(s\)](#)

resolver

ip - [35.235.124.140](#) (2020-06-30)

type - [forward](#)

forward - [eaw2ob.innerprofessional.courses](#)

domain - [innerprofessional.courses](#)

source - [urlscan](#)

[Query full result\(s\)](#)

ip - [35.235.124.140](#) (2020-06-30)

type - [forward](#)

forward - [tmp-eib.innerplicity.com](#)

domain - [innerplicity.com](#)

source - [urlscan](#)

[Query full result\(s\)](#)

ip - [35.235.124.140](#) (2020-06-30)





Open Data

Rapid7 Labs

HTTP GET Responses

[See All Datasets](#)

2,361

LAST UPDATED: 06/27/2020

Responses to HTTP/1.1 GET requests against various HTTP ports

Study Details

Study

[HTTP GET Responses](#)

Author

Project Sonar | [Rapid7](#)

Dataset Details

This dataset contains the responses to HTTP/1.1 GET requests performed against a variety of IPv4 public HTTP endpoints

[Dataset Schema](#)

Benign?

Top Actors

Stretchoid.com	3,701
----------------	-------

BinaryEdge.io	1,956
---------------	-------

NetCraft	1,508
----------	-------

Alpha Strike Labs	1,023
-------------------	-------

PDR Labs.net	772
--------------	-----

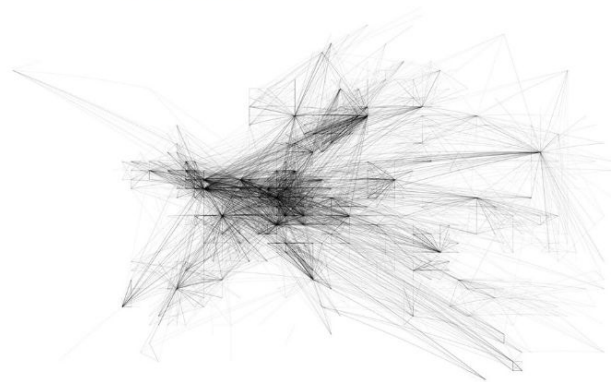
Benign?

http://www.pdrlabs.net/



PDR Labs Internet Mapping Experiment

PDR Labs is engaged in an ongoing experiment to continuously map the Internet in its entirety. Our crawls are not malicious or invasive, and are intended to understand what addresses on the Internet-at-large are in use. If you have additional questions, please contact research@pdrlabs.net.



What are you doing?

We are an industry research group focused on understanding large-scale traffic patterns, and so it is useful to understand what address space is being actively utilized. To accomplish this, our crawling network makes HTTP HEAD requests on the public ports 80 and 443 (web traffic) for IPv4 and sections of IPv6 address space. This lets us see which addresses are actively being used in large traffic patterns. We

Stretchoid is a platform that helps identify an organization's online services.

Sometimes this activity is incorrectly identified by security systems, such as firewalls, as malicious. Our activity is completely harmless. However, if you would prefer that we do not scan your infrastructure, please submit the following information:

Name

Email

IP/Block

/

Notes

Opt Out

Organization:

Actor:

DigitalOcean, LLC

Stretchoid.com

CounterStrike Server Scanner

Dockerd Scanner

Elasticsearch Scanner

FTP Scanner

HTTP Alt Scanner

+5 tags

> IP: 192.241.233.166 Country: United States Last Seen: 2020-06-27

> rDNS: zg-0428c-12.stretchoid.com

> Benign

Hosting

> View IP Detail

Organization:

Actor:

DigitalOcean, LLC

Stretchoid.com

CounterStrike Server Scanner

Dockerd Scanner

Elasticsearch Scanner



Elasticsearch Worm

HTTP Alt Scanner

+6 tags

> IP: 192.241.233.29 Country: United States Last Seen: 2020-06-27

> rDNS: zg-0428c-10.stretchoid.com

> Benign

Hosting

> View IP Detail

Organization:

Actor:

DigitalOcean, LLC

Stretchoid.com

Cassandra Scanner

CounterStrike Server Scanner

DNS Scanner

Dockerd Scanner

Elasticsearch Scanner

+29 tags

> IP: 192.241.237.229 Country: United States Last Seen: 2020-06-26

> rDNS: zg-0428c-455.stretchoid.com

Elasticsearch Worm

Category: Worm

This IP address has been observed sending requests that exploit an Elasticsearch code injection vulnerability.

FOFA



[Sign In or Sign Up](#)[Categories](#)[API&SDK](#)[Commom Rules](#)[FofaCli](#)[Vip Bar](#)[FOFA新版](#) Beta[问题反馈](#)今日热点搜索: [Coremail](#) [Weblogic](#) [九安视频监控](#)[Query Syntax](#)[Featured Categories](#)

TOP PROTOCOLS

http	793,726,644
https	199,326,991

TOP PORTS

80	642,695,133
443	395,218,101

Fofa.so

Anglerfish
42196 characters

Fofa.so



Fofa.so

Shodan: 12369 characters

FOFA: 28757 characters

Anglerfish
42196 characters

Who's the very best?
(like no one ever was)
A Quiz



Scenario 1

A security researcher believes they have found the new Misfortune Cookie and is interested in seeing all the pages from all the IPs that have port 7547 open in the last month.

Scenario 1

A security researcher believes they have found the new Misfortune Cookie and is interested in seeing all the pages from all the IPs that have port 7547 open in the last month.



Scenario 2

D-Link DSL-2750B has a command injection vulnerability according to ExploitDB, but the device name is at the bottom of its login homepage.

Scenario 2

D-Link DSL-2750B has a command injection vulnerability according to ExploitDB, but the device name is at the bottom of its login homepage





"DSL-2750B"

IPv4 Hosts

Page: 1/16 Results: 393

D-Link DSL-2750B



SHODAN

DSL-2750B

TOTAL RESULTS

63

FQFA Pro

"DSL-2750B" && after="2020-06-15"

Total results: 3,638 (IP results: 519), took 47 ms,

Scenario 3

I want to find data about a specific IP address, because it came up as possibly interesting from my company's IDS.



SHODAN



Censys

Takeaways

No scanning service is an entire toolbox



Censys



SHODAN

Questions?



adlda_adAstra

Thank you



adlda_adAstra