


black hat[®]
USA 2019
AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS

SHODAN SEEKER



whoami

Laura Garcia

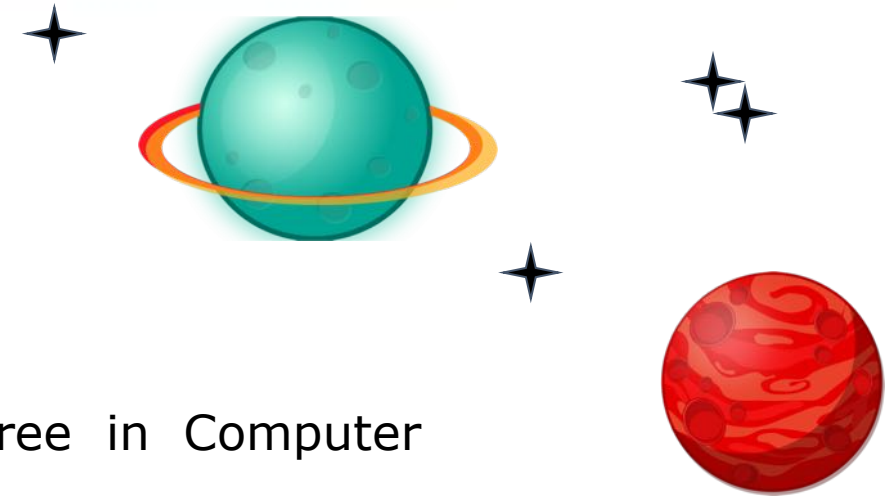
5-years degree in Computer Engineering and master's degree in Computer Security from the Polytechnic University of Madrid.


More than 10 years of experience in the field of Computer Security.

Currently working as Security Architect / Pentester at Deloitte Hack Team Spain.

Execution of controlled real-world attacks against systems, products and facilities. Perform penetration tests on various technologies, such as web applications, mobile applications, AD attacks, wireless media and infrastructures.

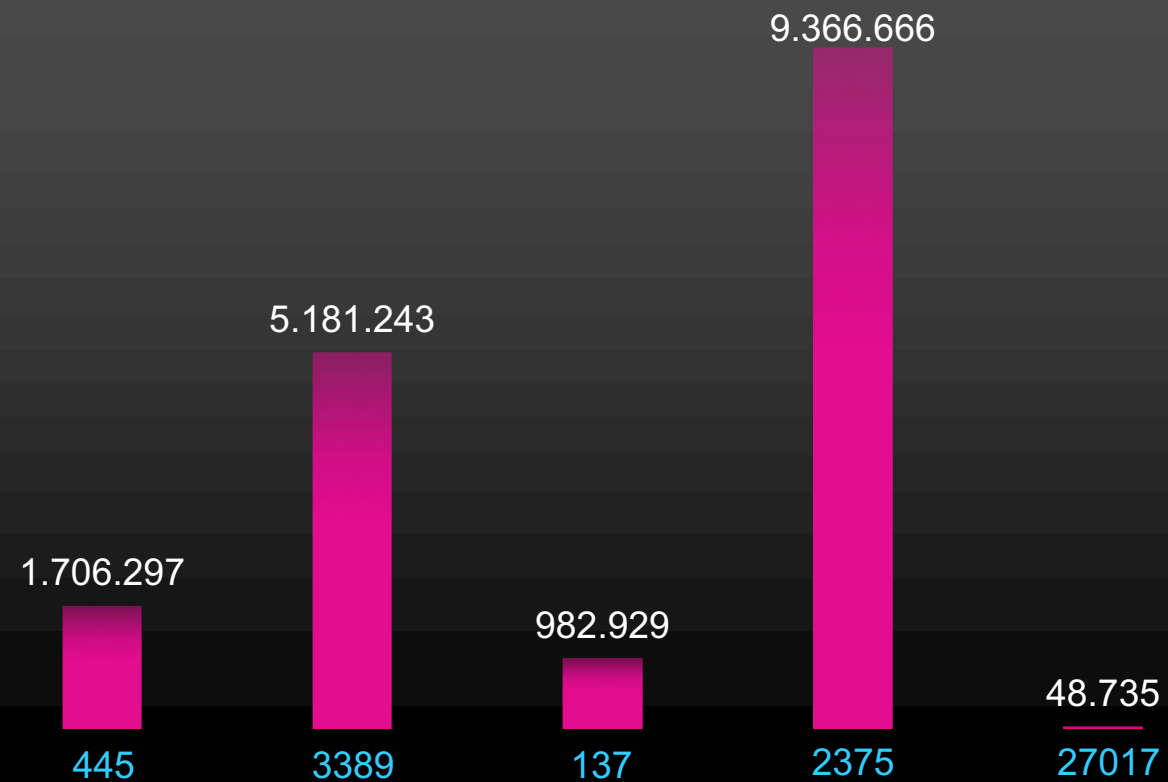
<https://es.linkedin.com/in/laura-garcia-cybersec>



The background of the slide is a satellite view of Earth at night, showing city lights and a large, dark, irregularly shaped landmass in the center. A bright green laser beam is visible on the left side of the image.

The large number of **assets** published on the Internet, increase the probability of services exposed that could put them at **risk**.

RISK OPEN PORTS



AESDDoS Botnet Malware



mongoDB

Cryptojacking campaign uses Shodan to scan for Docker hosts to hack

June 1, 2019 By [Pierluigi Paganini](#)

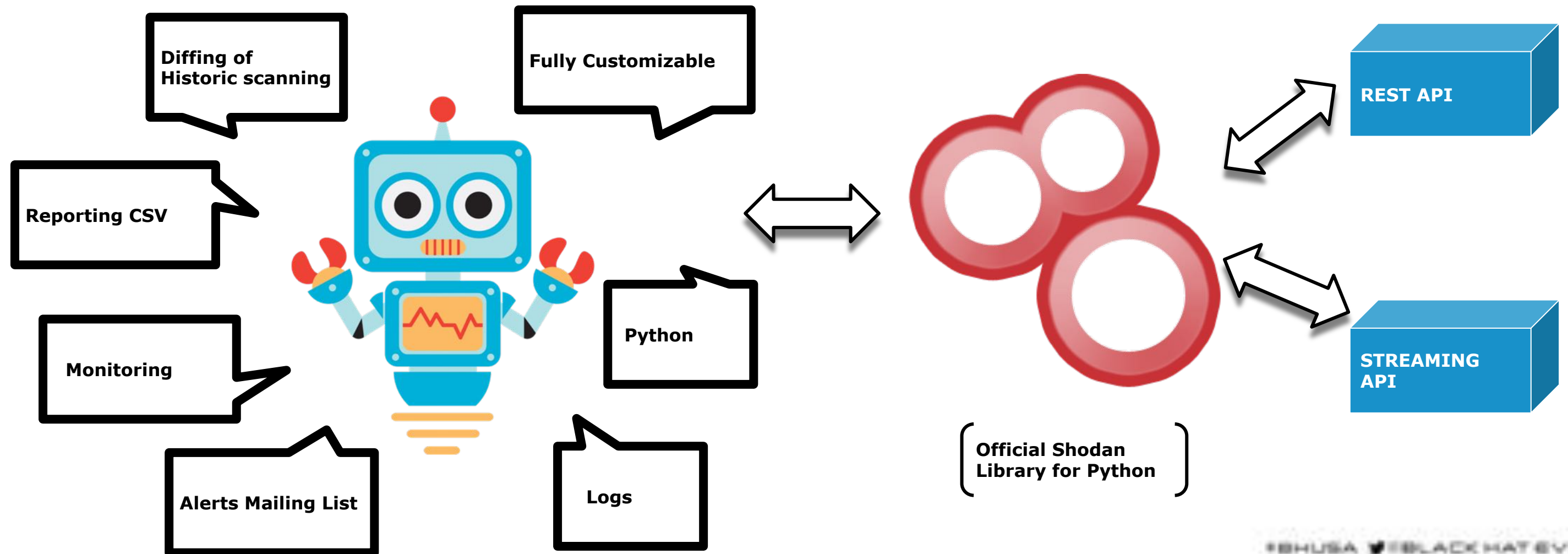
A new cryptojacking campaign was spotted by experts at Trend Micro, crooks are using Shodan to scan for Docker hosts with exposed APIs.



MongoDB server leaks 11 million user records from e-marketing service

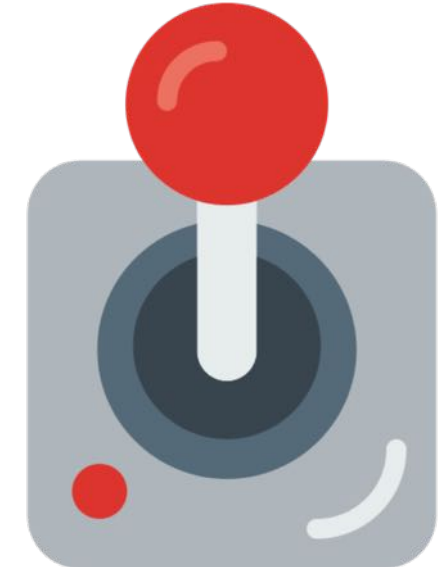
Database has now been secured. Server was also ransomed by a criminal group back in June.

SHODAN SEEKER



Usage - Scanning

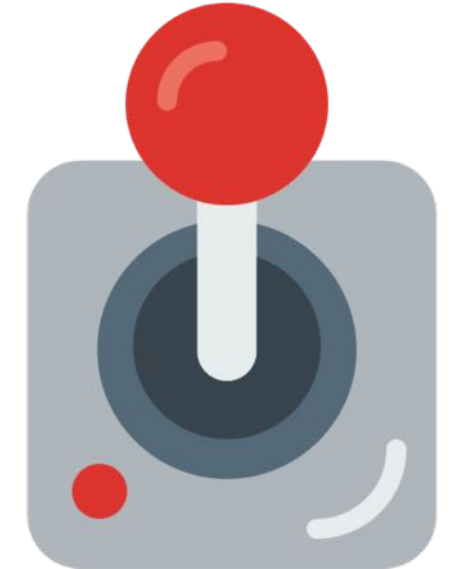
- ☐ Scan an IP/netblocks (args or file).
- ☐ Force Shodan to re-scan the provided IPs.
- ☐ List previously submitted scans.



Usage – Searching

- ☐ Get services published of an IP/netblock (args or file).
- ☐ Get all Historical services published.
- ☐ Get New Services published (Diffing).
- ☐ Output results in csv format.

- ☐ Send email with results.
- ☐ Attach csv results to an email.



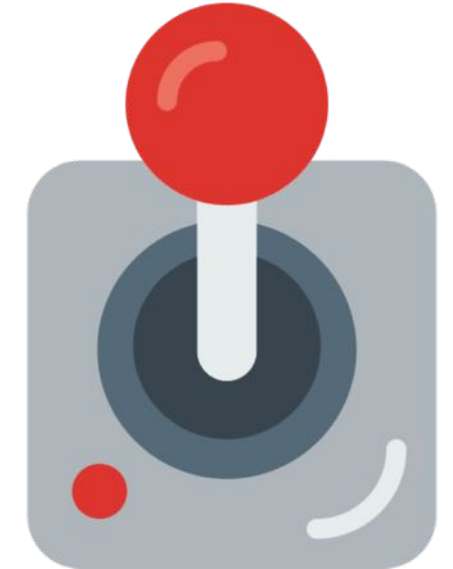
Usage - Monitoring

- ☐ Create network alerts for the IP/netblock (args or file).
- ☐ List of all the network alerts activated.
- ☐ Remove the specified network alert.

- ☐ Subscribe to the Private Horse Streaming.
- ☐ Monitoring for High Risk Services.
- ☐ Monitoring for New Services Published (Diffing).
- ☐ Monitoring for Tags.

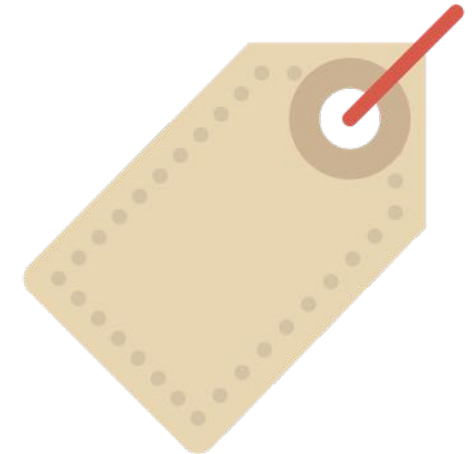
- ☐ Send email with alerts.
- ☐ Mailing lists customizable for each alert.

- ☐ Get protocols, services, ports and tags supported.



Tags supported by Shodan

| | |
|-----------------------|--------------------|
| cloud | compromised |
| cryptocurrency | database |
| devops | doublepular |
| honeypot | ics |
| iot | malware |
| medical | onion |
| scanner | self-signed |
| starttls | tor |
| videogame | vpn |



Technical issues

- Request rate limit reached (1 request/second) in API calls (REST API).
 - `sleep(0.5s)`
- Connection between the script and the server got broken (Streaming API).
 - `./sh` to respawn `shodan-seeker.py` script.
 - `ChunkedEncodingError` exception: call `self.function`.
- JSON output contains blank fields ("ports").
- Shodan takes a few hours, since on-demand scanning is launched, to update its databases with the results.
- IPs found with open ports did not appear in their database.

Diffing implementation

Request:

GET/shodan/host/{ip}&history=true

Response:

| | |
|-------------|------------|
| ip | |
| last_update | |
| port1 | timestamp1 |
| port1 | timestamp2 |
| port2 | timestamp3 |
| port3 | timestamp1 |
| port3 | timestamp3 |

list_port_uniq:

| | | |
|-------|-------|-------|
| port1 | port2 | port3 |
|-------|-------|-------|

list_timestamp_host_sort_uniq:

| |
|------------|
| timestamp1 |
| timestamp2 |
| timestamp3 |

timestamp_adjustment:

```
timestamp_ajustment =
datetime.now() + days=32
```

for port in port_uniq:

var list_timestamp_port:

| |
|------------|
| timestamp1 |
| timestamp3 |

for timestamp in list_timestamp_port:

if (last_update == timestamp) and (date <= timestamp_adjustment):

if (len (list_timestamp_port) == 1:

print "diff port open"

else:

next_timestamp_port = list_timestamp_port [1]

next_timestamp_host = list_timestamp_host_sort_uniq [1]

if (next_timestamp_port != next_timestamp_host):

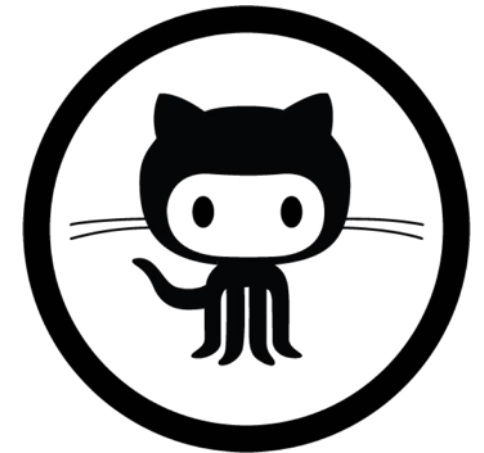
print "diff port open"

Pros and Cons

- Diffing implementation for assets discovery on Real-Time and REST API approach.
- Get information (History, Diffing) without consuming credits.
- Generate results on csv format without consuming credits.
- Reports easily integrated with Business Data Analytics frameworks.
- Fully customizable:
 - Input data via command-line or files.
 - Different output modes.
 - Sends alerts and output results to different mailing lists.
- Monitor all tags supported by Shodan.
- Command-line friendly :)
- API plan subscription needed.

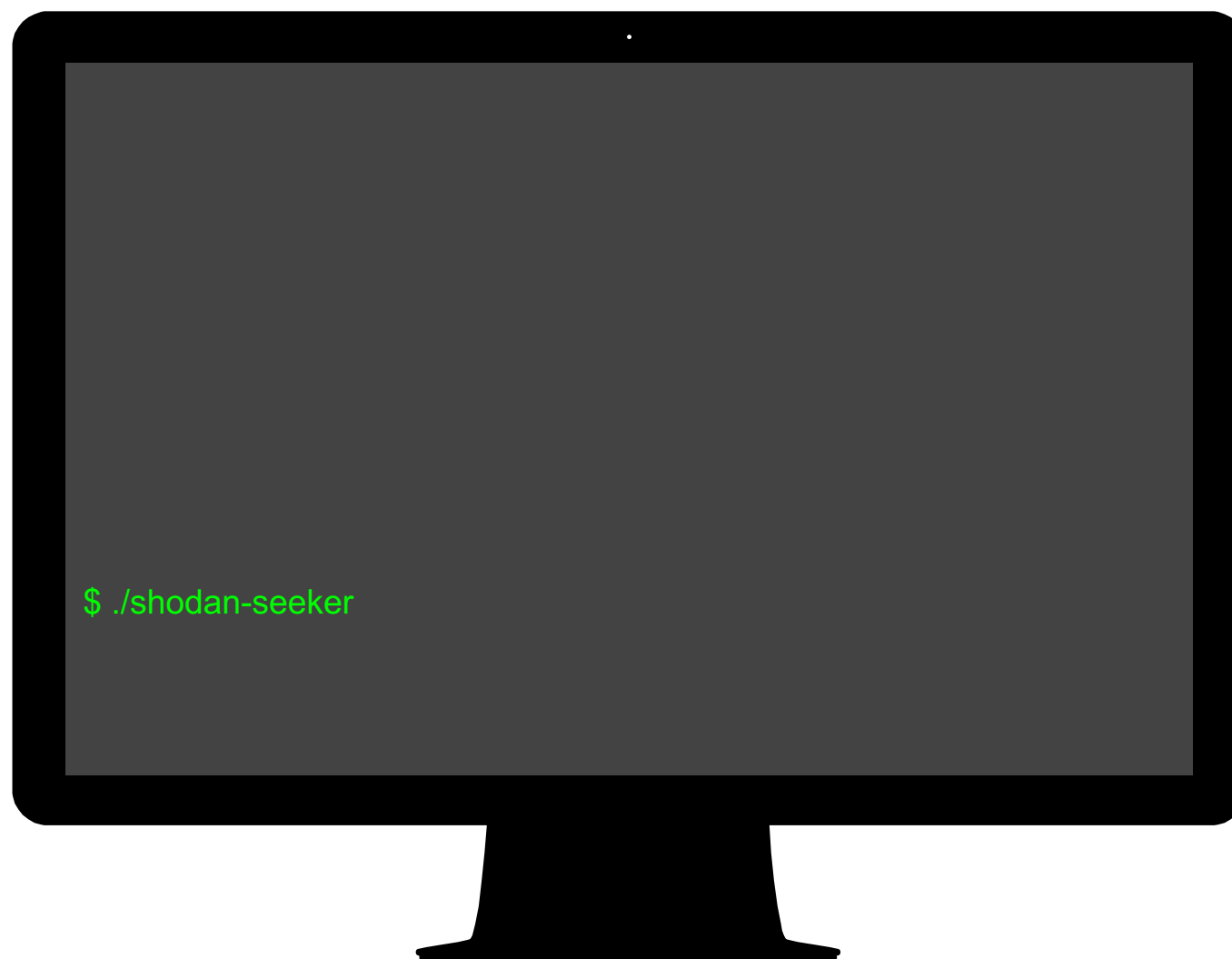
Downloads

Recommended clone from Git:



```
git clone https://github.com/laincode/shodan-seeker.git  
cd shodan-seeker  
./shodan-seeker # just run this script
```


Demo



```
set@shodan-seeker lair$ ./shodanseeker
Usage: python shodanseeker [options]
```

Options:

```
-h, --help            show this help message and exit
--mail=MAIL           Send email with results and alerts
-a                   attach csv results to an email
```

Scanning Options:

```
--sl=SCANIPsY         Scan an IP/netblock
--sf=SCANFILE          Scan an IP/netblock from file
--force               Force Shodan to re-scan the provided IPs
-l                   list previously submitted scans
```

Searching Options:

```
-i GETINFO             Get all information of an IP/netblock
-f GETINFOFROMFILE    Get all information of an IP/netblock from file
--history              Return all Historical banners
--diff                Detect New Services Published
--output=OUTPUT       Output results in csv format
```

Monitoring in Real-Time:

```
--ca=ADDALERT          Create network alerts for the IP/netblock
--cf=ADDALERTFILE      Create network alerts from file
--la                   List of all the network alerts activated
--da=DELALERT          Remove the specified network alert
--subs=SUBSALERTS      Subscribe to the Private Horse Streaming
--monitor=MONPORT      Monitoring for High Risk Services
--mondiff              Monitoring for New Services Published
--montag=MONTAG        Tags (ex: compromised, doublepulsar, self-signed)
--get=GET              Protocols, services, ports and tags supported
```

EXAMPLES:

```
./shodanseeker --sl "X.X.X.X X.X.X.X/24" # Scan IPs/netblocks
./shodanseeker --sf "pathfilename" # Scan IPs/netblocks from a file
./shodanseeker -l # list previously submitted scans
./shodanseeker -i "X.X.X.X X.X.X.X/24 Y.Y.Y.Y" # Get all information of IP/netblocks
./shodanseeker -f "pathfilename" # Get all information from a file of IPs/netblocks
./shodanseeker -i "X.X.X.X" --history # Get all historical banners
./shodanseeker -i "X.X.X.X" --diff # Detect new services
./shodanseeker -f "pathfilename" [--history|--diff] --output csv # Output results in csv format
./shodanseeker -i "X.X.X.X" --diff --output csv --mail toaddr -a # Send email with csv results attached
./shodanseeker --ca name "8.8.8.8 8.8.8.8/24" # Create network alerts for the IP/netblock
./shodanseeker --cf name "pathfilename" # Create network alerts from file
./shodanseeker --la # list of all the network alerts activated on the account
./shodanseeker --da [alertid] # Remove the specified network alert
./shodanseeker --subs [alertid] --monitor "389 22" [--mail toaddr] # Subscribe to the Streaming and monitoring for high risk services
./shodanseeker --subs [alertid] --mondiff [--mail toaddr] # Subscribe to the Streaming and monitoring for new services published
./shodanseeker --subs [alertid] --montag "compromised" [--mail toaddr] # Subscribe to the Streaming and monitoring for tags (ex: compromised, doublepulsar, self-signed)
./shodanseeker --get [protocols/services/ports/tags] # list of (protocols, services, ports, tags) supported
```

```
set@shodan-seeker lair$
```

References

- <https://developer.shodan.io/api>
- <https://developer.shodan.io/api/stream>
- <https://github.com/achillean/shodan-python>



AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS

THANK YOU !!