2016

A la découverte de SHODAN

L'OMBRE

HAL2DS16K

07/08/2016

CLAUSE DE NON-RESPONSABILITE

Ce document est un recueil de techniques, de moyens, d'explications et de situations à titre d'**exemple**. Il n'a pas vocation à vous former à des techniques **malveillantes**. Son auteur et/ou le site diffuseur ne pourront être tenus **responsables de vos actes** par aucun moyen.

Ce document est distribué de manière **gratuite**. Il est écrit par un **passionné** et non un expert. Cependant, je me suis efforcé de vérifier la véracité de mes informations, mais je suis faillible comme tout être humain.

Bonne lecture.

REMERCIEMENTS

Je tiens tout d'abord à remercier les membres de Hackademics pour leur patience et leur partage de connaissances.

Je veux aussi remercier les différentes personnes sur les différents forums, sites et autres plateformes qui lisent mes news et articles.

Et enfin, je remercie ma famille de m'avoir aidé à poursuivre ma passion.

L'OMBRE

TABLE DES MATIERES

SHODAN

INTRODUCTION

Fondateur du site : John Matherly
Site web : https://shodan.io
Blog : https://blog.shodan.io
Catégorie : Reconnaissance 🔴 , Analyse du réseau cible 🔵

Avant de parler de l'outil, intéressons-nous à sa provenance. Comme précisé ci-dessus, cet outil a été développé par John Matherly sur environ 3 ans. Son nom viendrait d'un personnage d'un ancien jeu vidéo *System Shock* développé par *TriOptimum Corporation*. L'univers de ce jeu est basé sur le piratage informatique et l'ennemi de ce jeu est SHODAN (***S****entient* ***H****yper-****O****ptimized* ***D****ata* ***A****ccess* ***N****etwork*), une Intelligence Artificielle qui se révèle hors de tout contrôle. Le but du joueur est donc de sauver la terre de cette IA maléfique !

Figure 1: Sentient Hyper-Optimized Data Access Network

Répondons maintenant à une question souvent posée sur cet outil, qu'est-ce que Shodan ? Shodan est un moteur de recherche de systèmes connectés à Internet. Pour simplifier, Shodan est un *Google* pour trouver des ordinateurs, des caméras, des ICS (systèmes de contrôles industriels) ainsi que tout autre système connecté à Internet.

FONCTIONNEMENT

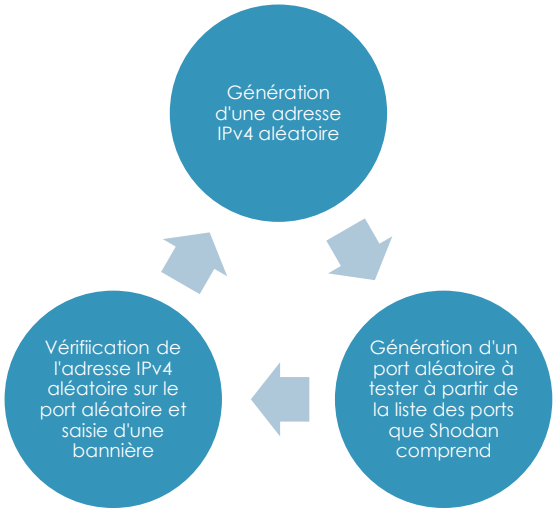
Shodan fonctionne grâce à des robots (ordinateurs qui effectuent des recherches de façon automatisée) qui travaillent 24/24 et 7/7 jours. Ces robots sont implantés partout dans le monde.
Voici une liste non-exhaustive d'implantations géographiques :

- USA
- Chine
- Islande
- France
- Taïwan
- Vietnam

- Roumanie
- République Tchèque

ALGORITHME BASIQUE DE SHODAN

Les robots utilisent l'algorithme ci-dessous :



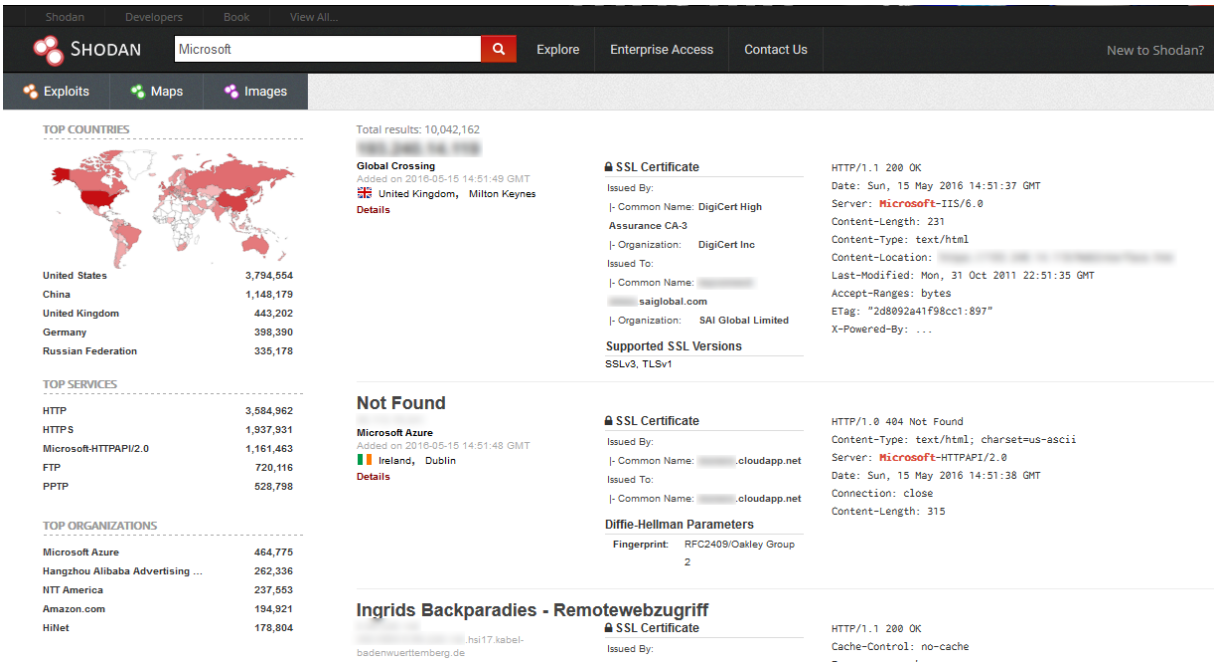
LES DIFFERENTES INTERFACES DE SHODAN

Shodan peut être utilisé de différentes manières, voici celles que nous allons voir :

- Shodan Search Engine
- Shodan Exploits
- Shodan Maps
- Shodan 3D
- Shodan ICS Radar
- Shodan Images
- Shodan CLI
- Shodan Mobile App (Android)

SHODAN SEARCH ENGINE

Shodan Search Engine est un moteur de recherche comme les autres, entrez-y simplement un mot. Nous allons tester ici Microsoft :



Comme nous le voyons, les résultats ne manquent pas. Rien qu'aux Etats-Unis d'Amérique, il y a 3 794 554 systèmes qui correspondent à la recherche plutôt simpliste que nous avons effectuée précédemment. Mais ce qui m'intéresse, c'est le nombre de serveur IIS en version 8.5 en France. Voyons voir comment filtrer tout ça afin d'obtenir le résultat demandé.

LES FILTRES

Les filtres sur Shodan sont fabriqués ainsi :

Filtre:valeur

Il en existe beaucoup, je vais ci-dessous vous donner les principaux :

FILTRES DE LOCALISATION

Filtres	Commandes	Exemples
Pays	country	country:FR
Ville	city	city:Paris
Code postal	postal	postal:95000
Position géographique	geo	geo:XX.X,YY.Y

FILTRES RESEAUX

Ce qui peut donner par exemple pour notre requête :

Filtres	Commandes	Exemples
Organisation	org	org:Microsoft
Réseau	net	net:192.168.0.1 net:192.168.0.14/21
Nom de la machine	hostname	hostname:choualbox.com
Port	port	port:21
IPv6	has_ipv6	has_ipv6:True
ASN	asn	asn:AS28708

FILTRES WEB

Filtres	Commandes	Exemples
Titre	title	title:Private
HTML	html	html:phpinfo.php html:robots.txt
Code erreur	Pas de commande	403 Forbidden 200 ok 401 Unauthorized

FILTRES PORTANT SUR LE LOGICIEL

Filtres	Commandes	Exemples
Système d'Exploitation	os	os:Kali
Produit	product	product:Apache
Version	version	version:2.0.2
Vulnérabilité	vuln	vuln:CVE-2014-0160

FILTRES DE TEMPS

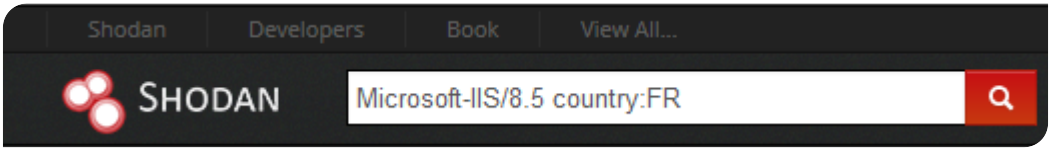
Filtres	Commandes	Exemples
Avant la date	before	before:DD/MM/AAAA
Après la date	after	after:DD/MM/AAAA

COMBINER FILTRES ET VALEURS

Maintenant que nous avons vu en détail les filtres de Shodan, vous êtes en mesure de répondre seuls à la question que je vous ai posé :

Mais ce qui m'intéresse, c'est le nombre de serveur IIS en version 8.5 en France. Voyons voir comment filtrer tout ça afin d'obtenir le résultat demandé.

Pour ceux qui n'ont pas trouvé, voici la syntaxe :



La combinaison des filtres s'effectue comme ci-dessous :

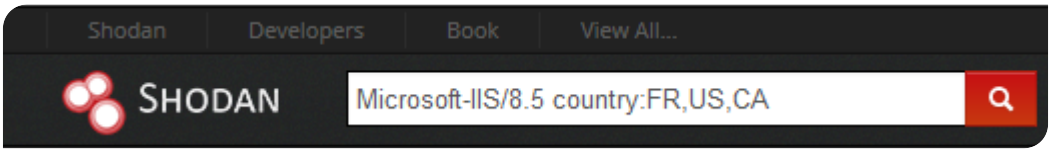
terme filtre1:valeur filtre2:valeur

La combinaison de valeurs s'effectue comme ci-après :

terme filtre1:valeur1,valeur2 filtre2:valeur1,valeur2,valeurX

Modifions donc l'énoncé de la recherche :

Mais ce qui m'intéresse, c'est le nombre de serveur IIS en version 8.5 en France, USA, Canada. Voyons voir comment filtrer tout ça afin d'obtenir le résultat demandé.

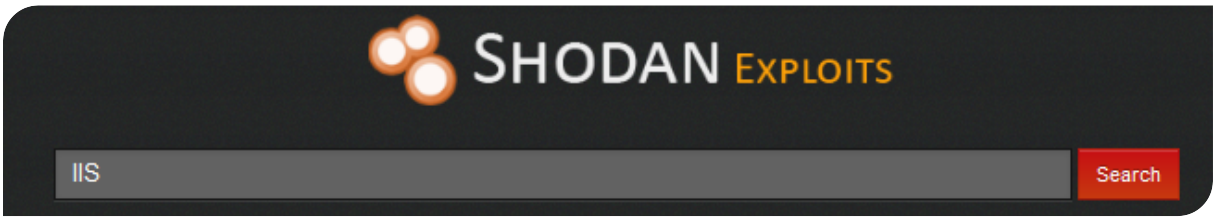


Attention, il faut ne faut ***pas*** mettre ***de filtre*** sur le ***premier*** terme de recherche.

Attention, si vous devez écrire une chaîne de caractères comprenant un espace, n'oubliez pas les guillemets autour de celle-ci.

Attention, il n'y a ***pas d'espaces entre le filtre et sa valeur***, juste le caractère **:** .

SHODAN EXPLOITS



Lien du service : https://exploits.shodan.io/welcome

Shodan Exploits vous permet de rechercher les vulnérabilités et les exploits dans les bases de données de :

- CVE
- Exploit-DB
- Metasploit

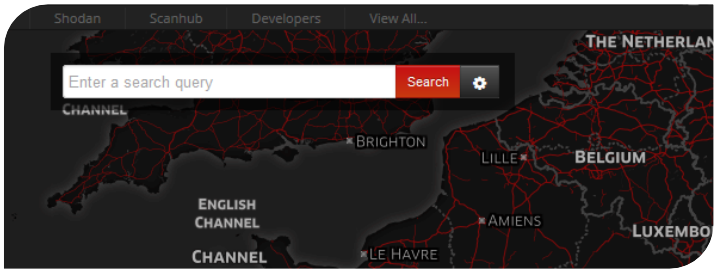
FILTRES SHODAN EXPLOITS

Contrairement aux autres interfaces, il dispose de ses propres filtres :

Filtres	Commandes	Exemples
Auteur	author	author:Rapid7
Description	description	description:access
Plateforme	platform	platform:"windows"
Type	type	type:"exploit"

On peut aussi combiner les filtres :

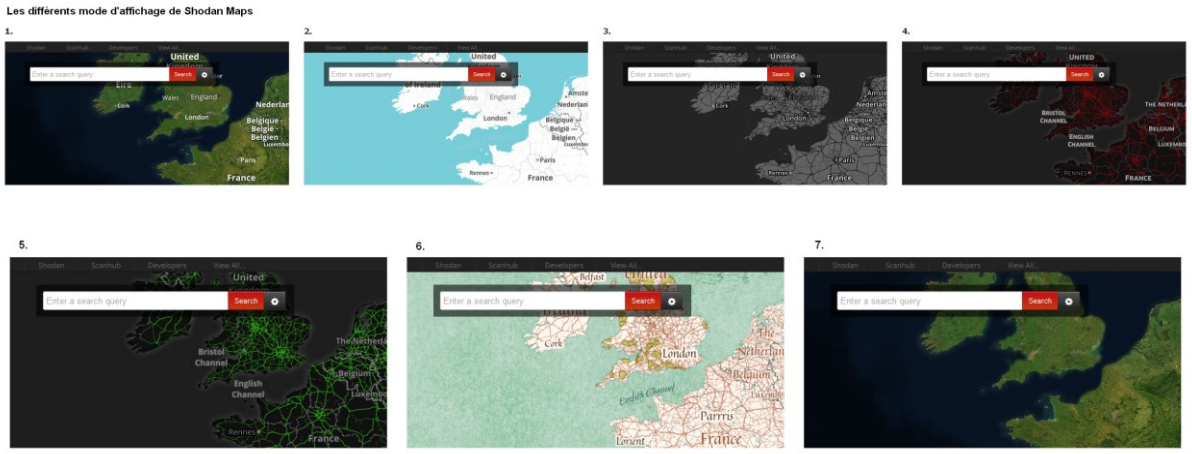
description:access platform:"windows" type:"exploit"



Lien du service : https://maps.shodan.io/

Shodan Maps vous permet de visualiser votre recherche sur une carte en deux dimensions. Les filtres fonctionnent comme sur une recherche Shodan Search Engine. Voici les différents modes d'affichage possibles :

1. Satellite
2. Street View (épuré)
3. Street View (Obsur)
4. Street View (Rouge)
5. Street View (Vert)
6. Pirate
7. Satellite (épuré)

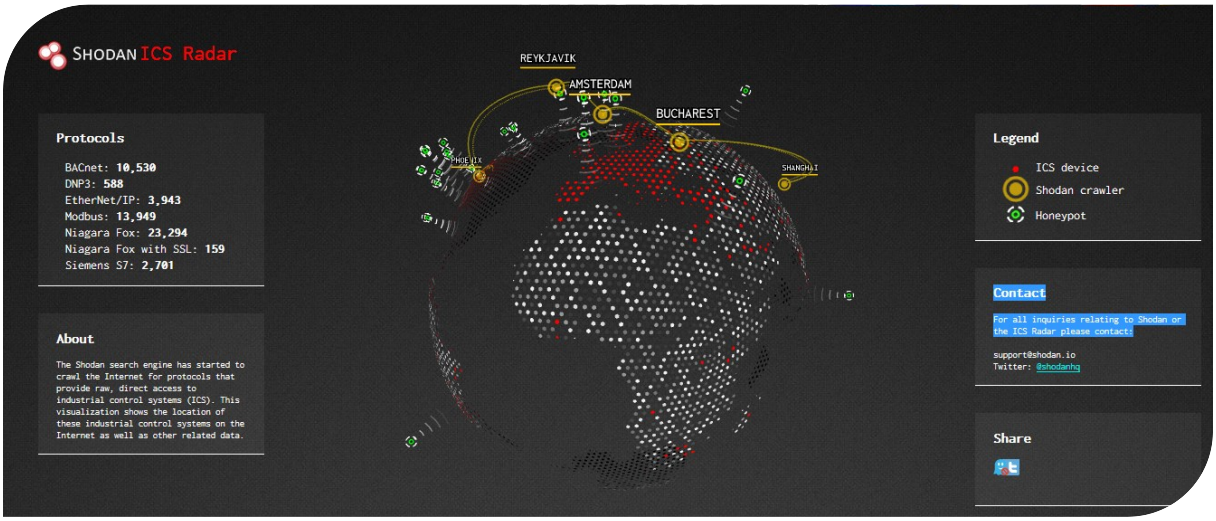


SHODAN 3D

Lien du service : https://3d.shodan.io/

L'interface 3 dimensions de Shodan, vous pouvez aussi utiliser les filtres de Shodan Search engine.

SHODAN ICS RADAR



Lien du service : https://ics-radar.shodan.io/

C'est une visualisation des données concernant les Systèmes Industriels de Contrôle connectés à internet.

SHODAN IMAGES

Lien du service : https://images.shodan.io/

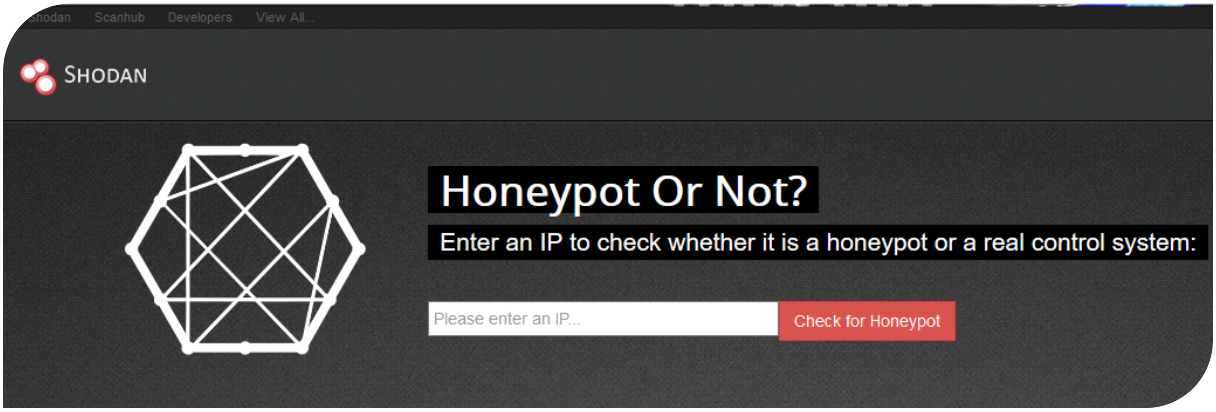
Vous pouvez visualiser des images prises par Shodan lorsque les systèmes laissent les mots de passe par défaut.

SHODAN WEBCAM BROWSER

Lien du service : https://webcambrowser.shodan.io/

C'est un navigateur de webcams. Il permet de voir en temps réel le flux vidéo des caméras connectées sur Internet et utilisant des mots de passe par défaut.

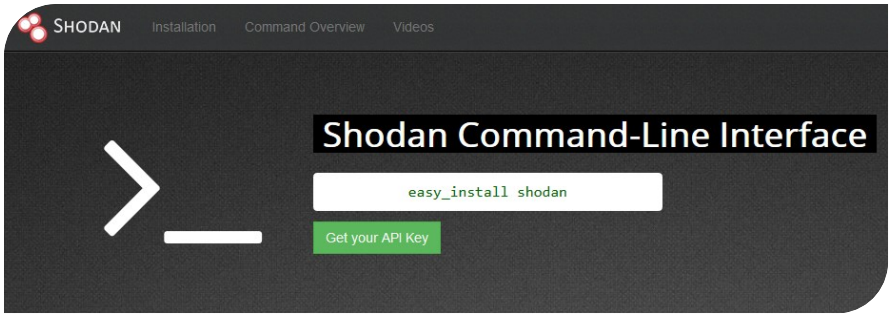
SHODAN HONEYSCORE



Lien du service : https://honeyscore.shodan.io/

Ce site permet de vérifier si une adresse IP est considérée par Shodan comme un piège (HoneyPot). Pour l'utiliser, il vous suffit simplement d'entrer l'adresse IP suspecte.

SHODAN CLI



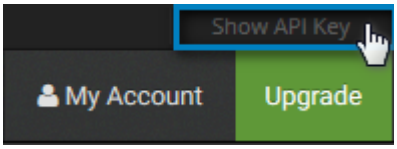
Shodan CLI est l'interface de Shodan accessible en ligne de commande. Elle dispose de ses propres commandes.

DEMANDER SON API KEY

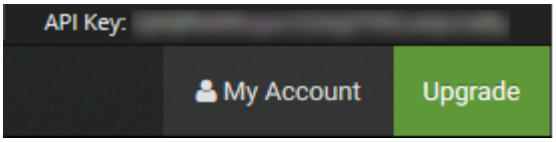
Pour demander une API key pour utiliser Shodan, rien de plus simple, il vous suffit de vous inscrire sur le site via cette url :

https://account.shodan.io/register

Puis une fois inscrit et connecté, il y a un bouton en haut à droite où il est écrit Show API Key :



Il vous suffit de cliquer dessus, vous aurez alors votre API Key qui apparait comme ci-dessous :



INSTALLATION

Pour installer Shodan CLI, il vous suffit de taper la commande suivante dans votre terminal :

```
root@kali:~# easy_install shodan
```

CONFIGURATION DE L'API KEY

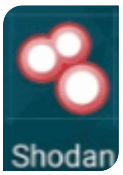
Pour configurer l'API key, il vous suffit d'entrer la commande suivante en remplaçant le mot CLE par votre API Key :

```
root@kali:~# shodan init CLE
```

LES COMMANDES DE SHODAN CLI

Shodan CLI possède ses propres commandes, les voici en détails :

Commandes	Actions	Exemples
--help	Affiche le manuel de Shodan CLI	shodan --help
alert	Gérer les alertes réseau de votre compte	shodan alert
convert	Convertir le fichier JSON compressé généré par Shodan dans un format de fichier différent. À l'heure actuelle, il ne prend en charge que le format **kml**.	shodan convert fichier-entrée.json.gz .kml
count	Retourne le nombre de résultats pour une recherche.	shodan count microsoft iis 10.0
download	Recherche Shodan et téléchargement des résultats dans un fichier où chaque ligne est une bannière JSON.	shodan download microsoft-data Microsoft iis 10.0
honeyscore	Vérifie si une IP est considérée comme un piège ou non par Shodan.	shodan honeyscore 192.168.0.1
host	Affiche les informations sur l'hôte, où il se trouve, quels ports sont ouverts et quelle est l'organisation qui détient l'adresse IP.	shodan host 192.168.0.1
info	Affiche les informations générales à propos de votre compte.	shodan info
init	Initialisation de Shodan CLI.	shodan init API-KEY
myip	Affiche votre IP Publique.	shodan myip
parse	Analyse un fichier qui a été généré en utilisant la commande **download**. Il vous permet de filtrer les champs qui vous intéressent, convertissez le JSON en un CSV. Cela est plus simple d'utilisation avec d'autres scripts.	shodan parse --fields ip_str,org,port --separator , Microsoft-data.json.gz
scan	Scanne une adresse IP ou une Plage IP avec Shodan.	shodan scan submit 192.168.0.1
search	Recherche dans la base de données Shodan.	shodan search --fields ip_str,port,org,hostnames microsoft iis 10.0
stats	Affiche les statistiques en lien avec votre recherche.	shodan stats --facets country apache
stream	Permet d'accéder, en temps réel, aux flux des données que les robots Shodan recueillent.	shodan stats --facets country ftp



Créateur : PaulSec
Github : https://paulsec.github.io/
Plateforme : Android

Cette application se présente comme celle officielle de Shodan.io, elle permet de retrouver l'interface Shodan Search Engine dans une application portée sur Android.

Pour l'utiliser, c'est simple, il vous suffit de la télécharger et ensuite de l'installer. Une fois cela fait, il va lors de la première ouverture vous demander d'entrer l'API Key (Se référer à cette page pour l'obtention : Demander son API KEY)

L'application se divise en 4 vues : La vue de recherche (Search), la vue des requêtes les plus soumises en ce moment (Queries), la vue de votre compte, cela inclus en clair votre API Key (Account) et la derrnière vue est celle où vous trouverez des informations sur l'applications comme le nom du créateur (Info). Vous pouvez effectuer la recherche avec les filtres existants sur l'interface web dans l'application.

Voici quelques captures d'écrans réalisées sur cette application :

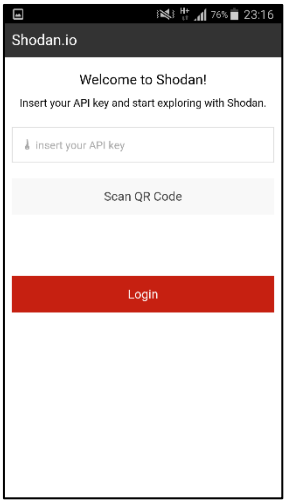


Figure 2: SMA Acquisition de l'API Key

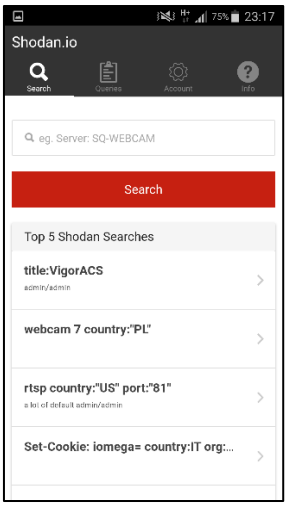


Figure 3: SMA Search

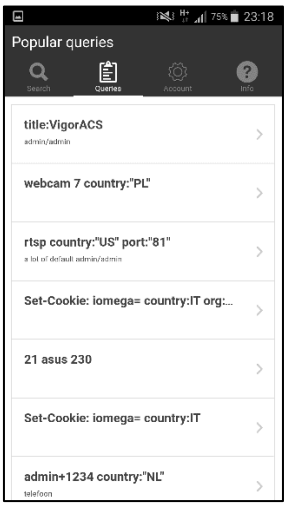


Figure 4: Queries

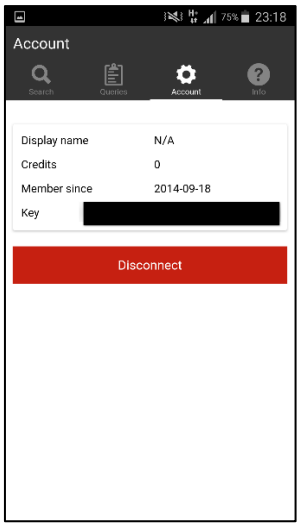


Figure 5: SMA Account

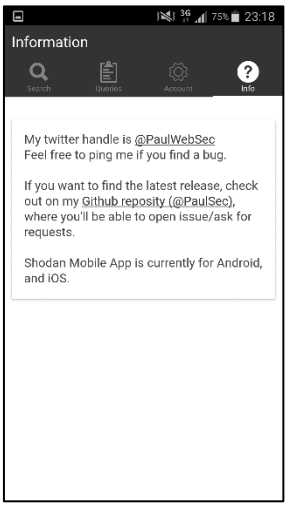


Figure 6: SMA Information

EXERCICES

Voici quelques petits exercices sur Shodan :

EXERCICE 1

Chercher le mot « Login » dans le titre des pages.

EXERCICE 2

Trouver les adresses IP de l'organisation Orange à Paris et qui possèdent une copie d'écran.

EXERCICE 3

Combien d'adresses IP en France sont vulnérables à Heartbleed et supportent SSLv2 ?

EXERCICE 4

Combien d'adresses IP dans l'organisation OVH sont vulnérables à Heartbleed ?

EXERCICE 5

Trouver tous les systèmes de contrôle Industriels dans la ville de Paris.

EXERCICE 6

Quel est le malware le plus répandu en France ?

REPONSES DES EXERCICES

EXERCICE 1

```
title:Login
```

EXERCICE 2

```
has_screenshot:1 country:FR city:Paris org:Orange
```

EXERCICE 3

```
vuln:CVE-2014-0160 country:fr ssl.version:sslv2

vuln:CVE-2014-0160 org:"OVH"
```

EXERCICE 4

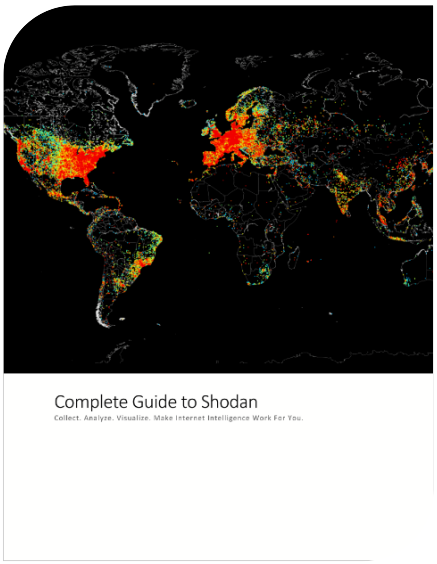
```
category:ics city:"PARIS"
```

EXERCICE 5

```
category:malware country:fr
```

ALLER PLUS LOIN

Shodan.io a un livre qui lui est dédié. Il est très bien expliqué mais en langue Anglaise :



Prix : ~2€

Langue : Anglais

Nombre de pages : ~78

Formats : PDF, ePub, Mobi

Lien d'achat : https://leanpub.com/shodan

Je vous encourage à l'acheter, son prix est faible, mais il contient beaucoup d'informations, utiles pour du Scripting avancé, par exemple.

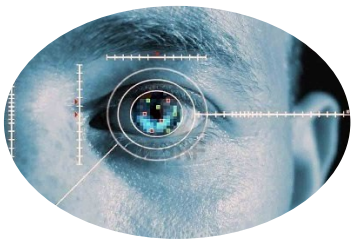
A PROPOS DE L'AUTEUR

Je suis un simple étudiant dans le domaine de la sécurité informatique. J'ai la chance jusqu'à présent de pouvoir travailler dans le domaine qui me plaît et qui est aussi ma passion.

Je suis tombé assez petit dans l'informatique et je me suis orienté vers des études en adéquation avec ma passion, j'ai pu allier mes études et le monde professionnel grâce à un régime d'études en alternance.

Le but majoritaire de mes publications est d'informer et de sensibiliser le grand public à des problématiques qui tournent autour de la sécurité informatique, surtout en ce qui concerne la vie privée.

Je suis actif sur le réseau social Twitter où je partage et publie quelques articles, news sur les sujets précédemment cités.



@SwitHak

Hackademics est une communauté informatique orientée sécurité. Nous sommes des white hackers, pratiquant le white hack. Hackademics met à disposition nombre de tutoriels sur le hacking (*Kali Linux, virus, virologie*), sur le développement et la programmation, sur les différents systèmes (*Linux, Windows, Mac*), sur les réseaux, ainsi que la cryptographie.
Notre communauté Hackademics a été fondée il y a 5 ans, et compte aujourd'hui près de 10 000 membres francophones.

Lien de la communauté : http://hackademics.fr

Twitter de la communauté :

@hackademics_