Threat Intelligence (CTI)

Un ensemble de ressources pour la CTI et comprendre les menaces cyber.

- [CTI] Ressources
- [CTI] Nuclei
- [CTI] Shodan

[CTI] Ressources

Introduction

Plusieurs types de ressources sont nécessaires en CTI, notamment les outils et les frameworks pour collecter ou enrichir vos listes d'IOCs, et les ressources pour comprendre les menaces et connaître les acteurs malveillants.

IOCs

CI Bad Guys

- https://threatfeeds.io/?feed=CI%20Bad%20Guys

Duggytuxy

- https://github.com/duggytuxy/malicious_ip_addresses

Actualités des menaces et CVE

Awesome annual reports

Repos Github actualisé avec les derniers rapports de threat intelligence :

- https://github.com/jacobdjwilson/awesome-annual-security-reports

Malpedia

- https://malpedia.caad.fkie.fraunhofer.de/library

AttackerKB

- https://attackerkb.com/

Krebs on Security

- https://krebsonsecurity.com/

The Hacker News

- https://thehackernews.com/

ThreatPost

- https://threatpost.com/

Dark Reading

- https://www.darkreading.com/

Zeroday Initiative

Permet de suivre les dernières CVE sorties :

- https://www.zerodayinitiative.com/advisories/published/

Onion 666

Permet de trouver les liens vers le dark net

- https://onion666.com/ON66IkM6Ybnv.html
- https://darknet-tor.com/meilleurs-sites-onion-deepweb.php

DeepDarkCTI

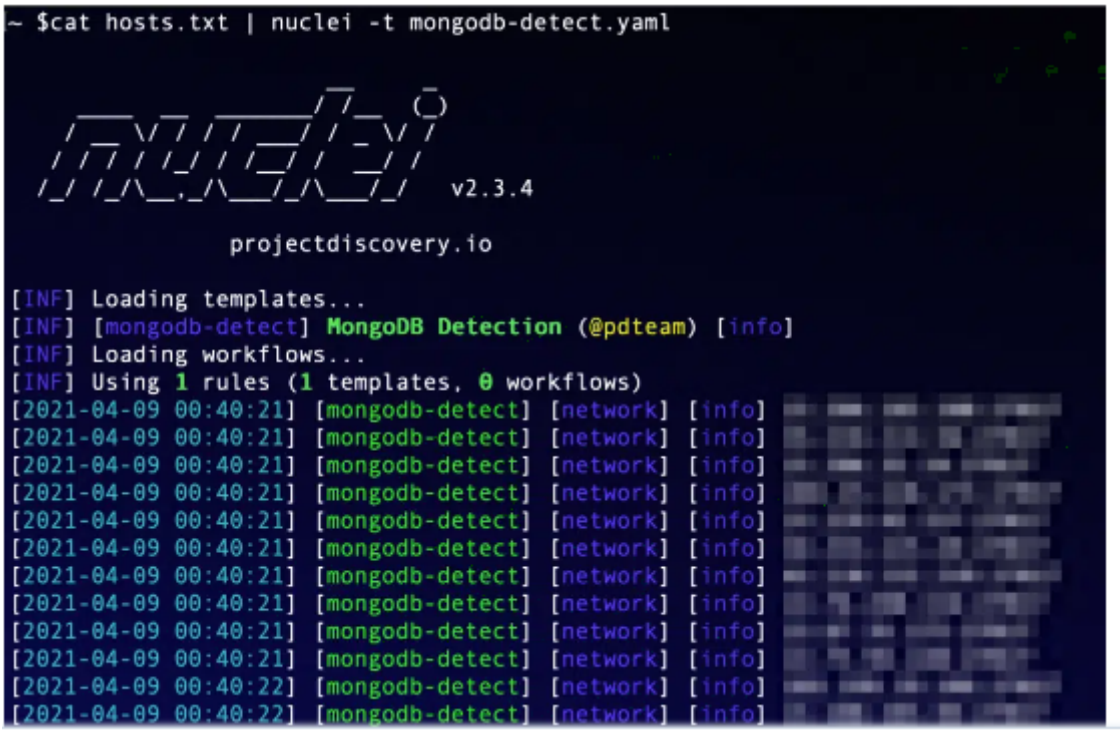
Donne des feeds sombres à suivre vers le darknet, Telegram et autres :

- https://github.com/fastfire/deepdarkCTI

[CTI] Nuclei

Introduction

Le logiciel Nuclei permet de tester l'exploitabilité d'une vulnérabilité sur des systèmes grâce à des templates au format YML.



```
~ $cat hosts.txt | nuclei -t mongodb-detect.yaml

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v2.3.4

                projectdiscovery.io

[INF] Loading templates...
[INF] [mongodb-detect] MongoDB Detection (@pdteam) [info]
[INF] Loading workflows...
[INF] Using 1 rules (1 templates, 0 workflows)
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] [redacted]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:22] [mongodb-detect] [network] [info]
[2021-04-09 00:40:22] [mongodb-detect] [network] [info]
```

Installation & MAJ

Projet

- https://github.com/projectdiscovery/nuclei

Installation

Pour installer Nuclei (go doit être installé au préalable) :

```
go install -v github.com/projectdiscovery/nuclei/v3/cmd/nuclei@latest
```

MAJ

Pour mettre à jour **Nuclei** :

```
nuclei -update
```

Pour mettre à jour les **templates** :

```
nuclei update
```

Manuel

Exemple template

Voici un exemple de template pour une CVE SSH (**cve-2024-6387.yaml**) :

```
id: CVE-2024-6387

info:
  name: RegreSSHion detect (based on software version)
  author: UnaPibaGeek
  severity: High
  description: Regression (CVE-2024-6387) software version checker.
  classification:
    cve-id: CVE-2024-6387
  metadata:
    max-request: 2
    vendor: OpenSSH
    product: OpenSSH
    tags: cve,cve2024,regression,openssh,ssh

tcp:
  - host:
    - '{{Hostname}}'
    - '{{Host}}:22'

    inputs:
      - data: "SSH-2.0-OpenSSH_9.0\r\n"
```

```
  matchers:
    - type: regex
      part: body
      regex:
      - 'OpenSSH_(8\.[5-9]p[1-2]?|9\.[0-7]p[1-2]?|[0-3]\.[0-9]p[1-2]?|4\.[0-3]p[1-2]?)'
```

Liste des cibles

Ici nous ciblerons des adresses IPs que nous indiquerons dans le fichier **ips.txt** :

```
192.168.5.40
```

> En cas d'attaque web, il peut s'agir d'URL et non d'adresse IP.

Exécution d'un template

```
nuclei -t cve-20224-6387.yaml -l ips.txt
```

[CTI] Shodan

Introduction

Shodan est un moteur de recherche permettant de trouver des machines exposées sur Internet avec des filtres.

Manuel

Vous pouvez accéder à l'interface de Shodan :

- https://www.shodan.io/dashboard

Usage

```
<FILTER>:<VALUE>
```

Filtres

Voici quelques filtres courants :

Filtres
ip
port
org
country
city
product
version
os

Sinon voici la liste complète des filtres :

- https://www.shodan.io/search/filters

Exemples

- Chercher des informations sur une IP spécifique :

```
ip:8.8.8.8
```

Chercher toutes les machines françaises de l'hébergeur Scaleway :

```
country:FR org:scaleway
```

Chercher toutes les machines Ubuntu ayant un service SSH :

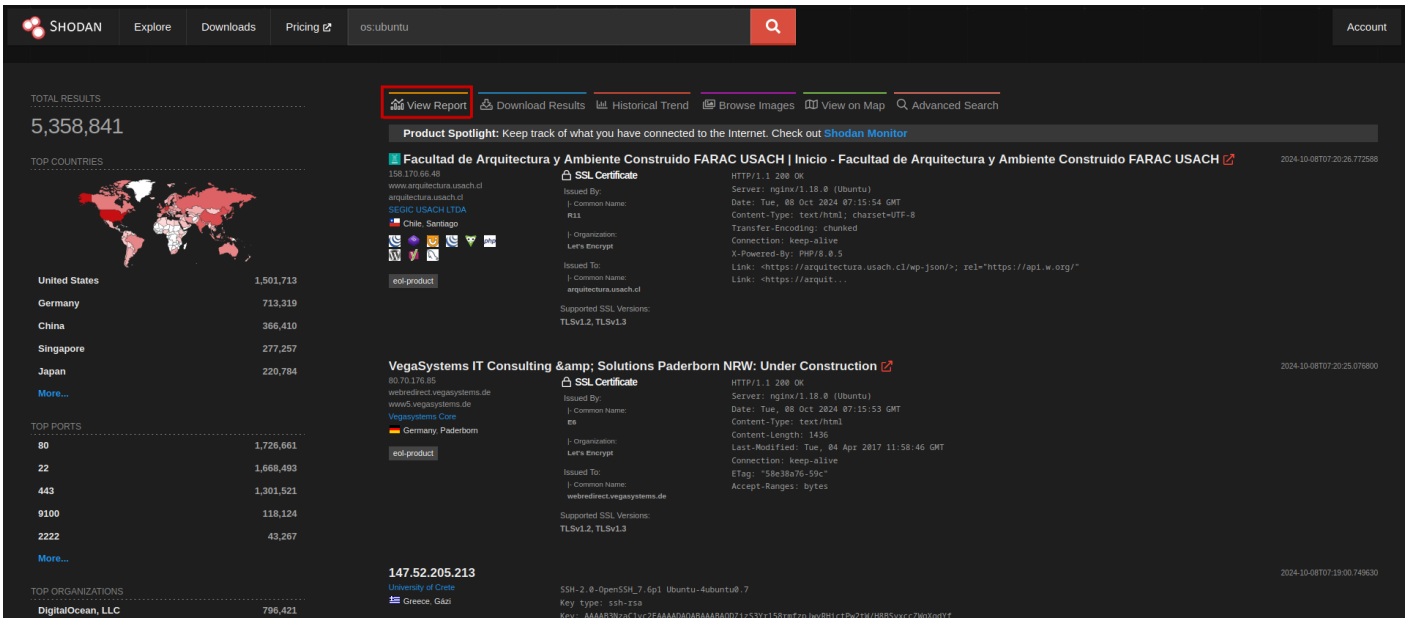
```
os:ubuntu port:22
```

Vous pouvez retrouver plus d'exemples :

- https://www.shodan.io/search/examples
- https://github.com/BushidoUK/OSINT-SearchOperators/blob/main/ShodanQueriesAppliances.csv

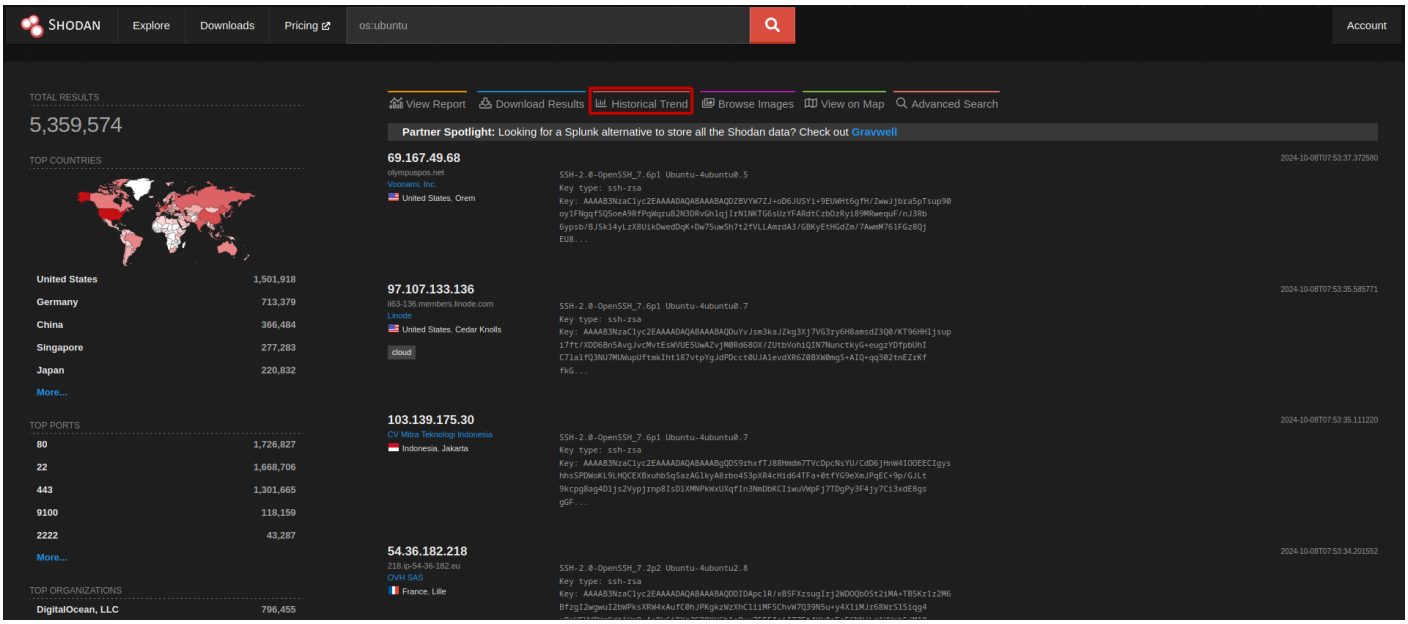
Analyse

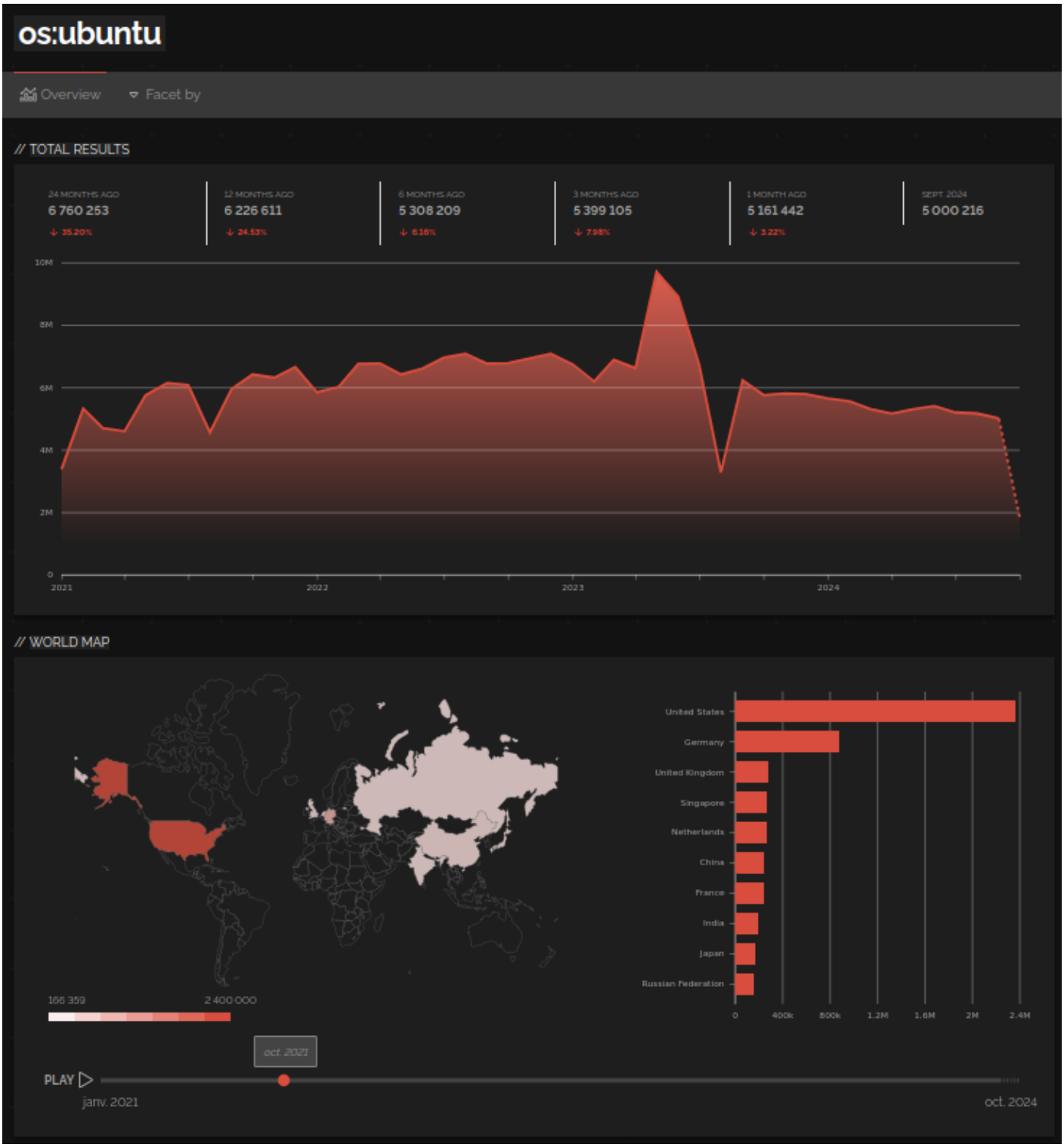
Vous pouvez analyser les résultats rapidement grâce à la section **View Report** :



On voir les ports les plus exposés, les services les plus utilisés, les hébergeurs les plus utilisés pour ces machines etc :

Vous pouvez aussi consulter les statistiques pour cette query dans le temps grâce à l'onglet **Historical Trends** :


SHODAN
Explore
Downloads
Pricing
os:ubuntu
Account
TOTAL RESULTS
5,359,574
TOP COUNTRIES
United States 1,501,918
Germany 713,379
China 366,484
Singapore 277,283
Japan 220,832
More...
TOP PORTS
80 1,726,827
22 1,668,706
443 1,301,665
9100 118,159
2222 43,287
More...
TOP ORGANIZATIONS
DigitalOcean, LLC 796,455
View Report
Download Results
Historical Trend
Browse Images
View on Map
Advanced Search
Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Graywell
69.167.49.68
olympuspos.net
Voonami, Inc.
United States, Orem
2024-10-08T07:53:37.372580
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDZBVYW7ZJ+oD6JUSYi+9EUWHt6gfH/ZwwJjbza5pTsup90
oy1FNgqf5QSoeA9RfPqWqruB2N3DRvGhlqjIrN1NKTG6sUzYFARdtCzbOzRyi89MRwequF/nJ3Rb
6ypsb/BJSk14yLzX8UikDwedDqK+Dw7SuwSh7t2fVLLAmrdA3/GBKyEtHGdZm/7AwmM761FGz8Qj
EU8...
97.107.133.136
li63-136.members.linode.com
Linode
United States, Cedar Knolls
cloud
2024-10-08T07:53:35.585771
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDuYvJsm3kaJZkg3Xj7VG3ry6H8amsdZ3Q0/KT9GHHljsup
i7ft/XDD6BnSAvgJvcMvtEsWVUE5UwAZvjM0Rd68OX/ZUtbVoh1QIN7NunctkyG+eugzYDfpbUhI
C71a1fQ3NU7MUWupUftmkIht187vtpYgJdPDcct0UJA1evdXR6Z08XW0mgS+AIQ+qq302tnEZrKf
fkG...
103.139.175.30
CV Mitra Teknologi Indonesia
Indonesia, Jakarta
2024-10-08T07:53:35.111220
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDS9zhxfTJ88Hmdm7TVcDpcNsYU/CdD6jHnW41OOEECIgys
hns5PDWoKL9LHQCEXBxuhbSqSazAGlkyA8zbo453pXR4cH1dG4TFa+0tfYG9eXmJPqEC+9p/GJLt
9kcpg8ag4Dljs2Vypjrnp81sDlXMNPkWxUXqfIn3NmDbKCIiwuVWpFj7TDgPy3F4jy7C13xdE8gs
gGF...
54.36.182.218
218.ip-54-36-182.eu
OVH SAS
France, Lille
2024-10-08T07:53:34.201552
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDDIDApc1R/xBSFXzsugIrj2WDQbOSt2iMA+TB5Kr1z2M6
BfzgI2wgwuI2bWPksXRW4xAufC0hJPKgkzWzXhC1i1MF5ChvW7Q39N5u+y4X1iMJrG8WrS1S1qg4



Tracking de serveurs C2

Certains filtres ont été mis en place pour chercher des serveurs de commande et contrôle (C2) :

- https://github.com/BushidoUK/OSINT-SearchOperators/blob/main/ShodanAdversaryInfa.md

Serveurs C2	Filtres

Metasploit	http.favicon.hash:-12788697 ssl:MetasploitSelfSignedCA http.html:"msf4"
Cobalt Strike	ssl.jarm:07d14d16d21d21d07c42d41d00041d24a458a375eef0c576d23a7bab9a9fb1 port:443 ssl.cert.serial:146473198 product:"Cobalt Strike Beacon" http.html:"cs4.4"
Brute Ratel	http.html_hash:-1957161625 product:"Brute Ratel C4"

Vous pouvez aussi retrouver des **JARM** de C2 qui sont des empreintes des certificats par défaut :

- https://github.com/BushidoUK/OSINT-SearchOperators/blob/main/ShodanAdversaryInfa.md

API

Pour utiliser l'API, il vous faut payer (une version premium à 69$ payable en une seule fois vous autorise à 100 queries par mois).

Une fois votré clé API récupérée, vous pouvez initialiser shodan :

```
shodan init <API_KEY>
```

Pour faire une recherche :

```
shodan search "<QUERY>"
```

Pour trouver des informations sur une IP :

```
shodan host <IP>
```

Pour télécharger les résultats d'une recherche au format **JSON** :

```
shodan download <OUTPUT>.json "<QUERY>"
```

Pour consulter les résultats :

```
shodan parse <OUTPUT>.json
```

Ou alors :

```
cat <OUTPUT>.json | jq
```