Méthodes de renseignement

OSINT, RECON, TOOLS

OSINT – Définition générale

- Receuillir des informations sur sources ouvertes
- Permet d'obtenir des informations sur une personne
- Permet de d'obtenir des informations sur une entreprise
- Est parfaitement légal et autorisé en europe
- Utilisé en Cybersécurité/CTI mais aussi dans d'autres domaines

OSINT – Types d'informations

- Medias (Journaux, Radio, TV…)
- Web (Blog, réseaux sociaux, forums…
- Données gouvernementales
- Données commerciales (Souvent paya
- Documents indexés (pdf, documents..

OSINT – Limites

- Tout n’est pas indexé
- Les résaux sociaux peuvent être bloqués
- Certaines documents sont confidentiels
- Les zones grises sont nombreuses (limites avec la légalité)
- Même en automatisant, cela demande un temps considérable

RECON – Renseigement semi-légal

- **Permet d'obtenir des informations sur des sources externes**
- **Complète l'OSINT**
- **Utilise diverses API et des bases de leaks**
- **Permet de scrapper des infos sur les entreprises**
- **Nécéssite une protection accrue**

GREYHATS

FRAMEWORK – Présentation des outils Python

- Daprofiler (User, téléphone, Skype, localisation, email)
- Maigret (Recherche par username sur 3000 sites FR)
- MrHolmes (Domaines, User, Phone, Social, email)
- Sherlock (Recherche par username)
- Social Analyzer (Réseaux sociaux, Sites X, Forums obscurs)
- SocialPwned (Recherche de leak via emails)

FRAMEWORK – Google Dorks

- Le premier outils OSINT du monde est GOOGLE
- Dorks est une méthode de recherche avec opérateurs
- Souvent appelé Google Hacking
- Permet d'obenir des infos de manière fine
- Peut dévoiler des informations qui ne devaient pas être indexées
- Automatisation avec « sitedorks » en Python

SITES INTERNET – Les plus courants

- FacecheckID (Retrouve un compte avec une photo)
- Shodan (Information IP et DNS)
- I Have Been PWNED (Base de leak email et phone)
- Netcraft (Annuaire IP et DNS)
- Grep.app (user et git repository)

PROTECTION – Les prérequis

- Utiliser un VPN no logs sans fournir d'informati
- Utiliser un OS minimal (Archlinux ou autre)
- Passer par un routage maillé (TOR)
- Utiliser des comptes emails dédiés (Proton)
- Ne jamais dévoiler son identité
- Automatiser sa relocalisation toutes les 10 min

INSTALLATION – Les indispensables

- Maitriser son OS (Windows est exclu, Unbuntu and co également)
- Installer Python et les dépendances nécéssaires
- Avoir un pare feu restrictif
- Être à l'aise avec le shell
- Configurer et connecter les API nécéssaires
- Savoir effacer ses traces (Utiliser un PC chiffré dédié à l'OSINT)

SCENARIO – ATTAQUANT – PHOTO INCONNU

- **Passage d'une photo sous facecheck ID (obtention du compte)**
- **Passage du pseudo sous DaProfiler (obtention IP, loc, mail, phone)**
- **Passage du pseudo sous Maigret (Obtention des sites internet)**
- **Passage du mail sous Social Analyser (Obtention des réseaux)**

SCENARIO – ATTAQUANT – PSEUDO EMPLOYE

- **Vous le passez sous Daprofiler (obtention IP, loc, mail, phone)**
- **Passage sous SitesDorks (Email et pseudo)**
- **Il travaille à Capgémini (obtention poste, collègues, compétences)**
- **Vous trouvez des données sensibles sur Github**
- **Appel voix masquée de l'utilisateur (obtention map réseaux…)**

SCENARIO – ATTAQUANT – PHISHING

- Vous avez le nom d'une personne (email et tel)
- Vous passez l'email et le tel dans les logiciels
- Vous obtenez la liste des sites louches de l'utilisateur
- Vous envoyez un email du gouvernemment (en lien avec les sites)
- L'amande est payable par bitcoin ou conversion / RIB
- Vous estorquez l'argent et maintenez une suite de mail (Pour éviter le signalement trop rapide aux autorités)

SCENARIO – ATTAQUANT – LE VIRUS

- Vous avez le nom d'une personne (email et tel)
- Vous passez l'email et le tel dans les logiciels
- Vous obtenez des informations sur son entreprise
- Vous trouvez son e-mail pro (via les logiciels)
- Envoi d'un mail de phishing ciblé (ex SG) contenant un virus
- Vous infectez l'entreprise et avez un point d'entrée dans la société

SCENARIO – DEFENSE OFFENSIVE – PHISHING

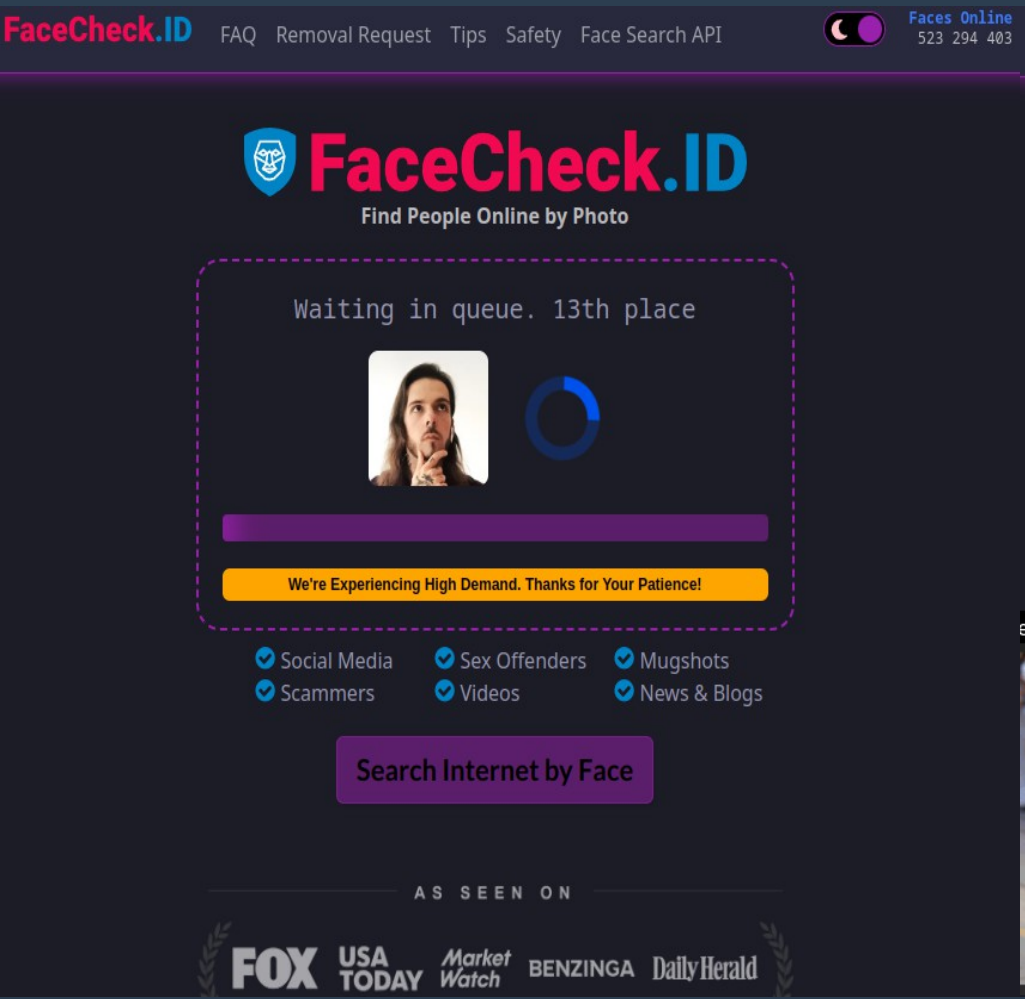
- **Vous réceptionnez un email de phishing**
- **Après analyse vous obtenez les IP associées aux sites**
- **Vous le passez sous les sites (Shodan, Netcraft, Abuse)**
- **Avec la recherche « SiteDorks » vous listez les cas connus**
- **Vous préparez un rapport contenant le plus d'infos possibles**
- **Vous le fournissez à l'équipe de traque et de réponse à incident**

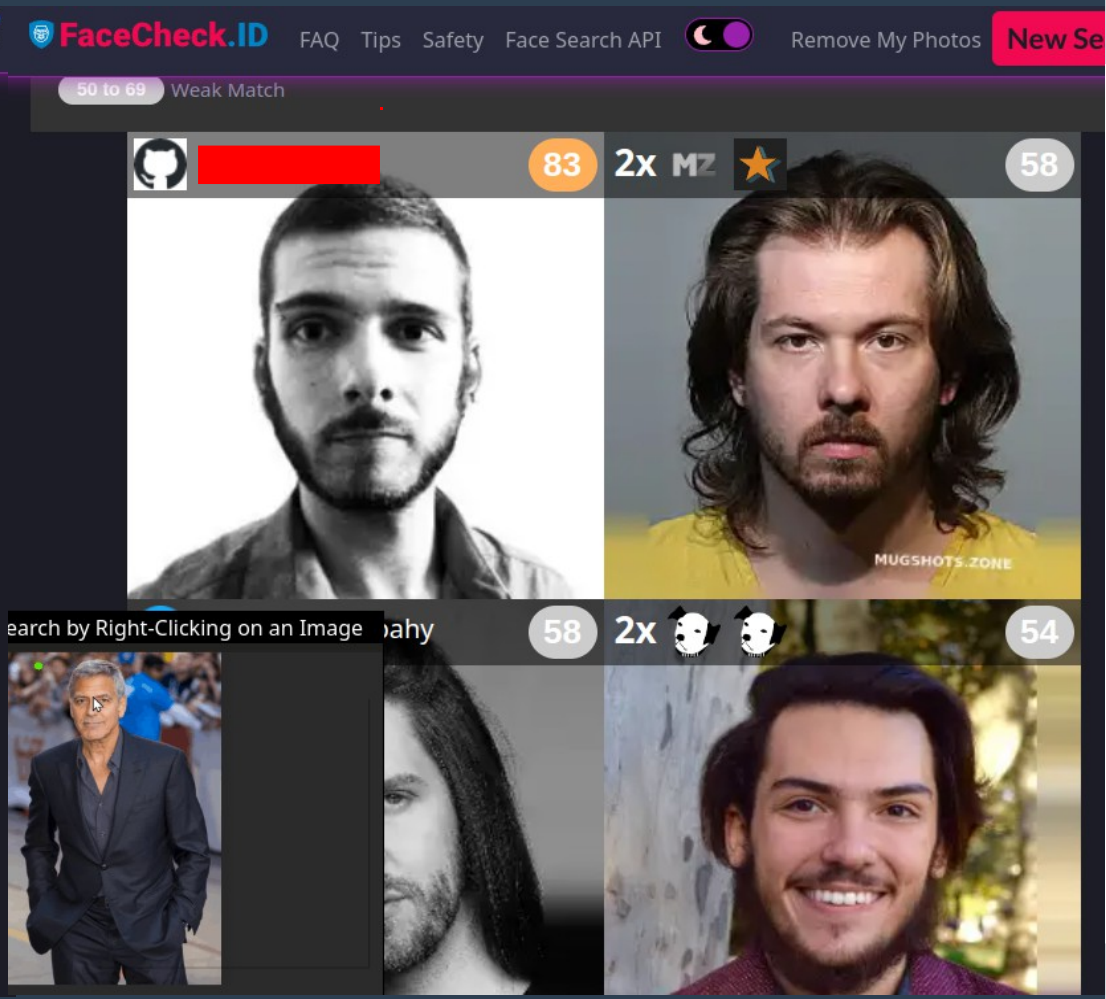
DEMONSTRATION – PHOTO ET ENTREPRISE

- **Cas pratique, retrouver quelqu'un avec une photo et obtenir le plus d'informations possibles**

- **Cas pratique, retrouver le plus d'infos sur une entreprise et en faire un rapport**

ETAPE 1 – FACECHECKID





ETAPE 2 – DaProfiler

Get someone's digital identity anonymously 👻
Made by TheRealDalunacrobate with 💝

```
usage: profiler.py [-h] [-n NAME] [-ln LASTNAME] [-json JSON] [-zp ZP]

options:
  -h, --help            show this help message and exit
  -n NAME, --name NAME  Victim name
  -ln LASTNAME, --lastname LASTNAME
                        Last name of victim
  -json JSON, --json JSON
```

Get someone's digital identity anonymously 👻
Made by TheRealDalunacrobate with 💝

```
🎭 Finding and filtering online identities ...
🎧 Searching for soundcloud profiles ...
   -> Found ! Visit : https://soundcloud.com/search/people?q=[redacted]
📔 Searching for Wattpad profiles ...
   -> Found ! Visit : https://www.wattpad.com/search/[redacted]people
📪 MailBox guessing ...
✅ Ready to be consulted !


benoit mateu
├── Adress - Phone
│   ├── Adress    : [redacted]
│   ├── Full Name : [redacted]
│   └── Phone     : [redacted]
├── Death Records
│   └── (44 ans) | Benoit MATHE | Bouguenais (Loire-Atlantique)
```

ETAPE 3 – Maigret

Username search report for [redacted]

Generated by Maigret at 2023-07-27 15:01:07

Supposed personal data

Fullname: [redacted]

Location: toulouse

Geo: us (3), in (3), cn (1), ao (1), ve (1), eg (1), ru (1)

Interests: photo (5), sharing (3), gaming (3), coding (2), art (1), reading (1), writing (1), tech (1)

First seen: 2020-03-26T10:07:59Z

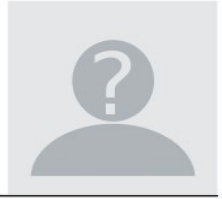
Brief

Search by username[redacted] returned 17 accounts. Found target's other IDs: 76561198112239620 (steam_id).
Search by steam_id 76561198112239620 returned 2 accounts. Extended info extracted from 5 accounts.

Invalid?

GitHubGist

Tags: coding, sharing
https://gist.github.com/[redacted]



Invalid?

GitHub

Tags: coding
https://github.com/[redacted]

Details

Uid	62696671
Created at	2020-03-26T10:07:59Z

```
~/l/O/maigret  main !91  python3 maigret.py "redgears33" --pdf  1m 11s
[-] Starting a search on top 500 sites from the Maigret database...
[!] You can run search by full list of sites with flag `-a`
[*] Checking username redgears33 on:
[+] GitHubGist [GitHub]: https://gist.github.com/[redacted]
[+] GitHub: https://github.com/[redacted]
 ├─uid: 62696671
 ├─image: https://avatars.githubusercontent.com/u/[redacted]=4
 ├─created_at: 2020-03-26T10:07:59Z
 ├─follower_count: 0
 ├─following_count: 0
 ├─public_gists_count: 0
 └─public_repos_count: 3
[+] Pinterest: https://www.pinterest.com/[redacted]/
[+] Steam: https://steamcommunity.com/id/[redacted]
 ├─steam_id: 76561198112239620
 ├─nickname: [redacted]†
 └─username: [redacted]
[+] Ultimate-Guitar: https://ultimate-guitar.com/u/[redacted]
[+] Wattpad: https://www.wattpad.com/user/[redacted]
[+] Zhihu: https://www.zhihu.com/people/[redacted]
[+] Ccm: https://ccm.net/profile/user/[redacted]
[+] Gravatar: http://en.gravatar.com/[redacted]
 ├─image: https://1.gravatar.com/avatar/71d40434277f1b4e10d5ae60968d73c7
 ├─username: [redacted]
 ├─name: [redacted]
 ├─gravatar_url: https://gravatar.com/71d40434277f1b4e10d5ae[redacted]
 ├─gravatar_username: [redacted]
 └─gravatar_email_md5_hash: 71d40434277f1b4e10d5ae60968d73c7
[+] AskFM: https://ask.fm/[redacted]
 ├─username: [redacted]
 ├─fullname: ben
 ├─posts_count: 3
 ├─likes_count: 0
 ├─image: https://casts.ask.fm/assets/noAvatar-2325eb51f8abe4e4678a25b16cb32a5399e84d9e82b5bc7efcc0b
2[redacted]
 └─location: toulouse
[+] Picuki [Instagram]: https://www.picuki.com/profile/[redacted]
[+] F6S: https://www.f6s.com/[redacted]
[+] Speedrun.com: https://speedrun.com/user/[redacted]
[+] ImageShack: https://imageshack.com/user/[redacted]
```

ETAPE 4 – SHERLOCK

```
~/l/O/sherlock/sherlock  master !37  python3 sherlock.py -h  1m 36s
sage: sherlock.py [-h] [--version] [--verbose] [--folderoutput FOLDEROUTPUT] [--output OUTPUT]
                  [--tor] [--unique-tor] [--csv] [--xlsx] [--site SITE_NAME] [--proxy PROXY_URL]
                  [--json JSON_FILE] [--timeout TIMEOUT] [--print-all] [--print-found] [--no-color]
                  [--browse] [--local] [--nsfw]
                  USERNAMES [USERNAMES ...]

herlock: Find Usernames Across Social Networks (Version 0.14.3)

ositional arguments:
 USERNAMES             One or more usernames to check with social networks. Check similar usernames
                       using {%} (replace to '_', '-', '.').

ptions:
 -h, --help            show this help message and exit
 --version             Display version information and dependencies.
 --verbose, -v, -d, --debug
                       Display extra debugging information and metrics.
 --folderoutput FOLDEROUTPUT, -fo FOLDEROUTPUT
                       If using multiple usernames, the output of the results will be saved to this
                       folder.
 --output OUTPUT, -o OUTPUT
                       If using single username, the output of the result will be saved to this file
 --tor, -t             Make requests over Tor; increases runtime; requires Tor to be installed and i
                       system path.
 --unique-tor, -u      Make requests over Tor with new Tor circuit after each request; increases
                       runtime; requires Tor to be installed and in system path.
 --csv                 Create Comma-Separated Values (CSV) File.
 --xlsx                Create the standard file for the modern Microsoft Excel spreadsheet (xslx).
 --site SITE_NAME      Limit analysis to just the listed sites. Add multiple options to specify more
                       than one site.
 --proxy PROXY_URL, -p PROXY_URL
                       Make requests over a proxy. e.g. socks5://127.0.0.1:1080
 --json JSON_FILE, -j JSON_FILE
                       Load data from a JSON file or an online, valid, JSON file.
 --timeout TIMEOUT     Time (in seconds) to wait for response to requests (Default: 60)
```

A	B	C	
username	name	url_main	url_user
[redacted]	AllMyLinks	https://allmylinks.com/	https://allmylinks.com/r
[redacted]	Enjin	https://www.enjin.com/	https://www.enjin.com/p
[redacted]	Fiverr	https://www.fiverr.com/	https://www.fiverr.com/r
[redacted]	Flickr	https://www.flickr.com/	https://www.flickr.com/p
[redacted]	Freelancer	https://www.freelancer.com/	https://www.freelancer.c
[redacted]	G2G	https://www.g2g.com/	https://www.g2g.com/re
[redacted]	GunsAndAmmo	https://gunsandammo.com/	https://forums.gunsanda
[redacted]	IRL	https://www.irl.com/	https://www.irl.com[redacted]
[redacted]	Quizlet	https://quizlet.com	https://quizlet.com[redacted]
[redacted]	Speedrun.com	https://speedrun.com/	https://speedrun.com/us
[redacted]	Spotify	https://open.spotify.com/	https://open.spotify.com
[redacted]	Twitch	https://www.twitch.tv/	https://www.twitch.tv/re
[redacted]	Wikipedia	https://www.wikipedia.org/	https://en.wikipedia.org/
[redacted]	ebio.gg	https:/ebio.gg	https://ebio.gg/[redacted]
[redacted]	jeuxvideo	http://www.jeuxvideo.com	http://www.jeuxvideo.co

ETAPE 5 – Social Analyzer

```
~/l/O/social-analyzer  main  python3 app.py --username
[init] Detections are updated very often, make sure to get the most up
[init] languages.json looks good!
[init] sites.json looks good!
[init] languages.json & sites.json loaded successfully
[Init] Selected websites: 999
[Info] username: [redacted]
[Checking] 24.wikia.com
[Checking] 500px.com
[Checking] admireme.vip
[Checking] airbit.com
[Checking] 7cups.com
[Checking] aahachat.org
[Checking] akniga.org
[Checking] adore.one
[Checking] 9gag.com
[Checking] airlinepilot.life
[Checking] 8tracks.com
[Waiting to retry] adore.one
[Checking] about.me
[Checking] airliners.net
[Checking] adultism.com
[Waiting to retry] adultism.com
[Checking] akbrny.com
[Checking] alik.cz
[Checking] alleywatch.com
[Checking] aliveshoes.com
[Checking] algowiki-project.org
[Checking] alimero.ru
[Checking] allthingsworn.com
[Checking] allmylinks.com
[Checking] angel.co
[Checking] anar.biz
```

```
[Detected] 11 Profile[s]
-----------------------
found        : 2
link         : https://career.habr.com/[redacted]
rate         : %100.0
status       : good
title        : Хабр Карьера
language     : Russian
country      : Russia
rank         : 1848
text         : Хабр Карьера Все сервисы Хабра Сообщество IT-специалистов Ответы на любые воп
рофессиональное развитие в IT Удаленная работа для IT-специалистов Войти Войти через Хабр Ак
стрироваться Вакансии Специалисты Эксперты Компании Рейтинг Зарплаты Образование Журнал Ошиб
жно, эта страница уже нашла работу мечты и\xa0закрыла свой профиль.\n К\xa0счастью,\xa0у\xa0
угих страниц. На главную страницу О сервисе Услуги и цены Каталог профессий Контакты Помощь
ля Для работодателя API сервиса Служба поддержки Документы Соглашение с пользователем Правил
слуг Прайс-лист Следите за нами в соцсетях Сейчас на сайте 3992 вакансии и 259713 резюме, в
ткликов на вакансию ©\xa0Habr Другие проекты Хабра Хабр Q&A Фриланс
type         : Computers Electronics and Technology > Computers Electronics and Technology
-----------------------
found        : 2
link         : https://countable.us/[redacted]
rate         : %100.0
status       : good
title        : unavailable
language     : unavailable
country      : unavailable
rank         : unavailable
text         : unavailable
type         : Internet
-----------------------
found        : 2
link         : https://es.pixilart.com/[redacted]
rate         : %100.0
status       : good
title        : filtered
language     : Spanish
country      : United Kingdom
rank         : 19254
```

ETAPE 6 – MR HOLMES

```
-------------------------------------------------------------------------------
|                              MR.HOLMES
|       ,_
|     ,'  `\,_            ______________________________________________
|     |_,-'_)            / I know, my dear Watson,                      |
|     /##c '\  (       /  that you share my love of all                 |
|     ' |'  -{.  ) /    that is bizarre and outside the conventions     |
|     /\__-' \[]   |    and humdrum routine of daily life.              |
|     /`-_`\       |____________________________________________________|
|     '     \
|
| A COMPLETE OSINT TOOL:)         CODED BY LUCKSI
|
|[+]VERSION:T.G.D-1.0.3
|Instagram:lucks_022
|Email:lukege287@gmail.com
|GitHub:Lucksi
|Twitter:@Lucksi_22
|Linkedin:https://www.linkedin.com/in/Lucksi
-------------------------------------------------------------------------------
[INSERT AN OPTION 'PRESS 0 TO REFRESH THE QUOTE']
(1)SOCIAL-ACCOUNT-OSINT         (2)PHONE-NUMBER-OSINT          (11
(3)DOMAIN/IP-OSINT              (4)CONFIGURATION               (12
(5)DATABASE(GUI)                (6)UPDATE                      (13
(7)PORT-SCANNER                 (8)E-MAIL                      (14
```

```
[I]DATE-FORMAT:[EU:DD/MM/YY]

[+]CHECKING IF [redacted] IS A VALID EMAIL
[v]THIS EMAIL IS VALID

[+]GENERATING HaveiBeenPowned LINK
[v]https://api.haveibeenpwned.com/unifiedsearch/[redacted]

[+]GENERATING IntelligenceX LINK
[v]https://intelx.io/?s=mateu.benoit@outlook.fr

[+]SEARCHING WHOIS INFORMATION FOR mateu.benoit@outlook.fr
[!]API-KEY NOT FOUND

[?]WOULD YOU LIKE TO PERFORM A GOOGLE/YANDEX DORK SEARCH?(1)YES(2)NO

[#MR.HOLMES#]-->1

[I]REMOVE OLD mateu.benoit@outlook.fr_Dorks.txt

[+]GENERATING POSSIBLE GOOGLE DORKS LINK...
[v][GENERAL-DORKS]:
[v]---------------------------------------------------------------------
----------------
[v]| https://www.google.com/search?q=intext:[redacted]
[v]| https://www.google.com/search?q=intext:([redacted])filetype:txt
[v]| https://www.google.com/search?q=intext:([redacted])filetype:csv
[v]| https://www.google.com/search?q=intext:([redacted])filetype:pdf
[v]| https://www.google.com/search?q=intext:([redacted])filetype:doc
[v]| https://www.google.com/search?q=intext:([redacted])filetype:docx
[v]| https://www.google.com/search?q=intext:([redacted])filetype:log
```

ETAPE 6 – MR HOLMES

```
[+]SCANNING NUMBER: +33640411462...

[I]THIS IS PROBABLY A REAL PHONE NUMBER

[v]INTERNATIONAL NUMBER: [redacted]
[v]LOCAL NUMBER: [redacted]
[v]COUNTRY PREFIX: +33
[v]COUNTRY CODE: FR
[v]COUNTRY: France
[v]AREA/ZONE: France
[v]CARRIER/ISP: Orange France
[v]TIMEZONE N°1: Europe/Paris

[v]AREA FOUND

[+]CHECKING NUMBER [redacted] APPROXIMATE GEOLOCATION
[v]LATITUDE: 46.603354
[v]LONGITUDE: 1.8883335
[v]GOOGLE MAPS LINK: https://www.google.it/maps/place/46.603354,1.8883335
[I]MAP SAVED ON: GUI/Reports/Phone/+33640411462/Area_GeoLocation.html

[v]TIMEZONE FOUND

[+]CHECKING NUMBER [redacted] APPROXIMATE GEOLOCATION
[v]LATITUDE: 48.8534951
[v]LONGITUDE: 2.3483915
[v]GOOGLE MAPS LINK: https://www.google.it/maps/place/48.8534951,2.3483915
[I]MAP SAVED ON: GUI/Reports/Phone/[redacted]Zone_GeoLocation.html

[+]CHECKING THE AFFIDABILITY OF THE NUMBER

[v]THIS NUMBER EXIST OR IS A VOIP NUMBER
```

```
[I]DATE-FORMAT:[EU:DD/MM/YY]

[+]SEARCH INFORMATION FOR: 8.8.8.8

[v]IP: 8.8.8.8
[v]NATION: United States
[v]NATION-CODE: US
[v]REGION-CODE: VA
[v]REGION-NAME: Virginia
[v]CITY: Ashburn
[v]TIMEZONE: America/New_York
[v]ISP: Google LLC
[v]ORG: Google Public DNS
[v]AS: AS15169 Google LLC
[v]LAT: 39.03
[v]LONG: -77.5
[v]ZIP/POSTAL-CODE: 20149

[+]GENERATING GOOGLE MAPS LINK...
[v]https://www.google.com/maps/place/39.03,-77.5
[I]MAP SAVED ON: GUI/Reports/Websites/Coordinates/Ip_Geolocation/8.8.8.8.

[+]WOULD YOU LIKE TO PERFORM A WHOIS LOOKUP?(1)SI(2)NO

[#MR.HOLMES#]-->
```

ETAPE 7 – GOOGLE HACKING (sitesdorks)

```
O/sitedorks  master  python3 sitedorks.py -query "Benoit Mateu" -count
ing -cat can open a whole lot of tabs/windows in your browser. Do you want to c

v.google.com/search?num=100&filter=0&q=Benoit%20Mateu+AND+(site:1drv.ms+|+site:
s.org+|+site:8kun.top+|+site:9gag.com+|+site:about.me+|+site:academia.edu+|+sit
iredby.co+|+site:activehosted.com+|+site:adobecqms.net+|+site:adoc.pub+|+site:a
n+|+site:amazonaws.com+|+site:anzdoc.com+|+site:apiary.io+|+site:apollo.io+|+si
 link+|+site:appdomain.cloud+|+site:apps.apple.com+|+site:apps.fcc.gov+|+site:a
io+|+site:aptoide.com+|+site:arcgis.com+|+site:atlassian.net+|+site:awstrack.me
 azure-api.net+|+site:azurecontainer.io+|+site:azureedge.net+|+site:azurefd.net
+|+site:azurewebsites.windows.net+|+site:b2b.getemail.io+|+site:b2clogin.com+|+
te:badgr.com/public
v.google.com/search?num=100&filter=0&q=Benoit%20Mateu+AND+(site:badgr.io/public
bamboohr.com/jobs+|+site:b-cdn.net+|+site:bcert.me+|+site:bcwt.webex.com+|+site
+|+site:bit.ly+|+site:bitly.com+|+site:bitbucket.org+|+site:bitchute.com+|+site
ckboard.com+|+site:blogspot.com+|+site:bluejeans.com+|+site:bmetrack.com+|+site
e:boards.4chan.org+|+site:books.google.com+|+site:boosty.to+|+site:box.net/shar
business.site+|+site:buymeacoffee.com+|+site:cdn.cloudflare.net+|+site:censys.i
e:chat.whatsapp.com+|+site:chegg.com/flashcards+|+site:ci.appveyor.com+|+site:c
dimensions.com/c+|+site:click.mlsend.com/link+|+site:clicktime.symantec.com+|+s
te:cloud.ovh.net+|+site:cloudapp.azure.com+|+site:cloudapp.net+|+site:cloudform
v.google.com/search?num=100&filter=0&q=Benoit%20Mateu+AND+(site:cloudfront.net+
+|+site:cmail19.com/t+|+site:cmail20.com/t+|+site:code.google.com+|+site:codebe
 io/gh+|+site:codepad.co+|+site:codepad.org+|+site:codepen.io+|+site:codeprojec
+|+site:coggle.it+|+site:cognitodocs.com+|+site:colab.research.google.com+|+sit
munity.spiceworks.com+|+site:comparably.com/companies+|+site:compliancerank.com
 convertkit-mail.com+|+site:convertkit-mail2.com+|+site:cookiepedia.co.uk+|+sit
windows.net+|+site:coursera.org/account/accomplishments+|+site:cram.com/flashca
+|+site:credly.com/badges+|+site:crunchbase.com+|+site:cupdf.com/document+|+sit
t.ly+|+site:d.sendibm3.com+|+site:dailymotion.com+|+site:dev.azure.com+|+site:d
```

Benoit Mateu AND (site:1drv.ms | site:4channel.org | site:4plebs.org | site:8kun.top | site:9gag.com | site:about.me | site:academia.edu | site:acemlnb.com | site:acquiredby.co | site:activehosted.com |

résultats (0,53 secondes)

Benoit Mateu AND (site:badgr.io/public | site:badoo.com | site:bamboohr.com/jobs | site:b-cdn.net | site:bcert.me | site:bcwt.webex.com | site:bgp.he.net | site:bit.do | site:bit.ly | site:bitly.com |

résultats (0,53 secondes)

Benoit Mateu AND (site:drive.google.com | site:dropbox.com/s | site:dyno.gg/server | site:e.customeriomail.com | site:ecitydoc.com | site:edgekey.net | site:edgesuite.net |

BONUS – NETCRAFT

ft

Search Web by Domain

xplore websites visited by users of the **Netcraft extensions**

Site contains | Capgemini

Example: site contains .netcraft.com

SEARCH

Search tips

netcraft

Hostnames matching capgemini

▸ Search with another pattern?

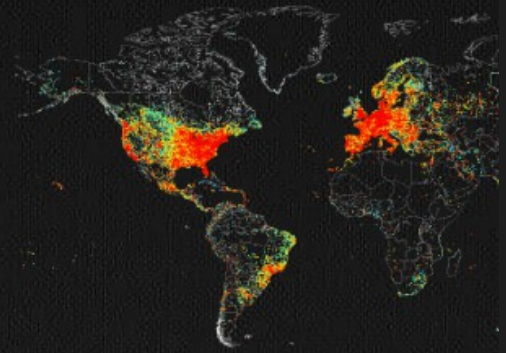
60 results (showing 1 to 20)

Rank	Site	First seen	Netblock	OS
17819	www.**capgemini**.com	October 2009	Amazon.com, Inc.	Linux
22926	signincert.**capgemini**.com	August 2021	A100 ROW GmbH	Linux
26443	signin.**capgemini**.com	October 2011	A100 ROW GmbH	Linux
43145	**capgemini**.tekstac.com	April 2023	Amazon Data Services India	unknown
50800	jobs.**capgemini**.com	April 2016	SAP	unknown
54724	**capgemini**.sharepoint.com	June 2017	Microsoft Corporation	Windows Serve

BONUS – SHODAN

SHODAN | Explore | Pricing | CAPGEMINI

Search Engine for the Internet of Everything



Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

SIGN UP NOW

View Report | Browse Images | View on Map

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

107.23.173.149 2023-07-25T18:31:22.842081

ec2-107-23-173-149.compute-1.amazonaws.com
Amazon.com, Inc.
United States, Ashburn

cloud
self-signed

SSL Certificate

Issued By:
|- Common Name: WSAMZN-GQA6I6TR.capgemini.workspace.com

Issued To:
|- Common Name: WSAMZN-GQA6I6TR.capgemini.workspace.com

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

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\:
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1607)/Windows Server 2016 (version 1
  OS Build: 10.0.14393
  Target Name: CAPGEMINI
  NetBIOS Domain Name: CAPGEMINI
  NetBIOS Comput...
```

144.76.117.22 2023-07-25T11:52:56.075730

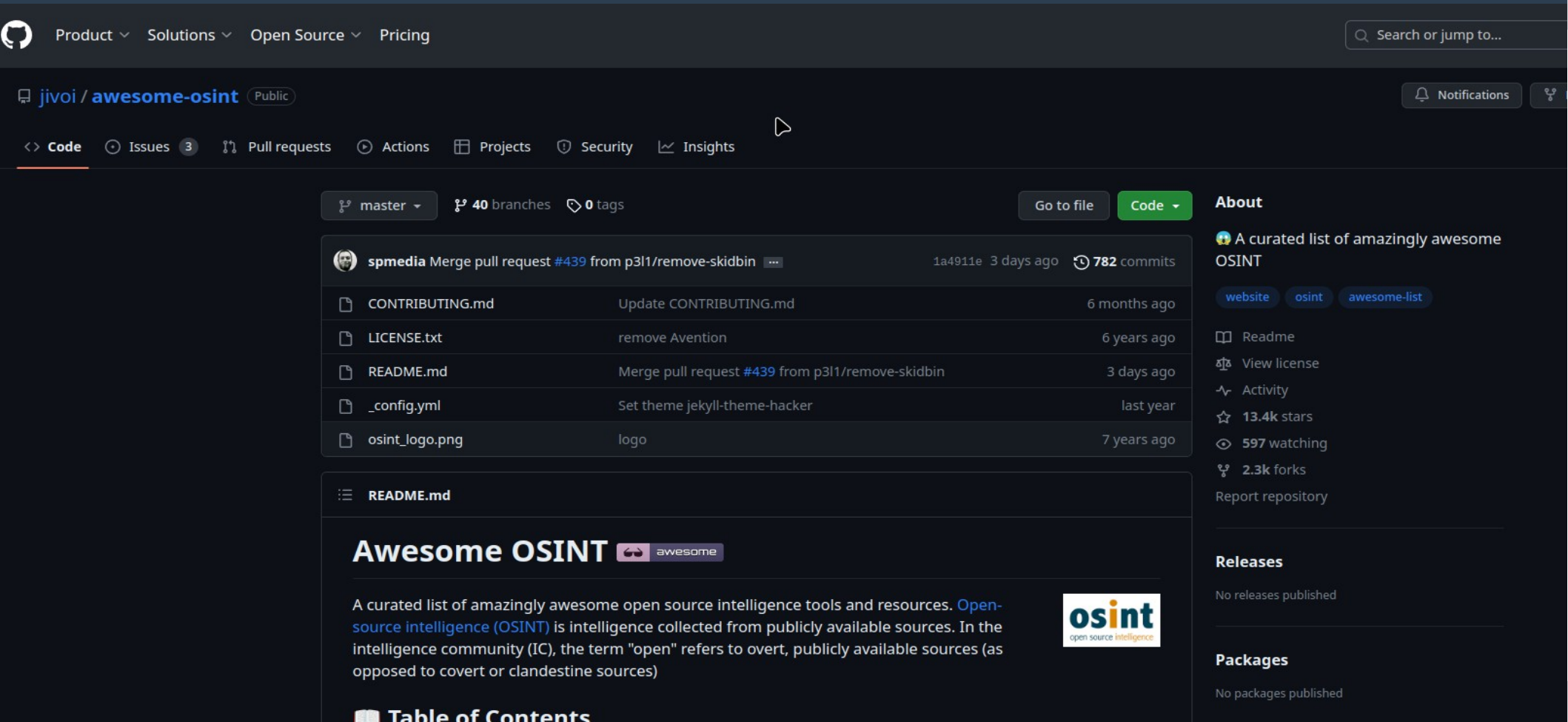
Hetzner Online GmbH
Germany, Falkenstein

SSL Certificate

Issued By:
|- Common

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\:
Remote Desktop Protocol NTLM Info:
  OS: Windows 8/Windows Server 2012
```

BONUS – LE BEST GITHUB



METHODOLOGIE – BONNE PRATIQUE

- Pensez à toujours générer des rapports (PDF,CSV, HTML…)
- Un seul logiciel ne vous fournira qu'une partie des informations
- Le principe de « Pivotage » est recommandé
- D'une ip, vous obtenez un mail, une localisation…
- En pivotant, vous trouverez les pseudos, conversations, documents
- Plus vous affinerez, plus vous aurez des résultats précis

DISCLAIMER – ZONE GRISE

- FacecheckID n’est pas RGDP (legal hors UE)
- Ces méthodes ne doivent pas servir à des fins criminelles
- Utiliser ces outils vous expose à des risques
- Franchir la limite de la zone grise peut exposer à des poursuites
- Il est possible d’aller plus loin avec des outils de pentesting
- Chaque action est traçable, même avec les meilleurs outils
- L’erreur est toujours humaine et vous en ferez

POUR ALLER PLUS LOIN

Quelques chaines/videos Youtube que je recommande :

- **HACKBACK**
- **OSINT : enquêteurs du net ou nouveaux espions ?**
- **SANDOZ (Bonus parce que drôle)**