Open **S**ource **INT**elligence
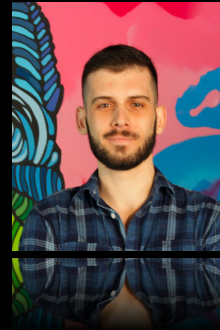
$ whoami

@dpuente-

@darodrig

Índice

CYBER
SEC 42

Tipos de inteligencia

SIGINT   Signal Intelligence

                Telefonía, radiofrecuencia

MASINT   Measurement and Signature

                Radar, Sónar, Acústica, Química, Biológica

HUMINT   Human Intelligence

                Agentes, informadores

IMINT   Imagery intelligence

                Satélites, videovigilancia

OSINT   Open Source Intelligence

CYBER SEC 42

OSINT

FUENTES ABIERTAS

Desde

Leyes
Estadísticas demográficas
Medios de comunicación
Presupuestos
Perfiles psicológicos
Análisis grafológicos
Boletines oficiales (BOE, BOCM)
Multas, concursos públicos

Hasta

Imágenes en redes sociales
Tweets
Metadatos de archivos
Reseñas de compras, restaurantes
Repositorios de código
Brechas de datos
Actividad en foros

CYBER SEC 42

Google Dorks

```
| Buscar archivos restringidos del gobierno |
---------------------------------------------
$ site:gov filetype:pdf allintitle:restricted

| Buscar brechas de de una página que contengan contraseñas y logins |
----------------------------------------------------------------------
$ filetype:txt site:web.com
password|passwords|contraseñas|login|contraseña

| Buscar usuarios y contraseñas de bases de datos |
---------------------------------------------------
DB USERNAME filetype:env
DB_PASSWORD filetype:enc=v

| Buscar documentos que contengan la palabra confidencial |
-----------------------------------------------------------
$ inurl:webkeyword filetype:doc confidential

| Busca feeds de cámaras de seguridad|
--------------------------------------
inurl:"ViewerFrame?Mode="
```
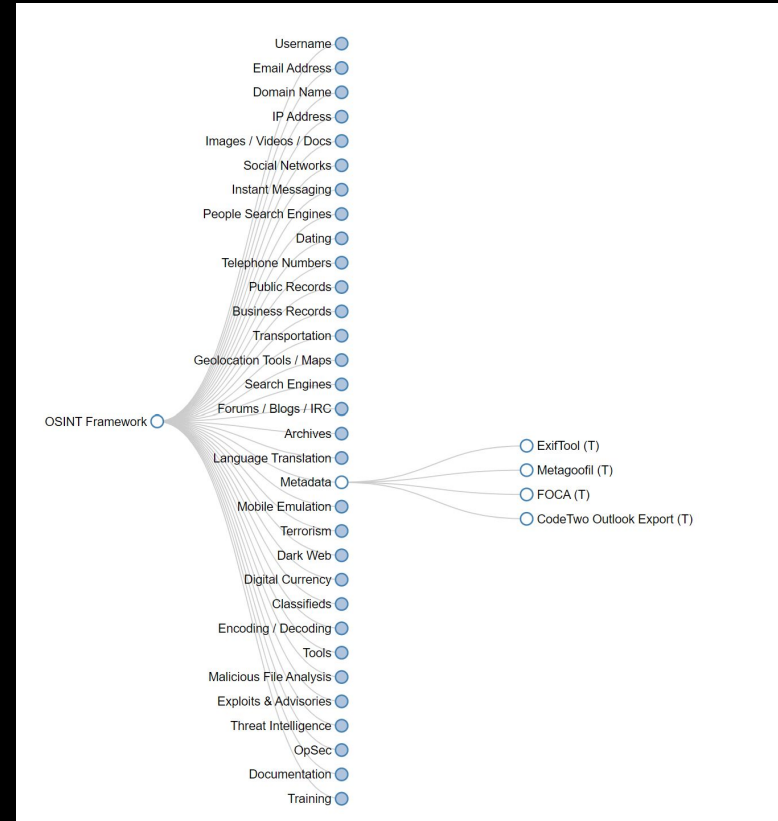
CYBER SEC 42

Osint Framework

https://bevigil.com/osint-api

Osintgram


```
 _____        .--      __
\_____  \  _____|_|____/  |_  _____  _____
 /   |   \ /  ___\|  |\   __\/  __ \_  __ \  \/  /
/    |    \\___ \|  |  |  |  \  ___/|  | \/   /
_____  /____  >__|__|  /__|   \___  >__|  /___/\ \
        \/     \/       \/          \/      \/     \/


Version x.x - Developed by Giuseppe Criscione

Type 'list' to show all allowed commands
Type 'FILE=y' to save results to files like '<target username>_<command>.txt
(default is disabled)'
Type 'FILE=n' to disable saving to files
Type 'JSON=y' to export results to a JSON files like '<target
username>_<command>.json (default is disabled)'
Type 'JSON=n' to disable exporting to files

Attempt to login...

Logged as example@example.com. Target: example_user [1234567890] [NOT FOLLOWING]

Run a command:
```

```
- addrs          Get all registered addressed by target photos
- captions       Get user's photos captions
- comments       Get total comments of target's posts
- followers      Get target followers
- followings     Get users followed by target
- fwersemail     Get email of target followers
- fwingsemail    Get email of users followed by target
- fwersnumber    Get phone number of target followers
- fwingsnumber   Get phone number of users followed by target
- hashtags       Get hashtags used by target
- info           Get target info
- likes          Get total likes of target's posts
- mediatype      Get user's posts type (photo or video)
- photodes       Get description of target's photos
- photos         Download user's photos in output folder
- propic         Download user's profile picture
- stories        Download user's stories
- tagged         Get list of users tagged by target
- wcommented     Get a list of user who commented target's photos
- wtagged        Get a list of user who tagged target
```

CYBER SEC 42

Sherlock

```
♥ sherlock ❯
```

```
# clone the repo
$ git clone https://github.com/sherlock-project/sherlock.git

# change the working directory to sherlock
$ cd sherlock

# install the requirements
$ python3 -m pip install -r requirements.txt

#####################


$ python3 sherlock username


# --tor, -t | --unique-tor, -u

# --site SITE_NAME

# --verbose

# multiple usernames
```
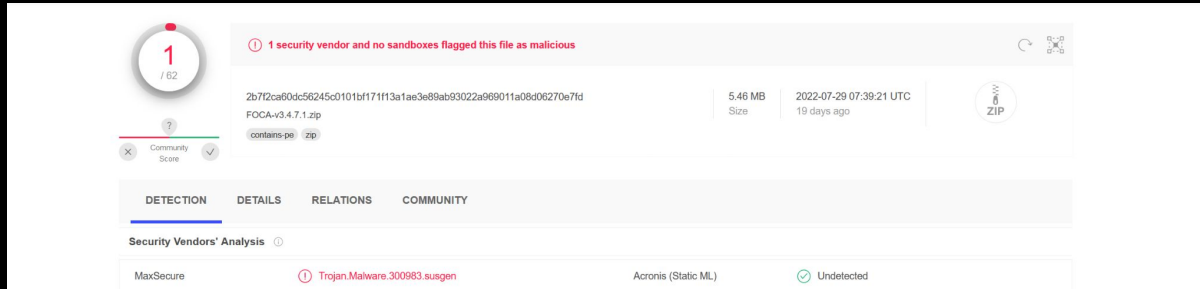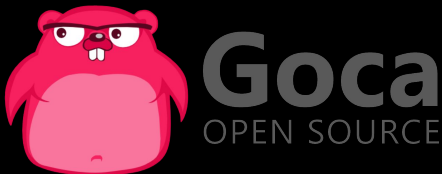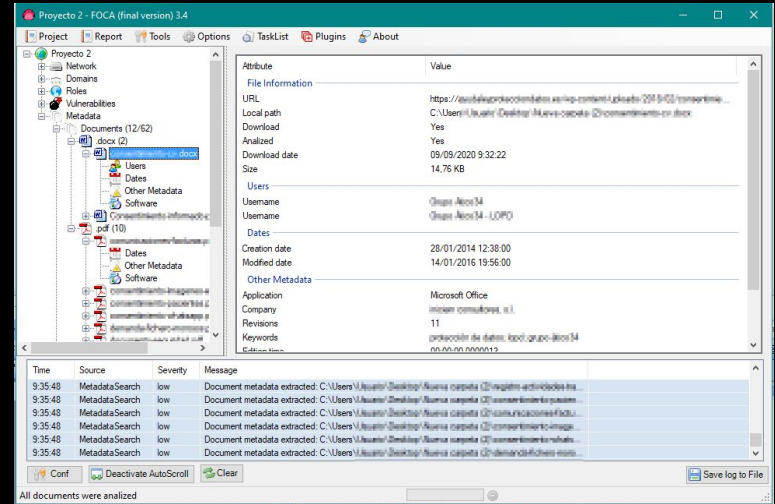
CYBER
SEC 42

File Osint

Goca
OPEN SOURCE

ExifTool
TOOL FOR READING, WRITING AND EDITING META INFORMATION IN FILES
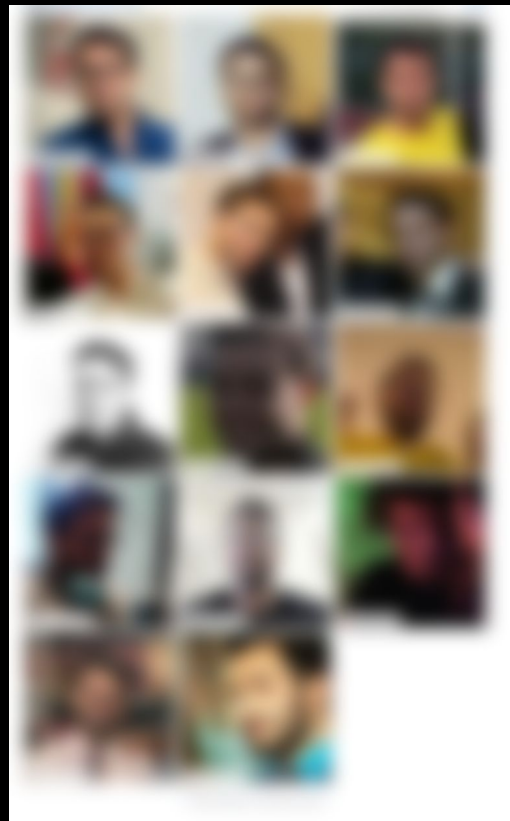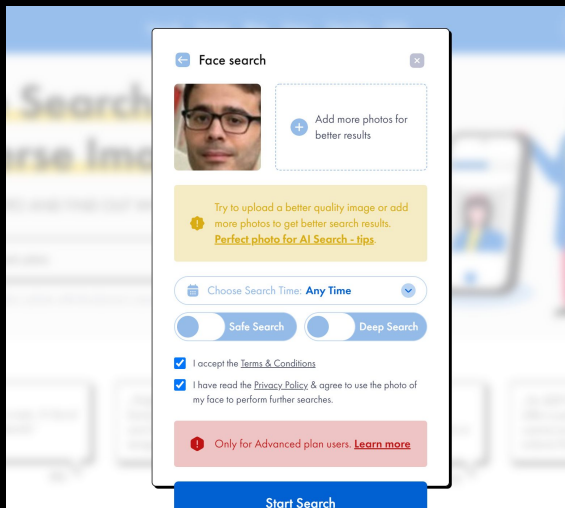
Metagoofil 2.2

FOCA / GOCA

PimEyes: reconocimiento facial

pimeyes.com

PimEyes: reconocimiento facial

- Busca solamente en lugares públicos
- Límite diario en versión gratuita
- No indexa redes sociales como Instagram, Twitter, Onlyfans…
- Es posible solicitar la eliminación de datos personales:
  https://pimeyes.com/en/opt-out-request-form

CYBER
SEC 42

Telegram

Bots para investigar nombres de usuario, emails, teléfonos

https://t.me/maigret_osint_bot

54 exact accounts found:
GitHubGist, Twitch, GitHub, Telegram, Trello, Pinterest, Fiverr,
Pornhub, Blogger, Unsplash, Issuu, Freelancer.com, Roblox,
AppleDiscussions, Scratch, Dreamstime, na.op.gg, Wattpad,
Discogs, Kaggle, Nitter, mercadolivre, MixCloud, Docker Hub,
Duolingo, amp.flipboard.com, BitBucket, Picuki, AdultFriendFinder,
AskFM, Gravatar, Flipboard, Codecademy, FortniteTracker, Picsart,
hi5, Codewars, TryHackMe, giters.com, Dumpor, Fatsecret,
LibraryThing, Libraries, Periscope, Kik, Archive.orgTwitterProfiles,
Archive.orgTwitterTweets, Friendfinder-x, Quizlet, Poshmark,
Tetr.io, Ourfreedombook, padlet.com, mql5.com

Telegram

Bots para investigar nombres de usuario, emails, teléfonos

https://t.me/maigret_osint_bot
https://t.me/m@pwned_robotaigret_osint_bot

Welcome .!
With this Bot you can **check if you have an account that has
been compromised in a data breach.**
https://haveibeenpwned.com

Breachedaccount is enabled, write your email or phone
number to check if you have an account that has been
compromised
🧑 You can change the service on the settings
                                                                    19:41

📖 Guide   ℹ️ Various info

⚙️ Settings
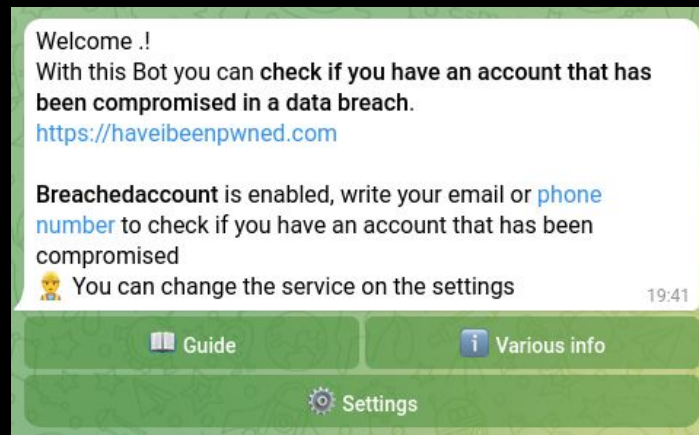
Brechas de seguridad, leaks

HaveIbeenPwned:
    https://haveibeenpwned.com/
Búsqueda:
    https://search.ddosecrets.com/data
Torrents de brechas completas*:
    https://ddosecrets.com/wiki/Special:AllPages
Últimas empresas atacadas por ransomware:
    https://ransomwatch.telemetry.ltd/#/recentposts

*Almacenar o distribuir el contenido de estas bases de datos es ilegal 🥳🧠

Dump_public_hinohomaru.net_2015.04.rar 75.29 MB
Dump_public_nute.ufsc.br_2014.06.rar 1.99 MB
Dump_public_ongab.ru_2021.rar 16.41 MB
Dump_public_onlinebloodbank.com_2018.01.22.rar 21.35 M
Dump_public_ordineavvocatiroma.org_2019.rar 319.92 MB
Dump_public_oursportscentral.com_none.rar 535.27 KB
Dump_public_ovh.com_2016.06.rar 55.76 MB
Dump_public_ozhiphop.com_2016.08.rar 129.75 KB
Dump_public_pally.live_2020.03.18.rar 144.52 MB
Dump_public_parapa.mail.ru_2016.08.rar 195.25 MB
Dump_public_parkmobile.com_2021.03.rar 1.87 MB
Dump_public_patari.pk_2021.06.rar 226.33 MB
Dump_public_paxel.co_2020.03.rar 1.63 GB
Dump_public_payad.me_2020.03.rar 31.30 MB
Dump_public_pbghpa.com_none.rar 273.25 KB
Dump_public_photolamus.com_2020.06.12.rar 289.91 MB
Dump_public_pixarra.com_2015.11.rar 97.34 KB
Dump_public_pizap.com_2017.12.07.rar 192.74 MB
Dump_public_planetminecraft.com_none.rar 8.68 MB
Dump_public_plastic4you.ru_none.rar 78.43 KB
Dump_public_playonrent.com_none.rar 1.12 MB
Dump_public_plex.tv_2015.rar 14.85 MB
Dump_public_pluto.tv_2018.10.12.rar 468.98 MB
Dump_public_powerlogo.ru_2020.04.09.rar 175.40 KB
Dump_public_primegaming.com_2014.10.rar 140.80 MB
Dump_public_promo.com_2020.06.22.rar 1.59 GB
Dump_public_ps3hax.net_2016.07.rar 30.44 MB
Dump_public_qnb.com_2015.07.rar 494.89 MB
Dump_public_rajabets.com_2021.rar 1.39 MB
Dump_public_raychat.io_2021.05.rar 211.00 MB
Dump_public_readnovel.com_2019.05.rar 634.52 MB
Dump_public_recordoftheday.com_2020.rar 443.50 KB

CYBER SEC 42

GeoInt

Tweets en ubicaciones:
> https://birdhunt.co/
> Útil para obtener datos de última hora, eventos en una localización, accidentes, movimientos de masas, etc

Buscador de instagram por ubicación:
> https://instahunt.co
> Puntos turísticos, zonas de interés

CYBER
SEC 42

LINKS

GOOGLE DORKS:
https://www.ma-no.org/es/seguridad/google-dorks-como-encontrar-datos-interesantes-y-buscar-como-un-hacker

OSINT FRAMEWORK:
https://osintframework.com/

PIMEYES:
https://pimeyes.com

r/OSINT
https://reddit.com/r/osint