8 octobre 2019- Ajaccio

CYBER DAY corsica

Initiation à l'OSINT

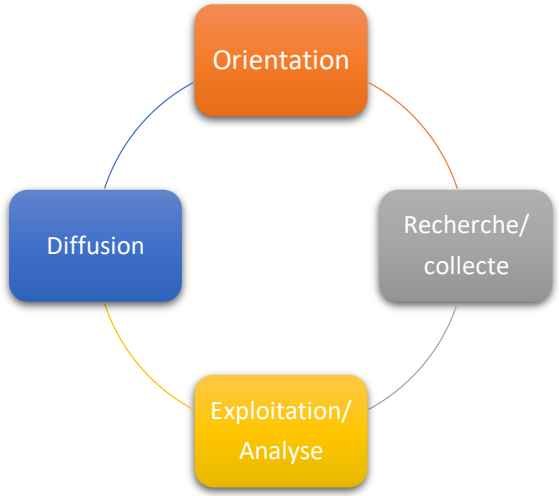
Jérôme FREANI – jerome@freani.com

L'« intelligence "

Définition

Intelligence = renseignement

Ensemble des activités coordonnées de collecte, de traitement et de diffusion de l'information utile à un acteur, en vue de son exploitation.



- **HUMINT – Human Intelligence** : Renseignement d'origine humaine
- **SIGINT – Signal Intelligence** : Renseignement d'origine électromagnétique (Radio…)
- **IMINT – Imagery Intelligence** : Renseignement d'origine image (Satellite, photos, Google maps...)
- **OSINT – Open Source Intelligence** : Renseignement d'origine source ouverte (web, journaux...)

OSINT

Définitions

La source a-t-elle délivré l'information de son plein gré ?

- **Oui** → information ouverte
- **Non** → information fermée

L'OSINT (Open Source Intelligence) est la collecte d'information en source ouverte.

Types de sources

Définitions

Deux types de sources :

- **Sources ouvertes :** sources d'information publique dont l'accès est facile et large → **70% de l'information disponible**

- **Sources fermées :** sources dont l'accès est protégé ou sources légales mais difficiles à approcher et à formaliser (sources informelles) → **30% de l'information disponible**

Types d'informations

Définitions

3 types d'informations

- **information blanche :** information aisément licitement accessible.
- **information grise :** information licitement accessible, mais caractérisée par des difficultés dans la connaissance de son existence ou de son accès.
- **information noire :** information à diffusion restreinte et dont l'accès ou l'usage est explicitement protégé.

95% des informations

Usages
Intérêt de l'OSINT

Pourquoi faire de l'OSINT?

- **Rechercher des informations ciblées**
- **Vérifier l'exposition de nos informations**
- **Se prémunir de social engineering (ingénierie sociale)**
- **Cartographier son environnement**
- **Mettre en place une veille (réputationelle, concurrentielle, législative,…)**

Rappel

Loi

- **Loi Godfrain :**

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 245 euros d'amende.

- **Code pénal – Art 226-4 :**

L'introduction dans le domicile d'autrui à l'aide de manœuvres, menaces, voies de fait ou contrainte, hors les cas où la loi le permet, est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

Cette présentation est faite dans un but éducatif et proscrit la recherche et l'exploitation d'informations interdites

Méthodes & outils

Le « dorking » - définition

L’objectif des Dorks est de détecter si des fuites d’information vous concernant vous ou votre entreprise sont visibles sur les moteurs de recherche, principalement Google.

Permet de récupérer :

- Des noms d’utilisateurs et les mots de passe
- Des listes d’email
- Des documents sensibles
- Des renseignements personnels, transactionnels ou financiers (PIFI)
- Les vulnérabilités des sites internet, des serveurs ou des plugins
- Etc..

Méthodes & Outils

Le « dorking » - utilisation

Exemples de « Google dorks » :

Requête	Résultat
Filetype:xls « nom prénom "	Documents Excel contenant le nom et prénom
Site:entreprise.com filetype:pdf « confidentiel "	Fichier PDF, contenant le mot confidentiel, en provenance de l'entreprise ciblée.
inurl:wp-config -intext:wp-config « 'DB_PASSWORD' "	Le fichier wp-config WordPress contenant le login et le mot de passe de l'administration du site

Plus de dorks : https://www.exploit-db.com/google-hacking-database

Méthodes & outils

Informations sur des personnes

- Réseaux sociaux (fb sleep stats, open graph search)
- Amis
- Ancienne école/entreprise
- Curriculum Vitae
- Sites généalogie
- Outils/sites de recherches

Méthodes & outils

Informations sur des personnes

- **Checkusernames.com**

Service gratuit qui permet de rechercher dans plus de 160 réseaux sociaux.

- **Namechk**

Recherche de pseudos dans plus d'une centaine de services mais aussi dans les extensions de noms de domaine les plus courantes.

- **Lullar**

Recherche de profils potentiels d'une personne non plus en fonction d'un pseudo mais à partir d'une adresse email.

- **Pipl.com**

Recherche de profils basé sur un point d'information (email, nom,…)

Méthodes & outils

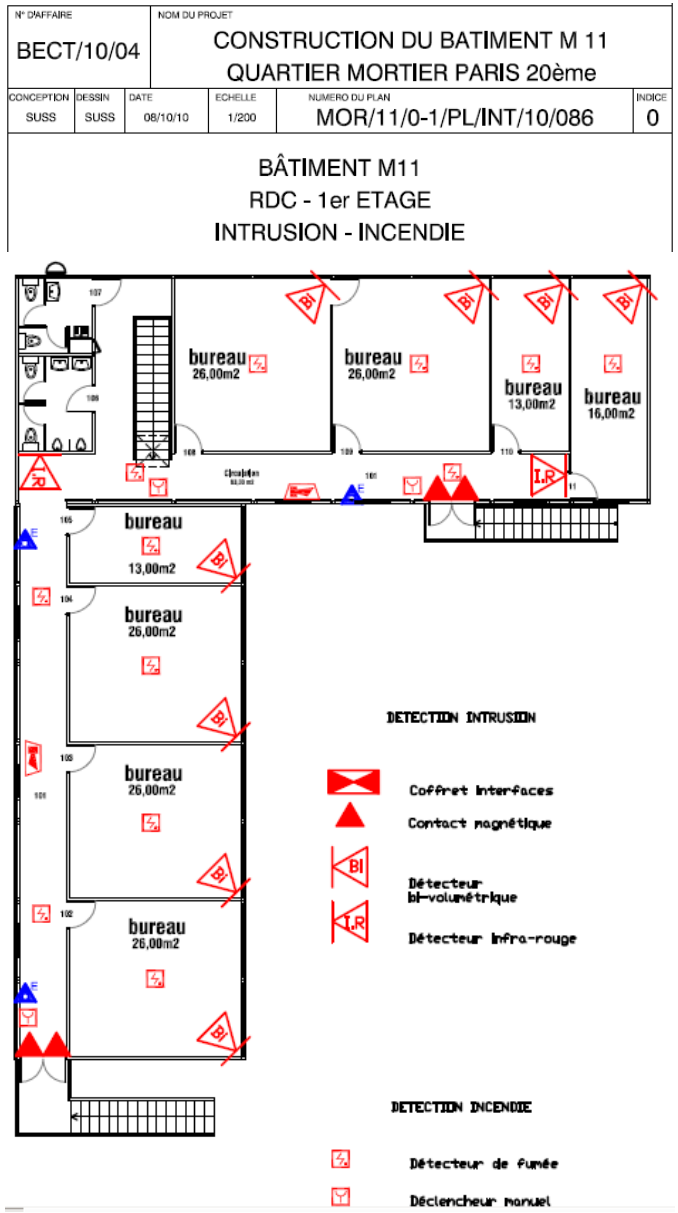
Informations sur des organisations

- Société.com
- Annuaires
- Presse
- Blog d'entreprise
- Rapports d'activités
- Appels d'offres / marchés publics

Annexe n°1 à l'acte d'engagement

BORDEREAU DE PRIX UNITAIRES ANTI-INTRUSION

N°	Description
195	Outil de gestion portable, écran 17'' Processeur core 2 Duo Windows 74 Go de Ram, lecteur/graveur cd/dvd compatible tout cd et dvd et lecteur de carte mémoire 5 en 1
196	Unité de stockage mobile 250Go Port USB2, ccompatible windows
197	Unite de stockage mobile 8GoPort USB2, compatible windows



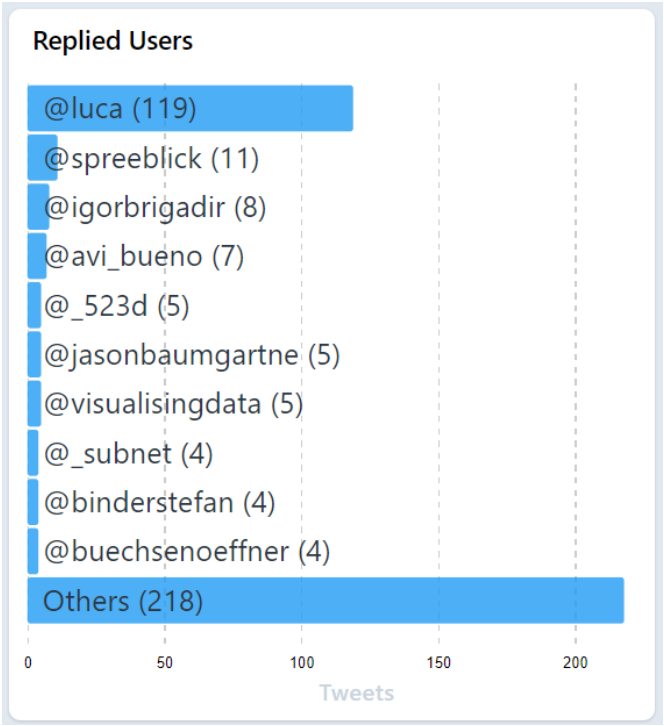
Méthodes & outils

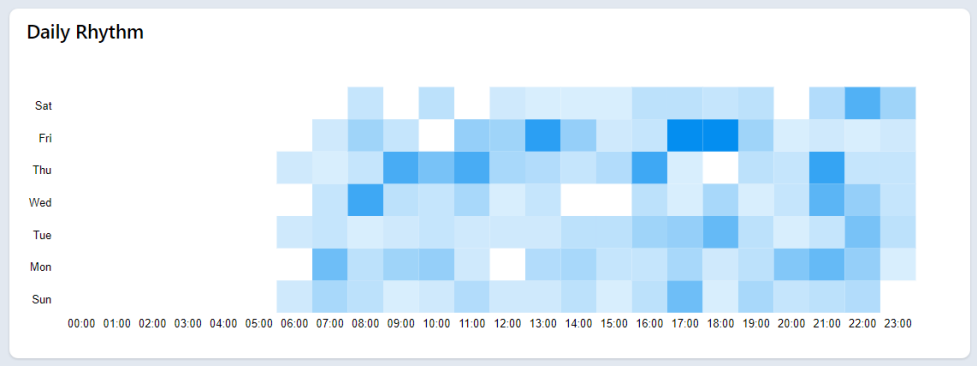
Twitter

Plateforme qui permet d'automatiser et cartographier certaines recherches :

- Recherche avancée : twitter.com/search-advance
- Recherche par géolocalisation : geocode:latitude,longitude,1km

- https://accountanalysis.app





Méthodes & outils

LinkedIn

Le réseau social professionnel est une mine d'information sur les personnes et un moyen simple d'entrer en contact.

LinkedIn peut être utilisé pour :

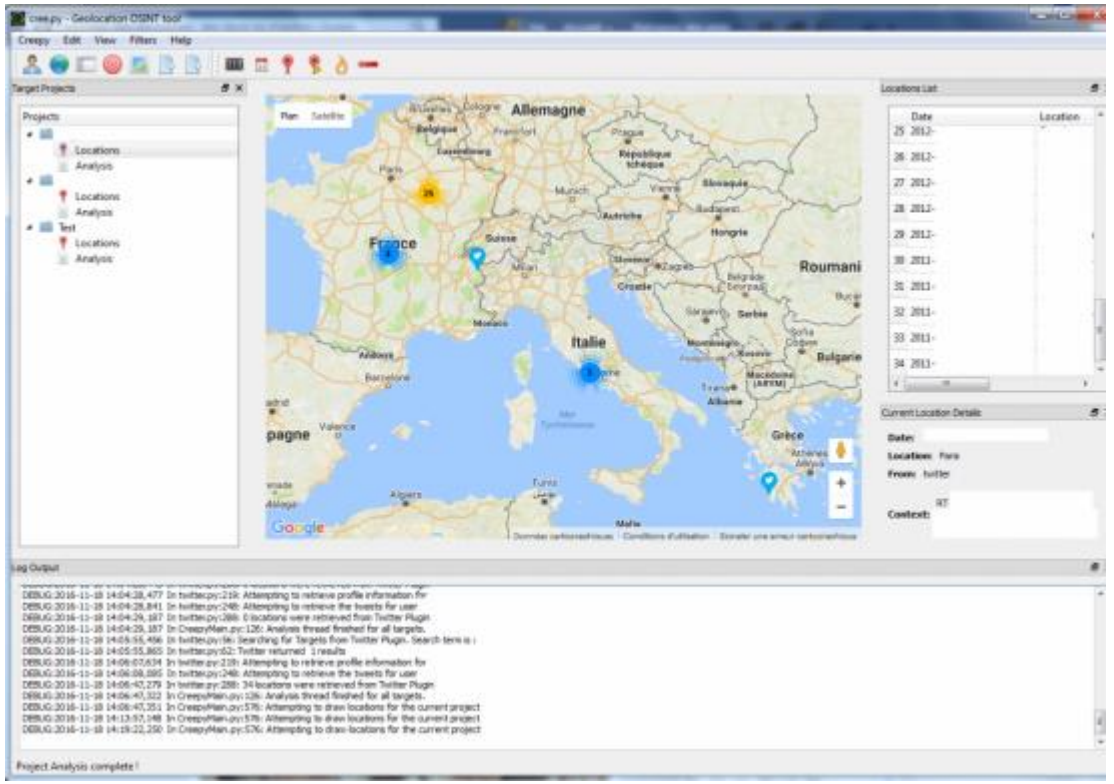
- Rechercher de l'information au travers de recherches simples ou complexes
  - Exemple : ((“Analyste financier” OR “comptable”) AND (“directeur financier”))
- Prendre contact (exemple « Getting in bed with Robin Sage – Blackhat 2010 »)
  - Prise de contact avec militaires, employés de fabricants d'armes, département de la défense...
  - Accès aux mails et comptes bancaires des victimes
  - Récupération d'horaires de décollage des hélicoptères américains

Méthodes & outils

Cree.py

Centralisation d'informations

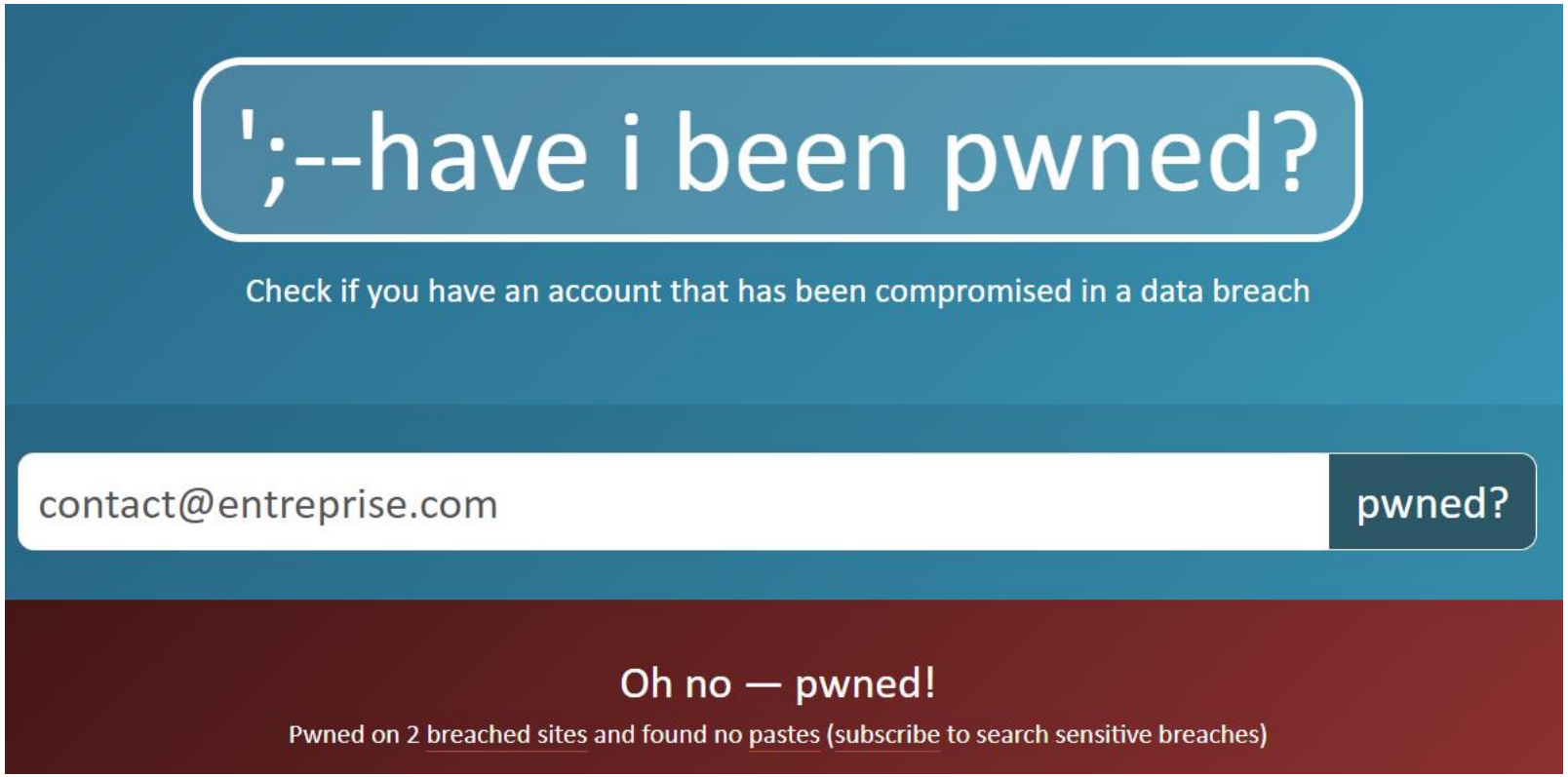
Cet outil permet de faire une recherche basée sur la géolocalisation des comptes de réseaux sociaux, de les regrouper et les cartographier.



Méthodes & outils

HaveIbeenPwnd.com

HaveIbeenPwnd.com est un site qui vous permet de savoir si une adresse email est présente dans une fuite de données.

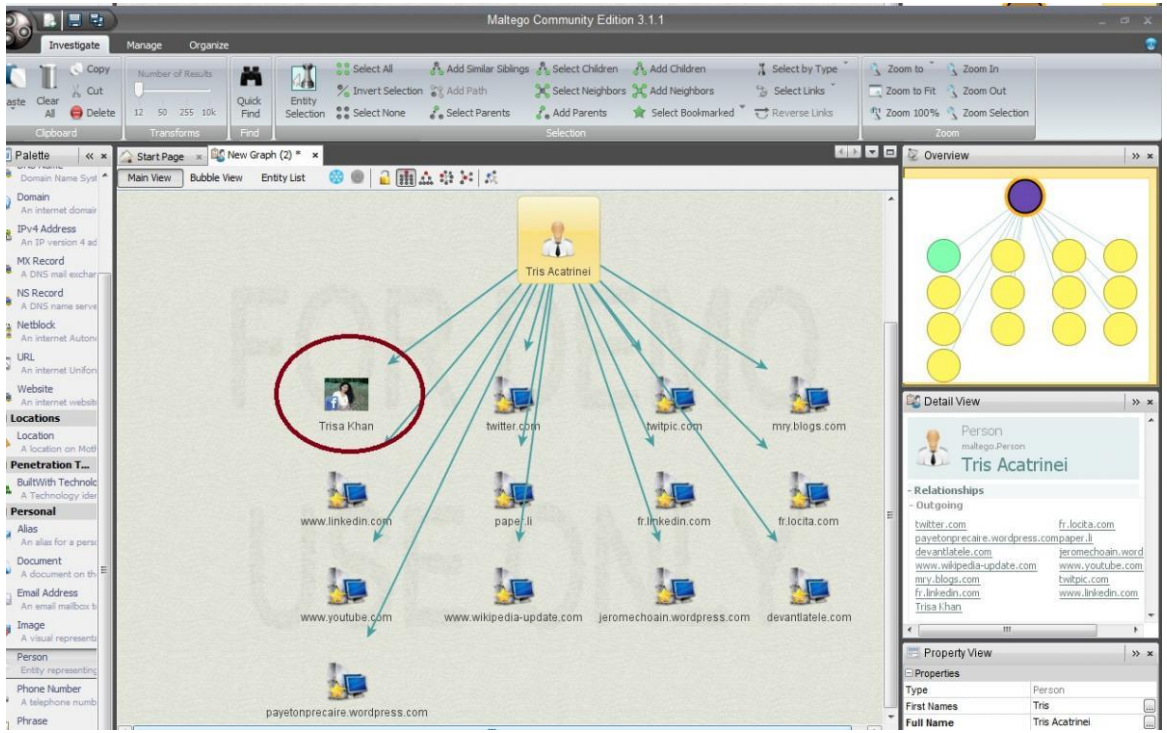


Méthodes & outils

Maltego

Plateforme qui permet d'automatiser et cartographier certaines recherches

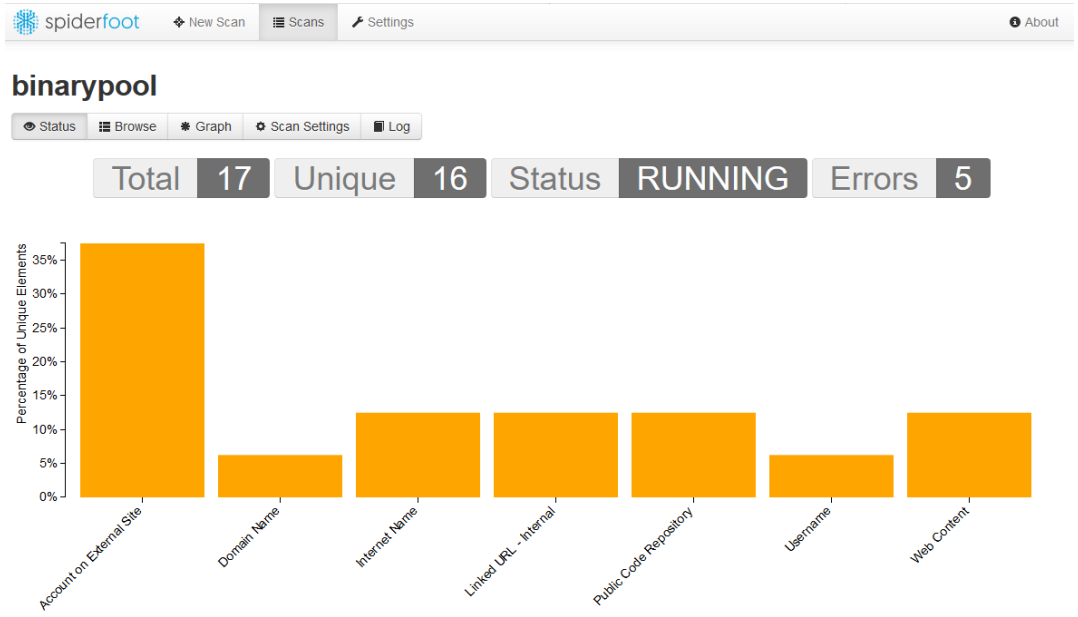
- Personnes
- Entreprises
- Entités administratives
- Services Web
- Bases de données

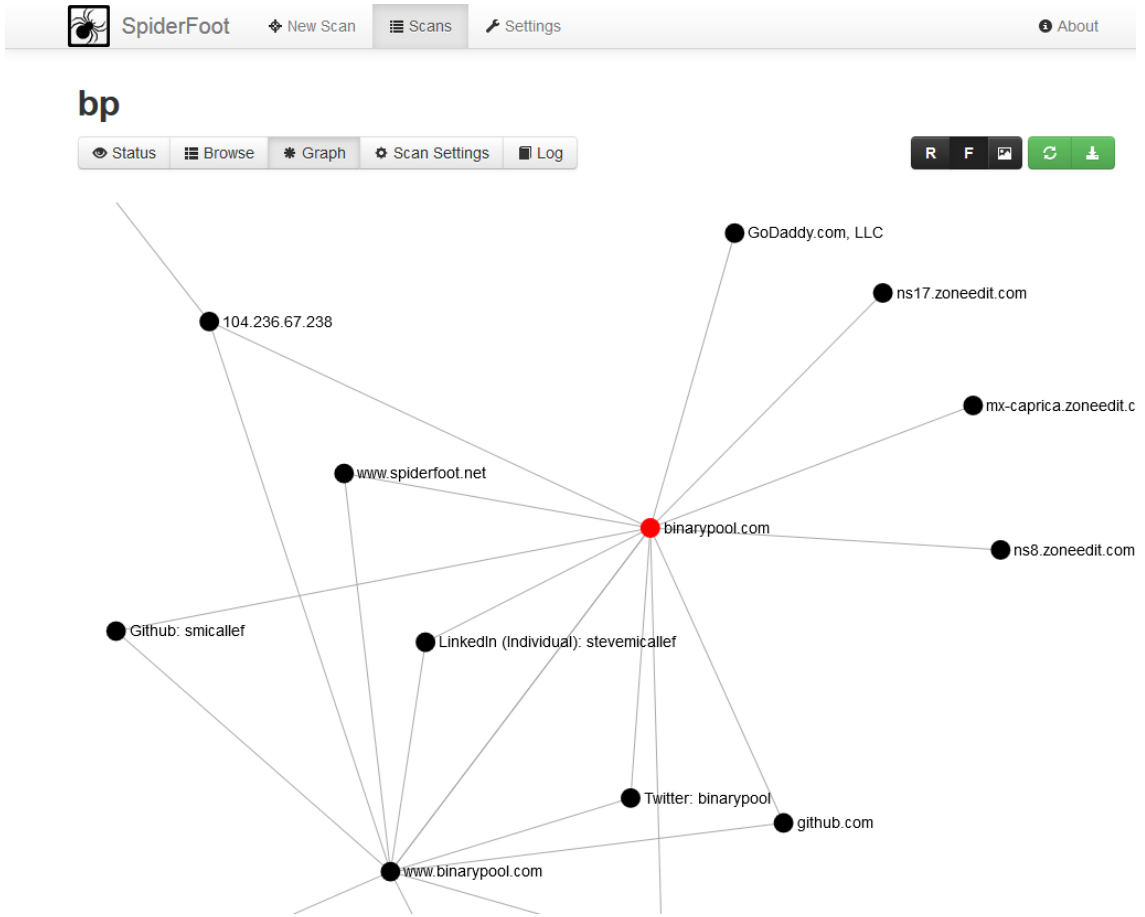


Méthodes & outils

SpiderFoot

Outil de reconnaissance permettant de générer des cartographies de liens



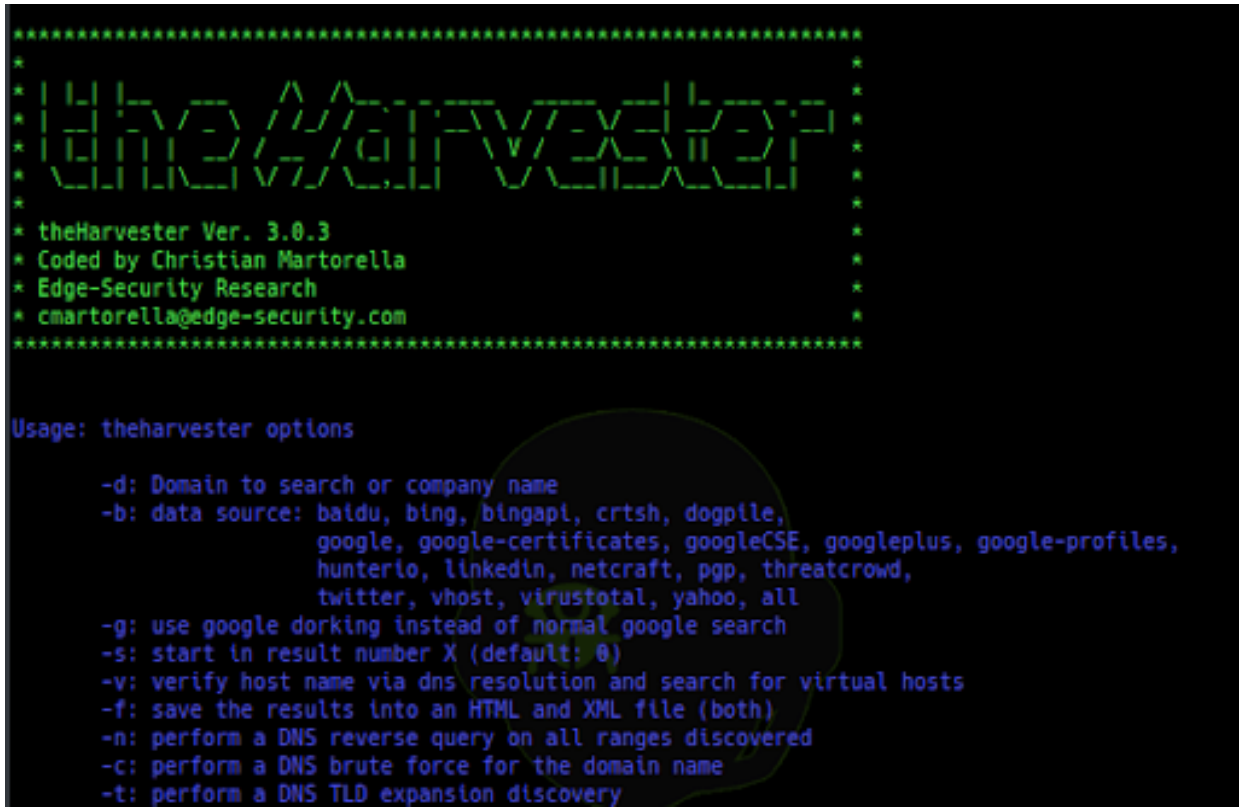


Méthodes & outils

theHarvester

Outil de collecte basé sur multiples sources :

- Noms de domaines
- Adresses emails
- Hôtes virtuels
- Ports ouverts
- Nom/prénom



Méthodes & outils

Exif viewer (Exchangeable image file format)

Un EXIF est un extrait de métadonnées

Permet d'extraire :

- Type d'appareil photo utilisé
- Heure/date
- Géolocalisation
- Retouches potentielles
- Copyrights

PNG

Animation	no
Bit Depth	8
Color Type	RGB with Alpha
Compression	Deflate/Inflate
Filter	Adaptive
Interlace	Noninterlaced
Gamma	2.2
SRGB Rendering	Relative Colorimetric
White Point X	0.3127
White Point Y	0.329
Red X	0.64
Red Y	0.33
Green X	0.3
Green Y	0.6
Blue X	0.15
Blue Y	0.06
Background Color	255 255 255
Image Size	305 × 303
Pixels Per Unit X	2,835
Pixels Per Unit Y	2,835
Pixel Units	meters
Virtual Image Width	305
Virtual Image Height	303
Virtual Page Units	0
Datecreate	2019-05-13T11:45:47+02:00 4 months, 25 days, 7 hours, 55 minutes, 31 seconds ago
Datemodify	2019-05-13T11:45:47+02:00 4 months, 25 days, 7 hours, 55 minutes, 31 seconds ago

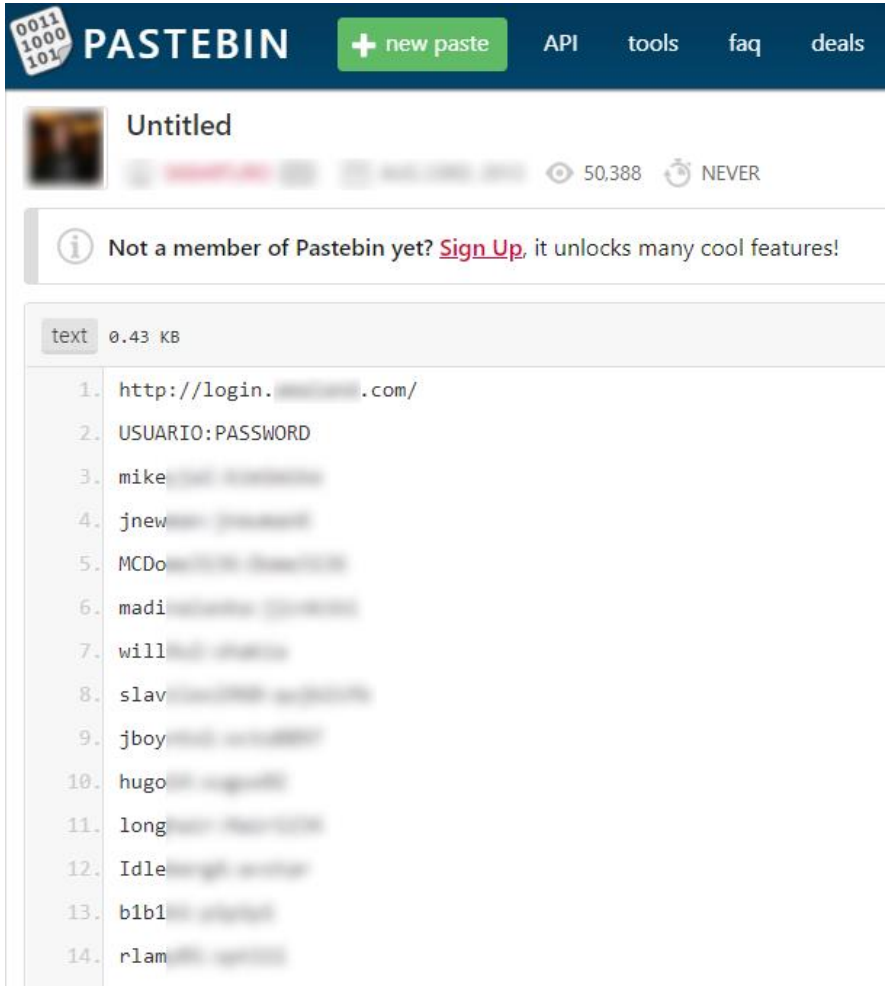
Méthodes & outils

Pastebin

Les pastebins sont des « blocs-notes » en ligne.

Certains sont publics, d'autres privés.

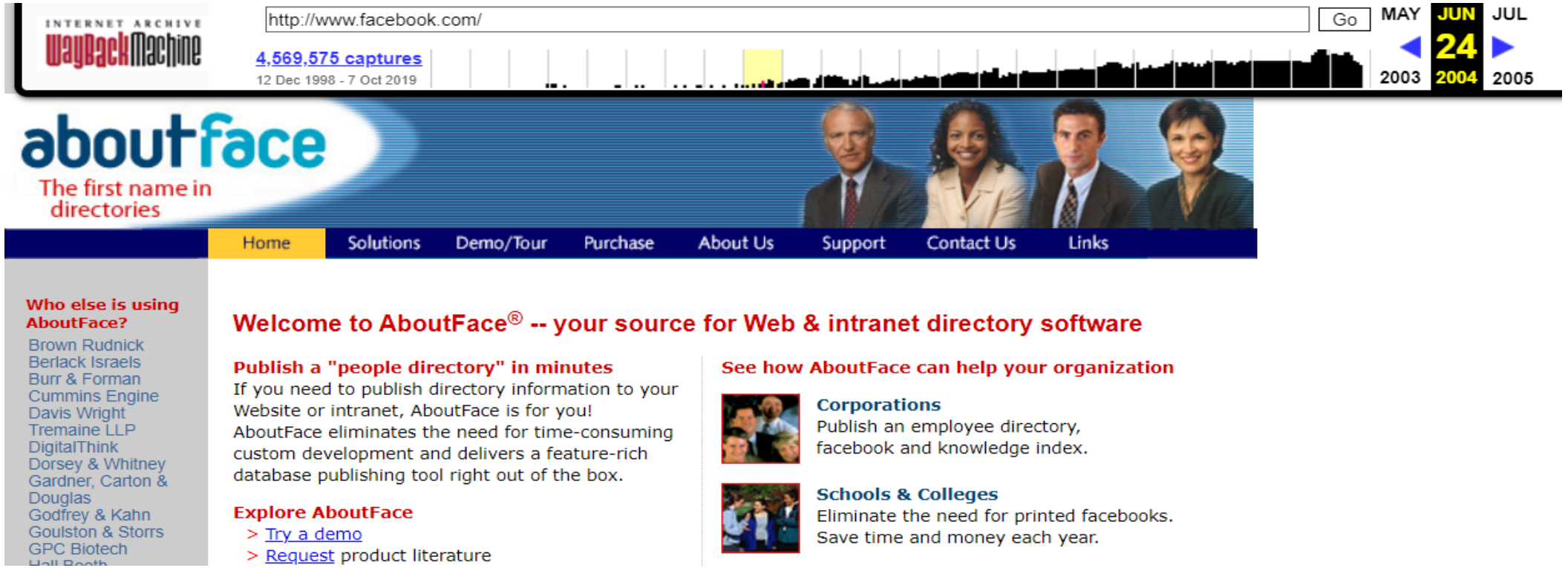
Ils sont parfois utilisés par des hackers ou des personnes peu regardante de la sécurité de leurs données pour les envoyer ou les stocker.



Méthodes & outils

Wayback machine

La Wayback Machine (https://archive.org/web) permet d'accéder à une version antérieure d'un site web.



Méthodes & outils

WHOIS

Le WHOIS permet de connaitre toutes les informations liées à site internet via son nom de domaine

- Nom du déposant
- Adresse
- Numéro de téléphone
- Date d'enregistrement
- Date de renouvellement

registrar: OVH
type: Isp Option 1
address: 2 Rue Kellermann
address: 59100 ROUBAIX
country: FR
phone: +33 8 99 70 17 61
fax-no: +33 3 20 20 09 58
e-mail: support@ovh.net
website: http://www.ovh.com
anonymous: NO
registered: 1999-10-21T12:00:00Z
source: FRNIC

nic-hdl: [redacted]
type: ORGANIZATION
contact: ANCIENS DE L'ECOLE DE GUERRE ECON
address: 1, rue [redacted]
address: 75007 Paris
country: FR
phone: [redacted]
e-mail: gf0hub6amxoifjbxmsro@k.o-w-o.info
registrar: OVH
changed: 2018-06-11T00:25:26Z nic@nic.fr
anonymous: NO
obsoleted: NO
eligstatus: not identified
reachstatus: not identified
source: FRNIC

Méthodes & outils

Shodan.io

Le moteur de recherche des objets connectés.

Permet d'identifier des périphériques vulnérables.

Filtrage par ville : "city:ajaccio"

Filtrage par pays : "country:FR"

Filtrage par nom de domaine : "hostname:societe.com"

Filtrage par organisation : "org :societe"

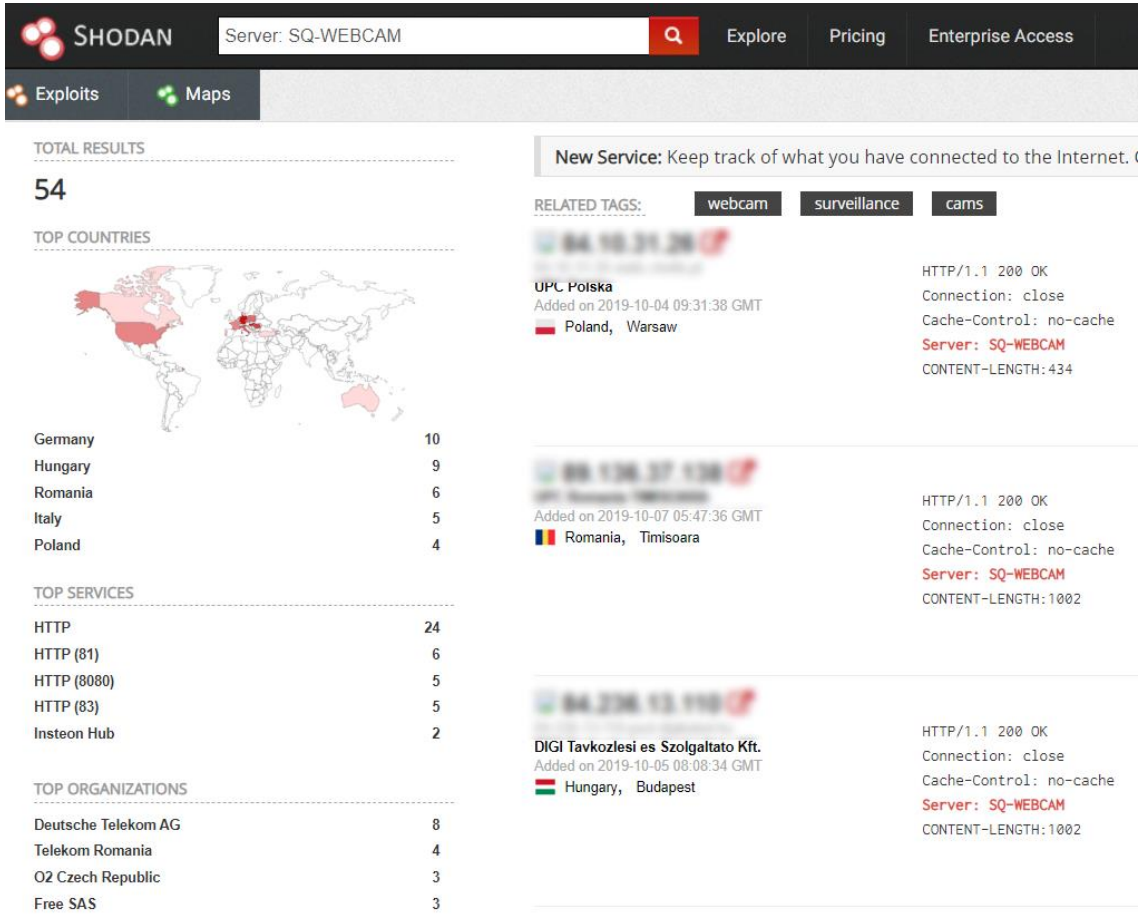
Filtrage par port : "port :8080"

Filtrage par adressage IP : "net:10.10.10.10"

Filtrage par produit : "product:apache"

Filtrage par système : "os:windows"

Filtrage par le titre de la page web : "title: "société X" "

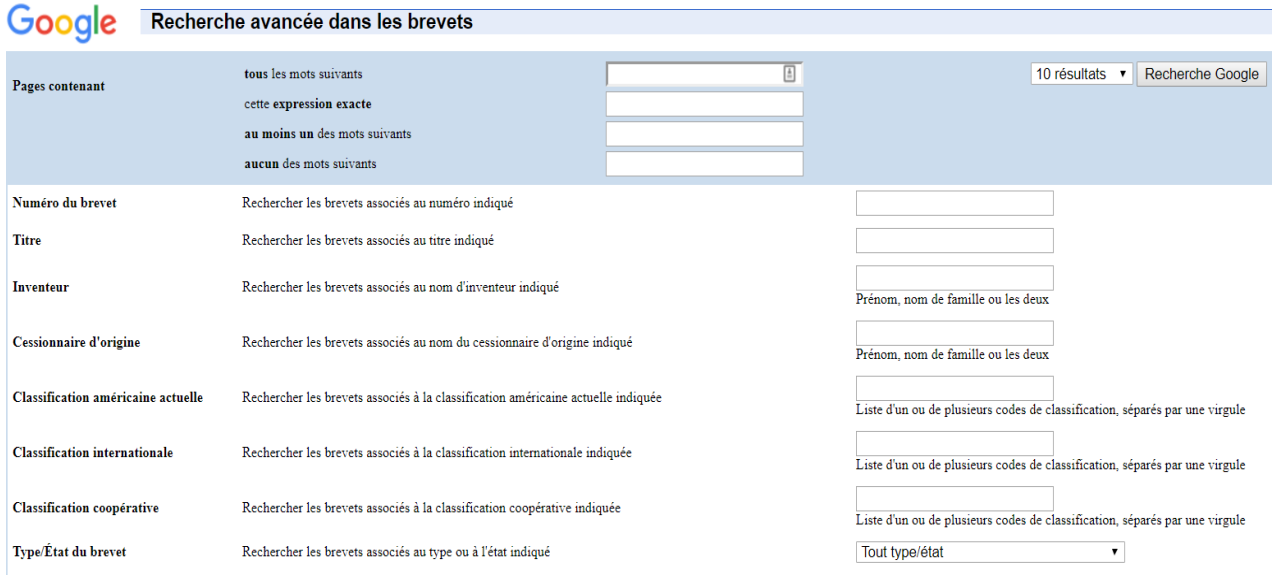


Méthodes & outils

Brevets

Patent Search - moteurs de recherche pour les brevets

Permet de chercher une information par rapport à un inventeur, un mot clé, une date…



Google **Recherche avancée dans les brevets**

Pages contenant	**tous** les mots suivants		10 résultats ▾ Recherche Google
	cette **expression exacte**		
	au moins un des mots suivants		
	aucun des mots suivants		
Numéro du brevet	Rechercher les brevets associés au numéro indiqué		
Titre	Rechercher les brevets associés au titre indiqué		
Inventeur	Rechercher les brevets associés au nom d'inventeur indiqué		Prénom, nom de famille ou les deux
Cessionnaire d'origine	Rechercher les brevets associés au nom du cessionnaire d'origine indiqué		Prénom, nom de famille ou les deux
Classification américaine actuelle	Rechercher les brevets associés à la classification américaine actuelle indiquée		Liste d'un ou de plusieurs codes de classification, séparés par une virgule
Classification internationale	Rechercher les brevets associés à la classification internationale indiquée		Liste d'un ou de plusieurs codes de classification, séparés par une virgule
Classification coopérative	Rechercher les brevets associés à la classification coopérative indiquée		Liste d'un ou de plusieurs codes de classification, séparés par une virgule
Type/État du brevet	Rechercher les brevets associés au type ou à l'état indiqué		Tout type/état ▾

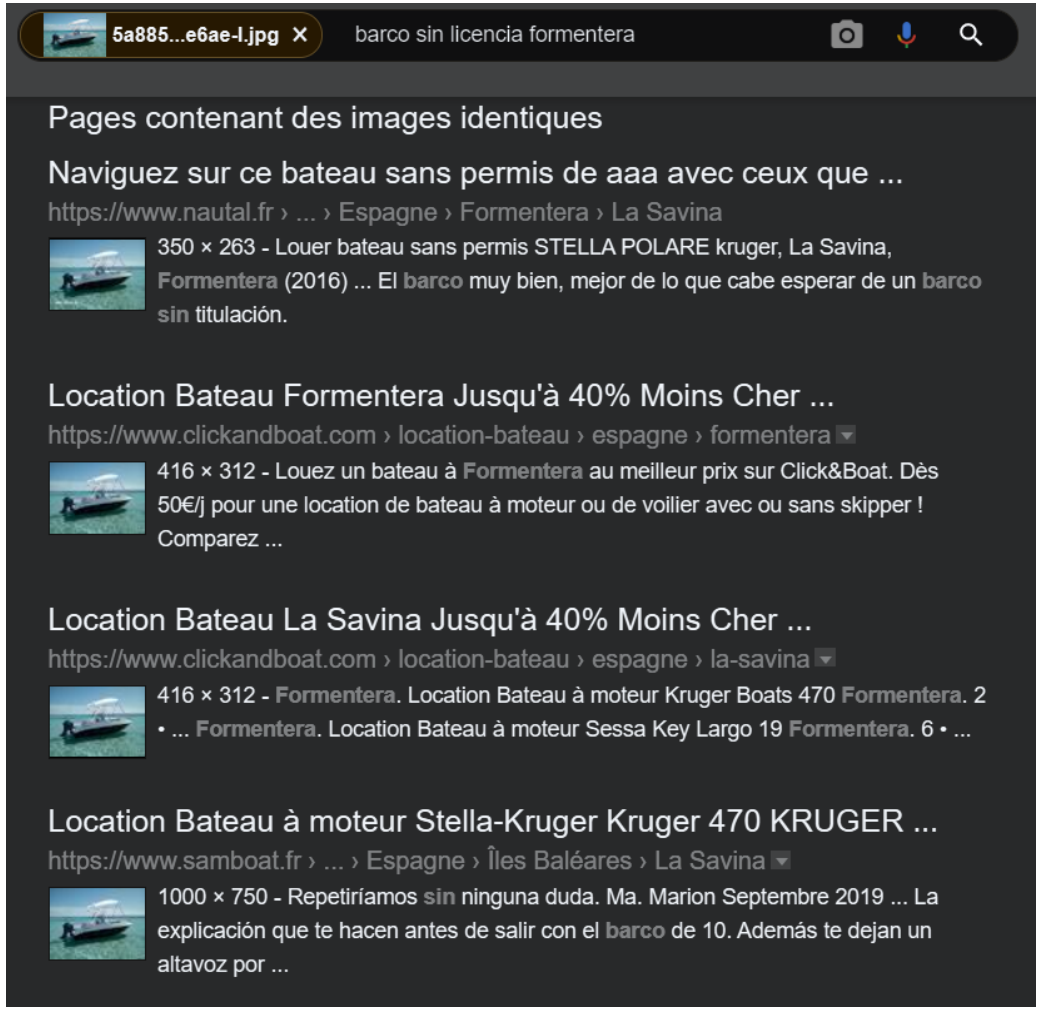
Méthodes & outils

Google image / TinEye

Google image et TinEye permettent de faire de la recherche inversée sur une image.

Permet d'identifier :

- les faux profils
- les images génériques
- les autres endroits où une photo est utilisée



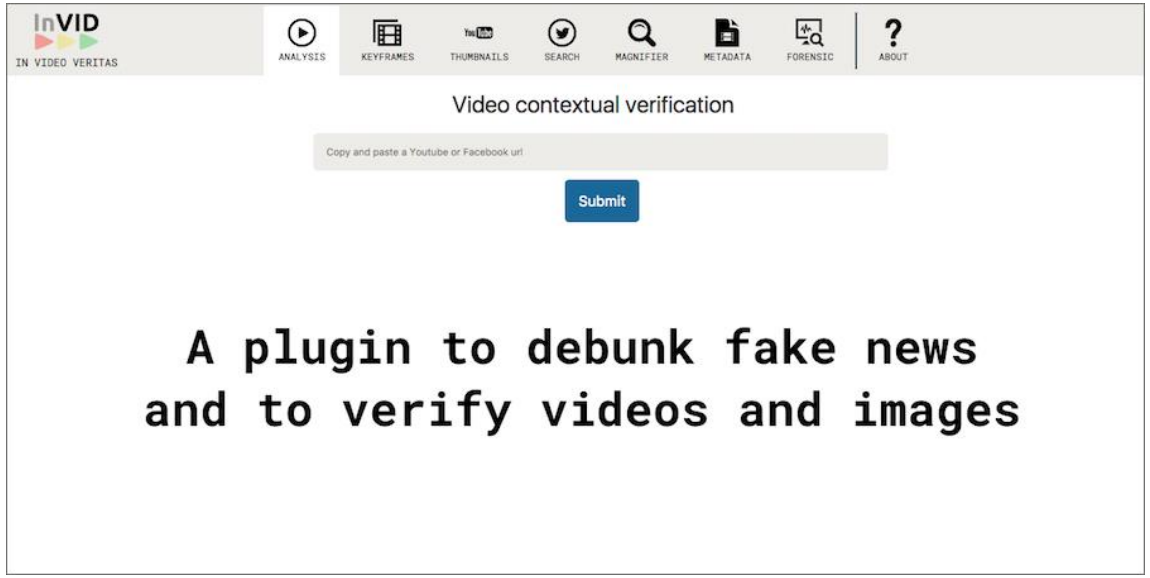
Méthodes & outils

InVID (In Video Veritas)

InVID est une extension Firefox et Chrome.

Résultat d'un projet européen visant à aider les journalistes à vérifier la véracité des images et vidéos circulant sur les réseaux sociaux

- Analyse métadonnées (titre, date, géolocalisation,…)
- Recherche d'image inversée (séquences, miniature YouTube)
- Filtres d'images



Méthodes & outils

La veille

La veille vise à la surveillance et au recueil d'informations sur un ou plusieurs sujets précis. Elle peut s'apparenter à un processus d'OSINT continu et automatisé.

Cela vous permet de suivre de façon quotidienne les nouvelles informations concernant une cible (vous-même, un concurrent, etc…). De nombreux outils existent:

- Veille nouveau résultat Google : Google alert
- Veille Pastebin : PasteLert
- Veille email piraté : HaveIbeenPwnd

Méthodes & outils

Social Engineering

L’ingénierie sociale est l’art de manipuler un individu afin de lui faire réaliser des actions ou divulguer des informations

Ces techniques nous aident à identifier des leviers psychologiques qui peuvent être utilisés sur une cible.

Exemple : l’arnaque au président

Se protéger
Les bonnes pratiques

Afin d'éviter la présence d'informations inutiles vous concernant sur internet, des bonnes pratiques doivent être appliquées :

- Pseudonymisation
- Maitriser son usage des réseaux sociaux
- Mettre en place une veille sur soi/son entreprise
- Mettre ses informations les plus sensibles en lieux sûrs
- Chiffrer (bitlocker) / cacher (deepsound) ses données
- Mot de passe unique / coffre-fort
- VPN

Ressources

Pour aller plus loin

L'OSINT c'est aussi la rechercher permanente de connaissances.

Quelques ressources :

- Bellingcat
- OpenFacto
- Spying Challenge
- Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information – Michael Bazzell
- "Petit traité de manipulation à l'usage des honnêtes gens" by Robert-Vincent Joule & Jean-Léon Beauvois
- https://github.com/jivoi/awesome-osint
- https://osintframework.com

Contact

Pour plus d'infos !

Jérôme FREANI

jerome@freani.com

Cyberologue

@Cyberologue

AEGE Club Cyber

EGE Ecole de Guerre Economique

CGI | Business Consulting