

“L'OSINT ne sert à rien”



🦋 Thibaud “Mhack” PERRARD 🦋

🎯 Pentester chez Thucy

🦋 Renseignement d'Origine Cyber

🔍 Chercheur de vulnérabilités 📱 & 🖥️

🌐 Fondateur Offensive-Intelligence.com

🛡️ Officier de réserve au COMCYBER

Alors, c'est quoi l'OSINT ?

CE QUE C'EST

Tout est déjà là, dehors, en accès libre.

Le talent, ce n'est pas de hacker, c'est de regarder au bon endroit, et de relier ce que personne n'a relié.

Une photo, un favicon, un email oublié dans un commit : pris séparément, du bruit. Recoupés, une identité.

CE QUE CE N'EST PAS

Ce n'est pas du piratage. On ne force aucune porte, on n'entre dans aucun système. On lit ce qui est public.

Ce n'est pas de la magie non plus. Aucun outil ne « trouve le coupable ». Les outils collectent, l'humain font le lien.

« L'OSINT ne sert à rien »



A

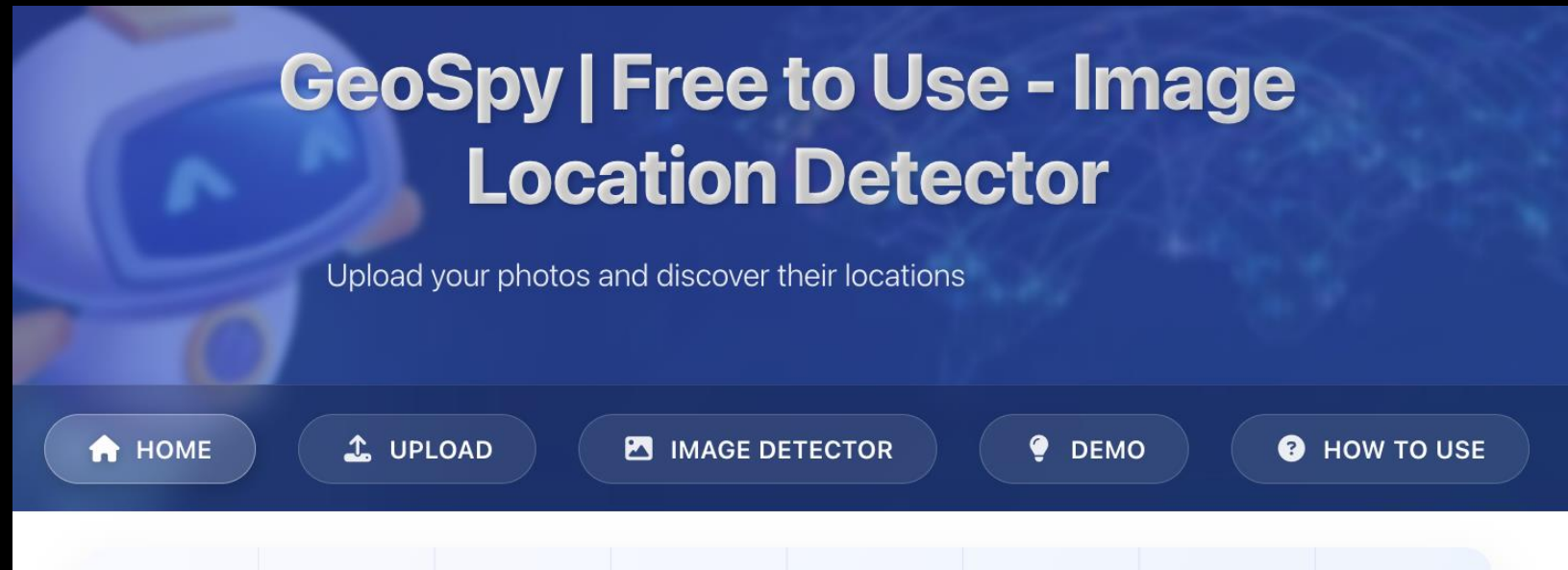
Des alternatives peu connues, souvent gratuites,
parfois redoutables.

GeoSpy

GÉOLOCALISATION D'IMAGE PAR IA

CE QUE ÇA FAIT

Estime où une photo a été prise à partir des seuls pixels — architecture, végétation, revêtements, mobilier urbain — sans aucune métadonnée EXIF. Le modèle Superbolt vise la précision au niveau de la rue.



geospy.net

Picarta

GÉOLOCALISATION D'IMAGE — SECONDE OPINION

CE QUE ÇA FAIT

Même principe que GeoSpy, modèle différent : prédit le lieu de prise de vue d'une photo. Croiser deux moteurs qui se trompent rarement de la même façon fiabilise une géolocalisation incertaine.



picarta.ai

Bellingcat OSM Search

RECHERCHE D'OBJETS CARTOGRAPHIQUES

CE QUE ÇA FAIT

Surcouche d'OpenStreetMap signée Bellingcat : chercher des combinaisons d'éléments (pont + stade + rivière) sur une zone, sans écrire de requête. Le point d'entrée idéal d'une géolocalisation par recoupement d'objets visuels.

The screenshot displays the Bellingcat OSM Search interface. On the left, under "Selected features", there are two entries:

- Fountain (any)**: amenity = fountain (with a REMOVE button)
- Public transport stop (point)**: public_transport is not null OR highway = bus_stop (with a REMOVE button)

On the right, under "Feature presets", there is a grid of buttons for various OSM features, including:

- Power pylon, Public transport stop, Road, Railroad, Bridge
- Road (motorway), Road (primary), Road (secondary)
- Road (residential), Unpaved road, 1-lane road, 2-lane road
- 3-lane road, 4-lane road, 5-lane road, 6-lane road, One way road
- Sidewalk, Pedestrian path, Bike path, Cliff, Waterway, Park
- Industrial area, Forest, Farmland, Water body, Plaza/square
- Building, Building (1 story), Building (2 story), Building (3 story)
- Building (4 story), Building (5-9 stories), Building (10+ stories)
- Beach, Church, Hospital, Military use, Restaurant
- Convenience store, Pharmacy, Supermarket, Shop (any)
- Fountain, Water

At the bottom right, there is a "Custom feature" section with a form to create a new condition: Feature type (any), OSM key, =, OSM value. Below the form are buttons for "ADD CONDITION" and "ADD CUSTOM FEATURE".

osm-search.bellingcat.com

GrayHatWarfare & scanners de buckets

LE STOCKAGE CLOUD LAISSÉ OUVERT

CE QUE ÇA FAIT

GrayHatWarfare indexe des centaines de millions de fichiers laissés publics sur les buckets cloud (S3, Azure, GCP) : recherche par mot-clé, extension, nom d'organisation. Et quand l'index ne suffit pas, des scanners (cloud_enum, S3Scanner) testent les buckets dérivés d'un nom — société-backup, société-prod, société-dev — que le naming prévisible trahit.

The screenshot shows the GrayHatWarfare search interface. The browser address bar displays 'buckets.grayhatwarfare.com/files?keywords=passport'. The page features a navigation menu with 'Home', 'Filter Buckets', 'Search Files', 'Docs / API', 'Top Keywords', and 'Buckets Stream'. A 'Login/Register' button is visible in the top right. A notification box states: 'As a free user you are searching in 2,936 from the 19,300 million files in the index. Registered users have double limits. Finally Premium users also have sorting enabled, full path search instead of only filename and file listing enabled for all buckets. Upgrade your account to enable all features and remove all limitations. More info about packages here'. The main search area is titled 'Search files' and includes a 'Saved searches' dropdown and a 'Random Files' button. The search criteria are: 'Keywords - Stopwords (start with minus -)' with the value 'passport', and 'Filename Extensions (php, xlsx, docx, pdf)' with the value 'php, xlsx, docx, pdf'. There are checkboxes for 'Full Path' and 'Treat as regex', and an 'Additional filters' dropdown. A 'Search' button is located at the bottom right.

grayhatwarfare.com · github.com/initstring/cloud_enum

Les alternatives à Shodan

QUAND UN SEUL MOTEUR DE SCAN NE SUFFIT PAS

CE QUE ÇA FAIT

Shodan n'est pas seul, et croiser plusieurs moteurs change tout. FOFA excelle au pivot par favicon, certificat ou bannière. Netlas ajoute la recherche par regex dans le contenu HTML. ZoomEye couvre des hôtes que les autres manquent, notamment en Asie. Et Validin remonte l'historique DNS — l'IP d'origine d'un domaine avant son passage derrière un CDN.



fofa.info · netlas.io · zoomeye.org · validin.com

urlscan.io

SCANNER D'URL ET BAC À SABLE WEB

CE QUE ÇA FAIT

Visite une URL et capture tout : DNS, requêtes, ressources chargées, capture d'écran, technologies, redirections. Et surtout, une base publique de millions de scans passés, interrogeable — où l'on retrouve les sites frères.

The screenshot displays the urlscan.io interface for a scan of **new.afsin.org**. The main header includes navigation links like Home, Search, Live, API, Blog, Docs, Pricing, Login, and a Security logo. The scan details show the IP **142.4.212.209** (Canada) and a public scan status. It lists the submitted and effective URLs, submission date (June 12, 2026), and origin (FR). A navigation bar offers tabs for Summary, HTTP (111), Redirects, Links (1), Behaviour, Indicators, Similar, DOM, Content, API, and Verdicts. The Summary section states: "This website contacted 7 IPs in 2 countries across 4 domains to perform 111 HTTP transactions. The main IP is 142.4.212.209, located in Canada and belongs to OVH OVH SAS, FR. The main domain is new.afsin.org. TLS certificate: Issued by R13 on April 17th 2026. Valid for: 3mo." It also shows the site was scanned 3 times and has a "No classification" verdict. The Live information section includes Google Safe Browsing status, current DNS A record (142.4.212.209), domain creation date (August 16th 2006), and registrar (OVH, SAS). The Screenshot section shows a live screenshot of the AFSIN website with "Live screenshot" and "Full Image" buttons. The Page Title is "AFSIN - Association francophone des spécialistes de l'investigation numérique".

urlscan.io

DNSDumpster

CARTOGRAPHIE DNS RAPIDE ET GRATUITE

CE QUE ÇA FAIT

Cartographie d'un domaine en un clic : sous-domaines, enregistrements, hôtes liés, le tout sur un graphe exportable.

Reconnaissance DNS gratuite et instantanée, sans installation.

The screenshot displays the DNSDumpster interface with the following sections:

- System Locations:** A world map with a blue highlight over North America.
- Hosting / Networks:** A box labeled "OVH - OVH SAS, F" with flags for France and Canada below it.
- Services / Banners:** A donut chart and a list of services:

Apache/2.4.66 (Debian)	1
SSH-2.0-OpenSSH_10.0p2 Debian-7	1
- A Records (subdomains from dataset):**

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
new.afsin.org	142.4.212.209	ASN:16276 142.4.192.0/19	OVH - OVH SAS, FR Canada	ssh: SSH-2.0-OpenSSH_10.0p2 Debian-7 http: unknown server tech: reCAPTCHA Bootstrap jQuery Migrate:3.4.1 WordPress:6.9 Debian jQuery PHP Apache HTTP Server:2.4.65 MySQL	3

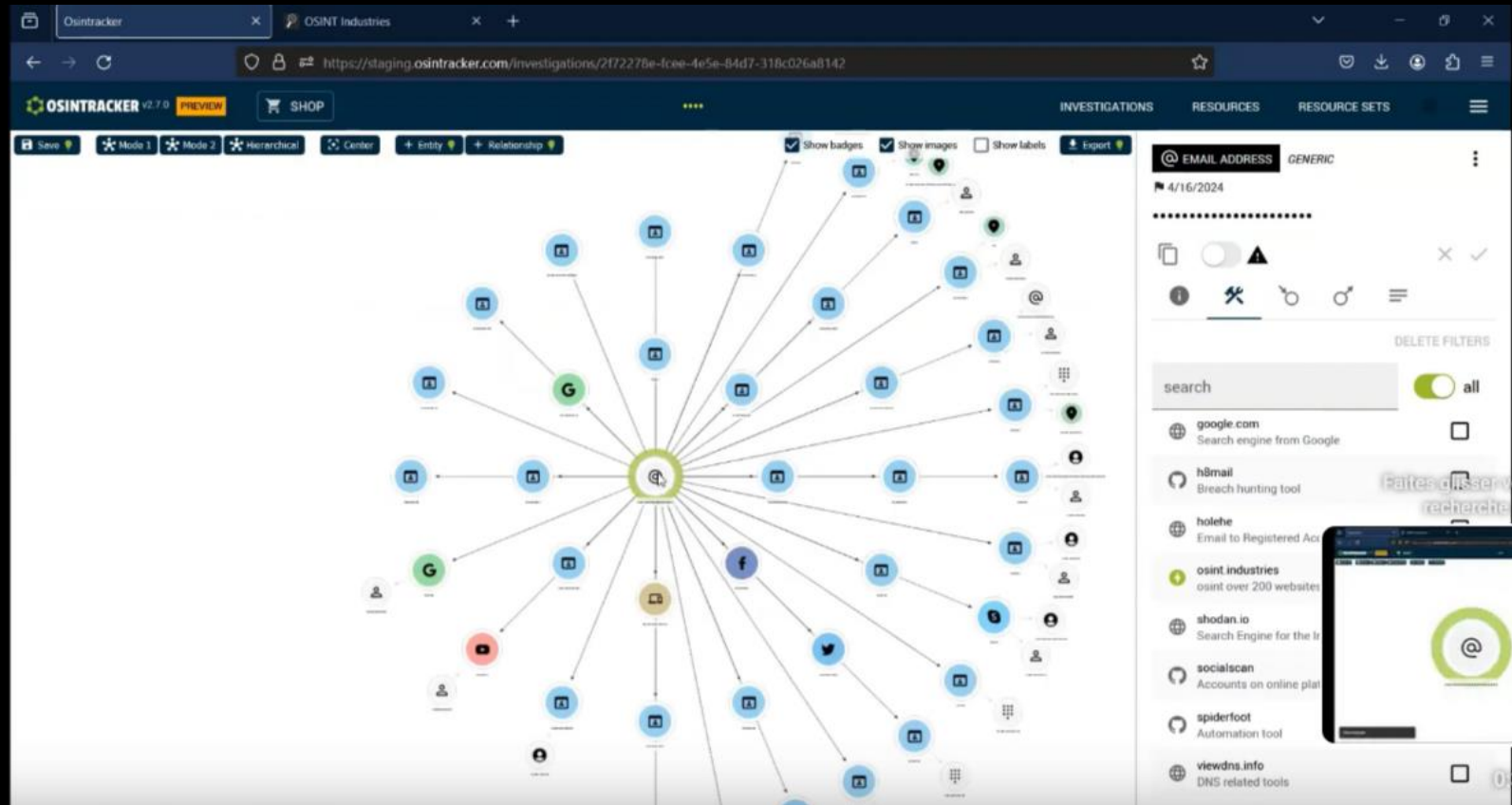
dnsdumpster.com

OSINTracker

CARTOGRAPHIE D'ENQUÊTE TOUT-EN-UN

CE QUE ÇA FAIT

Centralise une investigation : entités, liens, captures, géolocalisations et timeline sur un même graphe. Pensé pour documenter au fil de l'eau et exporter un rapport propre, là où Maltego demande du montage manuel.



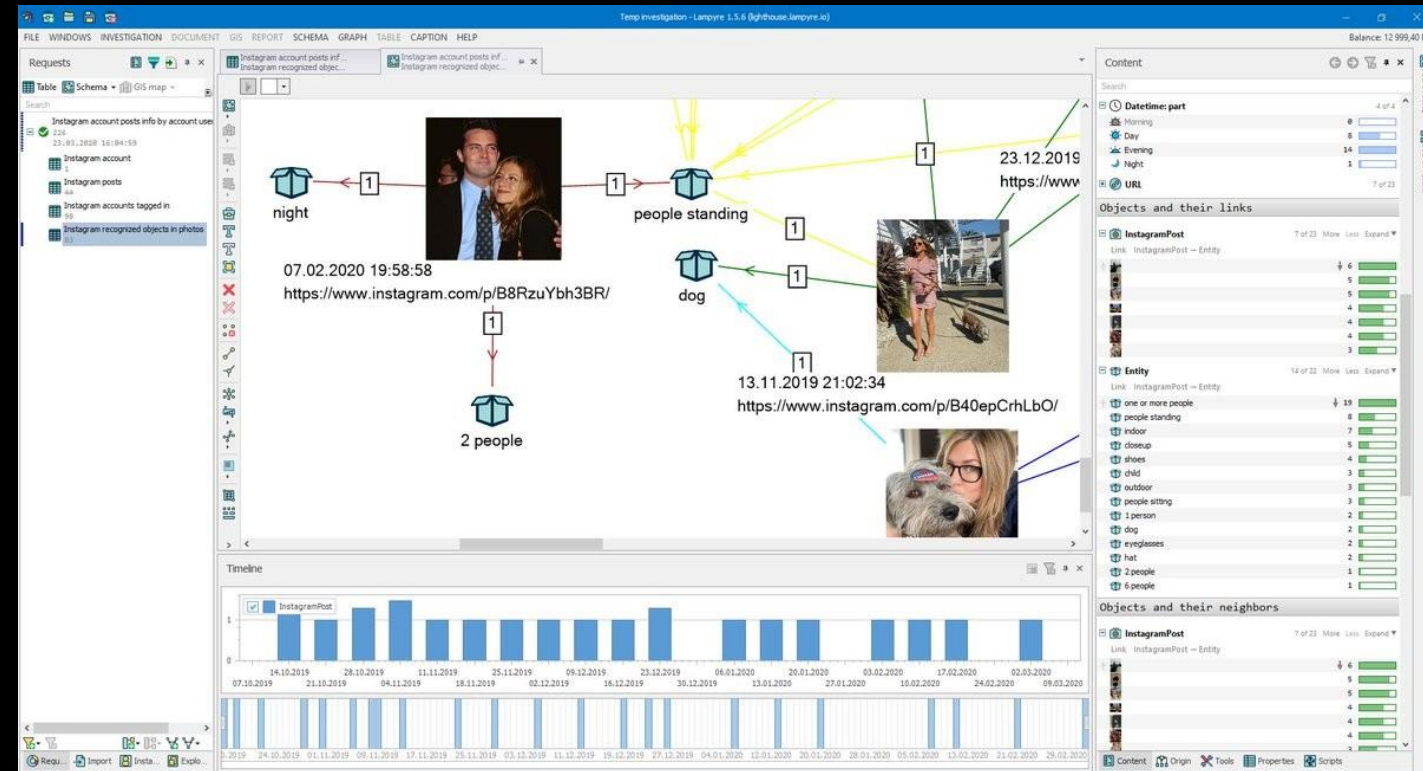
osintracker.com

Lampyre

ANALYSE RELATIONNELLE ET REQUÊTES À LA DEMANDE

CE QUE ÇA FAIT

Outil d'analyse de données et de graphes relationnels avec ses propres requêtes (téléphone, email, domaine, crypto) qui alimentent directement le graphe. Plus accessible que Maltego, paiement à la requête.



lampyre.io

WhatsMyName

ÉNUMÉRATION DE PSEUDO SUR 600+ SITES

CE QUE ÇA FAIT

Teste la présence d'un pseudonyme sur des centaines de plateformes en quelques secondes. La liste est maintenue par la communauté et limite les faux positifs. Le point de départ de toute enquête sur identité.

The screenshot displays the 'WhatsMyName Web' interface. At the top, there is a search bar with the username 'tiosnt13' entered. Below the search bar, it indicates 'Active Filter: ALL'. The search results show 'Found: 1 Processed: 100 / 732'. A table lists the results, with one entry for 'Arch Linux GitLab' where the account was found. The table has columns for SITE, USERNAME, CATEGORY, and LINK. The interface also includes a 'Filter by Username' section with a search box and a 'Show 50 rows' dropdown.

SITE	USERNAME	CATEGORY	LINK
Arch Linux GitLab	tiosnt13	social	https://gitlab.archlinux.org/tiosnt13

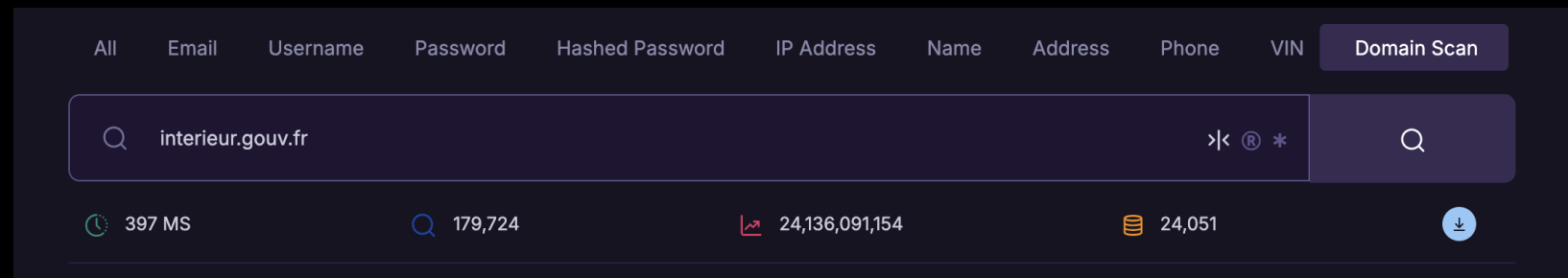
whatsmyname.app

DeHashed

RECHERCHE DANS LES FUITES DE DONNÉES

CE QUE ÇA FAIT

Moteur de recherche dans des milliards d'enregistrements issus de fuites : emails, identifiants, mots de passe, adresses, téléphones. Recherche croisée — un email mène à un mot de passe, qui mène à d'autres comptes.





















dehashed.com

Hudson Rock — Cavalier

CE QUE ÇA FAIT

Base mondiale des machines infectées par des infostealers. Sur un email, un domaine ou un username, révèle si la personne ou l'organisation a été compromise : identifiants volés, machines infectées, dates. API gratuite.

RENSEIGN

 Publix Super Markets publix.com	 Compromised Employees 7 429
	 Compromised Users 12 397
 iheartmedia iheartmedia.com	 Compromised Employees 18
	 Compromised Users 13
 Lam Research lamresearch.com	 Compromised Employees 65
	 Compromised Users 328
 Arrow Electronics arrow.com	 Compromised Employees 46
	 Compromised Users 2 895
 Celgene celgene.com	 Compromised Employees 10
	 Compromised Users 35
 Level 3 Communications level3.com	 Compromised Employees 82
	 Compromised Users 752

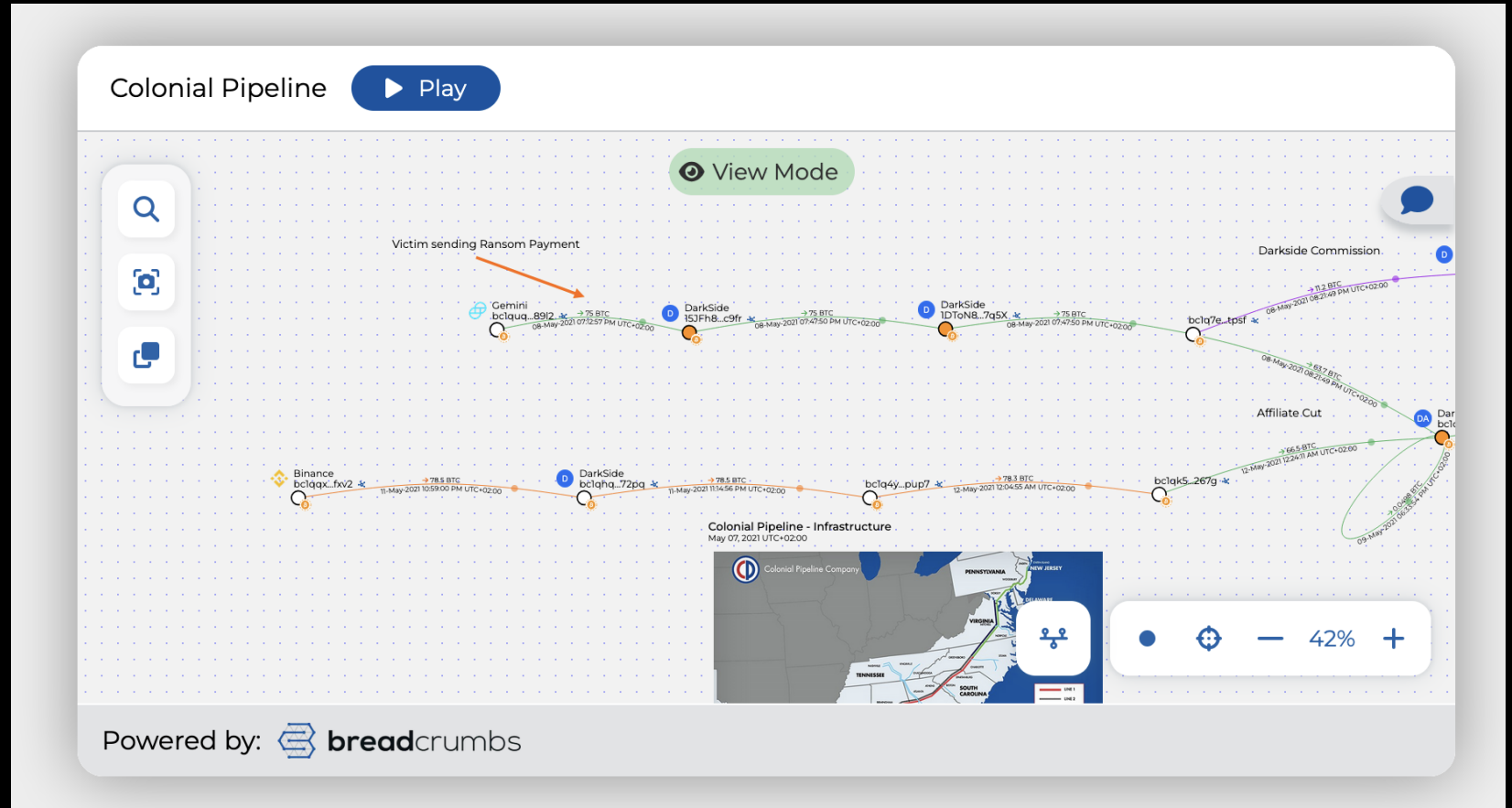
hudsonrock.com

Breadcrumbs

TRAÇAGE DE FLUX CRYPTO VISUEL

CE QUE ÇA FAIT

Outil de suivi des transactions blockchain orienté investigation : visualise les chemins entre wallets, étiquette les acteurs connus, exporte le graphe de flux. Une alternative accessible aux suites professionnelles.



breadcrumbs.app



B

Réflexes côté site web et images

Pas des outils — des gestes. Ce que tout site et toute image trahissent.

Le dépôt .git exposé

RECONSTRUIRE TOUT LE CODE SOURCE

LE RÉFLEXE

Quand un déploiement laisse le dossier .git accessible, on peut reconstituer l'intégralité du code source — et son historique. Les commits révèlent souvent l'email du développeur, des secrets supprimés, la chronologie du projet.

```
$ curl -s https://cible.tld/.git/HEAD
ref: refs/heads/main
$ git-dumper https://cible.tld/.git ./loot
$ cd loot && git log --format='%ae'
dev.scammer@gmail.com
```

`/.git/` • `git-dumper`

Les archives oubliées

LE ZIP DE TOUT LE SITE, À LA RACINE

LE RÉFLEXE

Les développeurs laissent souvent une sauvegarde à la racine : backup.zip, site.tar.gz, www.zip, old/. Téléchargeable d'un clic, elle contient parfois tout le code, les configs et les identifiants. Ton histoire de scammers démasqués par un zip entier.

```
# deviner les noms classiques
curl -sI cible.tld/backup.zip
curl -sI cible.tld/site.zip
curl -sI cible.tld/www.tar.gz
HTTP/2 200 · content-length: 48 MB
```

backup.zip · site.zip · old/ · www.tar.gz

Les fichiers de configuration

CLÉS ET IDENTIFIANTS EN CLAIR

LE RÉFLEXE

Un .env, un config.php.bak, un wp-config.php~ laissé accessible expose les identifiants de base de données, les clés d'API, les secrets de l'application. L'éditeur a sauvegardé, le serveur l'a servi.

```
curl -s cible.tld/.env
DB_PASSWORD=S3cr3t...
STRIPE_KEY=sk_live...
MAIL_USER=admin@cible.tld
# on constate. on ne s'en sert pas.
```

.env · config.php.bak · .conf~

Les source maps

DÉ-MINIFIER UNE APPLICATION WEB

LE RÉFLEXE

Les fichiers .js.map, livrés par erreur en production, permettent de reconstituer le code source original — lisible, commenté — d'une application 'minifiée'. On retrouve la logique, les routes d'API, parfois des secrets et des noms internes.

```
# le bundle référence sa source map
//# sourceMappingURL=index.js.map
$ curl -s cible.tld/assets/index.js.map \
  | npx source-map-explorer
→ code original, routes /api/admin, TODO nominatifs
```

`.js.map` • `sourceMappingURL`

Les erreurs et stack traces

LE SERVEUR SE CONFIE QUAND IL PLANTE

LE RÉFLEXE

Une erreur PHP ou applicative mal gérée affiche le chemin absolu sur le serveur, la structure des dossiers, la version des composants, parfois une requête SQL ou un identifiant. Provoquer une erreur, c'est faire parler le serveur.

```
Fatal error: in /home/scammer123/www/inc/db.php
Stack trace:
  #0 /home/scammer123/www/...
  → user système, arborescence, version PHP
```

chemins · versions · user système

Les métadonnées et la provenance C2PA

L'IMAGE AVOUE SA FABRICATION

LE RÉFLEXE

EXIF donne l'appareil, la date, parfois le GPS. Le manifeste C2PA, lui, prouve la génération par IA et embarque un certificat de signature — exploitable comme empreinte pour relier tous les visuels d'une même fabrique.

```
$ exiftool logo.png
Claim Generator : OpenAI Media Service
Digital Source  : trainedAlgorithmicMedia
Signature       : SSL.com C2PA (cert)
→ visuel généré par IA, daté, corrélable
```

exiftool · manifeste C2PA

Le favicon comme empreinte

UN HASH QUI DÉPLIE UN RÉSEAU

LE RÉFLEXE

Le favicon d'un site a un hash. Ce hash, requêté sur Shodan ou FOFA, retrouve tous les hôtes servant la même icône — y compris les IP d'origine derrière un CDN. Une icône partagée trahit une fabrique commune.

```
$ python3 -c 'import mmh3,requests,base64;
print(mmh3.hash(base64.encodebytes(
requests.get(URL+"/favicon.ico").content)))'
-1234567890
shodan: http.favicon.hash:-1234567890
```

mmh3 · http.favicon.hash

Les identifiants de tracking

RELIER LES SITES D'UN MÊME PROPRIÉTAIRE

LE RÉFLEXE

Un même code Google Analytics, AdSense ou Facebook Pixel sur deux sites trahit un propriétaire commun. Ces identifiants, en clair dans le code source, sont des empreintes de corrélation redoutables.

```
# dans le HTML
gtag("config", "G-AB12CD34")
# qui d'autre utilise ce même ID ?
publicwww.com "G-AB12CD34"
→ 6 domaines liés au même compte
```

UA- / G- / pixel → publicwww

Le code source et les commentaires

CE QUE LES DÉVELOPPEURS OUBLIENT

LE RÉFLEXE

Le HTML, le JS et les commentaires laissés en clair révèlent chemins de développement, noms internes, environnements de test, TODO nominatifs, anciennes URL. Lire la source brute reste un réflexe payant.

```
<!-- TODO: demander à karim de fix le paiement -->  
<!-- old: staging.cible-interne.tld -->  
<script src="/js/admin-debug.js">  
→ prénom, sous-domaine interne, script admin
```

view-source · Ctrl+U



IA appliquée à l'OSINT

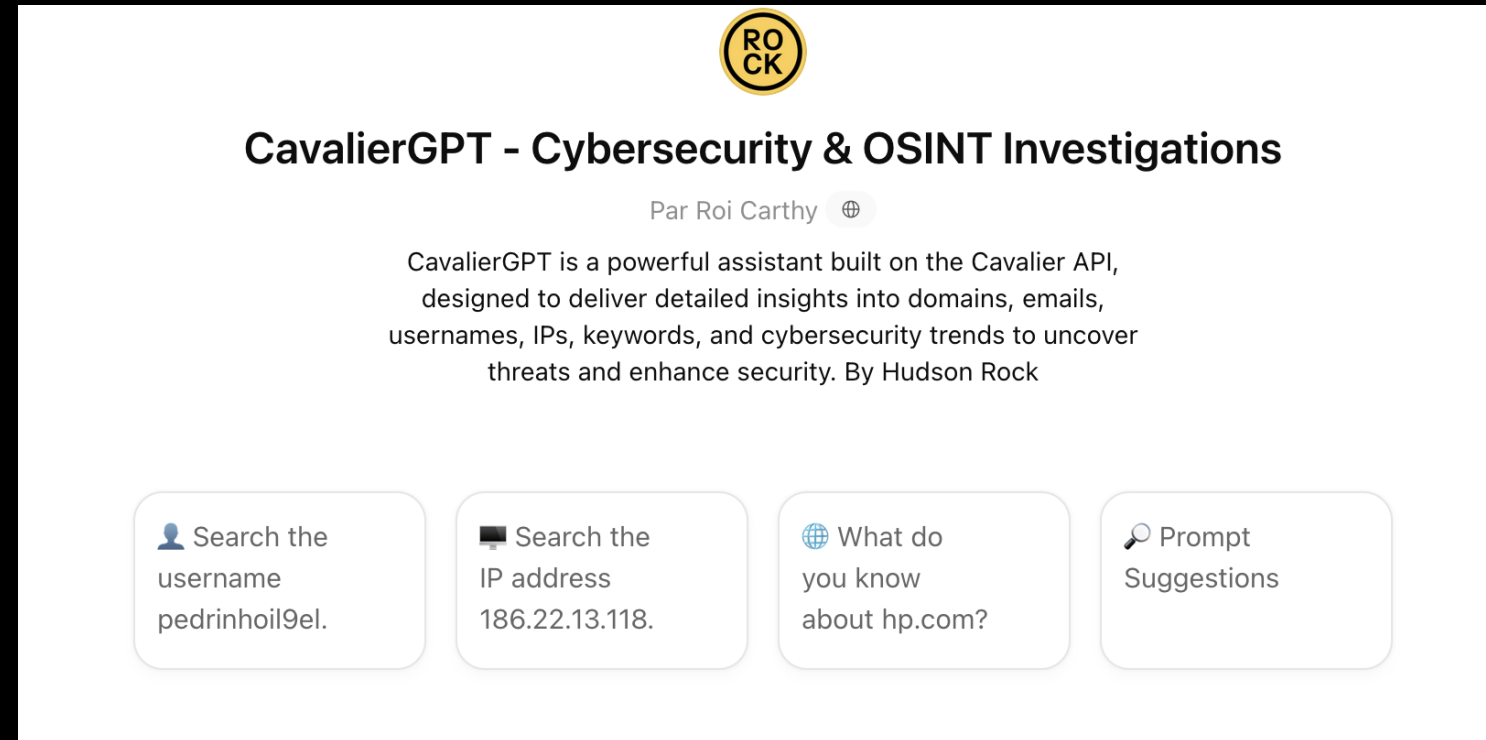
La nouvelle couche : accélérer, transcrire, corréler, géolocaliser.

Cavalier GPT

RENSEIGNEMENT INFOSTEALER EN LANGAGE NATUREL

CE QUE ÇA FAIT

L'interface conversationnelle de la base Hudson Rock : on interroge en langage naturel les compromissions par infostealer d'un email, domaine ou username, et l'IA synthétise machines infectées, identifiants et chronologie.



The screenshot displays the CavalierGPT interface. At the top center is the Hudson Rock logo, a yellow circle with 'ROCK' in black. Below it is the title 'CavalierGPT - Cybersecurity & OSINT Investigations' in bold black text. Underneath the title is the author 'Par Roi Carthy' with a globe icon. A paragraph describes the tool: 'CavalierGPT is a powerful assistant built on the Cavalier API, designed to deliver detailed insights into domains, emails, usernames, IPs, keywords, and cybersecurity trends to uncover threats and enhance security. By Hudson Rock'. At the bottom, there are four rounded rectangular buttons with icons and text: 1. A person icon, 'Search the username pedrinhoil9el.' 2. A computer monitor icon, 'Search the IP address 186.22.13.118.' 3. A globe icon, 'What do you know about hp.com?' 4. A magnifying glass icon, 'Prompt Suggestions'.

Disponible dans le GPT Store • hudsonrock.com

Transcription et analyse média par IA

FAIRE PARLER L'AUDIO

CE QUE ÇA FAIT

Les modèles multimodaux transcrivent un audio, traduisent, résumement une vidéo, décrivent une scène.

Des heures d'enregistrements ou de captations deviennent un texte searchable en minutes.

Transcription par IA gratuite

TurboScribe utilise l'IA pour transcrire vos fichiers audio et vidéo gratuitement.

Transcrire des fichiers

Fichier audio / vidéo



Glissez-déposez

MP3, MP4, M4A, MOV, AAC, WAV,
OGG, OPUS, MPEG, WMA, WMV

— OU —

PARCOURIR LES FICHIERS

Langue audio

Français 



 Reconnaissance des locuteurs et plus de paramètres 

TRANSCRIRE

Whisper (open source) • API multimodales



D

Créer vos propres outils

Quand aucun outil ne fait le job, on l'écrit. Quelques dizaines de lignes suffisent.

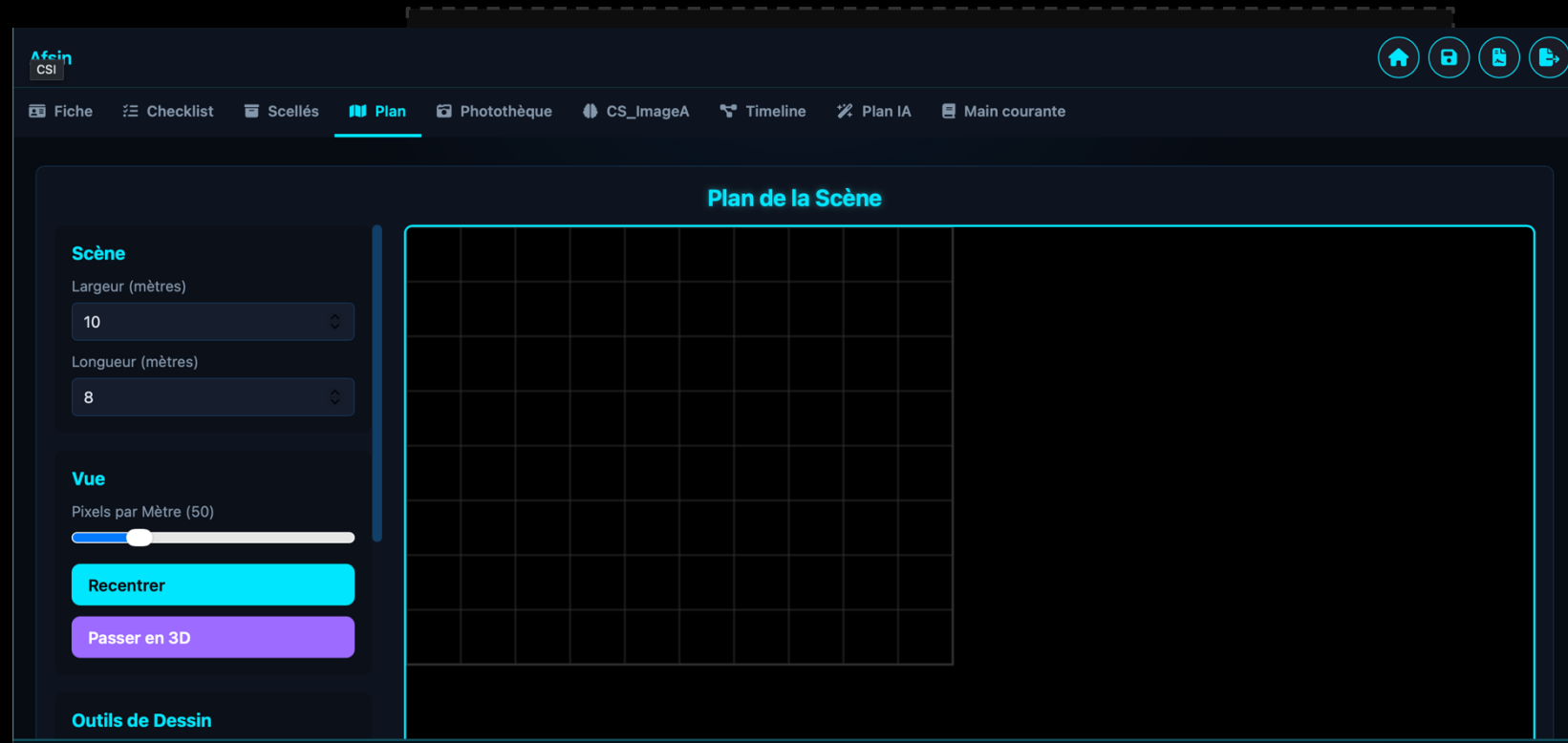
Le principe

POURQUOI CODER SES PROPRES OUTILS

LE PRINCIPE

Les outils publics sont génériques et parfois bridés. Un script maison fait exactement ce dont l'enquête a besoin, automatise le répétitif, et reste sous votre contrôle — aucune donnée ne part chez un tiers.

Trois briques suffisent : récupérer, analyser, enrichir. Assemblées, elles couvrent la majorité des besoins d'automatisation.



requests · BeautifulSoup · exiftool · API IA

Extracteur de liens

CARTOGRAPHIER UN SITE EN UNE DASSE

LE PRINCIPE

Un crawler parcourt un site et extrait toutes les URL : pages internes, liens externes, adresses mailto, numéros tel. En quelques secondes, on a la structure complète et les points de contact d'une cible — souvent un compte de paiement ou des emails cachés en pied de pages secondaires.

Récupère et classe **tous les liens** d'une page web (internes, externes, e-mails, ressources) via le moteur natif (sans CORS).

Extraire

✓ 122 élément(s) extrait(s).

internes (5)

externes (2)

ressources (114)

e-mails (1)

<https://new.afsin.org/adhesion-a-lafsin/>

<https://new.afsin.org/calendrier>

<https://new.afsin.org/cookie-policy/>

<https://new.afsin.org/forum-404/>

<https://new.afsin.org/politique-de-confidentialite/>

 Exporter

 Copier

requests · BeautifulSoup · urllib.parse

Extracteur automatique d'images

RÉCUPÉRER TOUS LES VISUELS D'UNE CIBLE

LE PRINCIPE

Un script collecte automatiquement toutes les images d'un site ou d'un profil : balises img, arrière-plans CSS, ressources liées. On constitue en une passe le corpus visuel complet — là où le clic-droit manuel prendrait une heure — prêt pour l'analyse de métadonnées en masse.

The screenshot displays the configuration interface of an image extraction tool. At the top, there is a button labeled "Ajouter profil". Below it, the "URL DE LA PAGE À ANALYSER" field contains "https://new.afsin.org". Three checkboxes are checked: "Afficher les images", "Lister les vidéos", and "Recherche récursive d'images". The "PROFONDEUR" dropdown is set to "2", and "PAGES MAX (BUDGET TOTAL)" is set to "40". There is also a checked checkbox for "Rester sur le même domaine" and an unchecked checkbox for "Incrémentation des pages". A blue "Lancer" button is visible. Below the configuration, a green checkmark indicates "Terminé.". The results section, titled "Images", shows "23 image(s) trouvée(s)". The first image is a poster for "GRUM4" dated "29 AVRIL 2026" in "MONTREAL, QUÉBEC, CANADA". Other images include a cityscape at night, a modern building, a group of people, a scenic view of a town, and a large building.

requests · BeautifulSoup · re

Analyse de métadonnées en masse

TOUTES LES IMAGES D'UN SITE, PASSÉES AU CRIBLE

LE PRINCIPE


Projet maison : on enchaîne l'extraction d'images d'un site et l'analyse automatique de leurs métadonnées — EXIF, GPS, logiciel créateur, provenance C2PA. Un site entier audité d'un coup, pour repérer fuites et fabrications.

Explore une page (et ses liens internes, en option) pour récupérer toutes les images, en extraire les métadonnées EXIF et cartographier celles qui contiennent des coordonnées GPS.


Analyser

Récursif (même domaine) Pages max Images max

55 image(s) analysée(s) · 7 avec EXIF · 0 géolocalisée(s).

 FORUM404.png 29 AVRIL 2026 641×336 · 306 Ko	
Dimensions	641×336
Taille	306.4 Ko
URL	https://new.afsin.org/wp-content/uploads/2026/04/FORUM404.png

Métadonnées images

 campus_marseille.jpg 1024×683 · 852 Ko	EXIF
--	-------------

requests · exiftool · traitement par lot

Appel et transcription par IA

FAIRE PARLER LES RÉPONDEURS

LE PRINCIPE

Projet maison : on fournit une liste de numéros, un service de téléphonie les appelle, enregistre l'annonce du répondeur, puis une IA transcrit l'audio et détermine si l'annonce révèle des informations sur le titulaire.

A · Capturer via Twilio

L'appel part d'un **numéro Twilio** (ton n° n'est pas exposé), enregistre l'annonce et la détecte (AMD).
Clés `twilio_sid/token/from` dans Paramètres.

NUMÉRO CIBLE (E.164)

+33612345678

NOM ATTENDU (POUR LE VERDICT, OPTIONNEL)

ex: Jean Dupont

 Appeler & capturer

Twilio · Whisper · API IA



E

Croque-escrocs

✓ Paiement 100% sécurisé ✓ Garantie 5 ans ✓ Expédition sous 24h ✓ +12 000 clients satisfaits

L'énergie premium au prix le plus bas du marché.

Batteries lithium haute performance, chargeurs rapides et powerbanks certifiés. Importés directement de nos usines — sans intermédiaire.





-70% AUJOURD'HUI

L'offre expire dans : **02:14:09**



Nos meilleures ventes

Sélection du moment — quantités très limitées

-65% 	-70% 	-60% 	-68% 
PowerCell X9 — 20 000 mAh ★★★★ (842) 29,90€ 89,90€ ⚠ Plus que 3 en stock	Chargeur UltraFast 120W ★★★★ (1 203) 24,90€ 82,90€ ⚠ Plus que 5 en stock	Powerbank Solar Pro ★★★★☆ (597) 34,90€ 87,90€ ⚠ Plus que 2 en stock	Batterie Garage 48V ★★★★ (311) 59,90€ 189,90€ ⚠ Bientôt épuisé

4,9/5
★★★★ note moyenne

12 480
clients satisfaits

24h
expédition garantie

-70%
jusqu'à ce soir

VoltKraft

Une fausse boutique de batteries « haut de gamme » à prix cassés. Encaisse, ne livre jamais.
Paiement carte et crypto. Beaucoup de victimes. Juste une URL.

LIQUIDATION TOTALE — Stocks limités ! Jusqu'à **-70%** sur toute la gamme · Livraison OFFERTE dès 49€

VoltKraft Accueil Batteries Chargeurs Powerbanks Pro Contact **Panier (0)**

✓ Paiement 100% sécurisé / Garantie 5 ans / Expédition sous 24h / +12 000 clients satisfaits

L'énergie premium au prix le plus bas du marché.

Batteries lithium haute performance, chargeurs rapides et powerbanks certifiées. Importés directement de nos usines — sans intermédiaire.

-70% AUJOURD'HUI

L'offre expire dans: **02:14:09**

Nos meilleures ventes

Sélection du moment — quantités très limitées

Produit	Remise	Note	Stock
PowerCell X9 — 20 000 mAh	-65%	★★★★ (842)	Plus que 3 en stock
Chargeur UltraFast 120W	-70%	★★★★ (1 203)	Plus que 5 en stock
Powerbank Solar Pro	-60%	★★★★ (597)	Plus que 2 en stock
Batterie Garage 48V	-68%	★★★★ (311)	Bientôt épuisé

4,9/5 ***** note moyenne
12 480 clients satisfaits
24h expédition garantie
-70% jusqu'à ce soir

VoltKraft Store © 2026 — VoltKraft Ltd. 128 City Road, London · contact@voltkraft-store.com · Paiement sécurisé Visa · Mastercard · Crypto

ACTE 1 Le terrain

On commence sans rien toucher. La réputation confirme l'arnaque — mais une trouvaille change l'échelle : la structure de la page a déjà été vue ailleurs.

Le site n'est peut-être pas seul.

OUTILS MOBILISÉS

Scamdoc

signal-arnaques

urlscan.io

→ l'historique urlscan montre la même page sous deux autres domaines. On creuse l'infra.

ACTE 2 L'infrastructure

Domaine de cinq semaines, derrière Cloudflare : l'IP réelle est masquée. Mais l'historique DNS garde la mémoire des premières heures, avant l'activation du CDN.

Dans cette fenêtre, l'IP d'origine était exposée.

OUTILS MOBILISÉS

whois / dig

Validin

DNSDumpster

crt.sh

→ Validin livre l'IP d'origine brute. crt.sh sort un sous-domaine old. oublié, encore en ligne.

ACTE 3 Le site se déshabille

Le sous-domaine old. sert un listing ouvert : un backup.zip de 60 Mo, le kit complet. À la racine, un .git exposé. git-dumper reconstruit le dépôt — et les commits lâchent l'email du développeur.

OUTILS MOBILISÉS

`.git → git-dumper`

`backup.zip`

`fichier .env`

`favicon hash`

`ID Analytics G-...`

→ email dev récupéré, ID de tracking et favicon notés comme empreintes de corrélation.

ACTE 4 Un site devient un réseau

Les empreintes uniques croisées sur plusieurs moteurs convergent. L'IP d'origine, le favicon et l'ID de tracking pointent les mêmes cibles.

La fabrique apparaît : six boutiques jumelles, un seul opérateur.

OUTILS MOBILISÉS

FOFA

ZoomEye

Netlas

PublicWWW

→ intersection des trois méthodes = une grappe de six sites. On passe d'un scam à un sériel.

ACTE 5 Les images parlent

On aspire les visuels des six sites et on les passe au crible. La plupart sont propres — mais quelques-uns ont échappé au nettoyage.

Un EXIF GPS oublié, un logo signé par l'IA, un arrière-plan géolocalisable.

OUTILS MOBILISÉS

Extracteur d'images (maison)

Analyse métadonnées (maison)

exiftool / C2PA

GeoSpy · Picarta

→ GPS sur trois photos produit, logo prouvé généré par IA, entrepôt géolocalisé en Europe de l'Est.

ACTE 6 On remonte à l'humain

L'email du .git devient le fil. Une plateforme d'agrégation déballe les comptes liés, un pseudo récurrent, une timeline. On déroule pseudo et fuites — puis vient le coup de grâce.

OUTILS MOBILISÉS

OSINT Industries

WhatsMyName · Maigret

DeHashed

Hudson Rock / Cavalier

→ l'opérateur a lui-même une machine infectée par infostealer. L'arroseur arrosé.

ACTE 7 Le téléphone

Le numéro sorti des fuites colle au profil géographique. On le qualifie, puis on le fait parler : un appel automatisé capte l'annonce du répondeur, qu'une IA transcrit et analyse.

OUTILS MOBILISÉS

PhoneInfoga

Twilio (maison)

Whisper + IA

→ l'annonce du répondeur contient un prénom et un nom. Ils recourent le GitHub de l'acte 6.

ACTE 8 L'argent

Une partie des victimes a payé en crypto. Le wallet n'est pas une impasse :
Les sauts successifs se suivent jusqu'à un point où l'anonymat se brise.

OUTILS MOBILISÉS

Arkham

Breadcrumbs

→ les fonds convergent vers un dépôt sur un exchange identifié — soumis à obligation d'identification.

ACTE 9 Le faisceau

LA CHAÎNE, D'UN BOUT À L'AUTRE

URL → réputation → IP d'origine → grappe → images (GPS/C2PA) → email → identité → téléphone → argent → **faisceau**

CE QU'ON A ÉTABLI

Un opérateur unique derrière six boutiques jumelles — même template, même backend, identité visuelle générée par IA. Relié à un email et un pseudo exposés par ses propres négligences (.git, fuites, infostealer), un téléphone confirmé à l'oral, un wallet traçable jusqu'à un exchange identifiable.

Aucune intrusion. On signale : abuse hébergeur, processeurs de paiement, exchange, autorités. L'OSINT documente et transmet — il ne franchit jamais la porte.

Merci
