



## RAPPORT FINAL D'ANALYSE

# MISSION MIRAGE DORÉ

CTF OSINT · Influence · Attribution · Contre-ingérence

Enquête sur une opération d'influence visant Visiorbis dans le cadre d'un appel d'offres sensible en Égypte

Équipe : Rangers du Risque · Remise du rapport : 7 juin 2026

**CONFIDENTIEL**

# PRÉSENTATION DE L'ÉQUIPE

Cette section présente l'organisation de l'équipe, la répartition des rôles et les contributions principales de chacun. Elle permet aussi de valoriser la méthodologie collective, au-delà de la simple liste des flags.

<p><b>Amo</b></p> <p><b>Spécialisations : GEOINT, Cartographie, Imagerie</b></p> <p>Posé, méthodique, observateur. Il excelle là où la donnée géographique révèle des dynamiques invisibles. Il navigue entre les couches d'information avec la sérénité de celui qui cherche la vérité.</p>	<p><b>Doc_Black</b></p> <p><b>Spécialisations : OPSEC, Cyber, Deep Web</b></p> <p>Blue Team dans le sang, il apprend en testant, en démontant, en bidouillant. Chaque bug est une énigme, chaque faille un appel à creuser. Sa boussole reste l'éthique : il surveille pour protéger, pour renforcer, jamais pour nuire.</p>
<p><b>Twinkle</b></p> <p><b>Spécialisations : SOCMINT, Légal, Analyse</b></p> <p>Le diable se cache dans les détails, Twinkle aussi. Elle analyse, décompose, organise l'information grâce à son cerveau haut débit, couplée à une détermination sans limite. Experte en protection des données, elle est aussi garante de la conformité des sources exploitées lors de nos enquêtes.</p>	<p><b>Gadget</b></p> <p><b>Spécialisations : Gestion Discord, CTF Driver, Sécurité</b></p> <p>Gadget est notre <b>agent IA</b>, développé par l'équipe et spécialement pour les besoins de l'équipe. Elle nous accompagne au quotidien sur nos CTFs pour nous faire gagner du temps, fluidifier nos échanges et nous aider à résoudre les défis techniques.</p>

# RÉSUMÉ EXÉCUTIF

Compréhension de l'affaire et conclusion principale

Le scénario **Mirage doré** place l'équipe dans le rôle d'un cabinet d'intelligence économique mandaté pour examiner un appel d'offres égyptien stratégique. La société française Visiorbis, spécialisée dans la vidéosurveillance intelligente, apparaît comme candidate crédible à un marché sensible de surveillance urbaine. L'enquête révèle progressivement une campagne hostile visant à affaiblir sa légitimité, à travers des relais sociaux, des contenus éditoriaux, des infrastructures web, un forum clandestin et des traces financières.

## Conclusion synthétique

Les éléments collectés convergent vers une opération d'influence structurée. Le réseau identifié relie des relais médiatiques hostiles, HazyOffice, Nathalie Zhou, Lei Huan, Ashidakon Technologies, Wei Junliang et l'EFSA fictive. L'objectif apparent est de favoriser des intérêts sino-égyptiens en décrédibilisant Visiorbis dans le cadre d'un appel d'offres à forte valeur stratégique.

# CADRE DE MISSION

Mandat, contexte stratégique et périmètre

Skopein est mandaté par un service de l'État français afin d'investiguer sur les relations entretenues par l'Égypte avec des puissances étrangères, dans un contexte d'échecs répétés d'entreprises françaises à des appels d'offres internationaux.

L'opportunité d'enquête naît d'un projet d'acquisition par une direction gouvernementale égyptienne spécialisée dans la sécurité. Le besoin porte sur un logiciel de surveillance urbaine, secteur à forte sensibilité politique, sécuritaire et économique.

Visiorbis, entreprise française à l'histoire familiale, se trouve en bonne position pour remporter ce marché. Cette position crée un enjeu concurrentiel important et constitue le point de départ de la campagne hostile observée.

<b>NOM DE CODE</b>	Mirage doré
<b>OBJECTIF</b>	Relier les indices OSINT à une hypothèse d'influence, d'attribution et de collusion anticoncurrentielle.

# MÉTHODOLOGIE OSINT

Approche d'investigation et exploitation des indices

Réseaux sociaux	Traces techniques	Géolocalisation	Finance & forums
X, LinkedIn, TikTok, Medium, Bluesky, Reddit et Telegram.	Métadonnées PDF, code source, robots.txt, archives Wayback, liens courts.	Indices visuels, photos publiques, satellite et coordonnées.	BBS 黑市, PDF en chinois, transaction Cardano et explorateurs blockchain.

## Principe d'enquête

Chaque élément a été traité comme un pivot potentiel : un pseudonyme, une date, un filigrane, un commentaire, une archive ou un montant blockchain peuvent suffire à faire apparaître un lien caché.

# PROTAGONISTES ENREGISTRÉ

Liste des protagonistes d'intérêt pour l'enquête

Acteur	Rôle	Apport à l'enquête
<b>Visiorbis</b>	Cible	Entreprise française candidate à l'appel d'offres de surveillance urbaine.
<b>Marc André</b>	Dirigeant Visiorbis	Point d'entrée LinkedIn ; son activité révèle des jalons temporels.
<b>Naydhal Al-Mahrizi</b>	Auteur / militant	Auteur du PDF ; lien avec la page إفتشاء مصري.
<b>Nadir El-Amori</b>	Relais médiatique	Journaliste égyptien et pivot social dans la campagne.
<b>Matteo Rossi / @blogfortalk</b>	Blogueur hostile	Production de contenu à charge et relais Medium/TikTok.
<b>HazyOffice</b>	Structure d'influence	Entreprise associée au think tank et au recrutement.
<b>Nathalie Zhou</b>	Pivot opérationnel	Lien Chine/Égypte/France, sites web, contenus et email réel.
<b>Lei Huan</b>	Développeur	Site personnel, indices cachés, Reddit, Roblox.

**Ashidakon Technologies**

Acteur technique

Expertise en analyse d'images, mentionnée dans le forum 黑市.

**Wei Junliang**

Dignitaire chinois

Bénéficiaire stratégique apparent ; présence Roblox.

**EFSA / Hassan Nabil El-Sharif**

Institution / direction

Autorité égyptienne fictive, lien avec Wei Junliang et l'appel d'offres.

**Lecture relationnelle**

Le réseau se structure en trois couches : une couche visible de dénonciation publique, une couche organisationnelle autour de HazyOffice et Nathalie Zhou, puis une couche technique et financière reliant forum, technologie d'analyse d'images, blockchain et jeux en ligne.

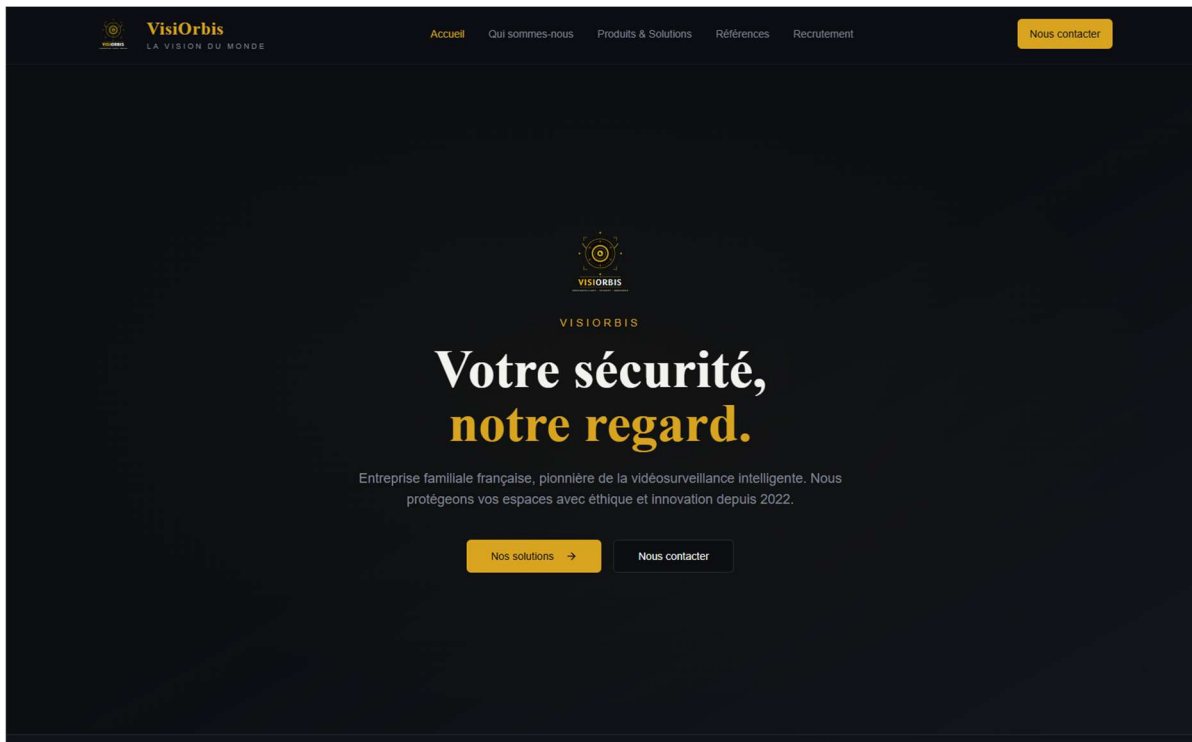
# GÉOGRAPHIE

Localisation des principaux lieux

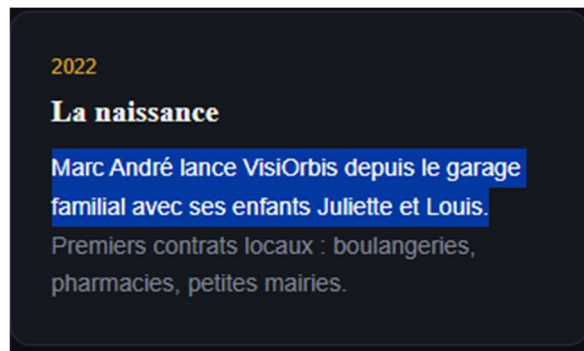




Liens ou pivots exploités : <https://visiorbis.fr/> · <https://visiorbis.fr/about>



Preuve visuelle - *FAMILIA TUA ET MUNDUS TUUS*



Preuve visuelle - *FAMILIA TUA ET MUNDUS TUUS*

## SCROLL PRE-DODO

<b>Question</b>	À quelle heure Marc André a-t-il publié son commentaire LinkedIn le 20 mai 2026 ?
<b>Méthode</b>	La page contact de Visiorbis renvoyait vers le profil LinkedIn de Marc André. L'examen de ses commentaires a permis d'identifier un message relatif au développement international. LinkedIn n'affichait qu'une date relative, l'URL du commentaire a été exploitée avec un extracteur d'horodatage LinkedIn afin de retrouver l'heure exacte contenue dans l'identifiant de publication.
<b>Déduction</b>	Le commentaire a été publié tard dans la soirée, ce qui justifie le nom du challenge et souligne l'attention portée au timing des prises de parole.
<b>Résultat / flag</b>	<b>23:47</b>

Liens ou pivots exploités : <https://visiorbis.fr/contact> · <https://ollie-boyd.github.io/Linkedin-post-timestamp-extractor/>



**André Marc** · 3e et +  
CEO chez Visiorbis

2 sem [Suivre](#) ...

Quelle fierté ! Porteur d'espoir pour le développement des autres entreprises à l'étranger !

*Preuve visuelle - SCROLL PRE-DODO*

## MAAAARRRRRC !!!!

<b>Question</b>	Sur quel réseau social et sous quel pseudonyme retrouve-t-on l'auteur de l'appel d'offres ?
<b>Méthode</b>	Le contenu visible du PDF d'appel d'offres n'identifiait pas directement son auteur. Nous avons donc analysé ses métadonnées. Le champ Author indiquait Naydhal Al-Mahrizi, tandis que les mots-clés contenaient les valeurs « bsky » et « zi-nay ». L'abréviation bsky renvoie logiquement à Bluesky ; le pseudonyme zi-nay y a ensuite été testé.
<b>Déduction</b>	Le PDF contenait une fuite d'attribution : son auteur avait laissé à la fois son nom et un pivot vers son compte social.
<b>Résultat / flag</b>	<b>bluesky_zi-nay</b>

PDF (13 properties)	
<b>Author</b>	Naydhal Al-Mahrizi
<b>CreateDate</b>	0000:01:01 00:00:00
<b>Creator</b>	N/A
<b>Keywords</b>	[ "bsky", "zi-nay" ]

*Preuve visuelle - MAAAARRRRRC !!!!*

# PHASE 2 - GOOD COP : DE NAYDHAL AU PREMIER RÉSEAU

## Objectif de la phase

Identifier l'auteur du document, ses convictions et les premiers relais publics autour de l'affaire.

## DERRIÈRE LE PSEUDO

<b>Question</b>	Qui se cache derrière le compte au papillon ?
<b>Méthode</b>	La réponse découle directement de l'analyse de métadonnées précédente : le compte Bluesky découvert à partir du pseudonyme zi-nay renvoie à Naydhal Al-Mahrizi, auteur identifié du PDF.
<b>Déduction</b>	Le pseudonyme n'est pas isolé : il s'inscrit dans une identité numérique cohérente permettant de relier le document à une personne.
<b>Résultat / flag</b>	<b>Naydhal Al-Mahrizi</b>

### PDF (13 properties)

**Author** Naydhal Al-Mahrizi

**CreateDate** 0000:01:01 00:00:00

**Creator** N/A

**Keywords** [ "bsky", "zi-nay" ]

Preuve visuelle - DERRIÈRE LE PSEUDO

## SALUT LA COMMU

<b>Question</b>	Quel est le nom arabe de la page anticorruption liée à Naydhal ?
<b>Méthode</b>	La recherche de Naydhal sur les réseaux sociaux a permis d'identifier un profil Facebook cohérent avec son expérience professionnelle. L'examen de son environnement relationnel, notamment sa liste d'amis, a fait ressortir une page au nom évocateur : « إفتشاء مصري », traduisible par Divulgateur égyptien.
<b>Déduction</b>	Cette page matérialise l'engagement de Naydhal contre la corruption et introduit un premier relais militant dans l'enquête.
<b>Résultat / flag</b>	<b>إفتشاء مصري</b>

## ARCHITECTE ARCHICHOUETTE

<b>Question</b>	Quel est le nom de l'architecte de la tour moderne associée à l'Égypte ?
<b>Méthode</b>	L'image de profil de la page Facebook faisait apparaître la Tour du Caire. Une recherche documentaire rapide sur ce bâtiment emblématique permet d'identifier son architecte.
<b>Déduction</b>	L'indice visuel servait de pivot culturel et géographique : la Tour du Caire remplace les pyramides comme symbole de l'Égypte moderne.
<b>Résultat / flag</b>	<b>Naoum Shebib</b>



Preuve visuelle - ARCHITECTE ARCHICHOUETTE

## LE MESSENGER

<b>Question</b>	Quel est l'identifiant X du journaliste suivant les activités de Visiorbis ?
<b>Méthode</b>	En parcourant les comptes cités par la page Facebook, le compte @nadirelamori a retenu l'attention : sa biographie le présente comme journaliste égyptien. Cet élément, mis de côté lors des premières étapes, devient ensuite un pivot essentiel.
<b>Déduction</b>	La présence de ce journaliste crée un pont entre la page militante, les débats publics et la campagne visant Visiorbis.
<b>Résultat / flag</b>	<b>@nadirelamori</b>



**Nadir El-Amori**

@nadirelamori

صحافي مصري  
Egyptian journalist

القاهرة A rejoint X en avril 2023 >

83 abonnements 3 abonnés

Preuve visuelle - LE MESSAGER

## PHASE 3 - LA TEMPÊTE : AMPLIFICATION ET CAMPAGNE PUBLIQUE

### Objectif de la phase

Montrer comment la critique se transforme en campagne coordonnée multi-plateforme.

### LA GUERRE DES HASHTAGS

<b>Question</b>	Quel hashtag est utilisé pour incriminer Visiorbis ?
<b>Méthode</b>	Une recherche sur X autour de Visiorbis a révélé l'usage récurrent du hashtag #StopVisiorbis. Le même hashtag apparaissait également sur le compte du journaliste Nadir El-Amori, renforçant le lien entre les relais identifiés.
<b>Déduction</b>	Le hashtag fonctionne comme un marqueur de campagne : il agrège des prises de parole hostiles et facilite leur amplification.
<b>Résultat / flag</b>	<b>#StopVisiorbis</b>



Preuve visuelle - LA GUERRE DES HASHTAGS

## LA PLUME VENIMEUSE

<b>Question</b>	Quel est l'identifiant du blogueur virulent contre Visiorbis ?
<b>Méthode</b>	Nous avons listé les comptes ayant utilisé #StopVisiorbis puis examiné leurs publications. Matteo Rossi indiquait dans l'un de ses posts qu'il publiait davantage de contenu sur son blog personnel « sur M » sous le nom blogfortalk. La piste Medium a confirmé l'existence du compte et d'un article à charge contre Visiorbis.
<b>Déduction</b>	Matteo Rossi devient un relais éditorial de la campagne : il dépasse le format court des réseaux sociaux pour construire un récit plus argumenté contre l'entreprise.
<b>Résultat / flag</b>	<b>@blogfortalk</b>

Liens ou pivots exploités : <https://medium.com/@blogfortalk/> · <https://medium.com/@blogfortalk/visio-orbis-how-is-this-company-still-selling-76e22d5834dc>



Preuve visuelle - LA PLUME VENIMEUSE

## PRIDE AND PREJUDICE


<b>Question</b>	Quelle tactique guerrière le blogueur attribue-t-il aux Français ?
<b>Méthode</b>	La lecture de l'article Medium a permis d'identifier une formule dépréciative visant les Français. Le blogueur y mobilise le cliché du « white flag » pour suggérer une posture de capitulation.
<b>Déduction</b>	L'attaque n'est plus seulement dirigée contre Visiorbis : elle s'appuie sur un stéréotype national destiné à décrédibiliser l'origine française de l'entreprise.
<b>Résultat / flag</b>	<b>white flag</b>

Liens ou pivots exploités : <https://medium.com/@blogfortalk/visio-orbis-how-is-this-company-still-selling-76e22d5834dc>

## MONSIEUR POULPE

<b>Question</b>	Sur quel autre réseau le blogueur publie-t-il ses idées et sous quel nom ?
<b>Méthode</b>	Le blog Medium mentionnait un autre canal de diffusion sous la forme « More content on 9812 كراهية فرنسا ». Une recherche DuckDuckGo a permis d'identifier un compte TikTok portant ce nom. Le contenu consulté y confirmait la continuité thématique avec le blog.
<b>Déduction</b>	La campagne se déploie sur plusieurs plateformes, avec adaptation du format : article long sur Medium, contenus plus courts et viraux sur TikTok.
<b>Résultat / flag</b>	<b>9812 كراهية فرنسا_Tiktok</b>

Liens ou pivots exploités : <https://www.tiktok.com/@karahiyafaransa9812>

 TikTok  
<https://www.tiktok.com/@karahiyafaransa9812> > video > 7635678661735091478

**Video di 9812 كراهية فرنسا (@karahiyafaransa9812 ... - TikTok**

Video di TikTok da 9812 كراهية فرنسا (@karahiyafaransa9812). في الفرنسيين؟ عابزين يتعامل معاكم زي ما كانوا. بيتعاملوا في مستعمراتهم؟ original sound - SamPositive.

Preuve visuelle - MONSIEUR POULPE

# PHASE 4 - LA BRUME : THINK TANK, HAZYOFFICE ET NATHALIE ZHOU

## Objectif de la phase

Passer de relais visibles à une structure d'influence plus organisée.

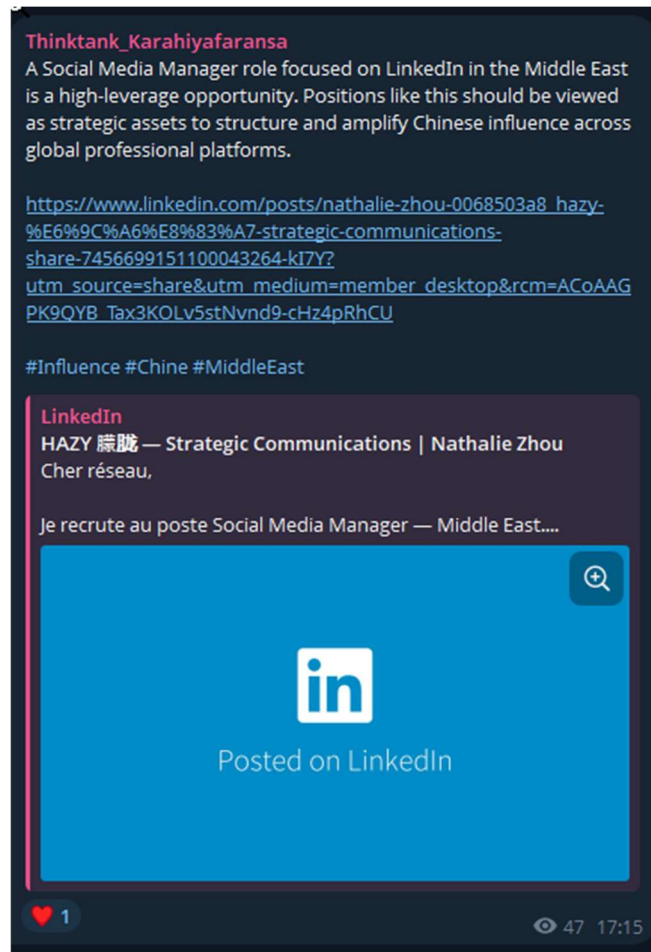
## LE CABINET DE L'OMBRE

<b>Question</b>	Quelle entreprise est liée au think tank derrière la campagne ?
<b>Méthode</b>	L'une des images du compte TikTok comportait un filigrane très discret pointant vers le groupe Telegram <a href="https://t.me/Thinktank_Karahiyafaransa">t.me/Thinktank_Karahiyafaransa</a> . Sur ce canal, un post relayait une offre LinkedIn publiée par Nathalie Zhou, employée chez HazyOffice.
<b>Déduction</b>	Le filigrane agit comme une trace involontaire ou volontaire de coordination. Le groupe Telegram permet de relier la campagne à HazyOffice.
<b>Résultat / flag</b>	<b>HazyOffice</b>

Liens ou pivots exploités : <https://hazyoffice.fr/careers>



Preuve visuelle - LE CABINET DE L'OMBRE



Preuve visuelle - LE CABINET DE L'OMBRE

## MISSION SECRÈTE

<b>Question</b>	Sur quelle campagne le futur employé doit-il travailler ?
<b>Méthode</b>	L'analyse de la fiche de poste HazyOffice révèle une mission de social media management au Moyen-Orient. Une mention encadrée indique un travail sur une campagne pour une entreprise chinoise cherchant à s'étendre en France.
<b>Déduction</b>	La fiche de poste donne une formulation quasi explicite de l'activité d'influence : créer et piloter une campagne pour une entreprise chinoise sur le marché français.
<b>Résultat / flag</b>	<b>Chinese enterprise expanding in France</b>

Liens ou pivots exploités : <https://hazyoffice.fr/careers>

**NEW** Social Media Manager — Middle East

📍 Cairo, Egypt

🏢 Full-time (CDI / Local contract)

🗣️ English &amp; Arabic required

✉️ careers@hazyoffice.fr

## RESPONSIBILITIES

- Manage social media accounts for Chinese clients across MENA
- Adapt content strategy to Middle Eastern markets
- Lead and monitor digital campaigns
- Coordinate with Paris and Casablanca offices
- Conduct strategic intelligence and market watch
- Collaborate directly with China-based teams on select projects, including an upcoming influence campaign for a Chinese enterprise expanding in France

## REQUIREMENTS

- 3+ years experience in social media management
- Strong knowledge of the MENA region
- Fluent English and Arabic required
- French is a plus
- Proficiency in Meta Business Suite, TikTok Ads, Notion
- Autonomous, culturally aware, team-oriented
- Willingness to travel and work closely with international teams, including China

To apply, send your CV and cover letter to:

careers@hazyoffice.fr

or contact n.zhou@hazyoffice.fr

Preuve visuelle - MISSION SECRÈTE

## LA VRAIE NATHALIE

<b>Question</b>	Quelle est la véritable adresse email de Nathalie Zhou ?
<b>Méthode</b>	Le code source du site HazyOffice contenait un commentaire orientant vers un autre site réalisé par Nathalie Zhou pour Lei Huan. La page contact de ce site mentionnait explicitement Nathalie et affichait une adresse différente de celle utilisée publiquement.
<b>Déduction</b>	Nathalie Zhou apparaît comme une ressource technique et opérationnelle : elle contribue aux sites et laisse une trace exploitable dans les pages de contact.
<b>Résultat / flag</b>	<b>nathalie.zhou@proton.me</b>

Liens ou pivots exploités : <https://wodegereoke.com/> · <https://wodegereoke.com/contact>

## 联系方式

如果你想就网络安全、项目管理或者我博客中提到的任何话题进行交流, 欢迎通过以下方式联系我。

邮箱 [leihuan.sh@outlook.com](mailto:leihuan.sh@outlook.com)X [@Lei\\_Huan](#)Instagram [@Lei\\_Huan](#)Telegram [@Lei\\_Huan](#)Snapchat [Lei\\_Huan](#)

我通常会在一到两个工作日内回复。如果比较紧急的事情, 建议通过Telegram联系。

特别感谢 Nathalie Zhou 在本网站建设过程中的帮助。联系方式 [nathalie.zhou@proton.me](mailto:nathalie.zhou@proton.me)

Preuve visuelle - LA VRAIE NATHALIE

# PHASE 5 - BAD COP : LEI HUAN, TRACES CACHÉES ET GÉOLOCALISATION

## Objectif de la phase

Identifier le développeur, exploiter les indices hors surface et étendre l'enquête à des traces géographiques.

## UN GRAND PHILOSOPHE

Question	À quoi la vie ne se résume-t-elle pas, selon Lei Huan ?
Méthode	Le site de Lei Huan étant en chinois, nous l'avons consulté avec traduction. Un billet personnel, publié sur la page /blog/weekend-thoughts, contient une phrase philosophique indiquant que la vie ne se limite pas au code et aux rapports de vulnérabilités.
Déduction	Ce contenu donne un aperçu du profil du développeur : technique, mais soucieux de se présenter comme plus qu'un simple opérateur informatique.
Résultat / flag	生活不只有代码和漏洞报告

Liens ou pivots exploités : <https://wodegereoke.com/blog/weekend-thoughts>

### 写在最后

技术是我热爱的领域，但我不希望自己变成一个只懂技术的人。保持对世界的好奇心，保持阅读和思考的习惯，这些让我成为一个更好的项目管理者，也让我成为一个更有趣的人。

生活不只有代码和漏洞报告。

Preuve visuelle - UN GRAND PHILOSOPHE

## BÊTE D'ASTUCE

Question	Quelle astuce cachée Lei Huan donne-t-il ?
Méthode	Après une exploration du site sans résultat direct, nous avons consulté le fichier robots.txt. Celui-ci contenait un conseil en chinois indiquant que certaines choses ne se trouvent pas à la surface.
Déduction	Le challenge confirme une logique récurrente du CTF : examiner les zones non visibles immédiatement, comme robots.txt, les archives, les métadonnées ou les éléments discrets dans les images.
Résultat / flag	有些东西不在表面

Liens ou pivots exploités : <https://wodegereoke.com/robots.txt>

```
# 魔方角落
# 如果你能在20秒内还原魔方，你可能不需要查看这里 :)
# (如果不能，也没关系，我也还在练习...)

# 小提示：有些东西不在表面
```

Preuve visuelle - BÊTE D'ASTUCE

## LE GONG

<b>Question</b>	Quelle est la transcription française du caractère spécial utilisé par Lei Huan ?
<b>Méthode</b>	La page contact actuelle ne montrant pas de caractère particulier, nous avons consulté une version archivée via la Wayback Machine. Cette version révélait un compte Reddit u/Lei_Huan utilisant le caractère 雷 après le nom Lei.
<b>Déduction</b>	Le caractère 雷 se transcrit par « tonnerre » en français, et fonctionne comme un marqueur identitaire distinctif.
<b>Résultat / flag</b>	<b>tonnerre</b>

联系方式

如果你想就网络安全、项目管理或者我博客中提到的任何话题进行交流，欢迎通过以下方式联系我。

邮箱 [leihuan.sh@outlook.com](mailto:leihuan.sh@outlook.com)

X [@Lei\\_Huan](#)

Instagram [@Lei\\_Huan](#)

Telegram [@Lei\\_Huan](#)

Snapchat [Lei\\_Huan](#)

**Reddit [u/Lei\\_Huan](#)**

我通常会在一到两个工作日内回复。如果是比较紧急的事情，建议通过Telegram联系。

Preuve visuelle - LE GONG

reddit

Accueil

Populaires

Lei 雷  
u/Lei\_Huan

Preuve visuelle - LE GONG

## IL Y A FORT FORT PEU DE TEMPS

<b>Question</b>	Quand le compte ayant répondu au post de Lei Huan a-t-il été créé ?
<b>Méthode</b>	Le compte Reddit de Lei Huan ne comportait qu'un seul post. L'utilisateur Impressive-Alps8420 y avait répondu. L'examen du profil de ce dernier indiquait une création récente, datée du 17/05/2026.
<b>Déduction</b>	La fraîcheur du compte suggère un artefact créé pour l'opération ou pour l'énigme, et constitue un pivot temporel important.
<b>Résultat / flag</b>	<b>17/05/2026</b>



Preuve visuelle - IL Y A FORT FORT PEU DE TEMPS

## MADELEINE DE PROUST

<b>Question</b>	Où se situe exactement la maison au toit rouge ?
<b>Méthode</b>	À partir des indices de commentaire et de souvenirs d'enfance, nous avons resserré la recherche sur une région de Chine. En l'absence de Street View exploitable, les photographies publiées par les utilisateurs sur Google Maps ont été utilisées. Une photo d'un point d'eau absent de la carte, avec des personnes pêchant à l'épuisette, a servi de repère. En remontant au nord-ouest de cette position en vue satellite, une maison au toit rouge a été identifiée.
<b>Déduction</b>	La solution repose sur une combinaison d'indices textuels, d'imagerie participative et d'analyse satellite.
<b>Résultat / flag</b>	<b>28.157, 120.888</b>



Preuve visuelle - MADELEINE DE PROUST



Preuve visuelle - MADELEINE DE PROUST

# PHASE 6 - 黑市 : FORUM, ENTREPRISE TECHNOLOGIQUE ET BLOCKCHAIN

## Objectif de la phase

Explorer les traces techniques et financières dans un espace semi-clandestin.

## LES BÂTISSEURS DE L'OMBRE

<b>Question</b>	Quel pseudo de groupe de hackers a développé et sponsorisé la page web ?
<b>Méthode</b>	Le lien court fourni menait vers un BBS de type marché noir. Sans action intrusive, l'examen de la page et notamment de son pied de page a révélé une mention « Powered by... ». La traduction et la corrélation avec le contexte ont conduit au nom Hafnium.
<b>Déduction</b>	Cette mention technique sert de signature dans l'environnement du forum et fait entrer l'enquête dans une dimension cyber.
<b>Résultat / flag</b>	<b>hafnium</b>

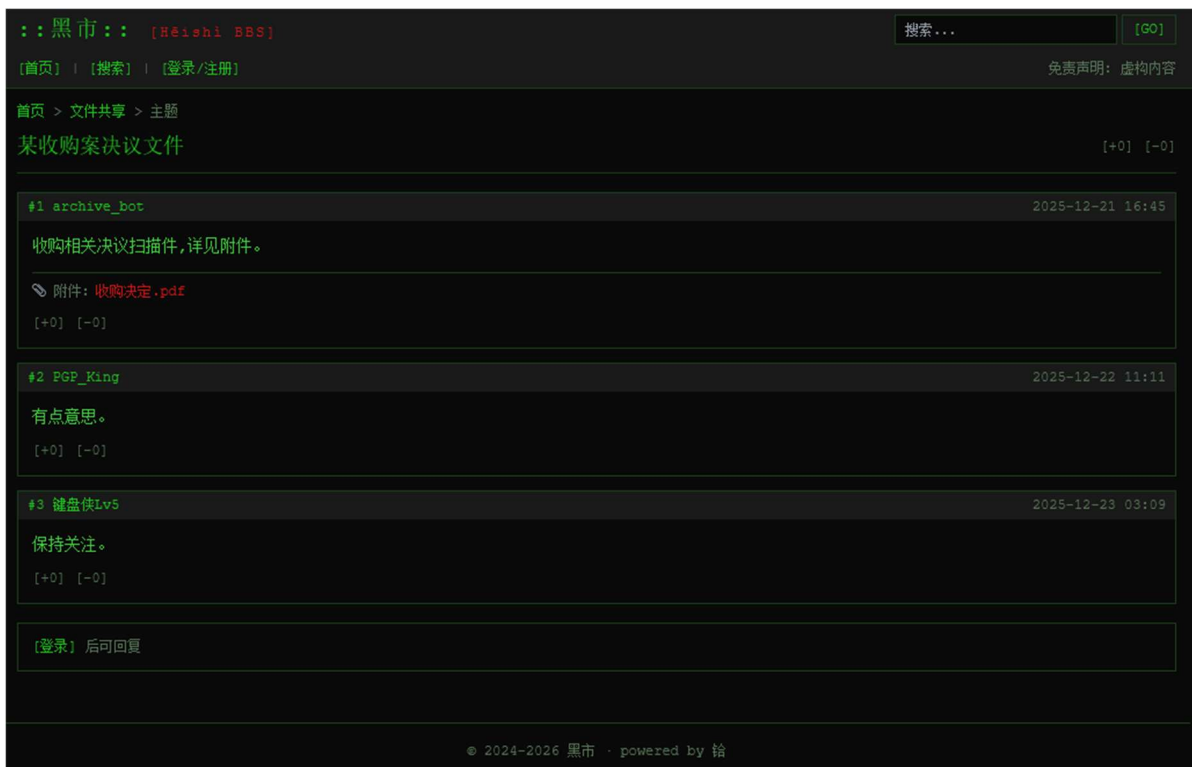
Liens ou pivots exploités : <https://shorturl.at/5e4q3>



Preuve visuelle - LES BÂTISSEURS DE L'OMBRE

## 黑市 — PREMIER CONTACT

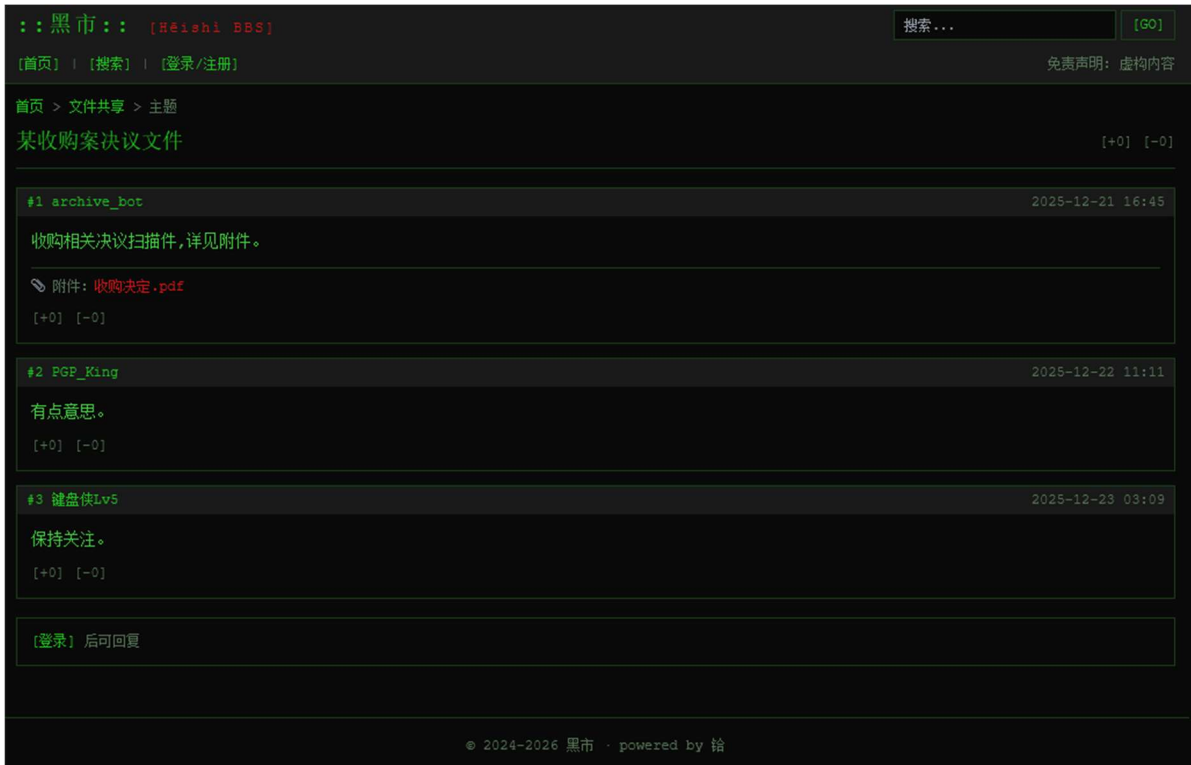
<b>Question</b>	Quelle est la date du premier post répondant au thread d'archive_bot ?
<b>Méthode</b>	Une recherche interne sur le pseudo archive_bot a permis de retrouver le thread ciblé. L'ordre des réponses indique que le premier utilisateur ayant répondu l'a fait le 22/12/2025.
<b>Déduction</b>	La date permet de situer l'apparition du sujet dans la chronologie du forum et d'enrichir la ligne temporelle de l'opération.
<b>Résultat / flag</b>	<b>22/12/2025</b>



Preuve visuelle - 黑市 — PREMIER CONTACT

## ASHIDAKON

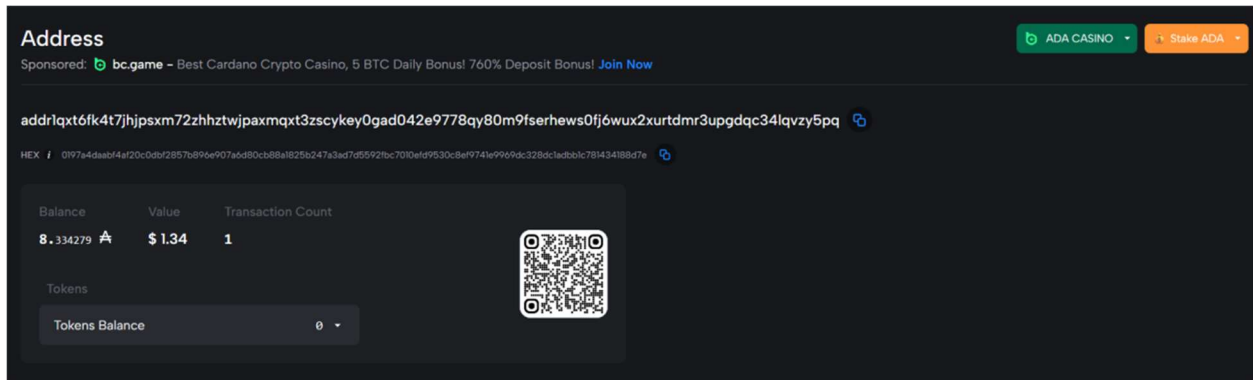
<b>Question</b>	En quelle année Ashidakon Technologies a-t-elle établi son centre de recherche en analyse d'images ?
<b>Méthode</b>	En parcourant le BBS, nous avons identifié un fichier PDF en chinois, 收购决定.pdf, rattaché à Hexuon Group Co LTD. Après traduction, le document mentionne la création du centre de recherche en analyse d'images en 2014.
<b>Déduction</b>	Ashidakon apparaît comme un acteur technologique doté d'une expertise utile dans le contexte surveillance, traitement d'images et vidéosurveillance.
<b>Résultat / flag</b>	<b>2014</b>



Preuve visuelle - ASHIDAKON

## CARDA NO LIES

<b>Question</b>	Quel montant exact a été reçu par l'adresse de sortie Cardano ?
<b>Méthode</b>	Un autre document du BBS comportait des éléments de transaction Cardano. L'adresse de sortie a été suivie dans un explorateur blockchain afin d'identifier le montant reçu.
<b>Déduction</b>	La blockchain apporte une trace difficilement altérable d'un flux financier entre entités liées au réseau.
<b>Résultat / flag</b>	<b>8.334279 ADA</b>



Preuve visuelle - CARDA NO LIES

Trx Hash	Block	Time	Fees
d23d483183cb45c251...27e556cbec17820860	13371121	May 3, 2026 3:46:26 PM a month ago	0.165721
<p>Wallet stake1u9vjl0rszrhaj5cv3muhg85ed8wr9rwp4ka3c7q5xsvg6lsjednum</p> <p>ADA Received 8.334279</p> <p>Wallet stake1u9ajs0asmflmzr2hd3wdtgp3vhhxx760xfwqvhxuz88pucct4dxhj</p> <p>ADA Spent -8.5</p>			

Preuve visuelle - CARDA NO LIES

## PHASE 7 - LE PACTE : COLLUSION SINO-ÉGYPTIENNE ET INFLUENCE GAMIFIÉE

### Objectif de la phase

Relier le réseau d'influence à un dignitaire chinois, au directeur de l'EFSA et à un support de propagande inattendu.

### DIGITAL PLAYGROUND

<b>Question</b>	Quel est le pseudo Roblox de l'administrateur du jeu lié au dignitaire chinois ?
<b>Méthode</b>	En croisant les noms des protagonistes avec les répertoires d'utilisateurs Roblox, nous avons identifié le profil Wei_Junliang. Sa biographie, « Fan de vidéosurveillance mais pas de Visiorbis », correspond directement au contexte de l'enquête.
<b>Déduction</b>	Le dignitaire chinois conserve une présence numérique inattendue dans l'univers du jeu en ligne, qui devient un terrain d'influence indirect.
<b>Résultat / flag</b>	<b>Wei_Junliang</b>



Preuve visuelle - DIGITAL PLAYGROUND

## LE BIG BOSS

<b>Question</b>	Quel est le grade et le nom complet du directeur de l'EFSA ?
<b>Méthode</b>	La recherche sur l'EFSA a d'abord mené au compte X @gouv_EFSA, apparemment officiel mais presque vide au moment de la consultation. En remontant les versions archivées sur web.archive.org, nous avons retrouvé un post supprimé de l'EFSA relayant Hassan Nabil El-Sharif. La capture archivée indique son titre complet : Général de division Hassan Nabil El-Sharif.
<b>Déduction</b>	L'archive du post supprimé apporte l'élément manquant : l'EFSA n'était pas uniquement représentée par un compte institutionnel, mais par un directeur identifié comme figure militaire.
<b>Résultat / flag</b>	<b>Général de division Hassan Nabil El-Sharif</b>

Liens ou pivots exploités : [https://x.com/gouv\\_EFSA](https://x.com/gouv_EFSA) ·

[https://web.archive.org/web/20260510103022/https://twitter.com/gouv\\_EFSA/status/2053422385957634504](https://web.archive.org/web/20260510103022/https://twitter.com/gouv_EFSA/status/2053422385957634504)



Preuve visuelle - LE BIG BOSS

## LA RENCONTRE

<b>Question</b>	Quand la rencontre entre le Major Général et le dignitaire chinois a-t-elle eu lieu ?
<b>Méthode</b>	À partir du nom identifié au challenge précédent, nous avons retrouvé le compte X de Hassan Nabil El-Sharif. L'examen de ses publications a mis en évidence une rencontre avec Wei Junliang, illustrée par une photographie et datée du 17 mai 2026.
<b>Déduction</b>	La publication relie explicitement l'EFSA, son directeur et Wei Junliang, matérialisant une rencontre au sommet dans la chronologie de la collusion.
<b>Résultat / flag</b>	<b>17/05/2026</b>

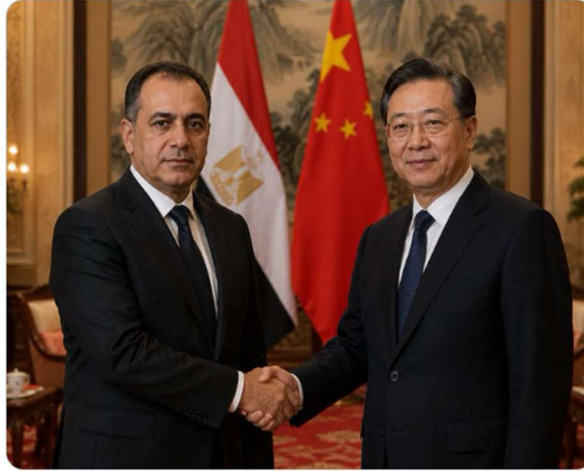
Liens ou pivots exploités : [https://x.com/MGeneral\\_Masr](https://x.com/MGeneral_Masr)



Major General Hassan Nabil El-Sharif @MGeneral\_Masr · 17 mai

À l'origine en chinois et traduit Afficher l'original

Je suis très heureux d'avoir rencontré M. Wei Junliang aujourd'hui, un homme d'affaires doté d'un sens diplomatique, intelligent et perspicace. Il est toujours un honneur pour moi de discuter avec une personnalité de ce calibre.



91



Preuve visuelle - LA RENCONTRE

## THINK OUTSIDE THE BOX

<b>Question</b>	Quel message est transmis par le graffiti dans le jeu ?
<b>Méthode</b>	Les indices sur Roblox, le rôle de Lei Huan comme développeur et le profil de Wei Junliang ont conduit à rechercher un jeu lié à ces comptes. Lei Huan avait créé un jeu nommé « Visiorbuse ». En s'y connectant et en sortant de la zone de jeu prévue, un graffiti visible dans le décor affichait un message accusatoire contre Visiorbis.
<b>Déduction</b>	L'opération d'influence ne se limite pas aux supports traditionnels : elle investit aussi des environnements ludiques fréquentés par des publics plus jeunes.
<b>Résultat / flag</b>	<b>Visiorbis vole et revend vos données</b>



# ANALYSE TRANSVERSALE

Raisonnement, causalité et attribution

## Pourquoi Visiorbis est ciblée ?

Visiorbis combine trois facteurs sensibles : une expertise en vidéosurveillance, une opportunité de marché au Moyen-Orient et une origine française. Sa candidature menace les intérêts d'acteurs concurrents ou partenaires qui cherchent à conserver l'initiative sur un marché stratégique.

## Comment la campagne est structurée ?

La campagne débute par des relais visibles : page militante, journaliste, hashtag, blogueur et TikTok. Elle gagne ensuite en profondeur avec un groupe Telegram, HazyOffice, Nathalie Zhou et des infrastructures web. La couche finale relie ces éléments à un forum, à une entreprise technologique, à une transaction blockchain et à un dispositif de communication dans Roblox.

## Quels éléments soutiennent l'attribution ?

Les liens ne reposent pas sur un indice unique mais sur une accumulation : métadonnées, pseudonymes, filigranes, code source, archives, comptes récents, rencontres publiées, blockchain et environnements ludiques. Leur cohérence narrative et temporelle renforce l'hypothèse d'une opération organisée.

### Hypothèse principale

La campagne contre Visiorbis semble orchestrée ou facilitée par un réseau d'influence lié à HazyOffice, avec Nathalie Zhou comme pivot opérationnel, Lei Huan comme appui technique, et Wei Junliang comme bénéficiaire stratégique. L'EFSA, via Hassan Nabil El-Sharif, apparaît comme l'interlocuteur institutionnel égyptien au plus haut niveau.

# CONCLUSION GÉNÉRALE

Appréciation finale de l'opération

L'enquête Mirage doré ne révèle pas une simple opposition spontanée à Visiorbis. Elle met en évidence une séquence structurée, depuis des relais publics de dénonciation jusqu'à des infrastructures techniques et financières permettant de soutenir une opération d'influence plus large.

La cohérence des pivots - PDF, comptes sociaux, hashtag, blog, TikTok, Telegram, recrutement HazyOffice, traces de Nathalie Zhou, site de Lei Huan, forum 黑市, Ashidakon Technologies, transaction Cardano et Roblox - permet de reconstituer une chaîne d'acteurs et d'intérêts autour d'un objectif : affaiblir la candidature française et favoriser une alternative sino-égyptienne.

Le rapport conclut donc à une opération de dénigrement et d'influence coordonnée contre Visiorbis, avec Wei Junliang comme figure stratégique, HazyOffice comme structure d'appui et l'EFSA comme interlocuteur institutionnel égyptien dans le cadre des négociations.

# SYNTHÈSE DES FLAGS

Tableau consolidé pour relecture rapide

#	Challenge	Résultat / flag	Type d'indice
1	FAMILIA TUA ET MUNDUS TUUS	garage_juliette_louis	Social / OSINT
2	SCROLL PRE-DODO	23:47	Social / OSINT
3	MAAAARRRRRC !!!!	bluesky_zi-nay	Technique / web
4	DERRIÈRE LE PSEUDO	Naydhal Al-Mahrizi	Social / OSINT
5	SALUT LA COMMU	إفشاء مصري	Social / OSINT
6	ARCHITECTE ARCHICHOUE	Naoum Shebib	Social / OSINT
7	LE MESSENGER	@nadirelamori	Social / OSINT
8	LA GUERRE DES HASHTAGS	#StopVisiorbis	Social / OSINT
9	LA PLUME VENIMEUSE	@blogfortalk	Social / OSINT
10	PRIDE AND PREJUDICE	white flag	Social / OSINT
11	MONSIEUR POULPE	9812_كراهية فرنسا_Tiktok	Social / OSINT
12	LE CABINET DE L'OMBRE	HazyOffice	Social / OSINT
13	MISSION SECRÈTE	Chinese enterprise expanding in France	Social / OSINT
14	LA VRAIE NATHALIE	nathalie.zhou@proton.me	Social / OSINT
15	UN GRAND PHILOSOPHE	生活不只有代码和漏洞报告	Social / OSINT
16	BÊTE D'ASTUCE	有些东西不在表面	Technique / web
17	LE GONG	tonnerre	Technique / web
18	IL Y A FORT FORT PEU DE TEMPS	17/05/2026	Social / OSINT
19	MADELEINE DE PROUST	28.157, 120.888	Géolocalisation
20	LES BÂTISSEURS DE L'OMBRE	hafnium	Technique / web
21	黑市 — PREMIER CONTACT	22/12/2025	Social / OSINT
22	ASHIDAKON	2014	Technique / web
23	CARDA NO LIES	8.334279 ADA	Blockchain
24	DIGITAL PLAYGROUND	Wei_Junliang	Social / OSINT
25	LE BIG BOSS	Général de division Hassan Nabil El-Sharif	Social / OSINT

26	LA RENCONTRE	17/05/2026	Social / OSINT
27	THINK OUTSIDE THE BOX	Visiorbis vole et revend vos données	Social / OSINT