



# Dark Web

*Fonctionnement, opportunités, menaces  
et retour d'expériences*

*Jeudi 18 juin 2026*



# LE DARK WEB

Le plus trouble et le plus dangereux de l'Internet



**WEB DE SURFACE**  
Accessible à tous



**DEEP WEB**  
(PROFOND WEB)  
Non indexé par les moteurs de recherche



**DARK WEB**  
(WEB SOMBRE)  
Non accessible par les moteurs de recherche



E-commerce



Social media



News sites



Terrorism



Human rights



Whistleblowers

1

INFORMATION



2

PROTECTION DES DONNÉES IMPORTANTE



3

REPUTATION



4

COMMERCIALISATION DES DONNÉES



5

OPPORTUNITÉS D'INVESTISSEMENT



6

RETRAICTION



7

SECOURS EN CAS D'URGENCE



# LE DARK WEB

Exploration du monde caché d'Internet



WEB DE SURFACE  
Accessible à tous



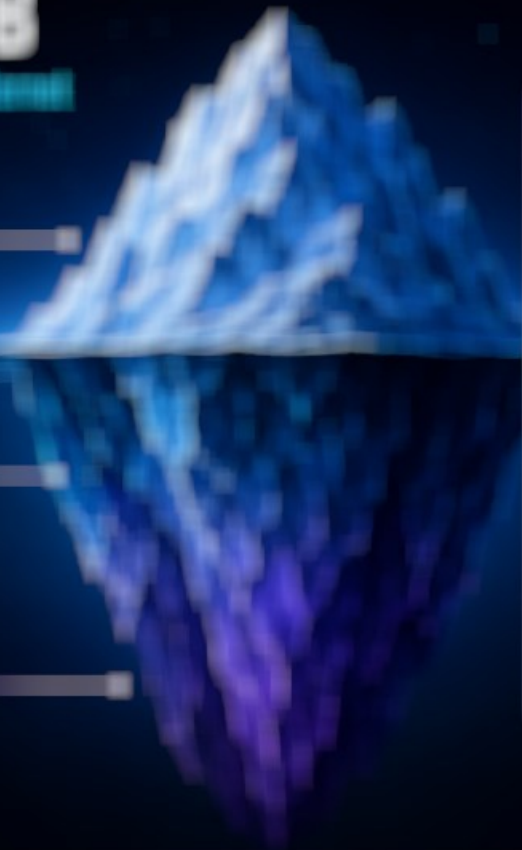
DEEP WEB  
PROFOND WEB

Non indexé  
et non accessible



DARK WEB  
WEB CACHÉ

Non accessible  
et non indexé



INTRODUCTION



POURQUOI C'EST IMPORTANT



DÉFINITIONS



COMMENT ÇA FONCTIONNE



OPPORTUNITÉS & MENACES



DÉMONSTRATION



SESSION Q&A AVEC LE PUBLIC

## 1 INTRODUCTION



## 2 POURQUOI C'EST IMPORTANT



## 3 DÉFINITIONS



## 4 COMMENT ÇA FONCTIONNE



## 5 OPPORTUNITÉS & MENACES



## 6 DÉMONSTRATION



## 7 SESSION Q&A AVEC LE PUBLIC





*Les réponses du Quiz sont à la fin de la présentation*



Pascal HENRY

RSSI



Membre actif



Présentateur



Deux fois vainqueur  
par équipe du CTF



# Introduction - Quiz

- **1 – Qu'est-ce que le Dark Web ?**
  - A) La face sombre d'Internet
  - B) Des sites web bien cachés dans Internet
  - C) Le mode sombre de votre navigateur Internet
  - D) L'ensemble des sites Web accessibles dans le Dark Net

# Introduction - Quiz

- **2 – Comment le Dark Web est-il caché ?**
  - A) En masquant les adresses IP des serveurs
  - B) Car aucun lien direct ne révèle sa présence
  - C) L'accès nécessite des outils spécifiques
  - D) Les réponses A, B et C

# Introduction - Quiz

- **3 – Est-ce que le Dark Web et le Dark Net sont en fait la même chose ?**
  - A) Oui
  - B) Oui en quelque sorte
  - C) Oui à 60%
  - D) Non



## En quoi le Dark Web nous concerne-t-il ?

# En quoi le **Dark Web** nous concerne-t-il ?

Devenu un nom « commun » avec la vulgarisation dans les médias « tout public »

- Fuites de données (diffusion d'information)
- Attaques informatiques (repère des groupes d'attaquants)
- Expliquer les enjeux (éclairer un angle mort et faire de la prévention)

# En quoi le **Dark Web** peut vous concerner ?

## Société dans le domaine de la recherche scientifique

- Sécurité des accès
- Protection des données internes ou sensibles
- Atteinte à l'image de l'entreprise
- Investigations expertises judiciaires
- Réglementaire (obligations de protection et de déclaration)
  - RGPD
  - Données de santé (déclarations EIG)

# En quoi le **Dark Web** me concerne-t-il ?

## Editeur de logiciel d'une application Saas de dématérialisation de documents

- Les vols d'identifiants via des **InfoStealers** se retrouvent en vente dans le Dark Web
  - Dans des forums d'échanges
  - Dans des places de marché
- Règlementaire : dans le cadre de la norme ISO 27001:2022, une veille de type "Renseignement sur la menace" est demandée (CTI – Cyber Threat Intelligence, A.5.7)
- Deux cas concrets seront expliqués dans la partie - Retours d'Expérience.



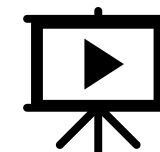
*Pour planter le décor*

## Définitions - Le Dark Web



Source de la vidéo complète :

<https://youtu.be/MaSA1PtEcEY>



Fichier : *Dark Web – Les mots clés.mp4*

# Définitions - Le Dark Web

- Le point clé : **l'anonymat**
- Le **Dark Web** est une partie du Web mondiale où nous sommes **anonymes**



# Dark Web ≠ Deep Web

Deep Web  
derrière une authentification

- Documents
  - d'entreprises
  - De gouvernements
  - D'universités
  - Des scientifiques
  - De la recherche



# Définitions - Les Dark Net

## TOR (The Onion Router)

*Le plus connu et le plus utilisé.*

## I2P (Invisible Internet Project)

*Conçu pour des communications anonymes et sécurisées.*

## Freenet


*Un réseau décentralisé pour partager des fichiers de manière anonyme.*

## GNUnet


*Réseaux pair-à-pair (P2P) sécurisés et anonymes.*

**TEDx PLV**  
x = independently organized TED event


### Quelques darknets




TOR



Freenet



I2P



GNUnet

Privategrity ?

Source : <https://youtu.be/p-u9EfTXEv0?t=236>



*Pour démystifier*

# Fonctionnement - Accès et anonymat

Résumé en 7 points du réseau TOR (  date de création 2002) :

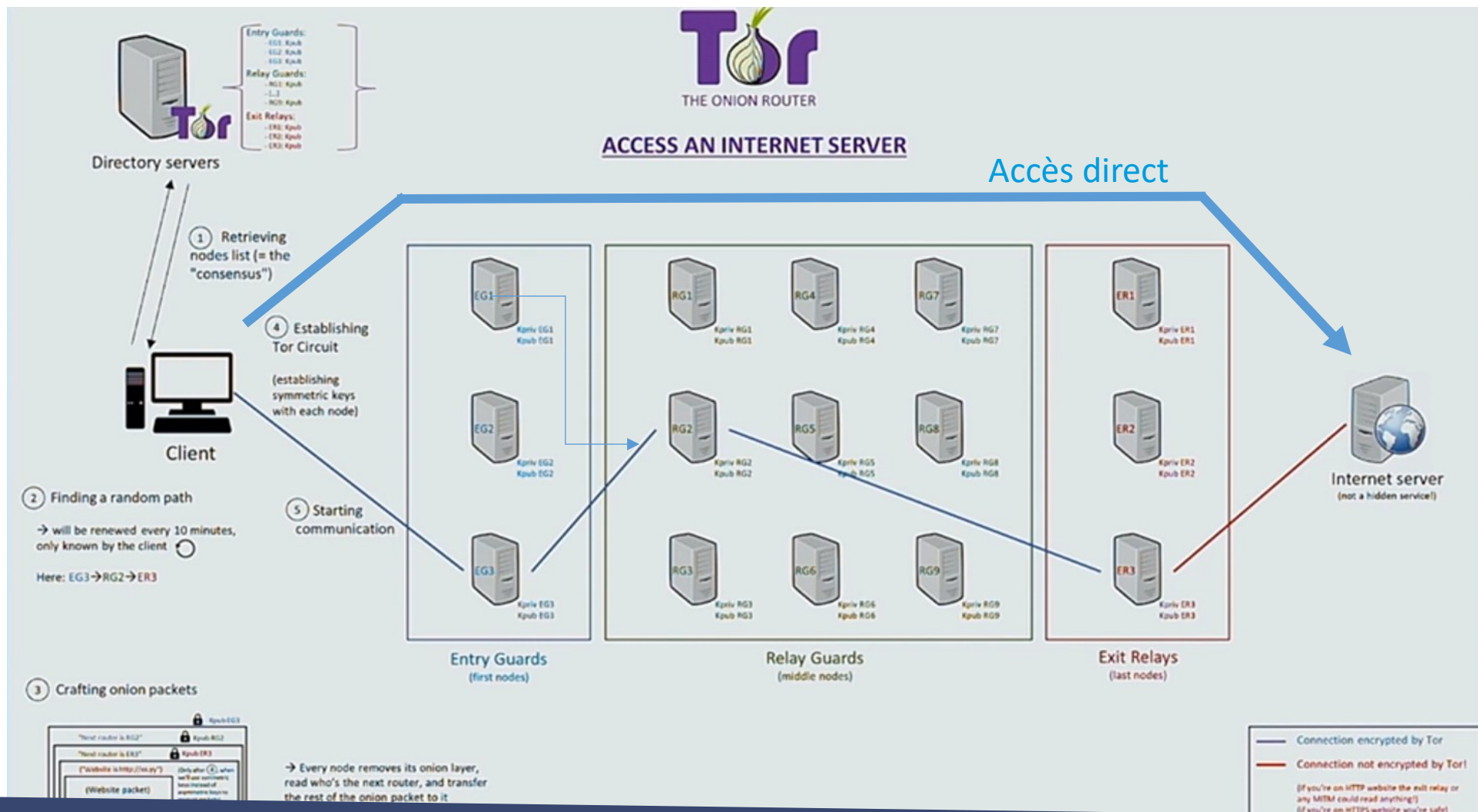
- **Anonymat** : TOR (The Onion Router) est conçu pour **anonymiser** les connexions Internet en masquant l'identité et la localisation des utilisateurs.
- **Routage en oignon** : Les données sont chiffrées et transmises à **travers plusieurs relais** (nœuds), chaque nœud ne connaissant que l'origine et la destination immédiate des données.
- **Navigation privée** : Utilisé pour naviguer sur Internet de manière **anonyme**, TOR permet d'accéder à des sites web sans révéler son adresse IP.
- **Contournement de la censure** : TOR est efficace pour **contourner les restrictions** et la censure sur Internet, permettant d'accéder à des contenus bloqués dans certaines régions.
- **Sécurité** : En chiffrant les données plusieurs fois, TOR protège **contre la surveillance et l'analyse de trafic**.
- **Utilisation légale** : Bien que souvent associé à des activités illégales, TOR est également utilisé par des journalistes, des militants et des citoyens ordinaires pour **protéger leur vie privée**.
- **Communauté et développement** : TOR est un projet **open-source** maintenu par une communauté de bénévoles et soutenu par diverses organisations pour promouvoir la confidentialité en ligne.

# Fonctionnement - Accès et anonymat

Accès direct ≠ Via TOR

Source : <https://youtu.be/IqofT1yt7Fk?t=571>

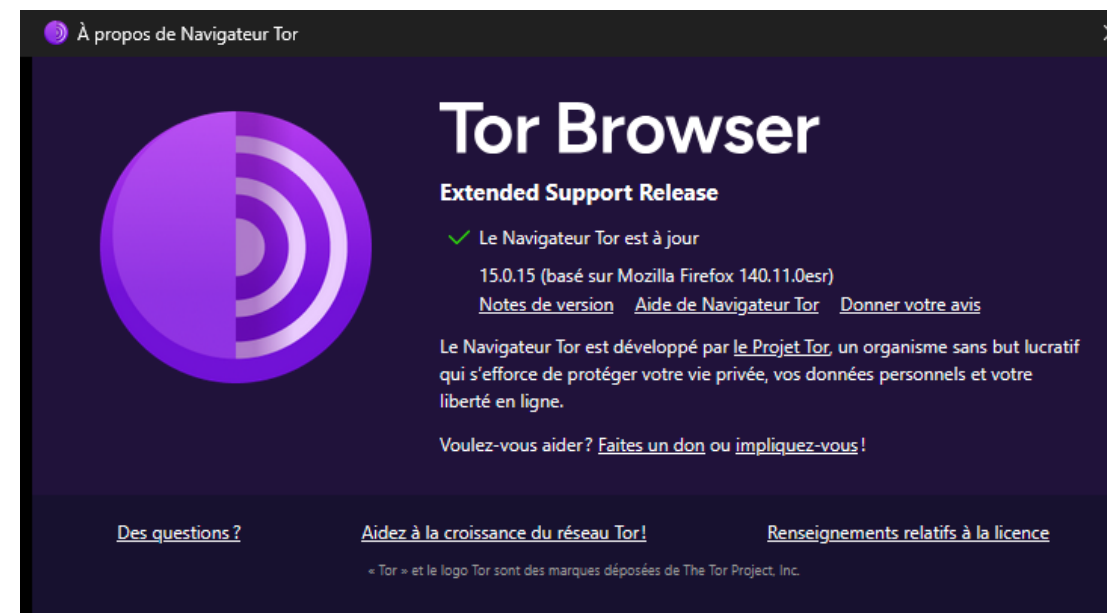
Comparaison en FR des modes de fonctionnement des « anonymiseurs »




Clear Web

# Fonctionnement - Accès et anonymat

Dark Web




Le **Dark Web** du réseau **Dark Net**  est une partie de l'Internet global :

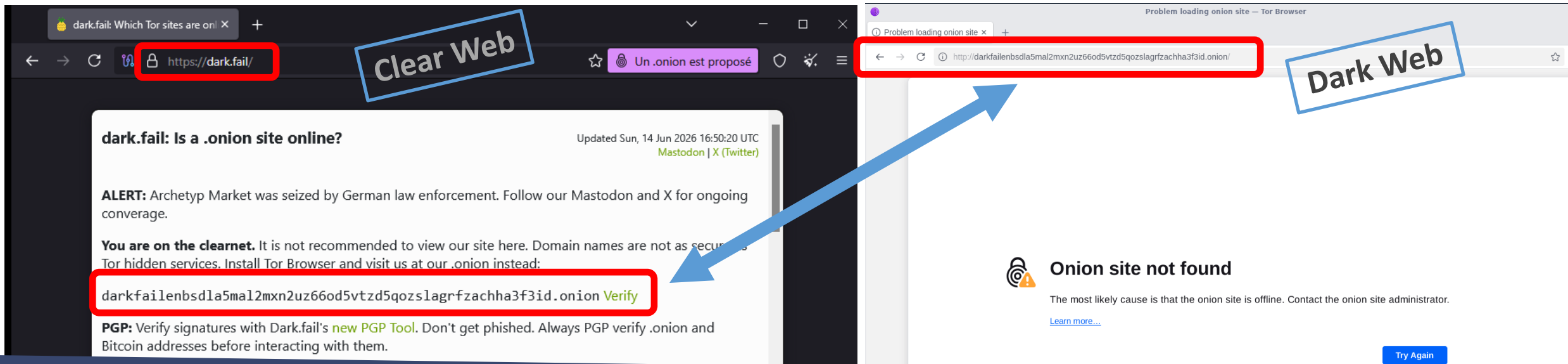
- 1) non\* accessible à l'aide des navigateurs Internet classiques tels que FireFox, Chrome, Edge, Safari, Brave, ...
- 2) accessible\* qu'à l'aide de navigateurs spécialisés tels que  **Tor Browser**

\* de manière prête à l'emploi (Out-of-the-Box)

# Fonctionnement – Structure et contenu

- Contrairement aux noms de domaine classique en *gTLD*, *geoTLD*, *sTLD* ou *ccTLD* (.com, .nyc, .gov, .fr) (Generic, Geographic, Sponsored, Country Code Top Level Domain)
- Pour le réseau  les adresses des sites web (Dark Web) sont en **.onion** (avec 56 lettres et chiffres)

Exemple : <https://dark.fail> - Le Wikipedia des places de marchés du Dark Web



The image shows two browser windows side-by-side. The left window is a dark-themed browser at <https://dark.fail/>. The address bar is highlighted with a red box. A blue box labeled 'Clear Web' is overlaid on the browser. The page content includes a warning about Archetyp Market and a list of .onion addresses, with one address [darkfailenbsd1a5mal2mxn2uz66od5vtzd5qozslagr-fzachha3f3id.onion](http://darkfailenbsd1a5mal2mxn2uz66od5vtzd5qozslagr-fzachha3f3id.onion) highlighted in a red box. A blue arrow points from this address to the right window. The right window is a light-themed browser showing a 'Problem loading onion site' error. The address bar is highlighted with a red box and contains the URL <http://darkfailenbsd1a5mal2mxn2uz66od5vtzd5qozslagr-fzachha3f3id.onion/>. A blue box labeled 'Dark Web' is overlaid on the browser. The error message says 'Onion site not found' and provides a 'Try Again' button.

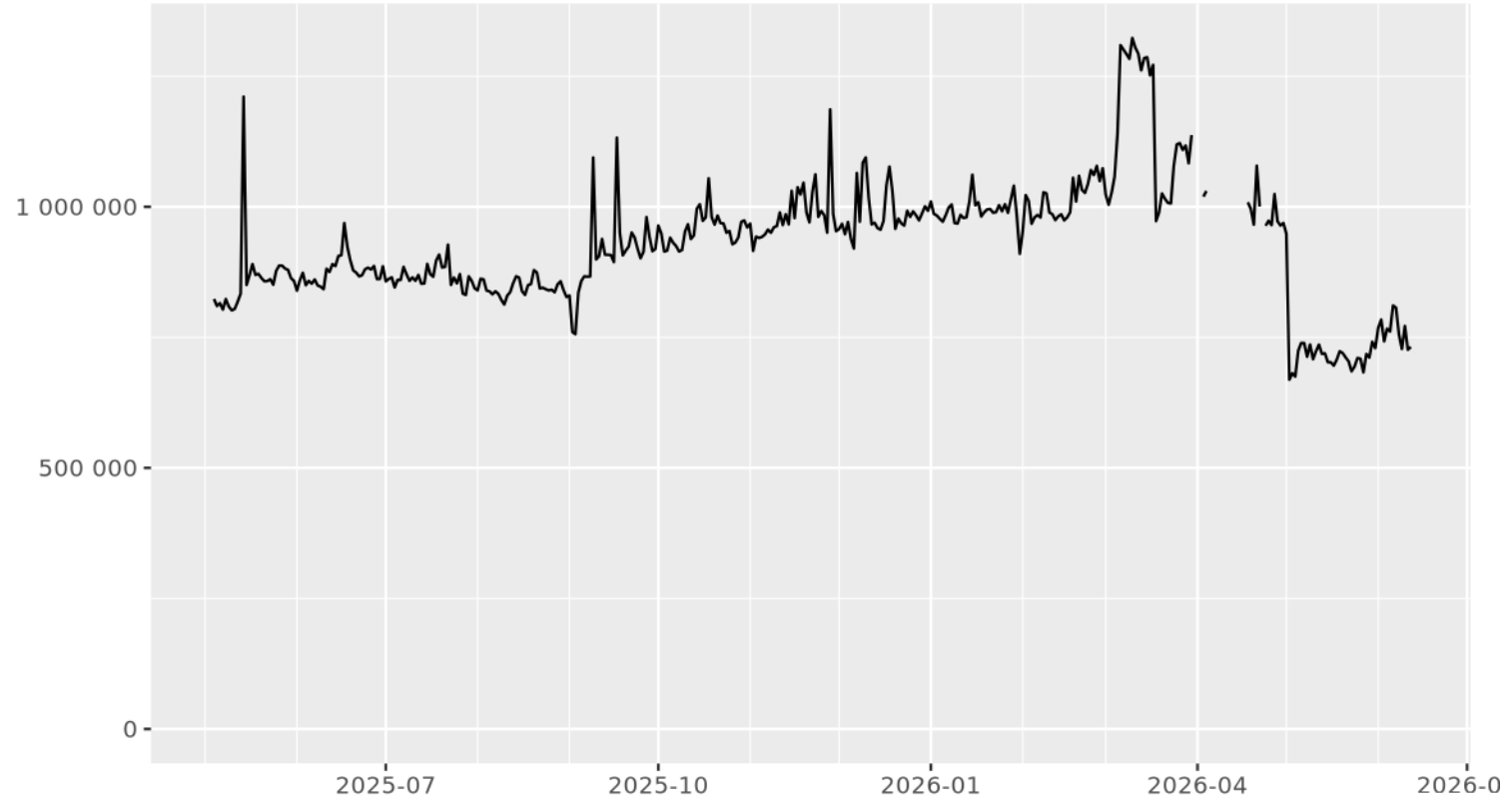
# Fonctionnement – Entrées dans l'annuaire



## Nombre de sites web

- Les adresses des sites web (Dark Web) en **.onion** sont désormais au format v3 avec *56 lettres et chiffres*.
- **Source :**  
<https://metrics.torproject.org/hidser-v-dir-v3-onions-seen.png?start=2025-05-01&end=2026-06-14>

Unique .onion v3 addresses



The Tor Project - <https://metrics.torproject.org/>

# Fonctionnement – Infrastructure

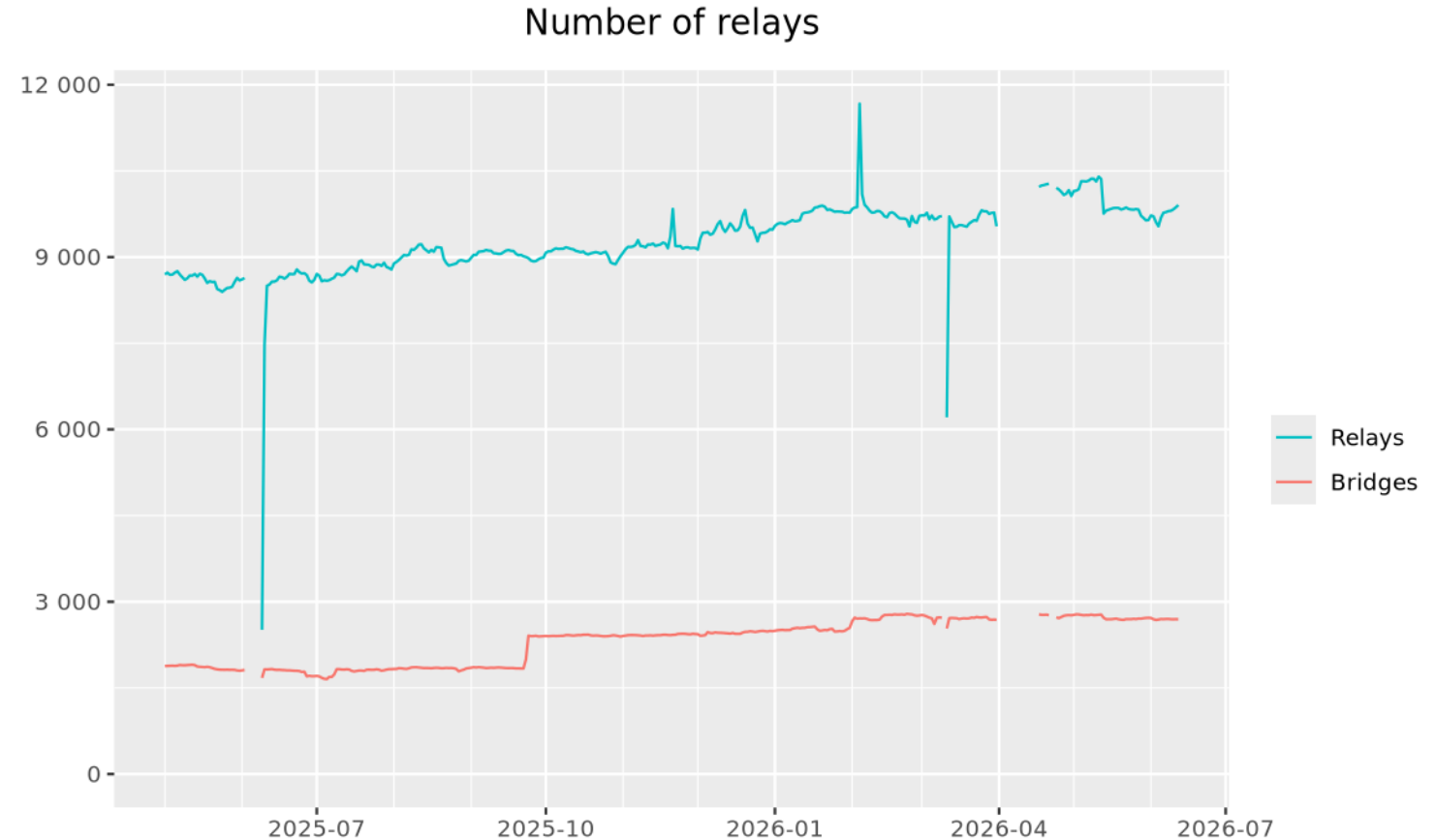


## Nombre de "Serveurs Tor" (Relays)

- Les serveurs Tor sont hébergés par la communauté.

Source :

<https://metrics.torproject.org/networksize.png?start=2025-05-01&end=2026-06-14>



The Tor Project - <https://metrics.torproject.org/>



## Fonctionnement – Contributeurs

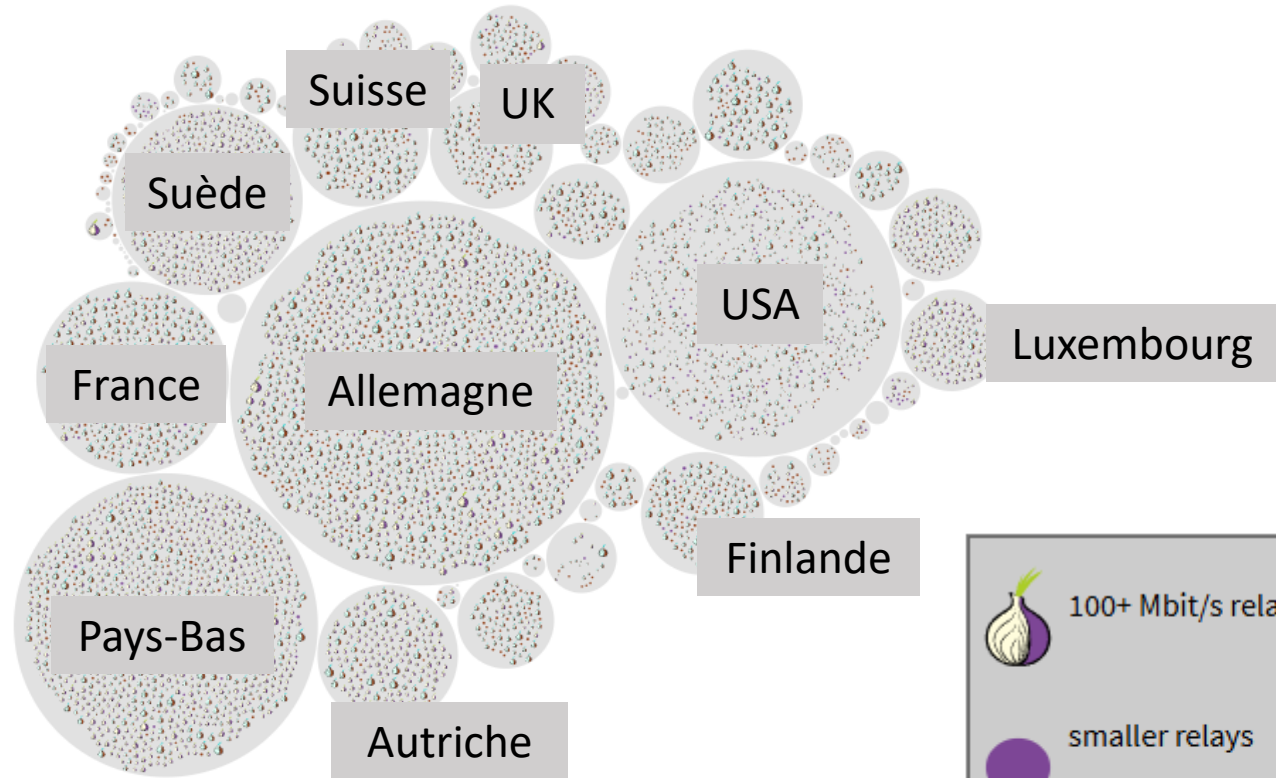


### Localisation des "Servers Tor" (Relays)

- Les pays avec le plus de "Relay Tor"

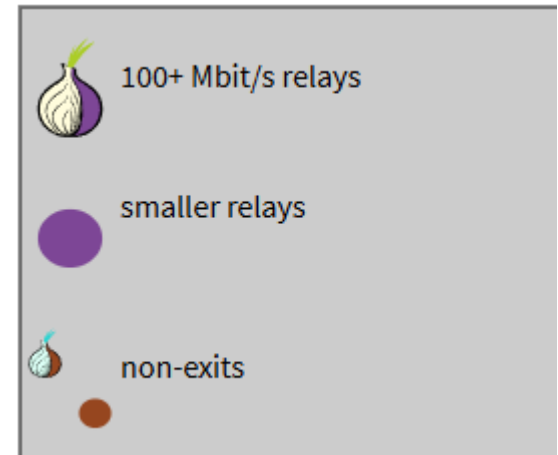
Source :

<https://metrics.torproject.org/bubbles.html#country>



77 countries with 9833 relays (5513 visible)

2026-06-14 20:00:00



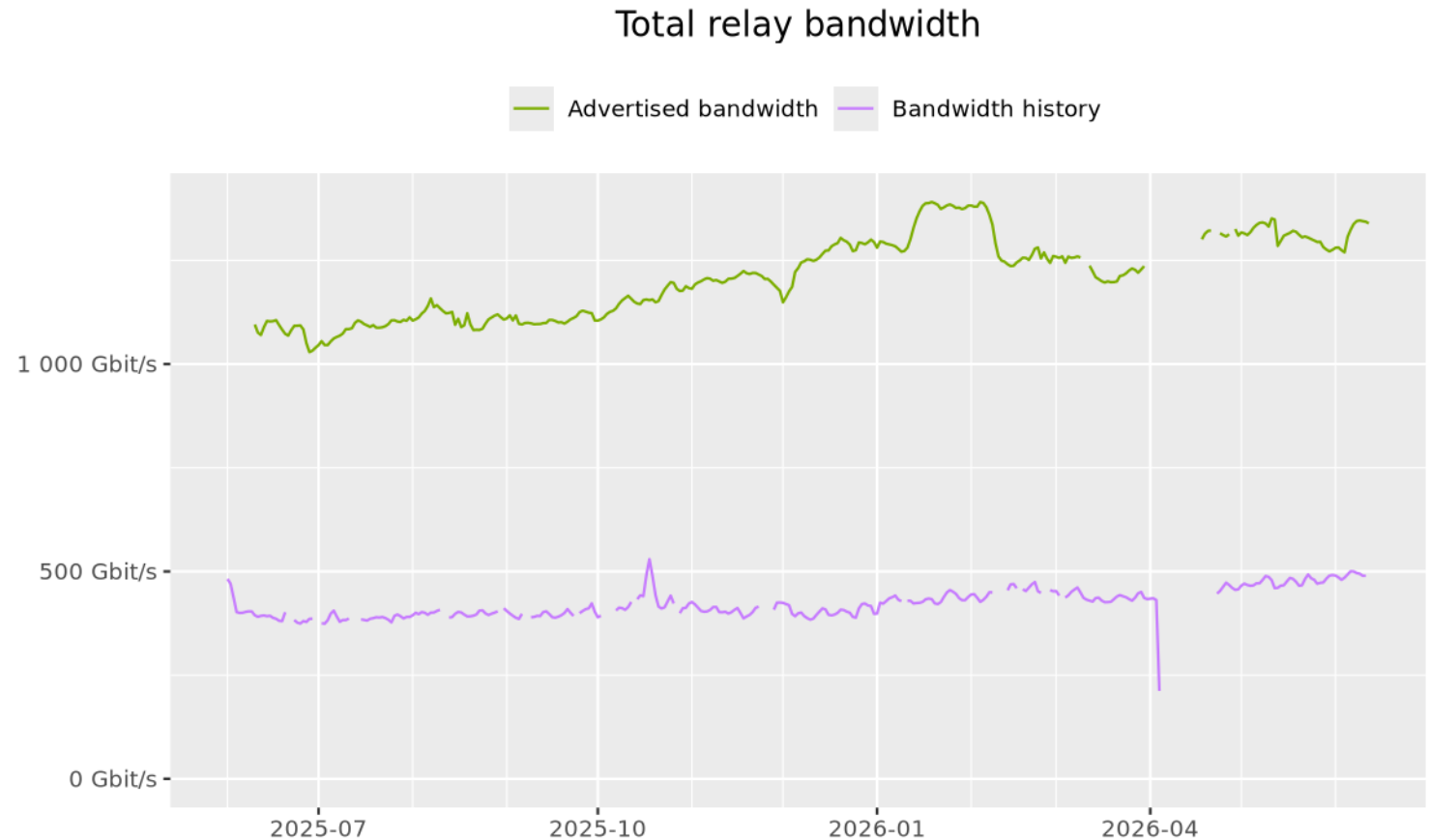
# Fonctionnement – Structure et contenu



## Bande passante des "Servers Tor" (Relays)

Source :

<https://metrics.torproject.org/bandwidth.png?start=2025-06-01&end=2026-06-14>



The Tor Project - <https://metrics.torproject.org/>



*Pour connaître les usages et les risques*

# Opportunités et menaces – Généralités

## Statistiques et tendances clés qui illustrent ce qu'est le Dark Web aujourd'hui

- Il y avait en moyenne entre de 2,5 et 3 millions de visiteurs quotidiens sur le **Dark Web** en 2025-2026. Stable depuis 2023.
- Près de 60 % du **Dark Web** est illégal en 2026, avec du contenu lié à la violence, aux plateformes extrémistes, aux marchés illégaux, aux drogues et aux forums de cybercriminalité. Stable.
- Les produits numériques illégaux les plus lucratifs disponibles à l'achat sur le **Dark Web** incluent les comptes crypto, la banque en ligne et les portefeuilles électroniques, en avril 2023.
- En 2025, les places de marchés du **Dark Web** ont augmenté de 28% : 15 Milliards d'identifiants circulent sur le **Dark Web**.

Source : <https://preyproject.com/blog/dark-web-statistics-trends> (étude actualisée le 9 juin 2026)

# Opportunités et menaces – Utilisation légitime

**Rappel : Un fondamental du Dark Net est le respect de l'anonymat**

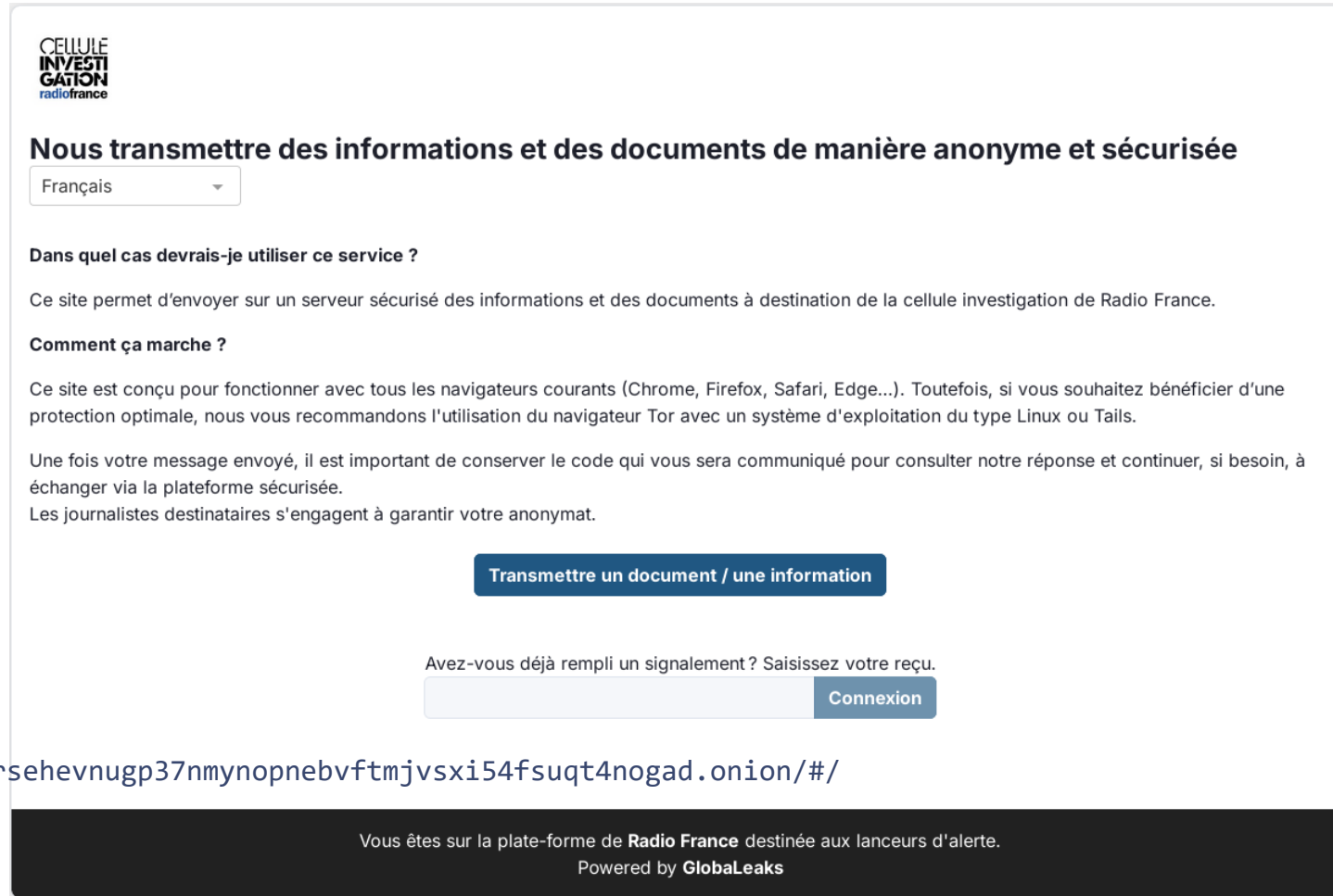
## Certaines organisations de notoriété publique ont une présence sur le Dark Web

- Facebook (Réseau Social)
- Le Washington Post (Journal éditorial)
- La CIA (Agence de renseignement)
- The Hidden Wiki (Annuaire et index de références comparable à Wikipédia)

## Qui utilise le Dark Web

- Les internautes résidant dans des pays où le gouvernement fait de la césure ou de la surveillance
  - Protection de la vie privée et de la liberté d'expression.
  - Communication sécurisée pour les journalistes et les activistes
- Les polices et les chercheurs en cyber sécurité

# Opportunités et menaces – Utilisation légitime



**CELLULE INVESTIGATION**  
radiofrance

## Nous transmettre des informations et des documents de manière anonyme et sécurisée

Français ▾

**Dans quel cas devrais-je utiliser ce service ?**

Ce site permet d'envoyer sur un serveur sécurisé des informations et des documents à destination de la cellule investigation de Radio France.

**Comment ça marche ?**

Ce site est conçu pour fonctionner avec tous les navigateurs courants (Chrome, Firefox, Safari, Edge...). Toutefois, si vous souhaitez bénéficier d'une protection optimale, nous vous recommandons l'utilisation du navigateur Tor avec un système d'exploitation du type Linux ou Tails.

Une fois votre message envoyé, il est important de conserver le code qui vous sera communiqué pour consulter notre réponse et continuer, si besoin, à échanger via la plateforme sécurisée.

Les journalistes destinataires s'engagent à garantir votre anonymat.

[Transmettre un document / une information](#)

Avez-vous déjà rempli un signalement ? Saisissez votre reçu.

[Connexion](#)

Vous êtes sur la plate-forme de **Radio France** destinée aux lanceurs d'alerte.  
Powered by **GlobalLeaks**

Source : <http://ckahyzrwg1nbgrsehevnugp37nmynopnebvftmjvsxi54fsuqt4nogad.onion/#/>

# Opportunités et menaces – Utilisation illégitime

## L'anonymat attire également une multitude d'activités moins légales

### Articles illégaux que l'on peut acheter sur le Dark Web :

- Drogues récréatives telles que le cannabis
- Médicaments illicites sur ordonnance et autres produits pharmaceutiques
- Drogues dures telles que l'héroïne
- Armes à feu
- Produits chimiques toxiques
- Pornographie
- Fausse monnaie

Source : <https://www.avast.com/fr-fr/c-dark-web-facts>

### Articles de fraude que l'on peut acheter sur le Dark Web :

- Numéros de carte de crédit
- Identifiants en ligne
- Comptes bancaires volés
- Numéros de cartes cadeaux
- Profils complets des victimes nécessaires pour l'usurpation d'identité
- Bases de données piratées
- Documents frauduleux tels que permis de conduire ou passeports
- Comptes piratés, tels que les comptes ChatGPT ou Netflix

# Opportunités et menaces – Utilisation illégitime

L'anonymat attire également une multitude d'activités moins légales

**Malwares** que l'on peut acheter sur le Dark Web :

- [Chevaux de Troie](#) d'accès à distance (RAT)
- [Botnets](#)
- [Ransomwares](#)
- Cryptomineurs ou autres outils de [cryptojacking](#)
- Outils de piratage tels que les craqueurs de mots de passe
- Autres types de [malwares](#)

Source : <https://www.avast.com/fr-fr/c-dark-web-facts>

**Malware-en-tant-que-service** (MaaS que l'on peut acheter sur le Dark Web :

- [Spam](#)
- [Attaques DDoS \(Distributed-Denial-of-Service\)](#) ou services d'amorçage (booter)
- Publication d'avis en masse
- Attaques par e-mail de type phishing, y compris les campagnes de [spear-phishing](#) personnalisées
- Vérification des antécédents (ce qui signifie que votre cible sera piratée ou [cyberharcelée](#))
- Piratage

# Opportunités et menaces – Prix du marché

**OTP BOT v.1.0**  
Operational | Uptime: 100%

OTP BOT have UNIQUE features that you can't find in any other bot.

Our bot is an Hybrid between OTP Bot and 3CX. its a professional Social Engineering kit for professional OTP users.

**MODES:** Banks, NFCs, Payment Services, Payment Gateways, Brokerages, Stores, Carriers, Emails, Crypto Exchanges, Crypto Hardwares, Social Medias, Cloud Services

**Features included:**

- 24/7 Support
- Automated Payment System
- Live Panel Feeling
- 12+ Pre-made Modes
- Customizable Caller ID / Spoofing
- 99.99% Up-time
- Customizable Scripts
- Customizable Panel Actions
- International Support
- Multilingual Support (60+ Voices)
- PGP / Conference Calls
- Live DTMF
- Call Streaming - Listen to call in Real-Time!

DAILY [\$25] / WEEKLY [\$110] / MONTHLY [\$285]

## Current pricing (2026):

ACCESS TYPE	TYPICAL PRICE	NOTES
Basic account credentials	\$1-\$15	Consumer accounts, streaming services
Corporate email access	\$15-\$50	Higher for executives
VPN credentials	\$50-\$200	Price scales with company size
RDP access	\$50-\$500	Direct network entry point
Domain admin access	\$500-\$5,000+	Full network control
Bank account access	\$500-\$2,000	Depends on balance and bank
AWS/cloud console access	\$200-\$2,000	Growing category

Source :

<https://www.breachsense.com/blog/dark-web-markets/> et Dark Web

# Opportunités et menaces – Lieu de divulgation d'info volées



Source : <https://www.larepubliquedespyrenees.fr/faits-divers/l-aeroport-et-eklore-deux-entites-de-la-cci-victimes-d-une-cyberattaque-19719090.php>

## Dans la presse quotidienne

*Dans la nuit du 12 au 13 mai 2024 l'aéroport et les écoles Eklöre de Pau étaient victimes d'une cyberattaque. Ce dimanche 26 mai, des données informatiques provenant potentiellement de cette opération ont été mises en ligne, sur le dark web.*



# Opportunités et menaces – Lieu de divulgation d'info volées

Wall of Shame

**Aéroport de Pau** 👁 3198

Full leak

2024-05-26 15:18:39

**Esc Pau Etudes-  
Conseils** 👁 3104

Colleges & Universities

2024-05-26 15:17:16

**CNPC Sport**

Colleges & Universities

MONTI
Aéroport de Pau

Aéroport de Pau

Full leak here

**Download links:**

air

[http://egtqjen\[REDACTED\]xstxzqqz2f5qad.onion/air](http://egtqjen[REDACTED]xstxzqqz2f5qad.onion/air)

📁 <a href="#">Fiches de sécurité/</a>	2024-05-23 21:46
📁 <a href="#">Formation Mecanique/</a>	2024-05-23 21:46
📁 <a href="#">Formation SSLIA/</a>	2024-05-23 21:51
📁 <a href="#">Formation evacuation aerogare/</a>	2024-05-23 21:46
📁 <a href="#">Formation personnel APT/</a>	2024-05-23 21:49
📁 <a href="#">Formations inscriptions/</a>	2024-05-23 21:51
📁 <a href="#">GARAGE/</a>	2024-05-23 21:51
📁 <a href="#">Heures Sup/</a>	2024-05-23 21:51
📁 <a href="#">INFO AERO/</a>	2024-05-23 21:52
📁 <a href="#">Info/</a>	2024-05-23 21:51
📁 <a href="#">Informatique/</a>	2024-05-23 21:53
📁 <a href="#">Logiciel SIA/</a>	2024-05-23 21:53
📁 <a href="#">Mngt Qualite/</a>	2024-05-23 21:53
📁 <a href="#">Navettes Ski/</a>	2024-05-23 21:53
📁 <a href="#">PISTE/</a>	2024-05-23 21:55
📁 <a href="#">PMR/</a>	2024-05-23 21:59
📁 <a href="#">Partenaires plateforme/</a>	2024-05-23 21:55
📁 <a href="#">Piste degivrage/</a>	2024-05-23 21:55
📁 <a href="#">Plan de surveillance/</a>	2024-05-23 21:55
📁 <a href="#">Planification/</a>	2024-05-23 21:59
📁 <a href="#">Planning/</a>	2024-05-23 21:59
📁 <a href="#">Planning Salles/</a>	2024-05-23 21:59
📁 <a href="#">Planning Support/</a>	2024-05-23 21:59
📁 <a href="#">Pole Avion/</a>	2024-05-23 21:59
📁 <a href="#">Projets IT/</a>	2024-05-23 21:59
📁 <a href="#">Promotion Tourisme/</a>	2024-05-23 22:11
📁 <a href="#">Qualite Securite/</a>	2024-05-23 22:11
📁 <a href="#">Réclamations clients/</a>	2024-05-23 22:12
📁 <a href="#">RH/</a>	2024-05-23 22:37
📁 <a href="#">Registre de securite/</a>	2024-05-23 22:12

Source : Dark Web

# Opportunités et menaces – Renseignements sur la menace



## Point juridique

**#371 ré-utiliser les data d'une fuite de données (**leak**), c'est pénal ou c'est légal ?**

- Écrit par Marc-Antoine LEDIEU - Avocat RSSI et conférencier
- Publié le 11 janvier 2022

Source : <https://technique-et-droit-du-numerique.fr/utiliser-les-data-dun-leak-penal-ou-legal/>

# Opportunités et menaces – Renseignements sur la menace

## ATTENTION !



Réponse



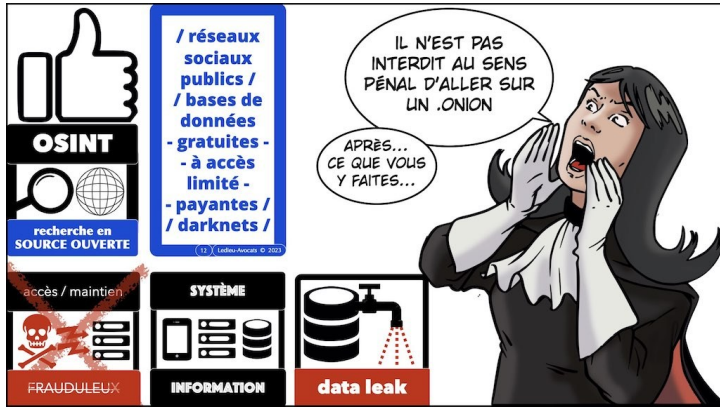
The infographic is divided into three main sections. The left section has a black header with the text "atteinte aux droits du producteur" and a blue box below with "CONTENU" and "base de données" next to a database icon. The middle section features a scale of justice icon with "article L.343-4" above and "Code PI" below. The right section contains the text: "lorsque le délit est commis en **bande organisée**, les peines sont portées à **7 ans [de prison]** et **750.000 Euros d'amende**".

Ne télécharger pas de « leak » chez votre employeur (usage de la connexion internet) ou sur un poste de travail de votre entreprise durant votre mission en tant qu'employé, seul ou en groupe.  
Cela constitue un délit pénal. Cela peut également vous mener à un licenciement pour faute sur le plan civil.

Source : <https://youtu.be/SfBz3fPy9XQ?t=2436>

Podcast : <https://www.nolimitsecu.fr/re-utiliser-un-leak-cest-legal-ou-cest-penal/>

# Opportunités et menaces – Visiter le Dark Web ?



Source : <https://technique-et-droit-du-numerique.fr/fic-2023-cyber-securite-et-droit-de-l-osint-le-probleme-des-leaks/>

En France, **accéder au Dark Web n'est pas illégal en soi.**

Plusieurs textes de loi peuvent s'appliquer à la consultation d'informations volées sur le Dark Web :

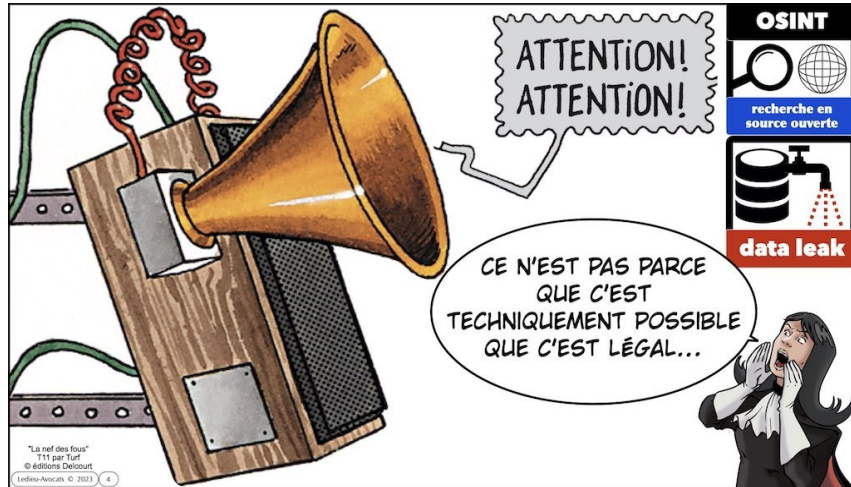
1. Code pénal :

- [Article 321-1 : Cet article punit le recel, c'est-à-dire le fait de détenir, utiliser ou profiter sciemment de biens provenant d'un crime ou d'un délit.](#)
- [Article 323-3 : Cet article concerne l'accès frauduleux à un système de traitement automatisé de données, ce qui peut inclure l'accès à des données volées.](#)

2. Loi pour la confiance dans l'économie numérique (LCEN) :

- [Article 6 : Cet article impose des obligations aux hébergeurs et aux fournisseurs d'accès à internet pour prévenir la diffusion de contenus illicites.](#)

# Opportunités et menaces – Visiter le Dark Web ?



## Le droit de collecter des "data" ?

- La **jurisprudence** « Bluetouff » de 2015 de la Cour de cassation nous apporte une réponse très claire :
  - soustraire des données « sans le consentement de leur propriétaire » constitue le délit pénal de vol.
- Attention, si vous n'êtes pas le « voleur » mais que vous téléchargez le produit d'un vol (hypothèse d'un leak disponible depuis un site .onion), vous êtes « **receleur** » de ce vol.
- Le receleur est la personne qui « détient une chose [...] en sachant que cette chose provient d'un crime ou d'un délit ». Sanction : 5 ans de prison et 375 000 € d'amende.

Source : Livre Blanc – Le cadre légal de l'OSINT (page 5)

(A débusquer dans la WayBack Machine)

et

<https://itlaw.fr/quel-est-le-cadre-legal-de-losint/>

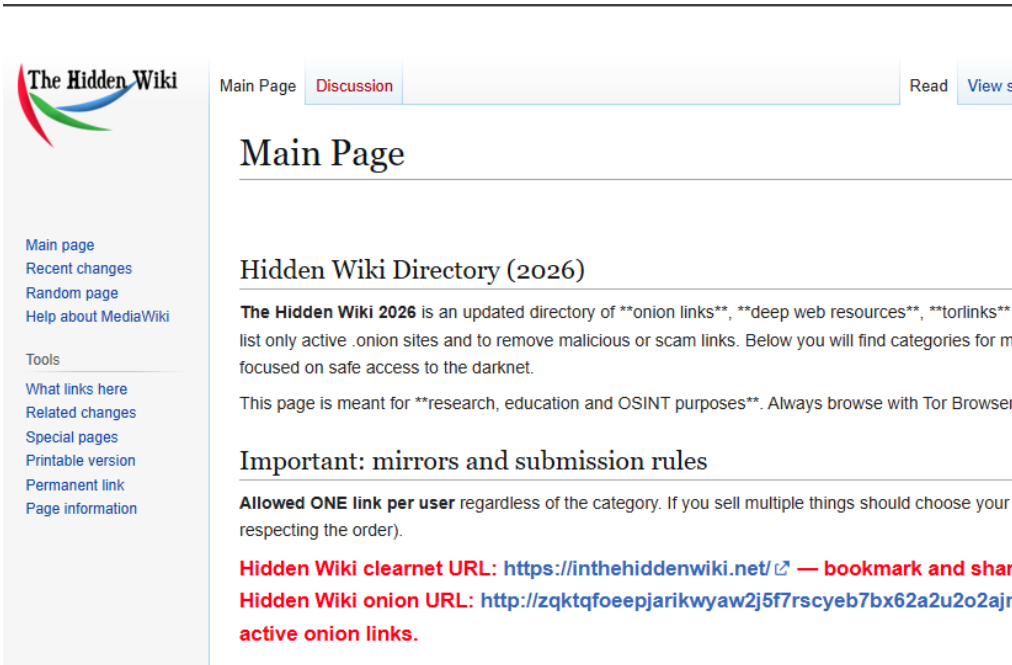
## 6 DÉMONSTRATION



*Pour chercher soi-même sur le Dark Web*

# Démonstration - Les points de départ

## Le "Hidden Wiki"



The Hidden Wiki

Main Page Discussion Read View s

### Main Page

#### Hidden Wiki Directory (2026)

The Hidden Wiki 2026 is an updated directory of **\*\*onion links\*\***, **\*\*deep web resources\*\***, **\*\*torlinks\*\*** list only active .onion sites and to remove malicious or scam links. Below you will find categories for m focused on safe access to the darknet.

This page is meant for **\*\*research, education and OSINT purposes\*\***. Always browse with Tor Browser

#### Important: mirrors and submission rules

**Allowed ONE link per user** regardless of the category. If you sell multiple things should choose your respecting the order).

**Hidden Wiki clearnet URL:** <https://inthehiddenwiki.net/> — bookmark and shar

**Hidden Wiki onion URL:** <http://zqktqfoepjarikwyaw2j5f7rscyeb7bx62a2u2o2ajr> active onion links.

Main page  
Recent changes  
Random page  
Help about MediaWiki

Tools

What links here  
Related changes  
Special pages  
Printable version  
Permanent link  
Page information

### Contents [hide]

- 1 Hidden Wiki Directory (2026)
- 2 Important: mirrors and submission rules
- 3 Wikis in different languages
- 4 Editor's picks
- 5 Volunteer
- 6 Guides
- 7 Directories of Onion Links
- 8 Scam Reporting Databases
- 9 Search engines
- 10 Tor
- 11 Financial
- 12 Deep Web Marketplaces
- 13 Drugs
- 14 Money Counterfeits
- 15 Commercial Services
- 16 Escrow
- 17 Popular sites on Tor
- 18 Porn Sites

- 19 Chans
- 20 E-mail services / messaging
- 21 Hosting, website developing
- 22 Anonymity & Security
- 23 Blogs / Essays / News Sites
- 24 Forums / Boards / Chats
- 25 Whistleblowing
- 26 Bitcoin, Monero, crypto and blockchain
- 27 Books / Archives
- 28 Non-English
  - 28.1 Brazilian
  - 28.2 Finnish / Suomi
  - 28.3 French / Français
  - 28.4 German / Deutsch
  - 28.5 Greek / ελληνικά
  - 28.6 Italian / Italiano
  - 28.7 Japanese / 日本語
  - 28.8 Korean / 한국어
  - 28.9 Chinese / 中国語
  - 28.10 Polish / Polski
  - 28.11 Russian / Русский



Source : The Hidden Wiki

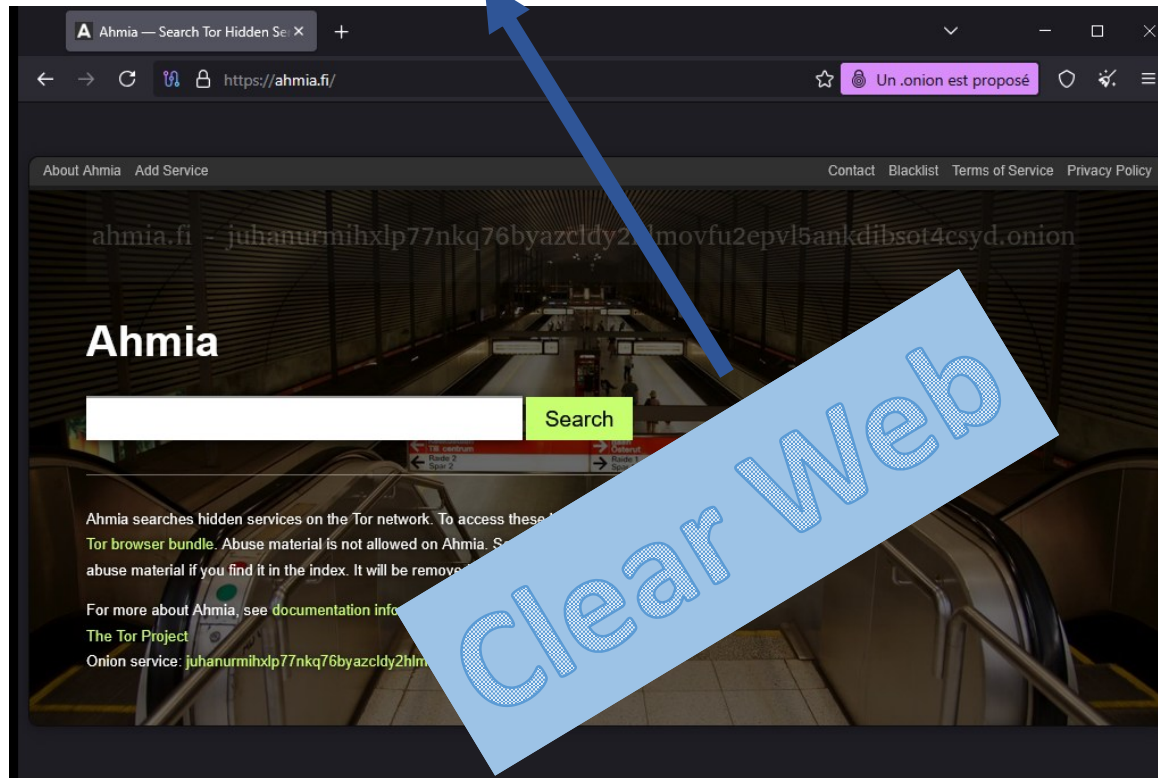
Clear Web : <https://inthehiddenwiki.net>

Dark Web : <http://zqktqfoepjarikwyaw2j5f7rscyeb7bx62a2u2o2ajmxcl46c7xeiid.onion>

# Démonstration - Les points de départ

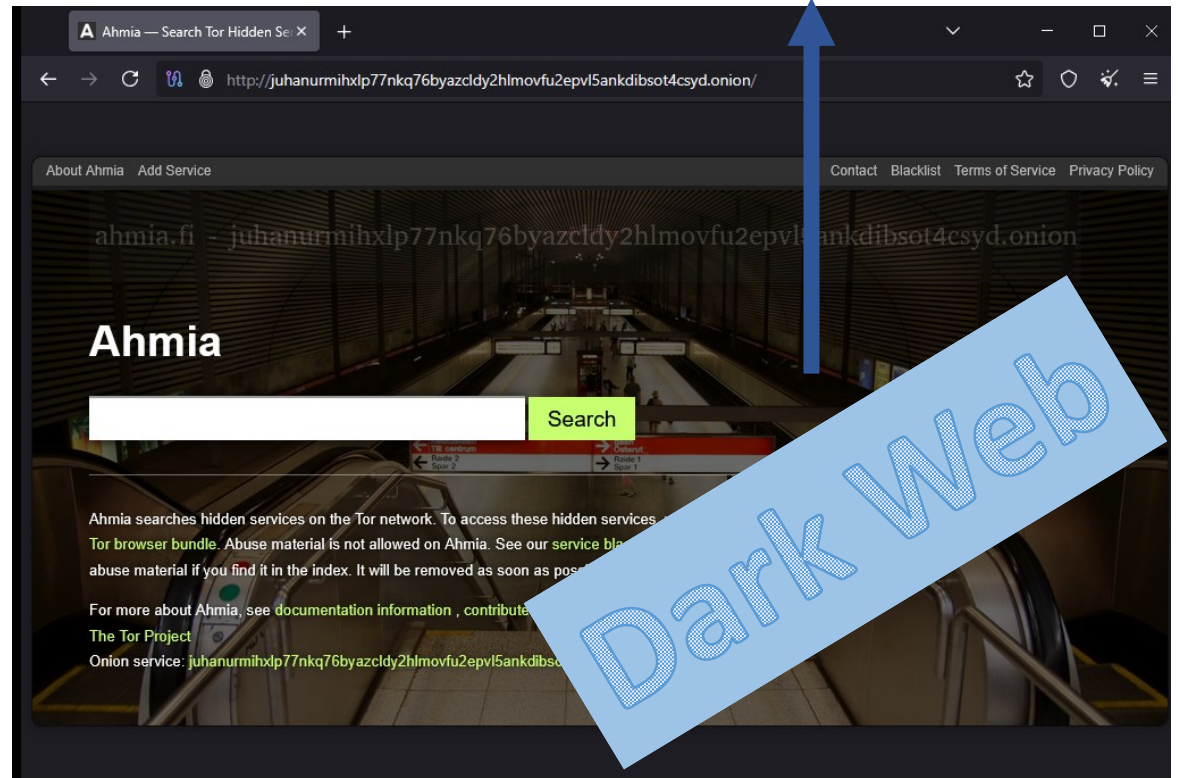
## Un moteur de recherche ...

Source : <https://ahmia.fi>



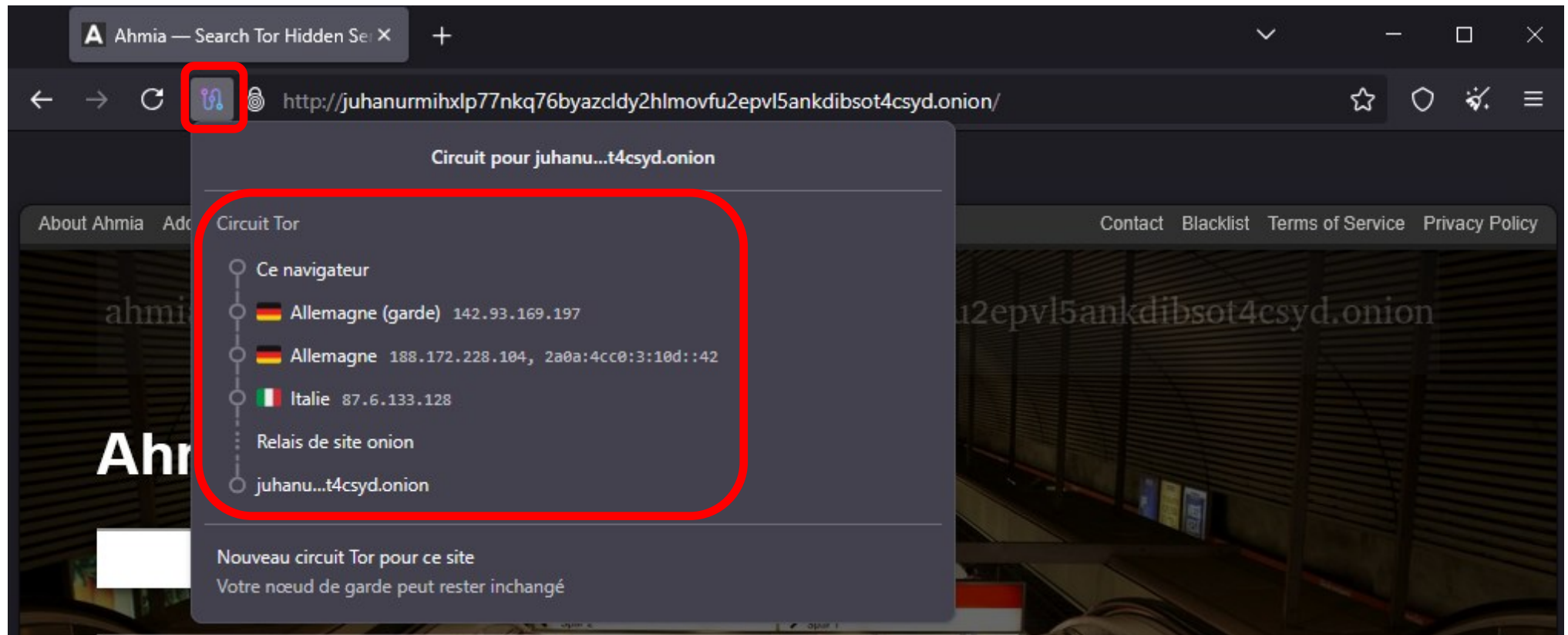
Source :

<http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/>



# Démonstration - Les points de départs

Le réseau TOR en fonctionnement (anonymisation) ...



# Démonstration - Les points de départs



## Les sites web des groupes de Ransomware / InfoStealer

Ransomware Database

Filter By Active

	NAME	RANSOMWARE TYPE	FIRST SEEN
Active	Spy Corporate	Data Broker	mai 2026
Active	Triple X	Data Broker	mai 2026
Active	Icarus	Data Broker	avril 2026
Active	MNT6	Data Broker	avril 2026
Active	M3RX	Crypto-Ransomware, Data Broker	avril 2026
Active	CMD Organization	Data Broker	avril 2026
Active	Aur0ra	Crypto-Ransomware, Data Broker	avril 2026
Active	TITAN	Crypto-Ransomware, Data Broker, RaaS	avril 2026
Active	TiMc	Data Broker	avril 2026
Active	Threat Market	Data Broker	mars 2026

## Ransomware - Triple X

### Triple X (Active)

**Description** This entry is under construction. However, we have included some details below.

**Ransomware Type** Data Broker

**First Seen** mai 2026

**Extortion Links**

MOYEN	LIEN
TOR	<a href="http://ojcmpbdncjo5dhaxll44bq6to3kwqtoeraevgsjquhdt4uv5l4igid.onion">http://ojcmpbdncjo5dhaxll44bq6to3kwqtoeraevgsjquhdt4uv5l4igid.onion</a>

**Extortion Types**

- Direct Extortion
- Double Extortion
- Free Data Leaks

**Communication**

MOYEN	IDENTIFIANT
Exploit.IN	<a href="https://forum.exploit.in/profile/240235-apt8172/">https://forum.exploit.in/profile/240235-apt8172/</a>

**Known Victims**

INDUSTRY SECTOR	PAYS	EXTORTION DATE	AMOUNT (USD)
Banking & Finance	Indonesia	2026-05-11	

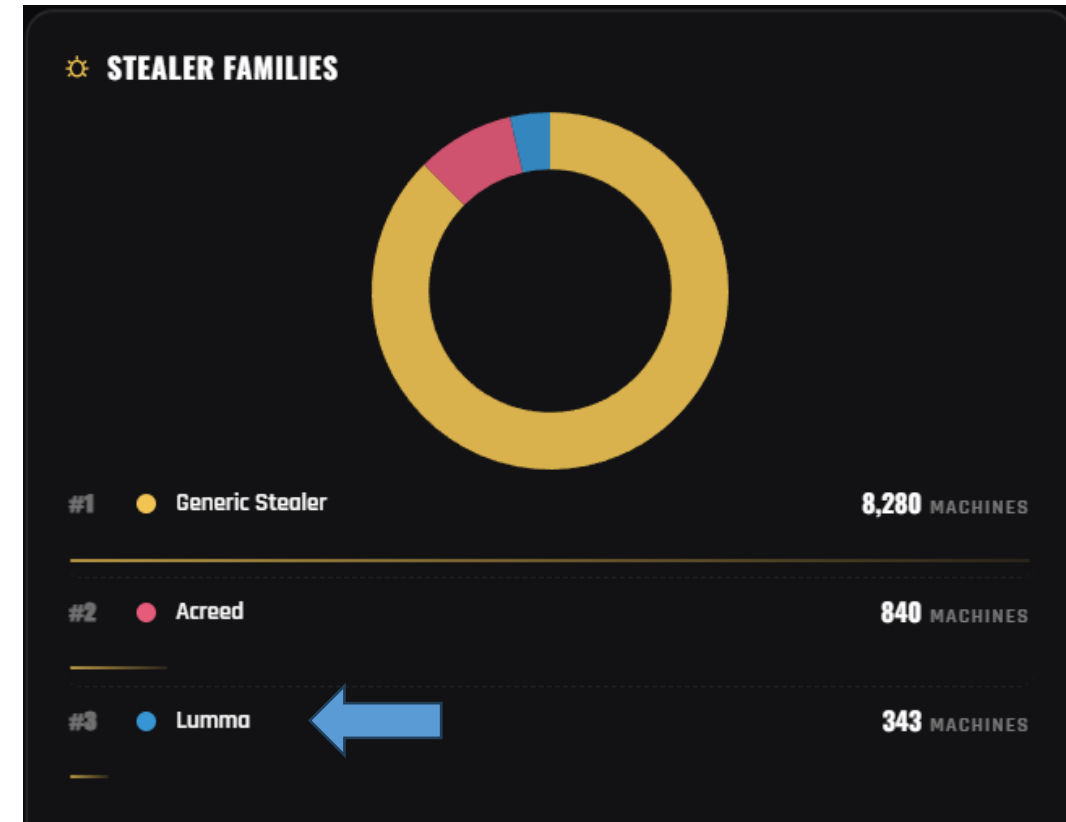
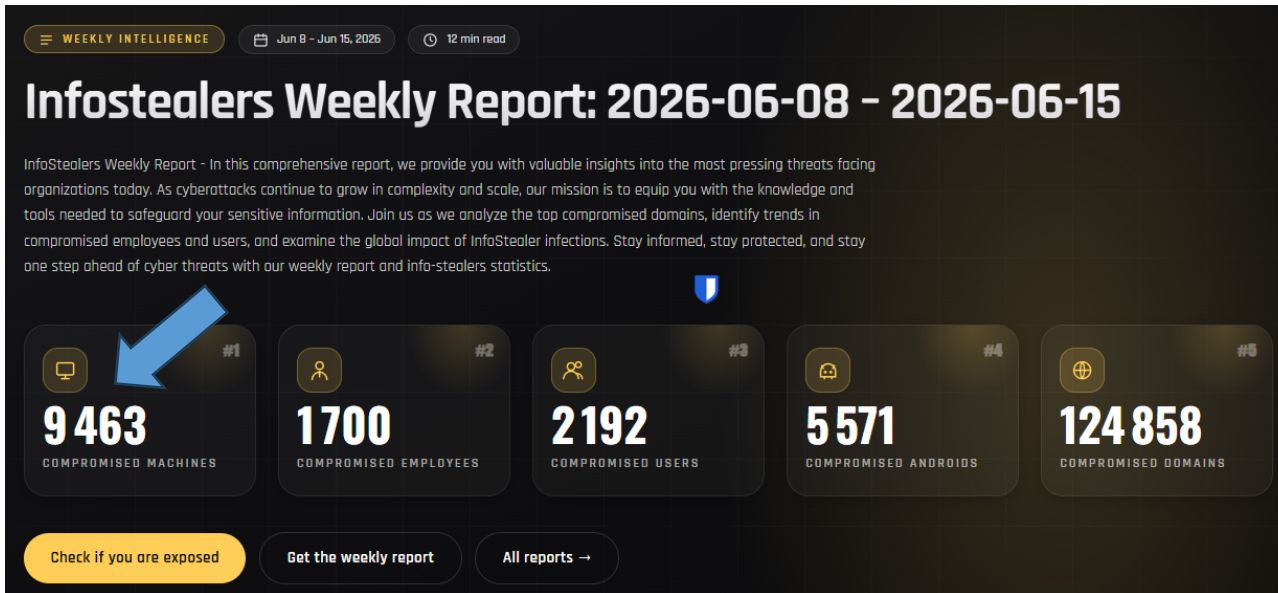
Source : WatchGuard

<https://www.watchguard.com/fr/wgrd-security-hub/ransomware-tracker>

# Démonstration - Les points de départ



## Les sites web des groupes de Ransomware / InfoStealer



Source : HudsonRock

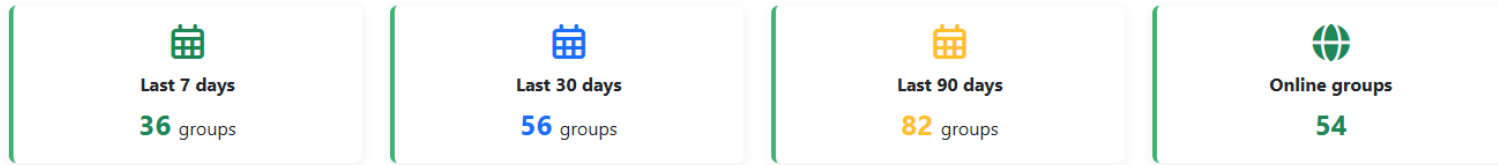
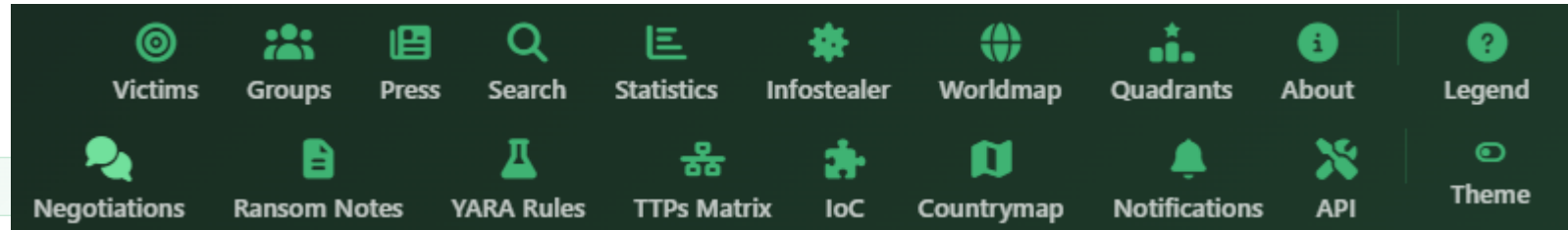
<https://www.info stealers.com/report/info stealers-weekly-report-2024-09-23-2024-09-30/>

# Démonstration - Les points de départs

## Les victimes attaquées et les groupes de Ransomware / InfoStealer

### Active Groups Summary

Only groups with at least one victim discovered in the last 90 days are shown in this summary.



GROUP	FIRST VICTIM *	LAST VICTIM	VICTIMS (7D)	VICTIMS (30D)	VICTIMS (90D)	ONLINE
shinyhunters	2024-04-23	2026-06-15	15	21	53	Online
anubis	2025-02-25	2026-06-15	2	7	20	Online
safepay	2023-11-10	2026-06-15	7	23	46	Online
nova	2025-03-22	2026-06-15	5	33	43	Online
krybit	2026-03-30	2026-06-15	7	22	50	Offline
thegentlemen	2023-02-28	2026-06-15	26	87	253	Online
qilin	2022-10-08	2026-06-15	24	92	321	Online

Source : Ransomware Live (sponsorisé par Hudson Rock)  
<https://www.ransomware.live>

# Démonstration - Les points de départs

## Les fuites de données

The screenshot displays the French Breaches website interface. At the top, there is a navigation bar with the logo 'French Breaches' and the tagline 'Votre référence N°1 sur les fuites de données en France'. The navigation menu includes 'Accueil', 'Blog', 'Carte BETA', 'Statistiques', 'Que faire?', and 'Signaler une fuite'. Below the navigation, there are filter options for 'Secteur (Tous)', 'Volume (Tous)', 'Type de données (Tous)', and 'Date (Toutes)', along with a 'Reinitialiser' button. The main content area shows a grid of breach cards. The first card, dated 16 juin 2026, is labeled 'FUIITE NEW Confirmée' and shows 'IMPACT SIGNALÉ n/c personnes impactées' for 'Achat-Or-Et-Argent'. The second card, also dated 16 juin 2026, is labeled 'FUIITE NEW Revendiquée (crédible)' and shows 'IMPACT NOTABLE 20K personnes impactées' for 'AUTOSUR'. The third card, dated 16 juin 2026, is labeled 'FUIITE NEW Revendiquée (crédible)' and shows 'IMPACT ÉLEVÉ 105K personnes impactées' for 'Inter Mutuelles Habitat'. Each card includes a brief description of the breach and buttons for 'Adresse e-mail', 'Adresse postale', and 'Historique des commandes'. The bottom row shows the start of another row of cards, including one dated 15 juin 2026 labeled 'RANSOMWARE'.

Source : <https://frenchbreaches.com/>

# Démonstration - Avec un simple navigateur Tor

## Le navigateur "Tor"



Télécharger le Navigateur Tor

Protégez-vous contre le suivi à la trace, la surveillance et la censure.

Télécharger pour Windows

Télécharger pour macOS

Télécharger pour Linux

Télécharger pour Android

[Signature](#)

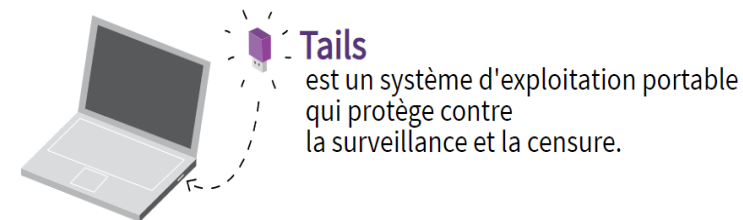
[Signature](#)

[Signature](#)

Source : The Tor Project

<https://www.torproject.org/fr/download/>

# Démonstration - Les environnements préconfigurés

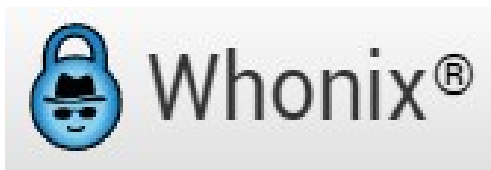


## Les "environnements" spécialisés (logiciel libre – Debian GNU/Linux)

- **Boîte à outils numérique**
  - Tails est fourni avec une sélection d'applications permettant de travailler sur des documents sensibles et de communiquer en sécurité.
- **Amnésie**
  - C'est à chaque fois dans le même état sain que Tails démarre et **tout ce que vous faites disparaît automatiquement lorsque vous éteignez Tails.**
- **Stockage persistant**
  - Vous pouvez enregistrer des fichiers et certaines configurations dans un stockage **persistant chiffré sur la clé USB** : vos documents, vos marque-pages du navigateur, vos courriers électroniques et même des logiciels supplémentaires.

Source : Tails  
<https://tails.net>

# Démonstration - Les environnements préconfigurés



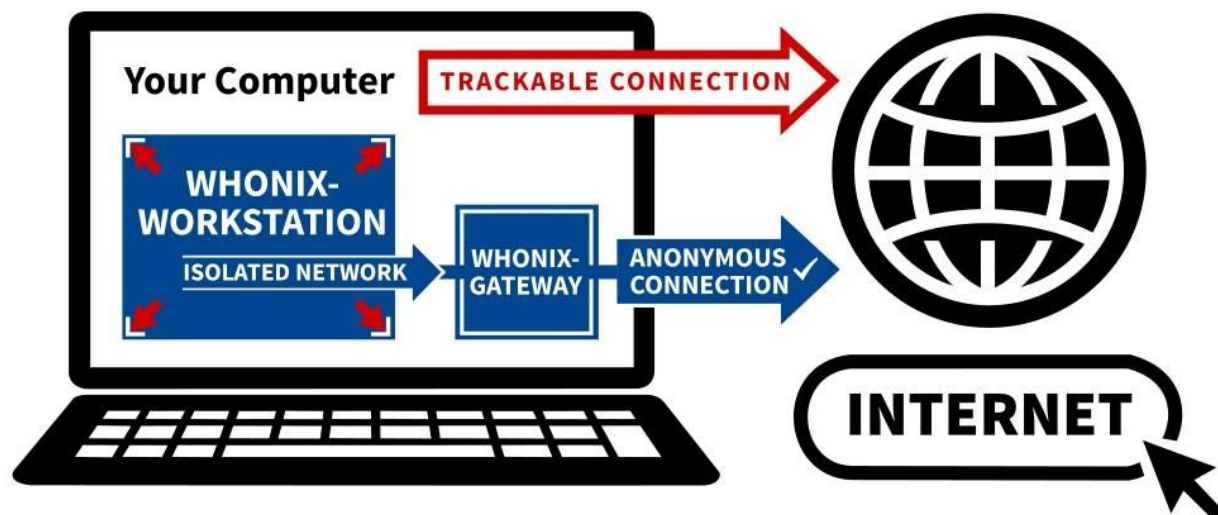
## Les "environnements" spécialisés (logiciel libre – Kicksecure/Debian GNU/Linux)

- **Sécurisé par défaut**
  - Whonix est un système d'exploitation anonyme qui fonctionne comme une application et redirige tout le trafic Internet via le réseau d'anonymat Tor.
  - Il offre une protection de la vie privée et de l'anonymat en ligne et est disponible pour tous les principaux systèmes d'exploitation.
- **En deux parties**
  - Une machine « Gateway » et une machine « Workstation »

Source : Whonix  
<https://www.whonix.org/>

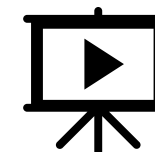
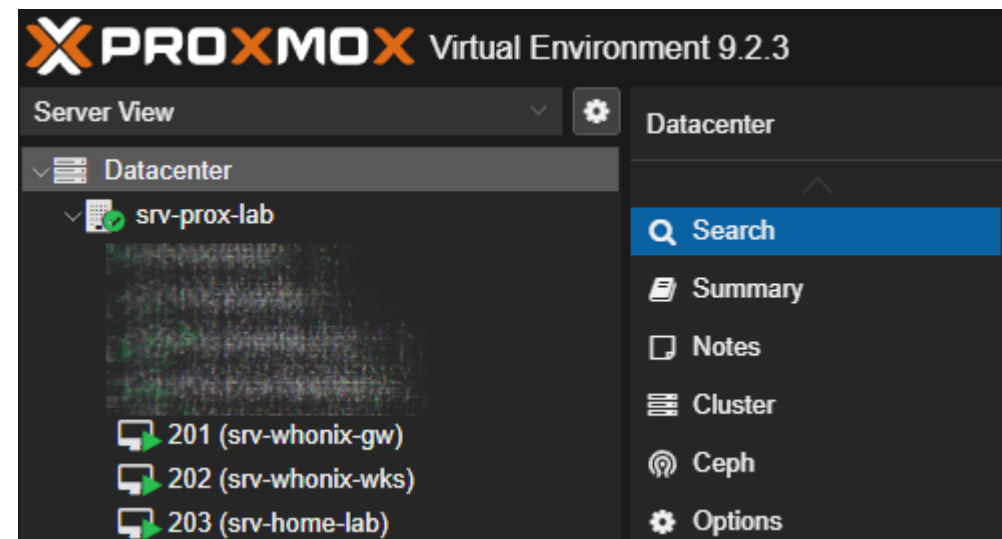
# Démonstration – Live !

## Whonix Anonymity Architecture



The red arrows  indicate that misbehaving / leaky applications can't break out of **Whonix-Workstation**.

All network connections  are forced to go through **Whonix-Gateway** where they are torified and routed to the Internet.



Fichier : *Dark Web – Démonstration Live.mp4*

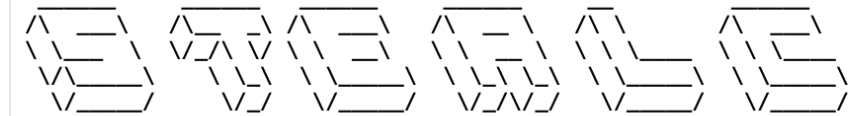
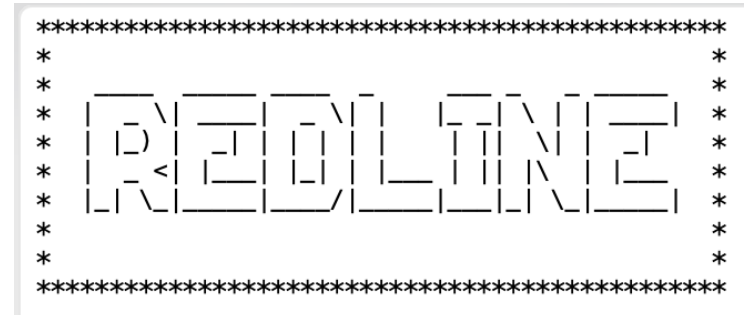
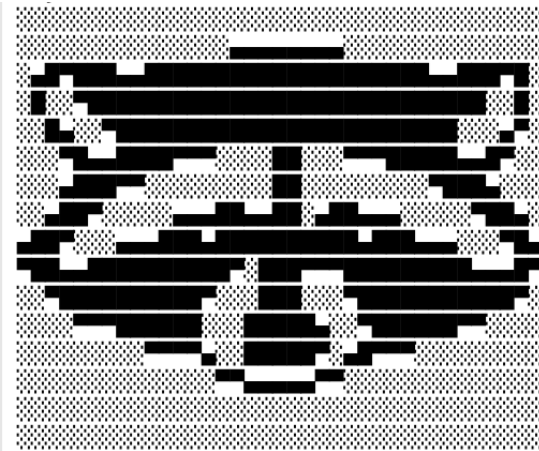


## *Comment surveiller le Dark Web*

# Retours d'expérience - Les InfoStealers

## Les « InfoStealer »

- “Les voleurs d’informations sont des malwares qui volent des données sensibles, également appelées logs, pour être vendues dans des forums ou partagées dans des groupes de discussion.”



stealc stealer

powerful native stealer based on C lang

# Retours d'expérience - Les InfoStealers

## Les logs des « InfoStealer » en clair



FRESH REDLINE LOGS JUNE.zip

Archive de 15 Go, contient 19 532 ordinateurs compromis

Name	Size	Packed Size	Modified
Autofills	41 954	9 179	2024-06-17 13:42
Cookies	159 683	71 735	2024-06-17 13:42
Discord	0	0	2024-06-17 15:28
FileGrabber	12 605	9 907	2024-06-17 13:42
Telegram	4 223 130	4 204 158	2024-06-17 13:42
a8ZItZ.txt	33	33	2024-06-18 17:10
DomainDetects.txt	752	276	2024-06-18 17:10
ImportantAutofills.txt	2 363	658	2024-06-18 17:10
InstalledBrowsers.txt	691	141	2024-06-18 17:10
InstalledSoftware.txt	5 462	1 932	2024-06-18 17:10
Passwords.txt	81 745	7 976	2024-06-18 17:10
ProcessList.txt	3 190	174	2024-06-18 17:10
UserInformation.txt	1 381	633	2024-06-18 17:10

=====

URL: <https://www.amazon.fr/ap/signin>

Username: richardmathieu@gmail.com

Password: lucie371

Application: Google\_[Chrome]\_Profile 5

=====

# Retours d'expérience - Les InfoStealers

## Les « InfoStealer »

*Extrait du Russian Market.*

<b>Source</b>	Rusmarkethgwhfbn.onion
<b>URL</b>	<a href="http://rumarkstror5mvgzzodzofkji3fna7lndfylvmzeisj5tamqnr4ad.onion/logs#2662a7">http://rumarkstror5mvgzzodzofkji3fna7lndfylvmzeisj5tamqnr4ad.onion/logs#2662a7</a>
<b>Status</b>	Online (Last check: Jun 4, 2026)

```
"Stealer": "rhamadanthys",
"Vendor": "d0####ey\n[Diamond]",
"Country": "Castille-La Mancha\nISP: TDENET (Red de servicios IP)\n",
"Date / Size": "2026.06.02\n0.33Mb",
"Outlook": "-",
"Info": "-\n",
"Struct": "",
"Links": "Login: + \nPassword: + \nCookie: -\napp-eul.hubspot.com | Login: + \nPassword: - \nCookie: + google.com |\nLogin: + \nPassword: - \nCookie: -",
"Archive Data": "\n var dirList33848768 =\n[\n {name: \"archive.zip\", iconSkin: \"pIcon01\", children: [ {name:\n\"Brute.txt\"}, {name: \"Passwords.tx",
"Price Sortable": "$ 10.00",
"Action": "Buy",
"Log ID": "33848768"
```

# Retours d'expérience - Les InfoStealers

## Les « InfoStealer »

*Extrait du Russian Market.*

Les ventes de fuites d'identifiants sur les marchés du Dark Web, peuvent également contenir le « Cookie » qui permettra peut être de contourner le 2FA si la session est toujours « active / valide »

*Ce vol (contenant 770 lignes) est vendu 10 USD*

Login: + Password: +Cookie: +	loewe.com
Login: + Password: +Cookie: +	login.live.com
Login: + Password: +Cookie: +	poliigon.com
Login: + Password: +Cookie: +	remotedesktop.google.com
Login: + Password: +Cookie: +	sketchucation.com
Login: + Password: + Cookie: -	account.bimobject.com
Login: + Password: + Cookie: -	accounts.logme.in
Login: + Password: + Cookie: -	dreamlove.es
Login: + Password: + Cookie: -	dropbox.com
Login: + Password: + Cookie: -	es.scribd.com
Login: + Password: + Cookie: -	es-la.facebook.com
Login: + Password: + Cookie: -	facebook.com
Login: + Password: + Cookie: -	fefcleon.alexiaclassroom.com
Login: + Password: + Cookie: -	id.mercedes-benz.com
Login: + Password: + Cookie: -	login.iberia.com
Login: + Password: + Cookie: -	materiales.cgate-coaat.com
Login: + Password: + Cookie: -	web2.alexiaedu.com
Login: + Password: + Cookie: +	amazon.es
Login: + Password: + Cookie: +	ikea.com
Login: + Password: + Cookie: +	sketchucation.com
Login: + Password: + Cookie: +	textures.com

# Retours d'expérience - Les InfoStealers

## Les « InfoStealer »

Keyword	<b>*mot clé surveillé*</b>		
Target	<a href="https://one.com.url">https://one.com.url</a> (URL complète)		
User	<b>*identifiant en clair*</b>		
Password	<b>*mot de passe en clair*</b>		
Victim IP	93.xx.xx.231		
Leak Date	2026-06-01T21	25	08Z
Detection Date	2026-06-10T15	08	31.216490Z
Machine Name	DESKTOP-6IUL6DM (5a3f1c7ec0209b3c)		
User Session	<b>*nom de la session en clair*</b>		
Malware Location	C:\Users\admin\AppData\Roaming\bl2clgfi.fuz\x\1527633244.exe		
Malware Name	Generic Stealer		

**Credentials exfiltrated by infostealers**  
**1/4 Minor**

Incident detection - JFIE2Z  
Jun 11, 2026



*Les identifiants et mots de passe stockés dans les gestionnaires de mots de passe des navigateurs ne sont pas « en sécurité »*

# Retours d'expérience - CTI

## Le renseignement sur la menace (CTI)

Claimed at ↓	Category	Victim	Industry	Country	Threat Actor
Jun 15, 2026 17:57 UTC	Data Leak	LocalEmploi localemploi.fr	Commercial	France	OxSec
Jun 15, 2026 15:28 UTC	Data Leak	Superimmo.Com superimmo.com			
Jun 15, 2026 14:01 UTC	Data Leak	Free free.fr			
Jun 14, 2026 23:01 UTC	Data Leak	JeVeuxAider.Gouv.Fr jeveuxaider.gouv.fr			
Jun 14, 2026 19:03 UTC	Data Leak	Autonomous Parisian Transport Administration ratp.fr			
Jun 14, 2026 12:45 UTC	Data Leak	Immo Facile immmo-facile.com			
Jun 13, 2026 18:23 UTC	Data Leak	Digital Avocat digital-avocat.fr			
Jun 13, 2026 16:25 UTC	Data Leak	Figaro Immobilier immobilierpro.lefigaro.fr			
Jun 13, 2026 16:07 UTC	Data Leak	National Network Of Junior Association juniorassociation.org			
Jun 13, 2026 14:16 UTC	Data Leak	Réseau National Des Juniors Associations juniorassociation.org			
Jun 13, 2026 14:03 UTC	Data Leak	Explorimmo.Com, Figaro Immobilier, Immobilier.Lefigaro.F...	Commercial, Retail, Technology	France	ChimeraZ

Claimed at ↓	Category	Victim	Industry	Country	Threat Actor
Jun 15, 2026 09:01 UTC	Ransomware	CONSTRUCTIONS PIRAINO, Piraino.Fr piraino.fr	Construction	France	The Gentlemen
Jun 14, 2026 05:15 UTC	Ransomware	Council Of Europe coe.int	Government	France	ShinyHunters
Jun 12, 2026 00:48 UTC	Ransomware	Fetis Group, SECOM Engineering secomengineering	Manufacturing, Technology	France	ANUBIS
Jun 11, 2026 16:58 UTC	Ransomware	Free free.fr	Technology, Telecommunications	France	Cryptix
Jun 11, 2026 16:29 UTC	Ransomware	DISCOLAB Industry disco-lab.fr	Chemical, Manufacturing	France	INC RANSOM
Jun 9, 2026 12:56 UTC	Ransomware	Centre Ellipse centre-ellipse.fr	Healthcare	France	akira
Jun 8, 2026 17:17 UTC	Ransomware	Opéra Comique opera-comique.com	Entertainment	France	Qilin
Jun 4, 2026 04:02 UTC	Ransomware	Service Alimentaire 2000 sa2000.com	Retail, Technology	France	STORMOUS



## *Pourquoi surveiller le Dark Web ?*

# Mon point de vue

*La surveillance du Dark Web est importante pour plusieurs raisons :*

- **Détection précoce des fuites de données** : Elle permet aux entreprises de détecter les fuites de données rapidement, souvent avant que ces informations ne soient utilisées à des fins malveillantes.
- **Prévention de la fraude et de l'usurpation d'identité** : En identifiant les informations volées, les entreprises et les individus peuvent prendre des mesures pour sécuriser leurs comptes et protéger leurs identités.
- **Conformité réglementaire** : Certaines réglementations exigent des entreprises qu'elles surveillent et protègent les données personnelles. La surveillance du **Dark Web** peut aider à respecter ces obligations légales.

Source : ITrust

<https://www.itrust.fr/definition-dark-web-monitoring/>



MERCI

• *Le savoir partagé est la meilleure défense.* •

# Bonus

*Réponses du Quiz*

*Lectures et Vidéos pour approfondir vos connaissances*

# Réponses au Quiz

- **1 – Qu'est-ce que le Dark Web ?**
  - A) La face sombre d'Internet
  - B) Des pages cachés dans Internet
  - C) Le mode sombre de votre navigateur internet
  - D) Les sites Web accessibles dans le Dark Net

## Réponse D) le Dark Web est :

- L'ensemble des sites Web que l'on retrouve dans le Dark Net

# Réponses au Quiz

- **2 – Comment le Dark Web est-il caché ?**
  - A) En masquant les adresses IP
  - B) Car aucun lien direct ne révèle sa présence
  - C) L'accès nécessite des outils spécifiques
  - D) Les réponses A, B et C

## Réponse D) le Dark Web est caché par :

- **Non-indexation** : Il n'est pas indexé par les moteurs de recherche traditionnelles
- **Logiciels spécifiques** : Il nécessite des logiciels comme TOR pour y accéder.
- **Adresses .onion** : Les sites ont des adresses spécifiques accessibles uniquement via TOR.
- **Chiffrement** : Les données sont fortement chiffrées pour protéger l'anonymat.

# Réponses au Quiz

- **3 – Est-ce que le Dark Web et le Dark Net sont en fait la même chose ?**
  - A) Oui
  - B) Oui en quelque sorte
  - C) Oui à 60%
  - D) Non

## Réponse D) :

- **Non, le Dark Web est une partie du Dark Net, mais le Dark Net inclut également d'autres réseaux privés et anonymes**

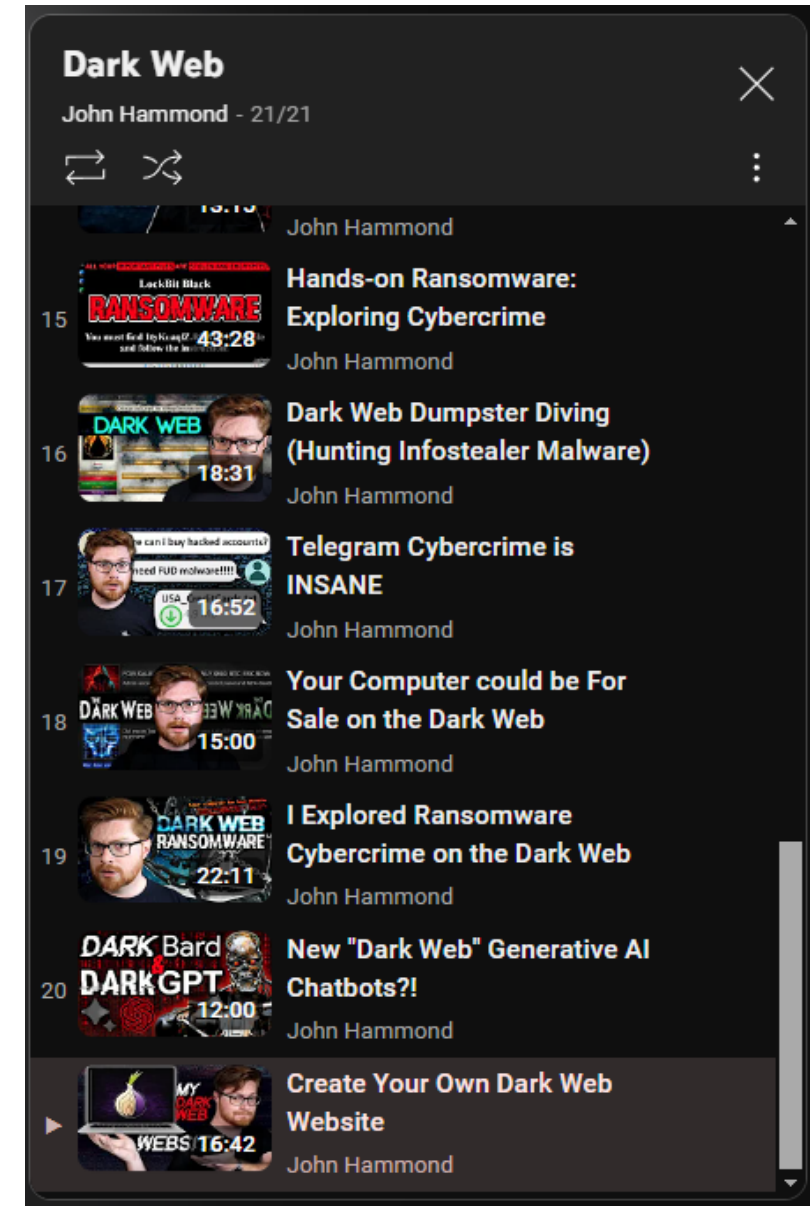


## Bonus - Le Dark Web

John Hammond (YouTube en anglais)

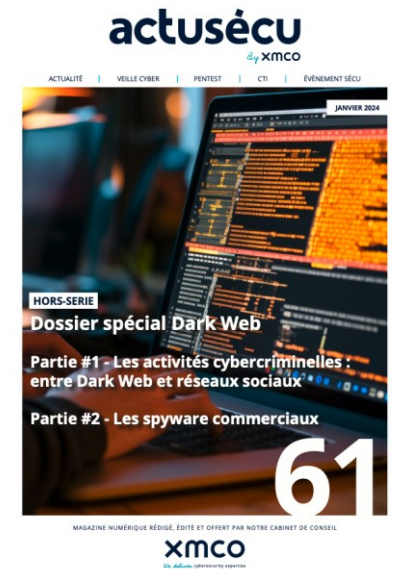
- Une série de 21 vidéo documentaires « éducatives » sur le Dark Web réalisées un professionnel de la Cyber
- *En autres, comment installer les différents environnements cités en exemple pour se connecter au Dark Web*

Source : <https://www.youtube.com/watch?v=QTizSz73yYU&list=PL1H1sBF1VAKU8aP5FC-makTTBknb1EWYC>





## Bonus - Le Dark Web



### Cabinet XMCO – Paris (e-magazine PDF en Français)

- **ActuSécu #52 (Nov. 2019) - Dossier spécial Dark Web en 2 parties**

- Partie #1 : Anonymat et TOR
- Partie #2 : Démantèlement des forums

[https://www.xmco.fr/wp-content/uploads/2021/11/52.XMCO-ActuSecu-52-Dossier\\_Darkweb-min.pdf](https://www.xmco.fr/wp-content/uploads/2021/11/52.XMCO-ActuSecu-52-Dossier_Darkweb-min.pdf)

- **ActuSécu #61 (Fév. 2024) - Hors-série spécial Dark Web**

- Les activités cybercriminelles : entre Dark Web et réseaux sociaux
- Les spywares commerciaux

<https://www.xmco.fr/wp-content/uploads/2024/02/XMCO-ActuSecu-61-Dark-Web-Spyware.pdf>

