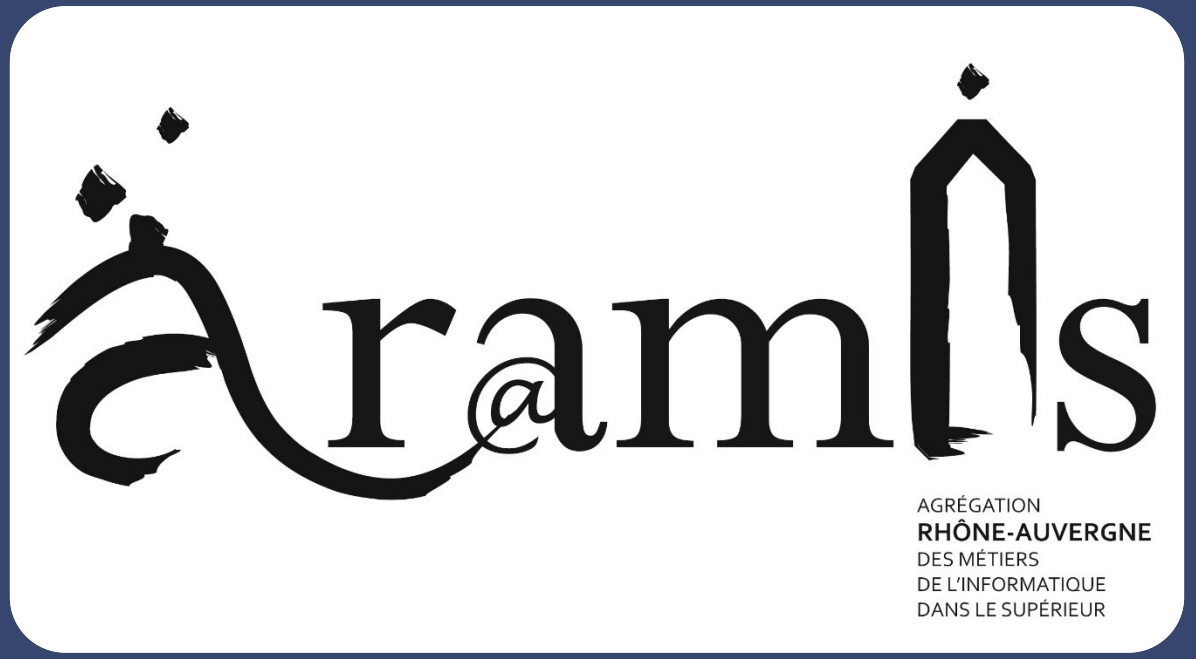
CLUSIR
Auvergne-Rhône-Alpes



Dark Web

Fonctionnement, opportunités, menaces et retour d'expériences

Jeudi 18 juin 2026

LE DARK WEB

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

LE DARK WEB

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

ESKER

Membre actif

CLUSIR Auvergne-Rhône-Alpes

Présentateur

LES JOURNÉES DE LA CYBER

Deux fois vainqueur
par équipe du CTF

CSI AUVERGNE-RHÔNE-ALPES
LES CHALLENGES DE LA SÉCURITÉ DE L'INFORMATION

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/MaSAlPtEcEY

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

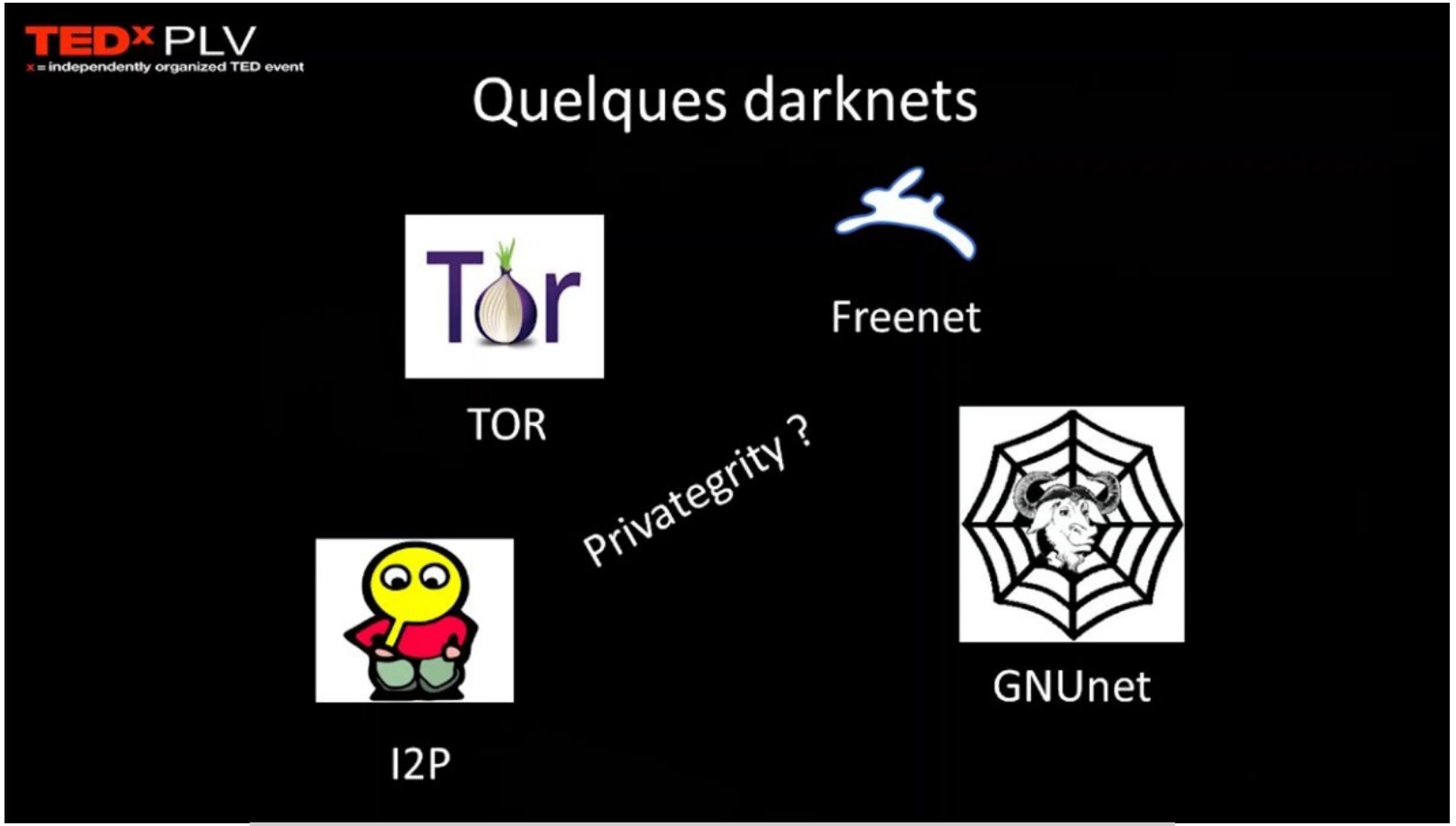
Définitions - Les Dark Net

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.



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

Pour démystifier

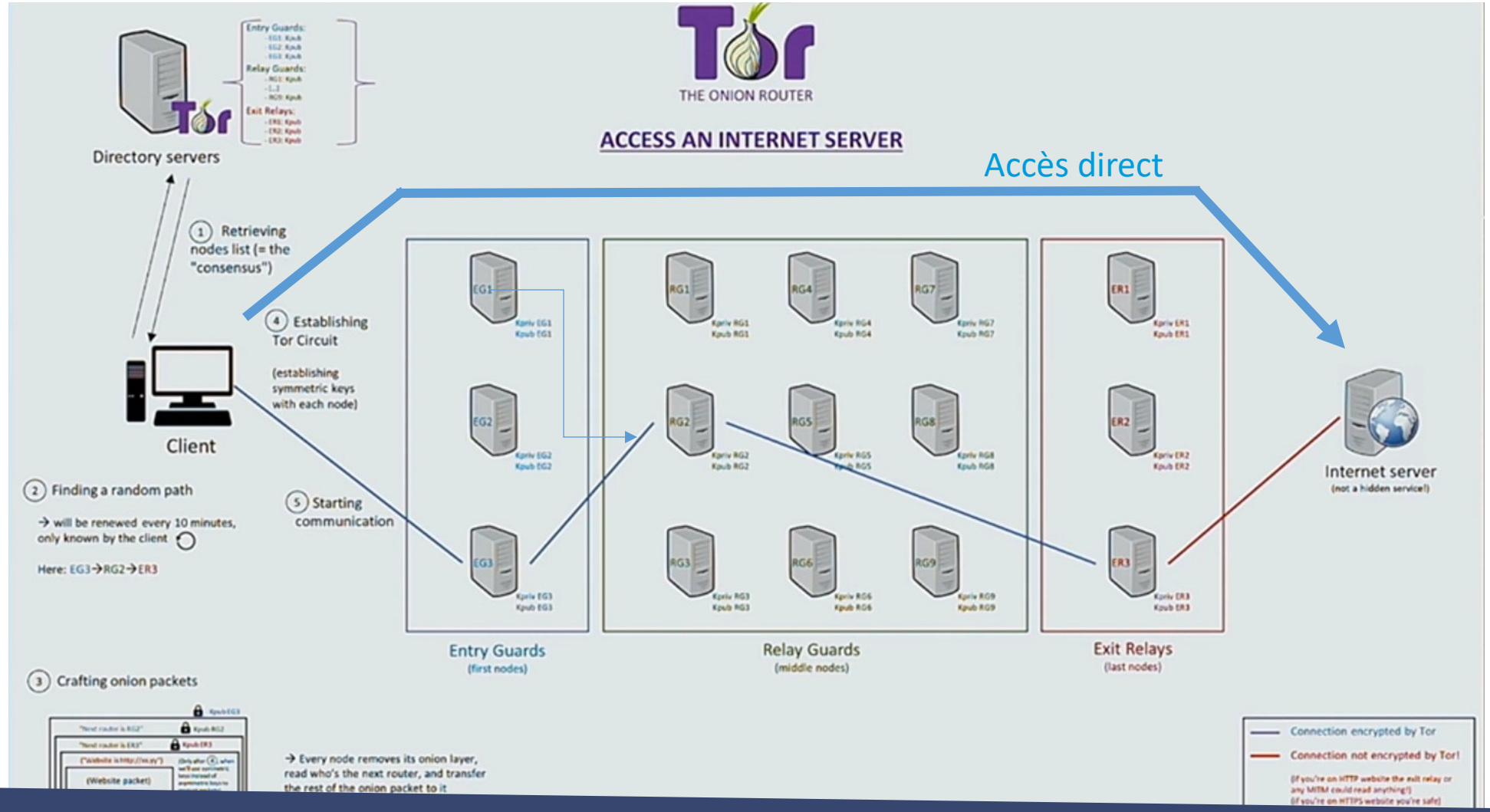
Fonctionnement - Accès et anonymat

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



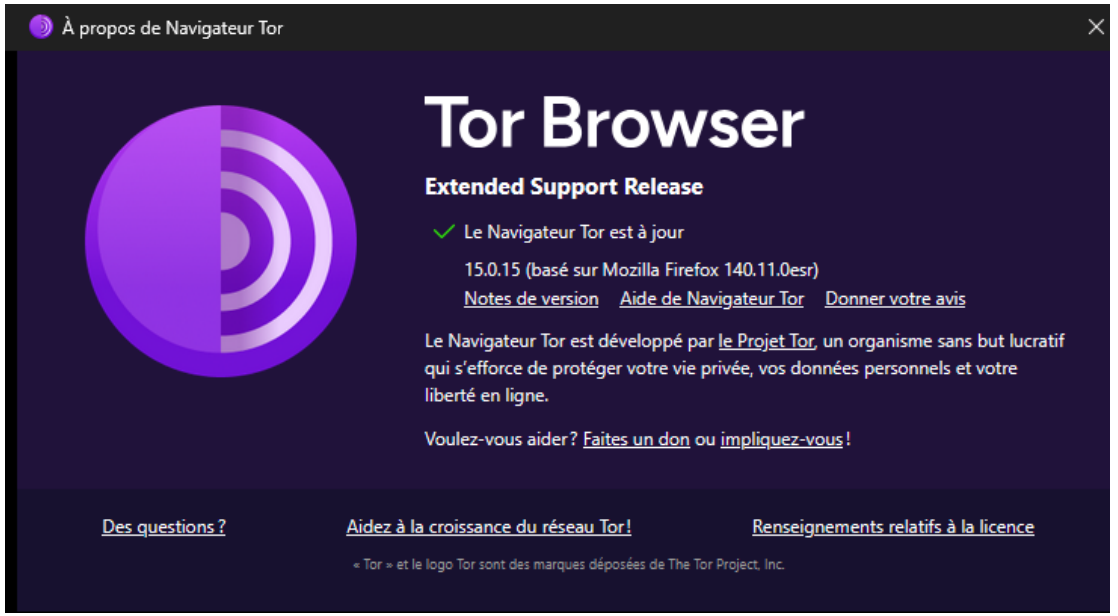
Source : https://youtu.be/IqofT1yt7Fk?t=571

Comparaison en FR des modes de fonctionnement des « anonymiseurs »

Clear Web

Fonctionnement - Accès et anonymat

Dark Web



Le **Dark Web** du réseau **Dark Net** Tor 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

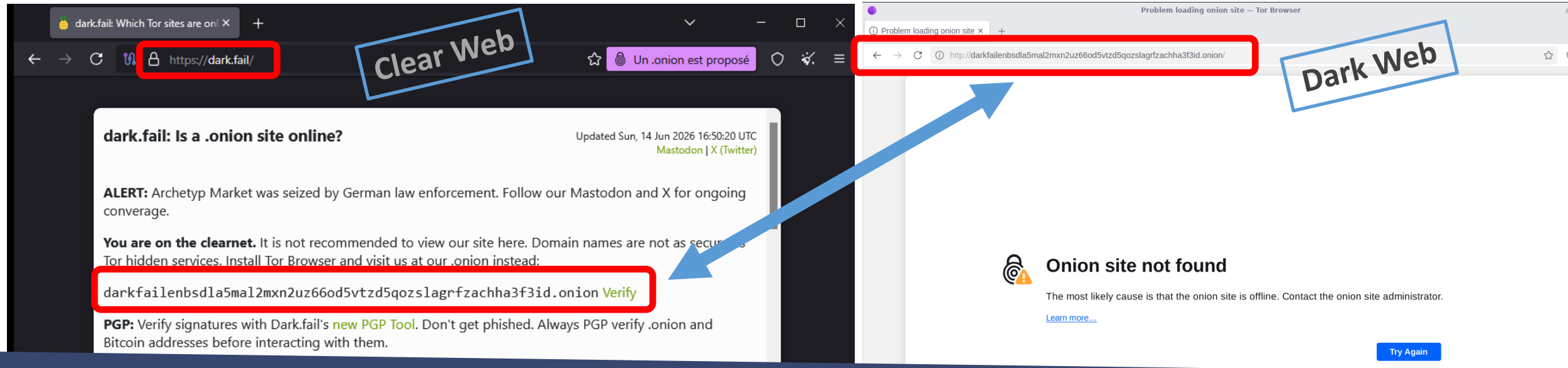
* de manière prête à l'emploi (Out-of the Box)

Fonctionnement – Structure et contenu

- Contrairement aux noms de domaine classique en *gTLD, geoTLD, sTLD ou ccTLD (.com, .nyc, .gov, .fr)*
  (**G**eneric, **Geo**graphic, **S**ponsored, **C**ountry **C**ode **T**op **L**evel **D**omain)

- Pour le réseau Tor 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

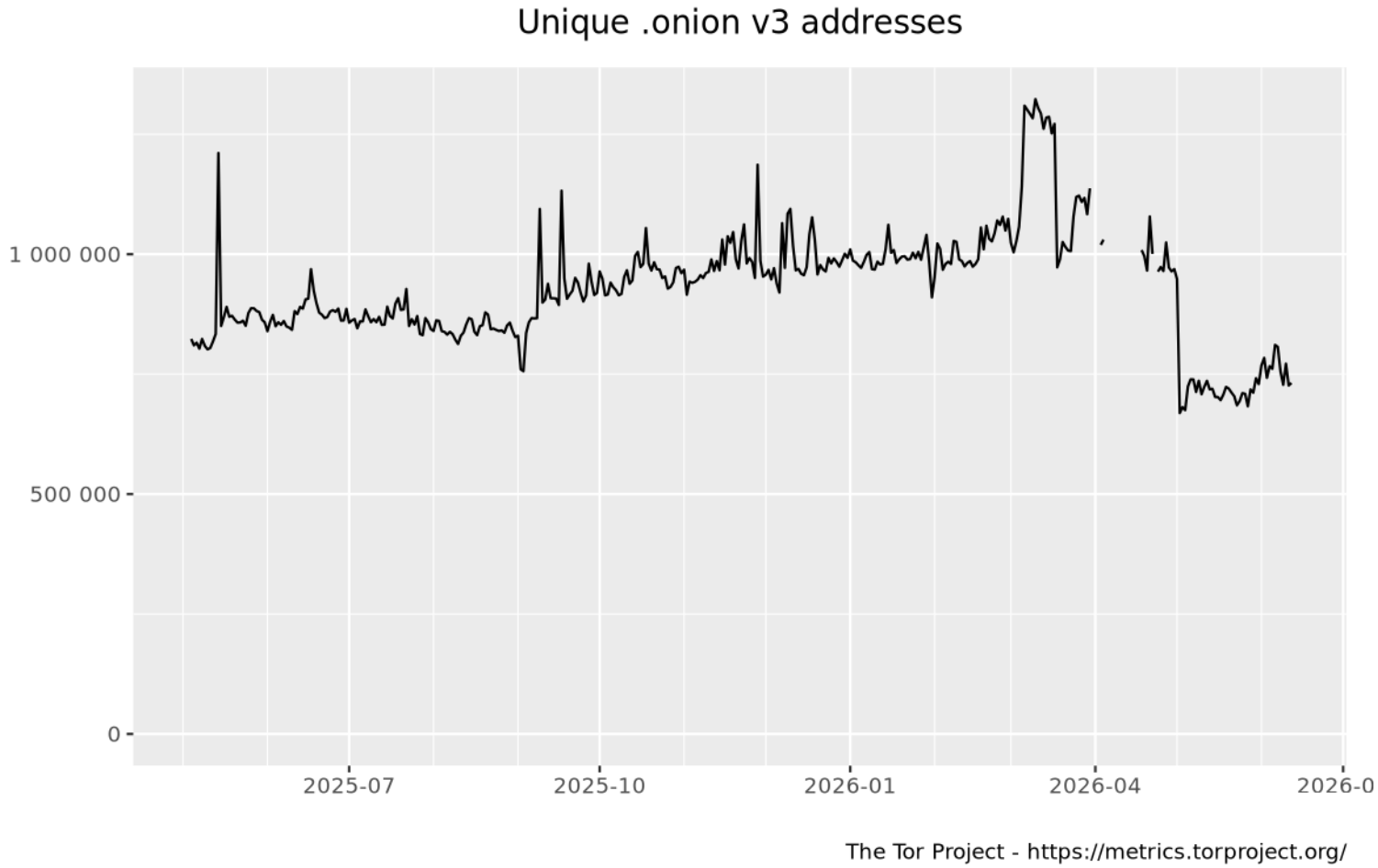


Fonctionnement – Entrées dans l'annuaire

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/hidserv-dir-v3-onions-seen.png?start=2025-05-01&end=2026-06-14

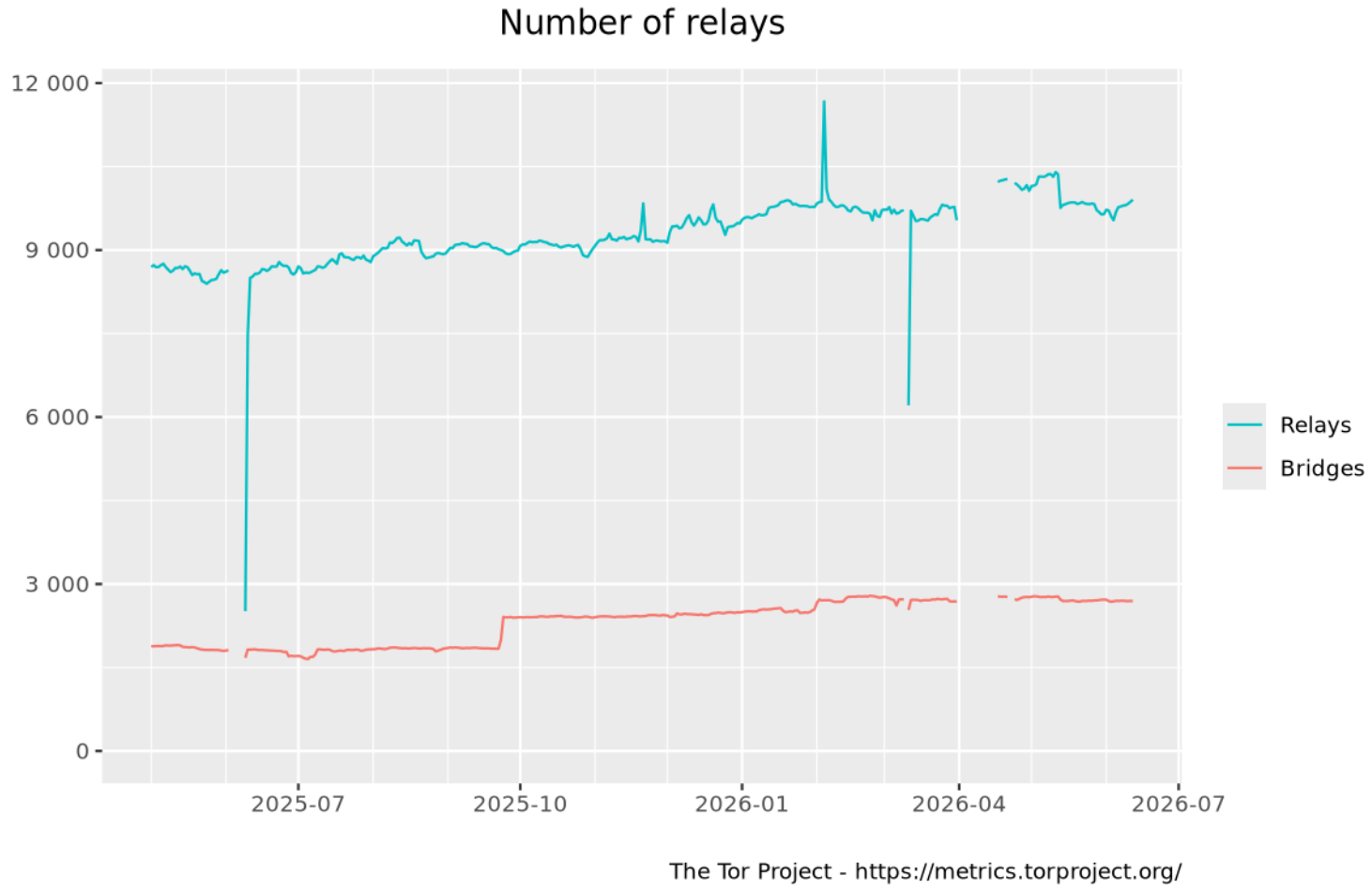


Fonctionnement – Infrastructure

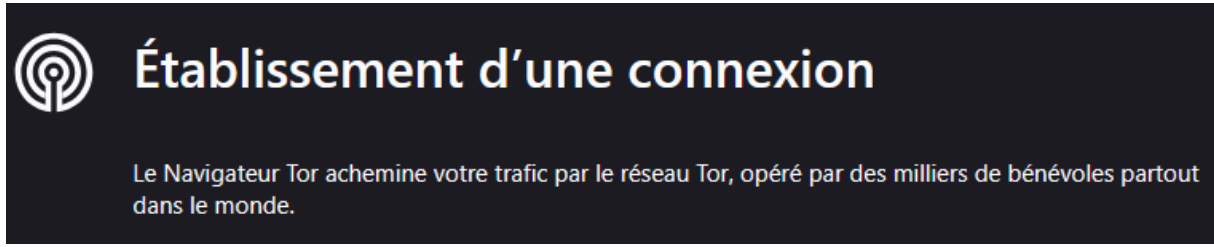
Nombre de "Serveurs Tor" (Relays)

- Les serveurs Tor sont hébergés par la communauté.

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



Fonctionnement – Contributeurs

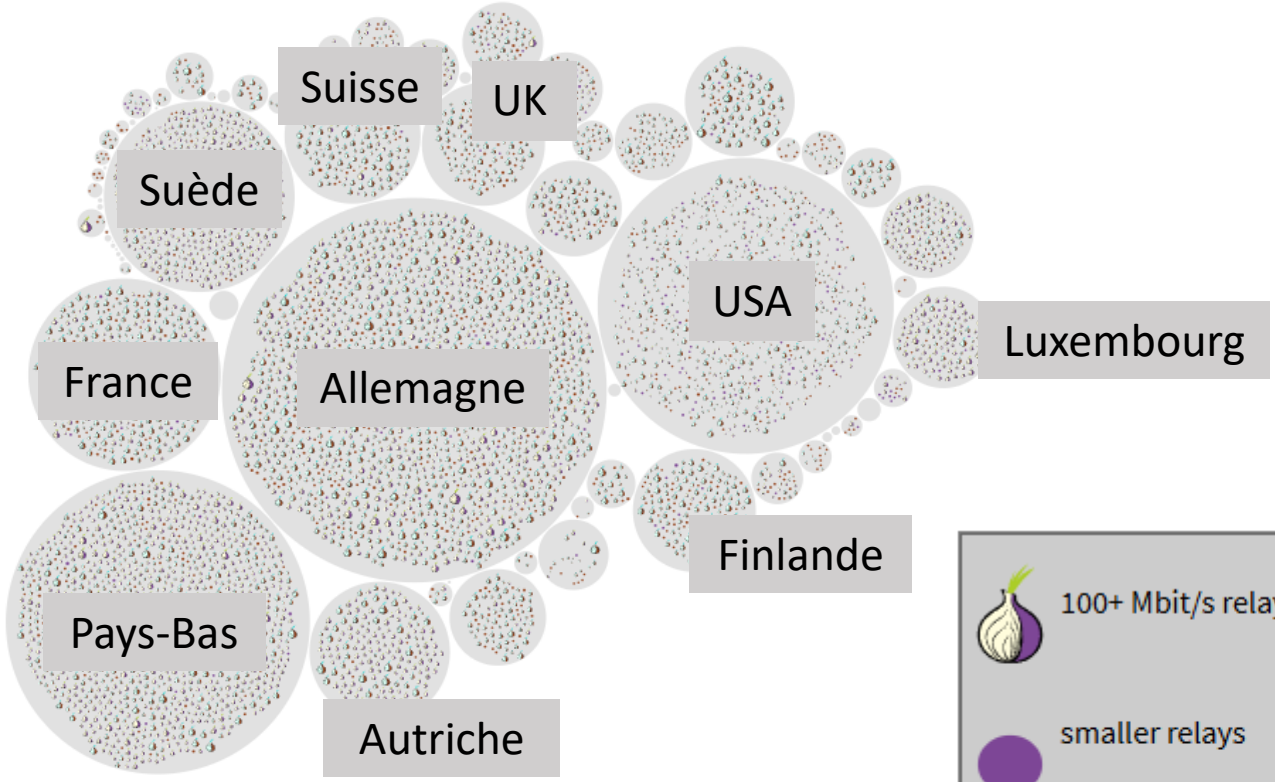


Tor | Metrics

Localisation des "Servers Tor" (Relays)

- Les pays avec le plus de "Relay Tor"

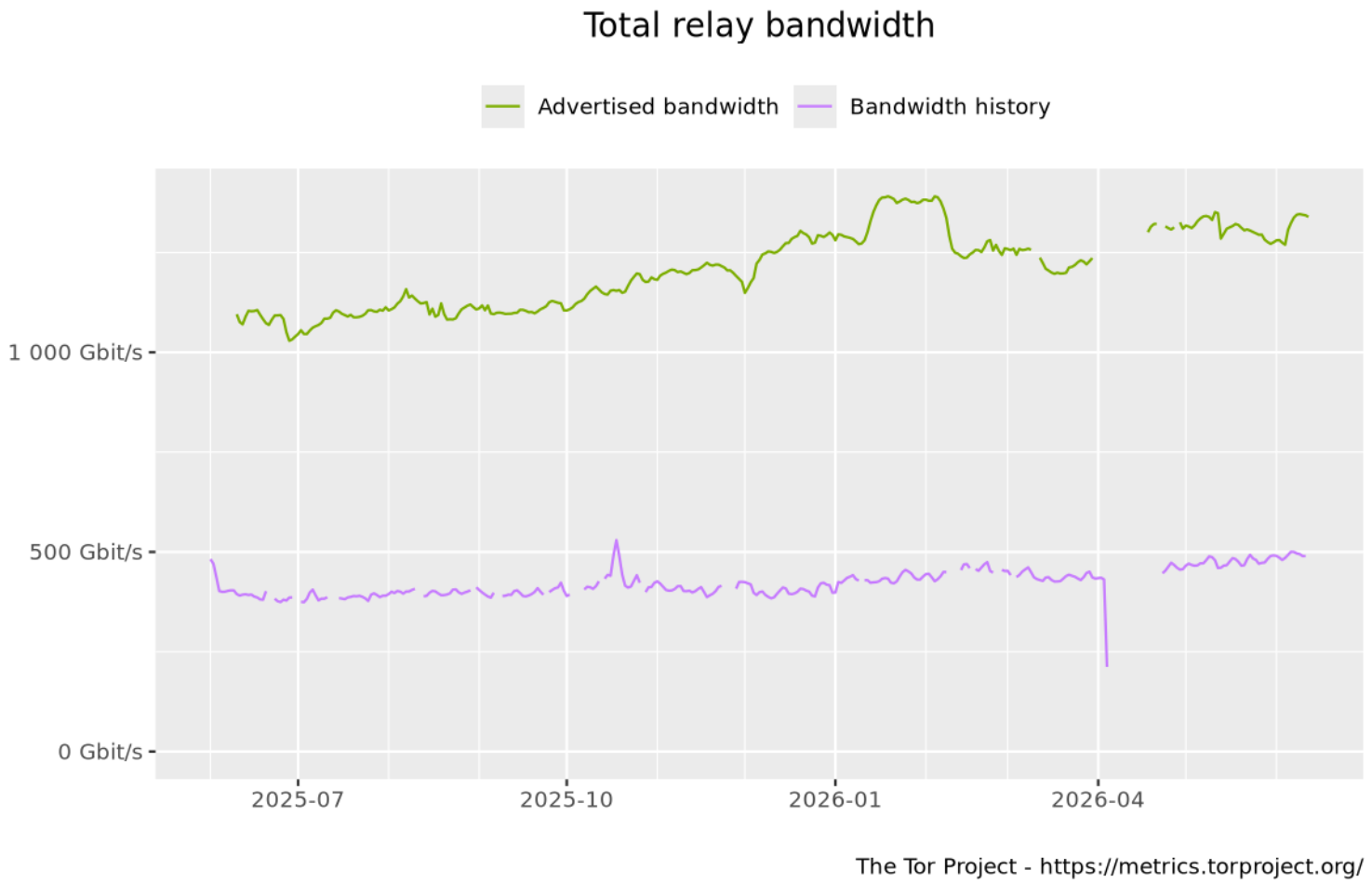
Source :
https://metrics.torproject.org/bubbles.html#country

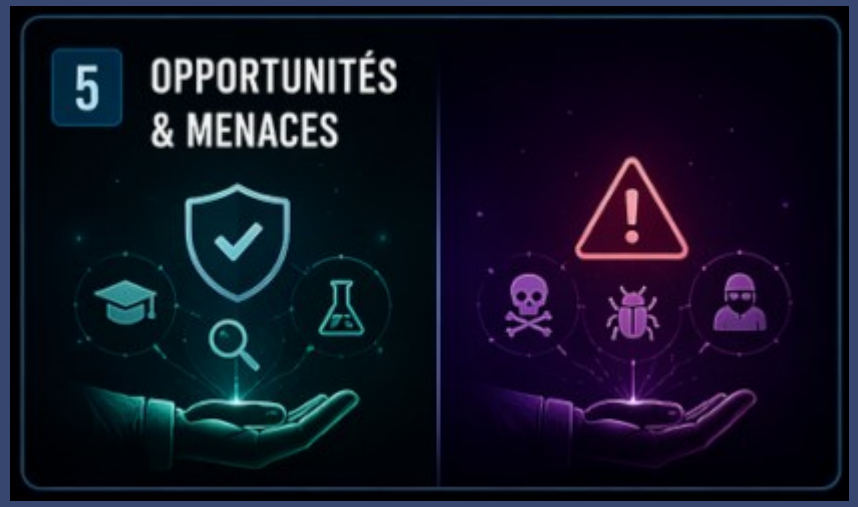


Fonctionnement – Structure et contenu

Bande passante des "Servers Tor" (Relays)

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





Pour connaitre 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 machés 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

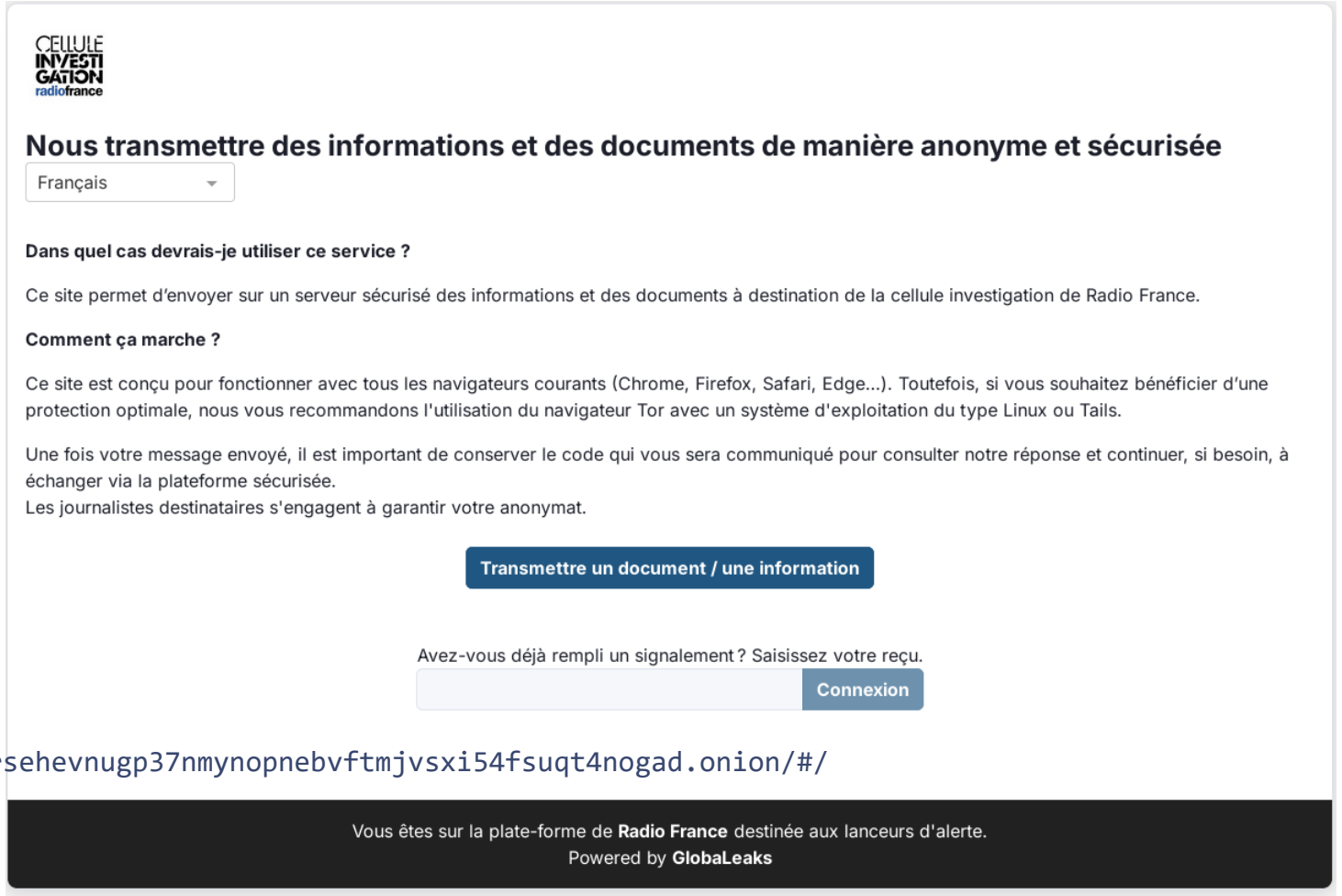
Certaines organisations de notoriété publique ont une présence sur le Dark Web

- 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 gouvernent 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**



Source : `http://ckahyzrwglnbgrsehevnugp37nmynopnebvftmjvsxi54fsuqt4nogad.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 :

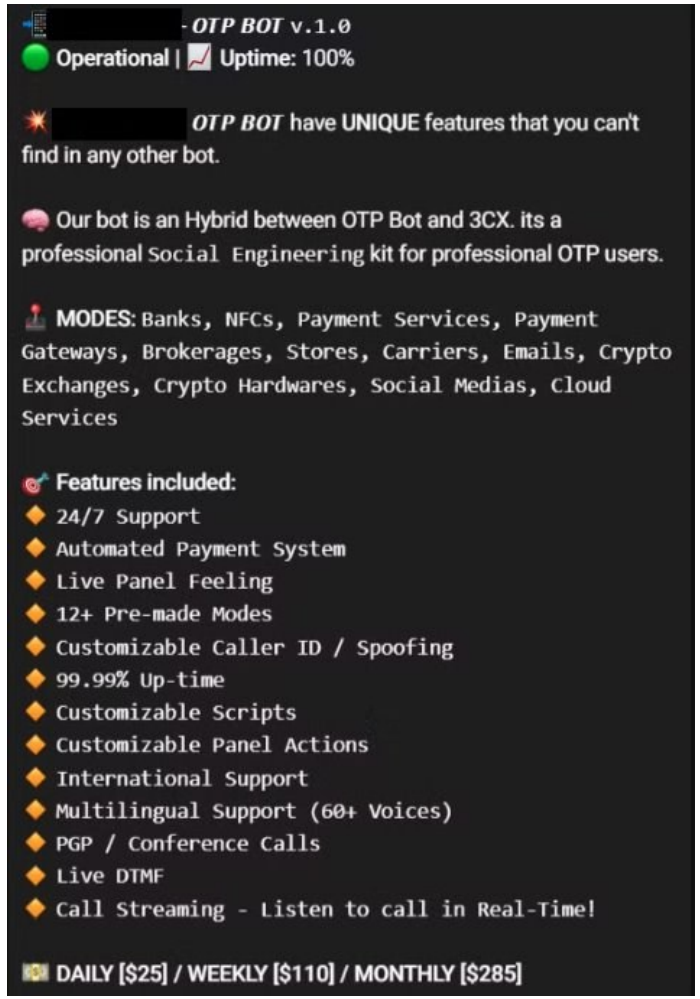
- Chevaux de Troie d'accès à distance (RAT)
- Botnets
- Ransomwares
- Cryptomineurs ou autres outils de cryptojacking
- Outils de piratage tels que les craqueurs de mots de passe
- Autres types de malwares

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



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

La Rép des Pyrénées

FAITS DIVERS

L'aéroport de Pau et Eklore, deux entités de la CCI, victimes d'une cyberattaque

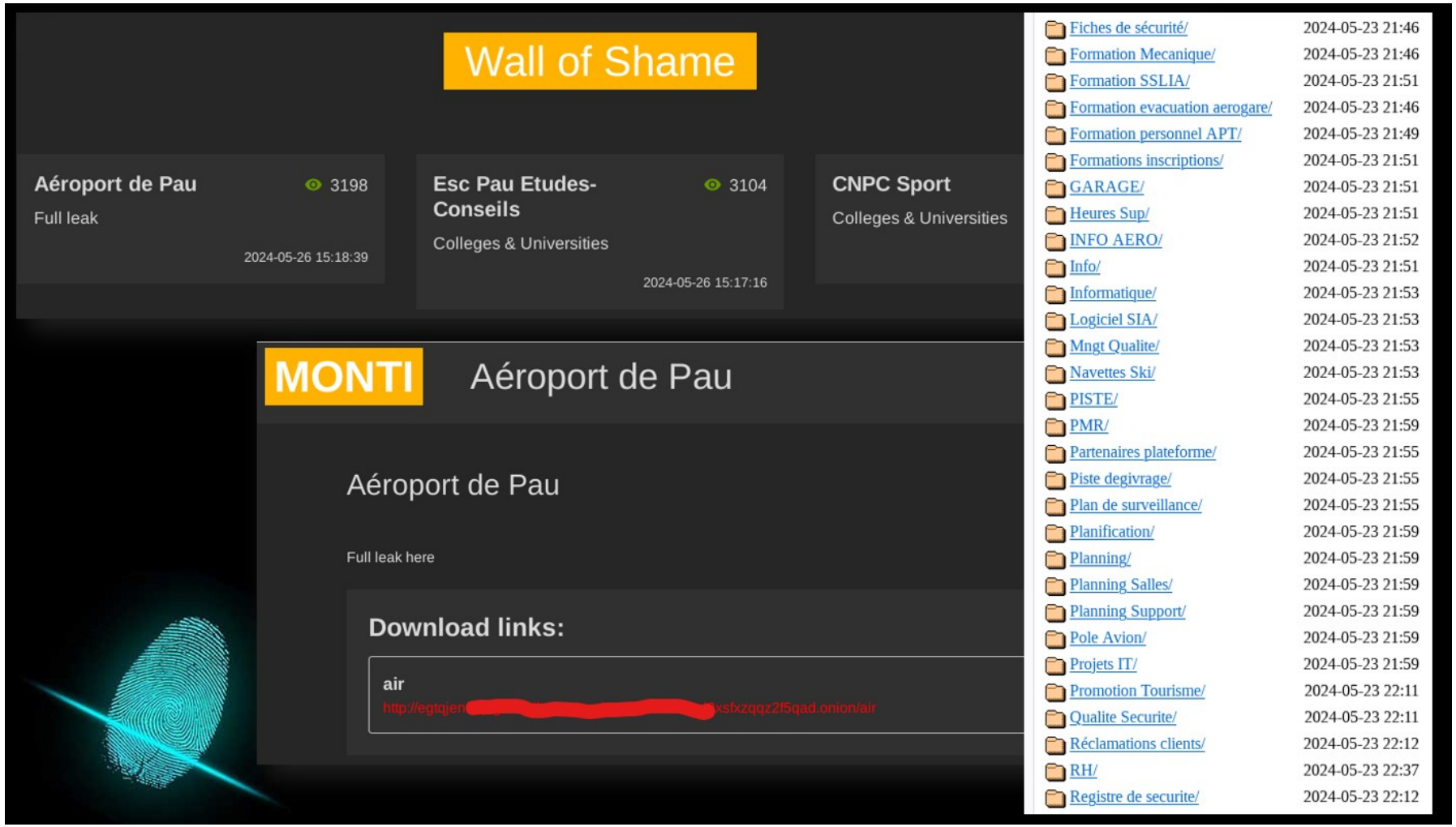
Dans la presse quotidienne

*Dans la nuit du **12 au 13 mai** 2024 l'aéroport et les écoles Eklore 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.*

Pau : les données piratées de l'aéroport et des écoles Eklore potentiellement publiées sur le dark web

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

Opportunités et menaces – Lieu de divulgation d'info volées



Source : Dark Web

Opportunités et menaces – Renseignements sur la menace

Point juridique

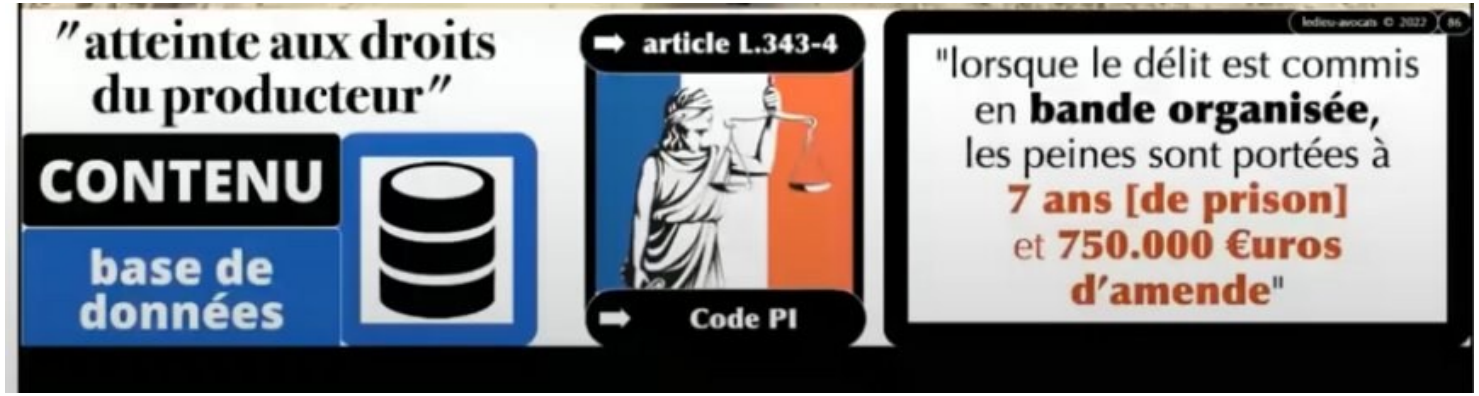
#371 ré-utiliser les data d'une fuite de données (leak), c'est pénal ou c'est légal ?

- 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 !

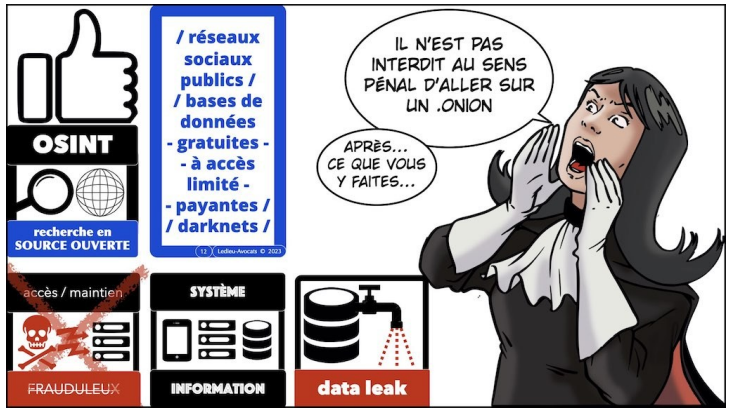


Réponse

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 ?

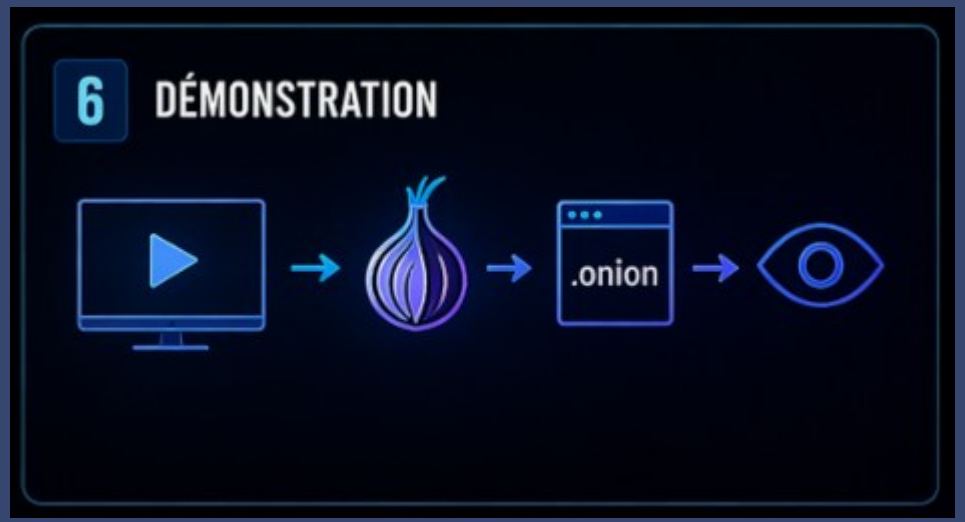
Source : Livre Blanc – Le cadre légal de l'OSINT (page 5)
(A débusquer dans la WayBack Machine)
et
https://itlaw.fr/quel-est-le-cadre-legal-de-losint/

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.

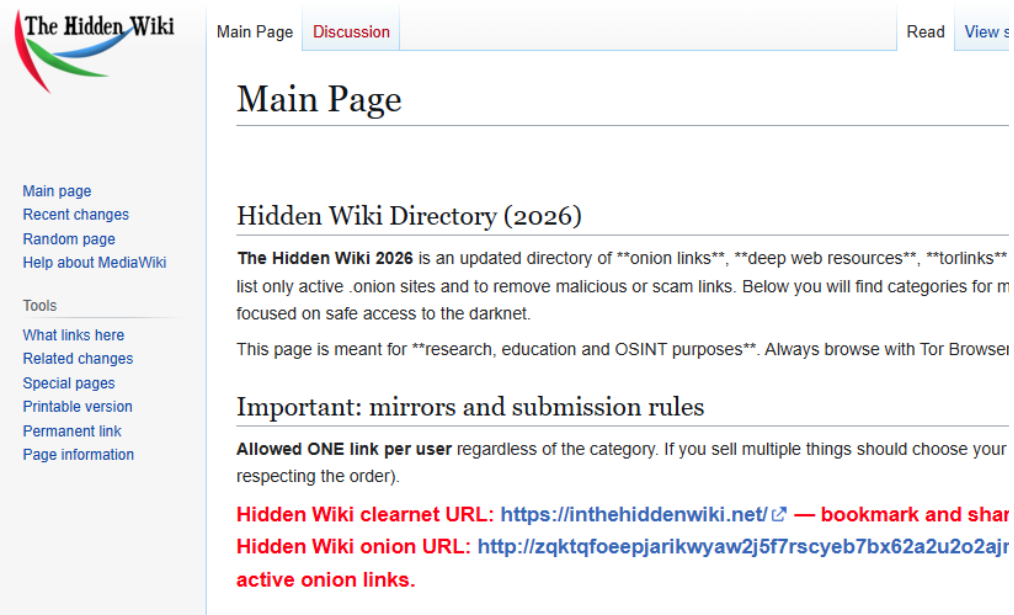
- Le receleur est la personne qui « détient une chose […] en sachant que cette chose provient d'un crime ou d'un délit ». Sanction : 5 ans de prison et 375 000 € d'amende.



Pour chercher soi-même sur le Dark Web

Démonstration - Les points de départs

Le "Hidden Wiki"

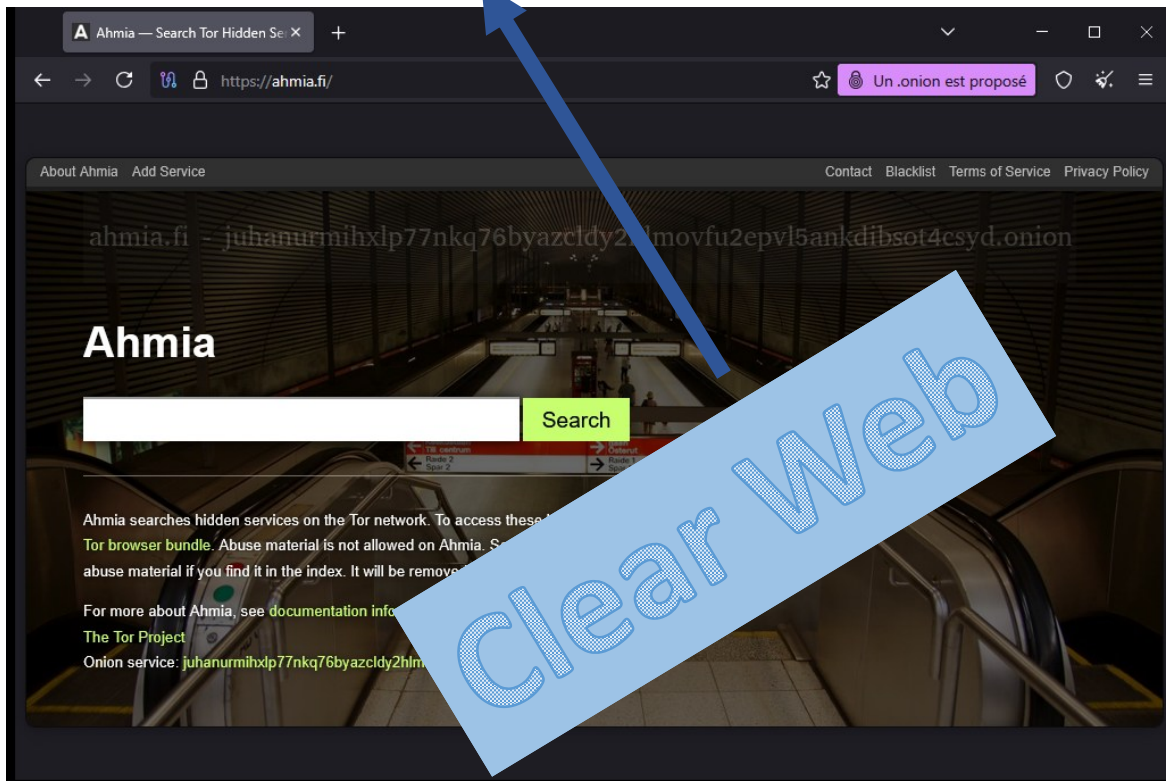


Source : The Hidden Wiki
Clear Web : https://inthehiddenwiki.net
Dark Web : http://zqktqfoeepjarikwyaw2j5f7rscyeb7bx62a2u2o2ajmxcl46c7xeiid.onion

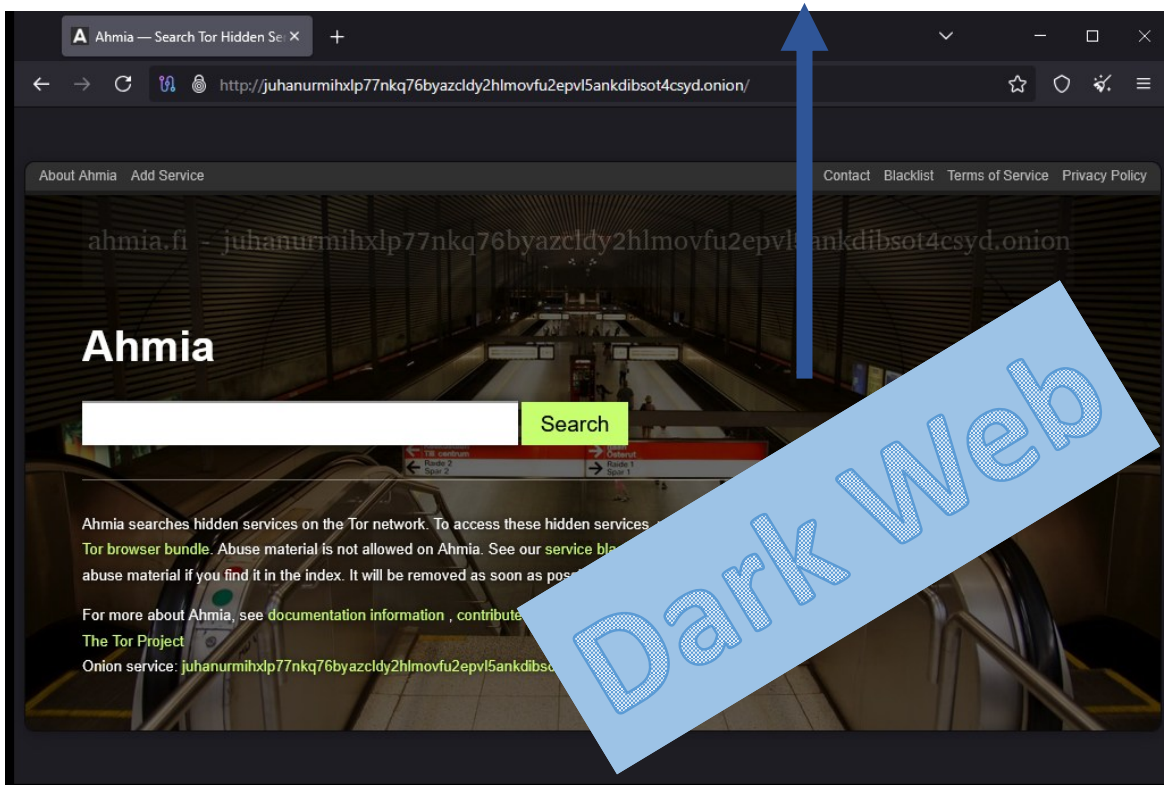
Démonstration - Les points de départs

Un moteur de recherche …

Source : https://ahmia.**fi**

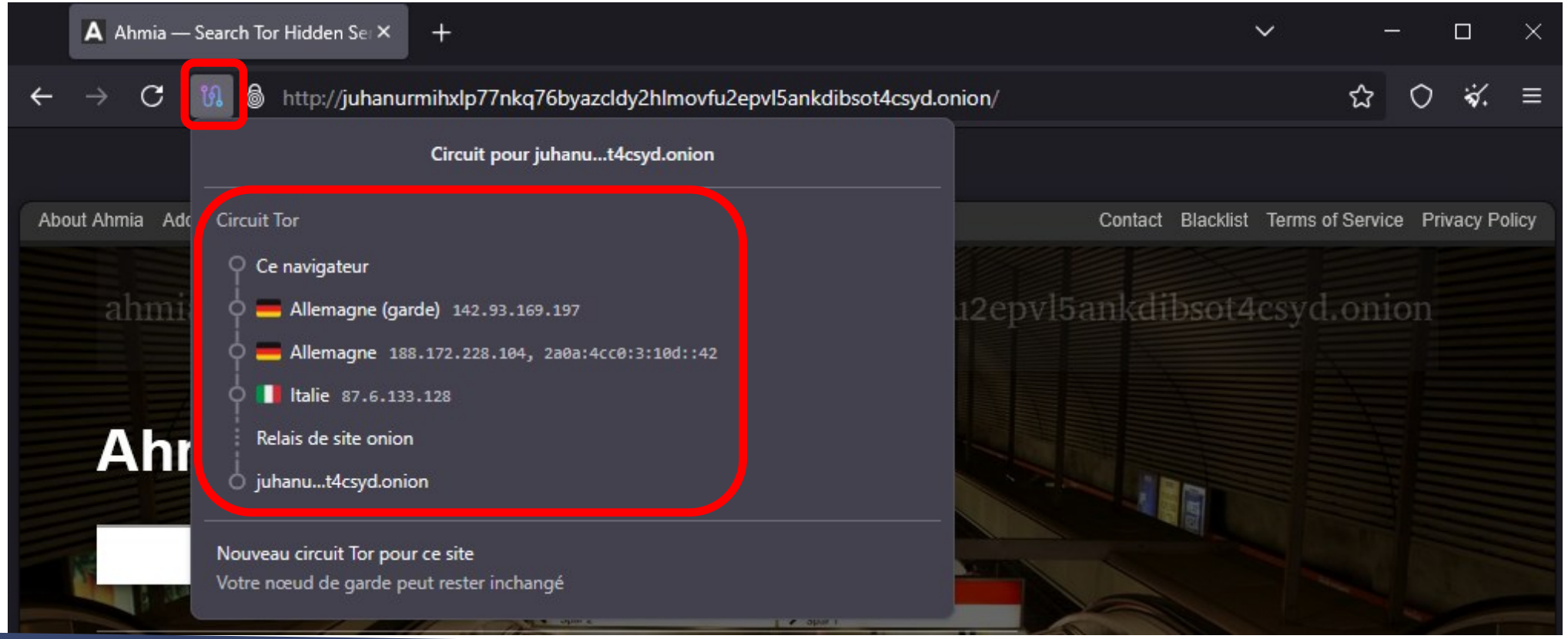


Source : http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.**onion**/



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	http://ojcmpbdncjo5dhaxxll44bq6to3kwqtoeraevgsjquhdtt4uv5l4igid.onion
Extortion Types	Direct Extortion	
	Double Extortion	
	Free Data Leaks	
Communication	**MOYEN**	**IDENTIFIANT**
	Exploit.IN	https://forum.exploit.in/profile/240235-apt8172/

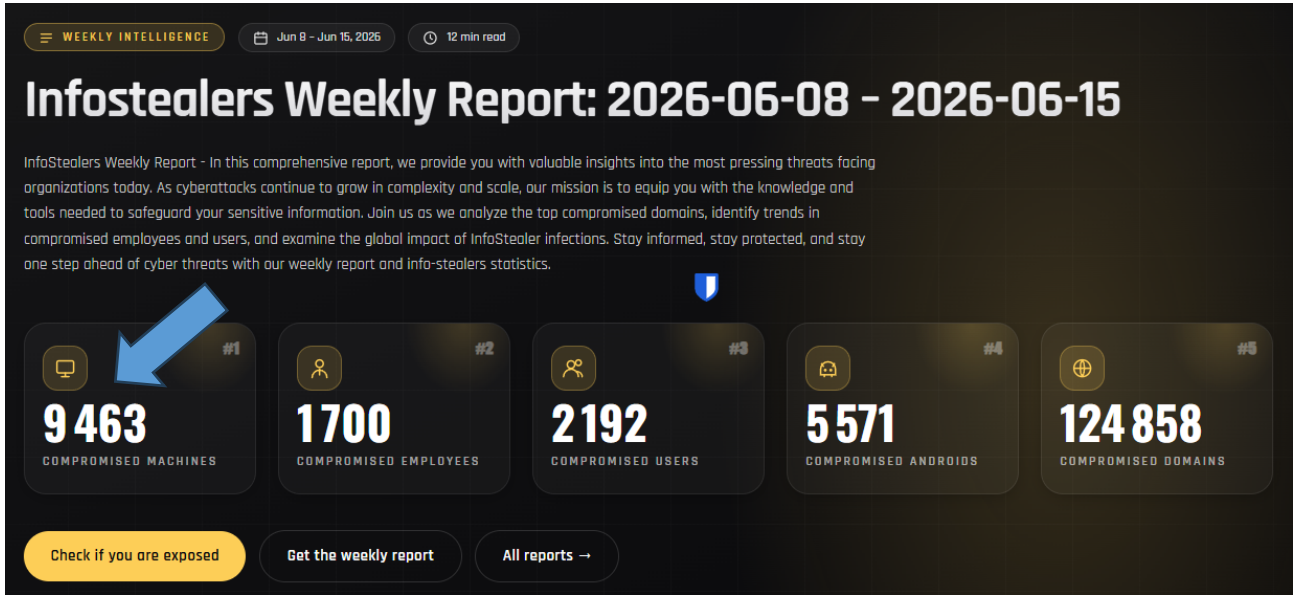
Known Victims	INDUSTRY SECTOR	PAYS	EXTORTION DATE	AMOUNT (USD)
	Banking & Finance	Indonesia	2026-05-11	

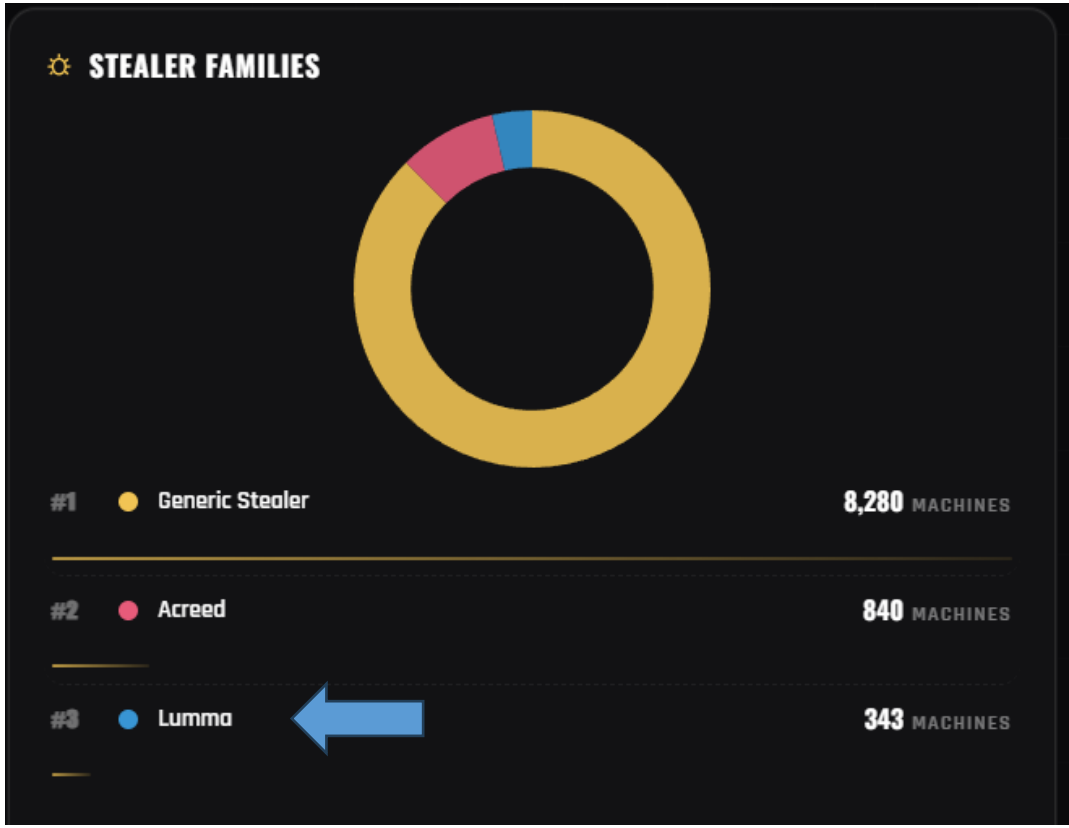
Source : WatchGuard

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

Démonstration - Les points de départs

Les sites web des groupes de Ransomware / InfoStealer





Source : HudsonRock
https://www.infostealers.com/report/infostealers-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.

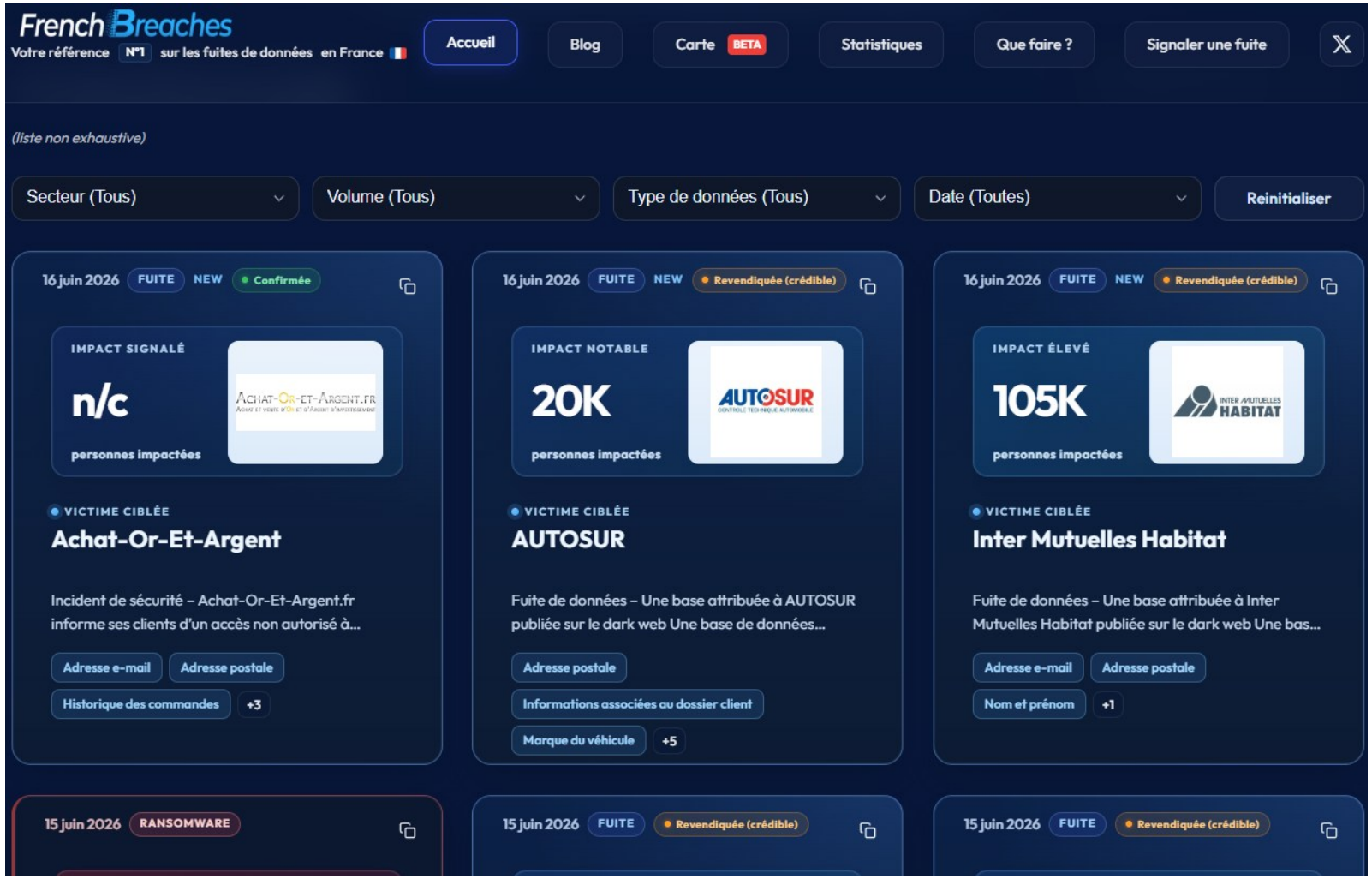
Last 7 days	Last 30 days	Last 90 days	Online groups
36 groups	56 groups	82 groups	54

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



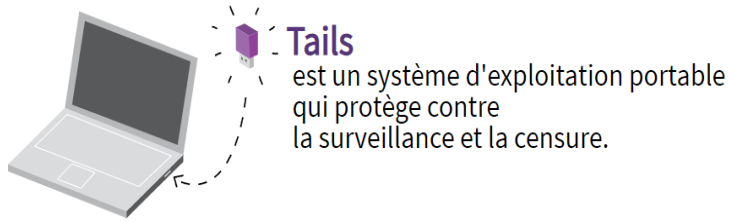
Source : https://frenchbreaches.com/

Démonstration - Avec un simple navigateur Tor

Le navigateur "Tor"

Source : The Tor Project
https://www.torproject.org/fr/download/

Démonstration - Les environnements préconfigurés



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

- Boite 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

Whonix®

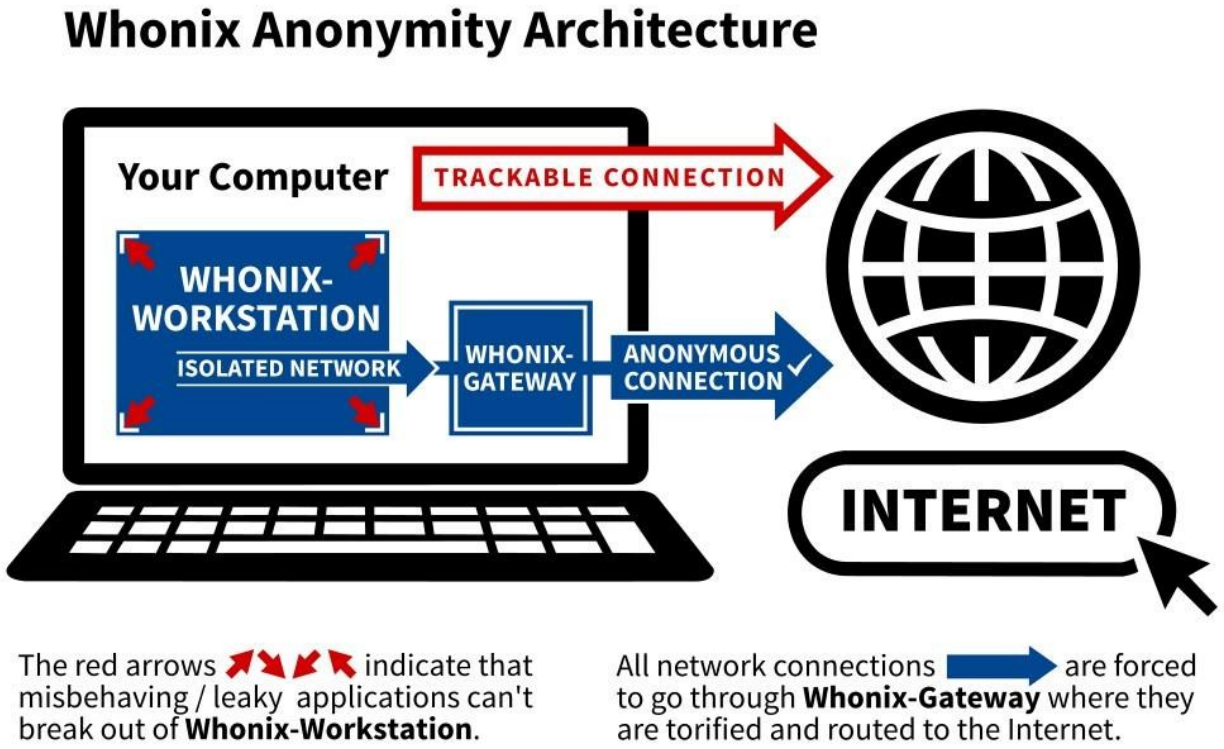
Les "environnements" spécialisés (logiciel libre – Kicksecure/Debian GNU/Linux)

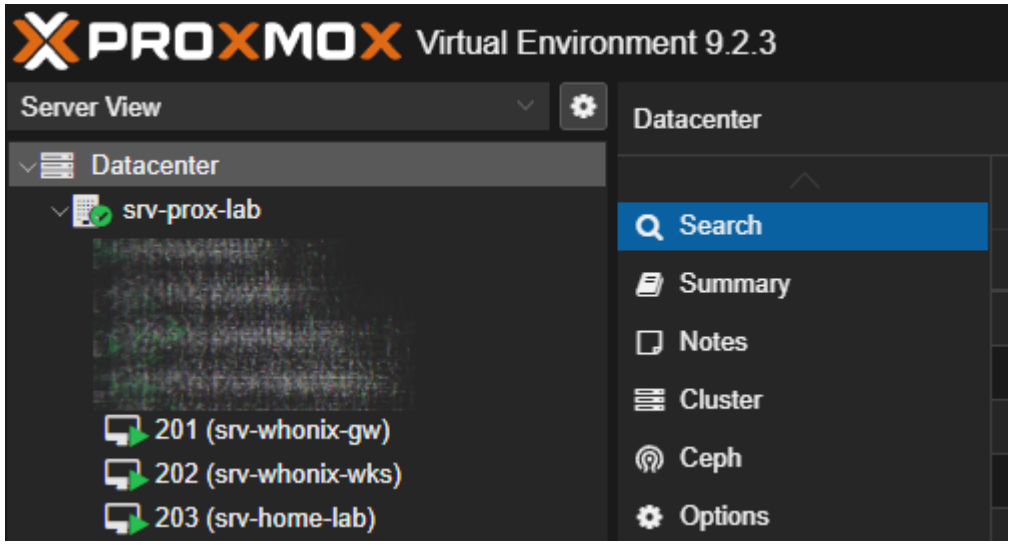
- Sécurisé par défaut
  - Whonix est un système d'exploitation anonyme qui fonctionne comme une application et redirige tout le trafic Internet via le réseau d'anonymat Tor.
  - Il offre une protection de la vie privée et de l'anonymat en ligne et est disponible pour tous les principaux systèmes d'exploitation.

- En deux parties
  - Une machine « Gateway » et une machine « Workstation »

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

Démonstration – Live !





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

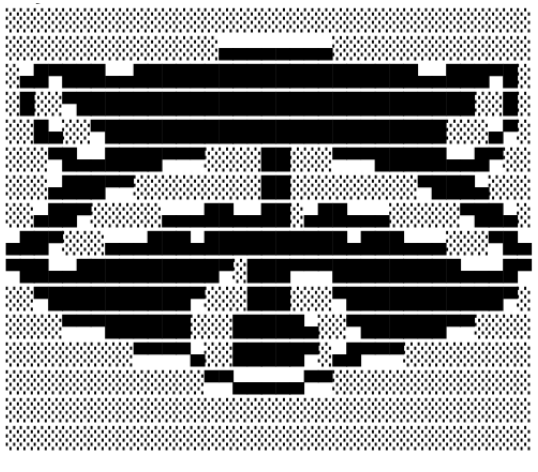
Fichier : *Dark Web – Démonstration Live.mp4*

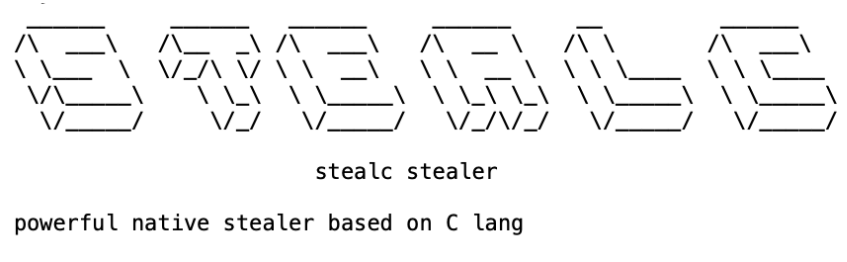
Comment surveiller le Dark Web

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.”





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
a8ZJtZ.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.

Source	Rusmarkethgwhfbn.onion
URL	http://rumarkstror5mvgzzodqizofkji3fna7lndfylmzeisj5tamqnwnr4ad.onion/logs#2662a7
Status	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-eu1.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	***mot clé surveillé***
Target	https://one.com.url (URL colmplète)
User	***identifiant en clair***
Password	***mot de passe en clair***
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	***nom de la session en clair***
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 - JF1E2Z
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	Local'Emploi localemploi.fr	Commercial	France	0xSec
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**

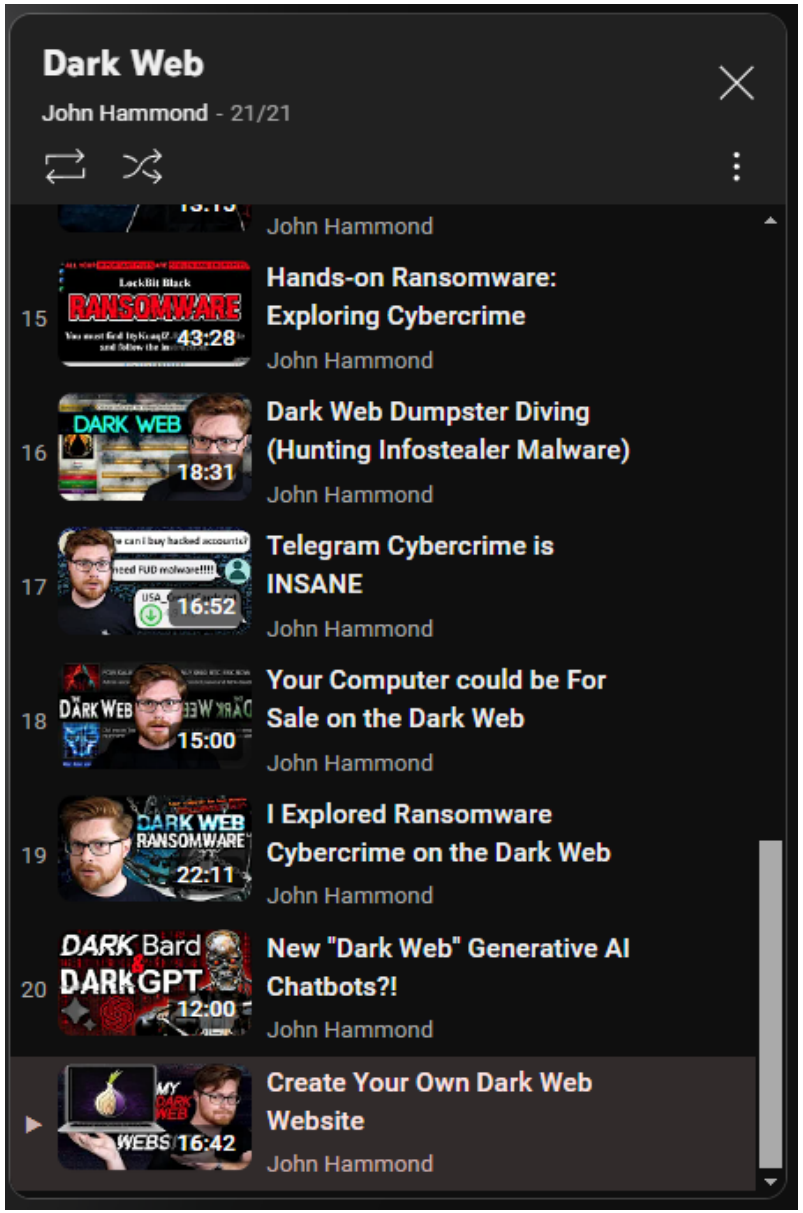
Bonus - Le Dark Web

John Hammond (YouTube en anglais)

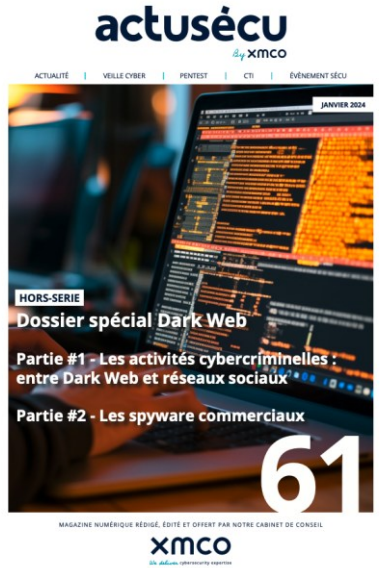
- **Une série de 21 vidéo documentaires « éducatives » sur le Dark Web réalisées un professionnel de la Cyber**

- *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)

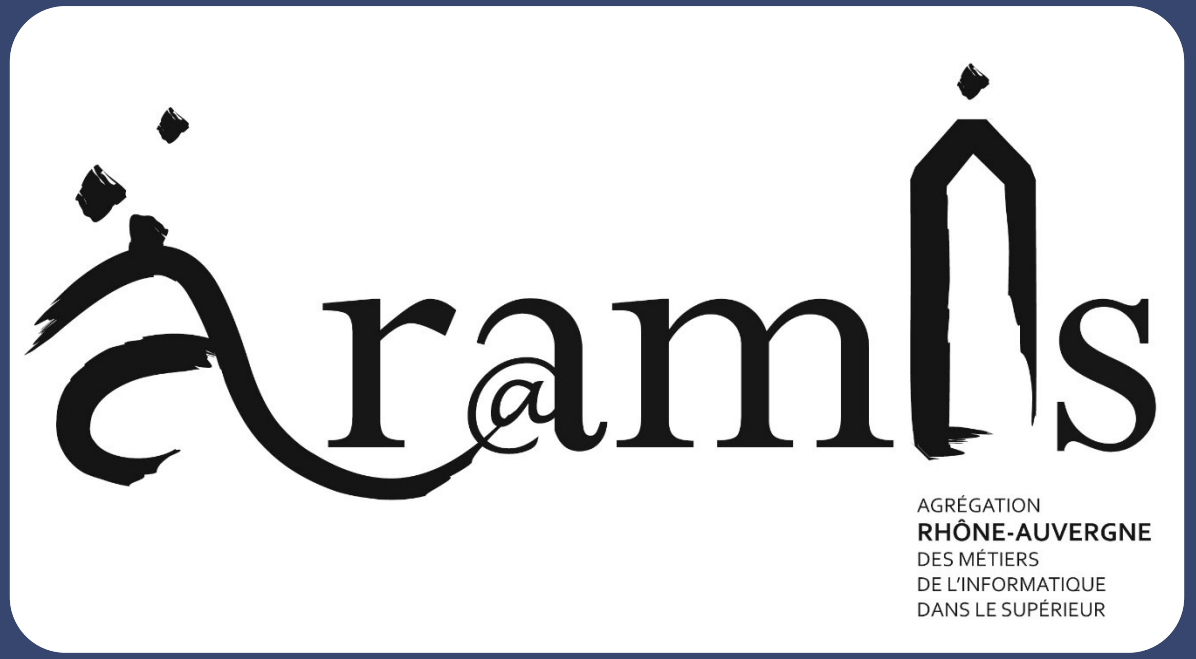
- **ActuSécu #52 (Nov. 2019) - Dossier spécial Dark Web en 2 parties**
  - Partie #1 : Anonymat et TOR
  - Partie #2 : Démantèlement des forums

  https://www.xmco.fr/wp-content/uploads/2021/11/52.XMCO-ActuSecu-52-Dossier_Darkweb-min.pdf

- **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


CLUSIR
Auvergne-Rhône-Alpes


AGRÉGATION
RHÔNE-AUVERGNE
DES MÉTIERS
DE L'INFORMATIQUE
DANS LE SUPÉRIEUR