Le Dark Web, au-delà des idées reçues

Fonctionnement, usages et comparaisons avec l'internet traditionnel

Jean-François AUDENARD

orange™

Expertise Security

Une présentation créée par
Jean-François AUDENARD - DSEC
Pierre DENOUEL – INNOV/IT-S

FR - v1r0 du 15 décembre 2025

Security Expertise

Reconnaître et sécuriser les talents de demain

Répondre aux questions et défis de nos sponsors

Transmettre et renforcer nos compétences

Valoriser l'expertise en interne et en externe

Nos missions et raison d'être

Avertissement

Cette présentation sur le réseau Tor et le Dark Web a une finalité purement pédagogique.

Les contenus, exemples et démonstrations visent la compréhension des risques et bonnes pratiques, et ne sont pas des guides d'action.

Toute utilisation de ces informations à des fins contraires à la loi, aux règlements, aux politiques de l'entreprise ou à l'éthique est strictement proscrite.

Ni Orange ni le présentateur ne cautionnent ni n'assument de responsabilité pour de tels usages. Vous êtes tenu de respecter le cadre légal en vigueur dans votre juridiction.

Clear, Deep & Dark

Clear Net

Le web comme vous le connaissez

Contenus indexés

Contenus non-indexés

Deep Net

Sites et informations accessibles mais dont l'accès est contrôlé

Dark Net

Des réseaux chiffrés recherchant discrétion et un haut niveau d'anonymat

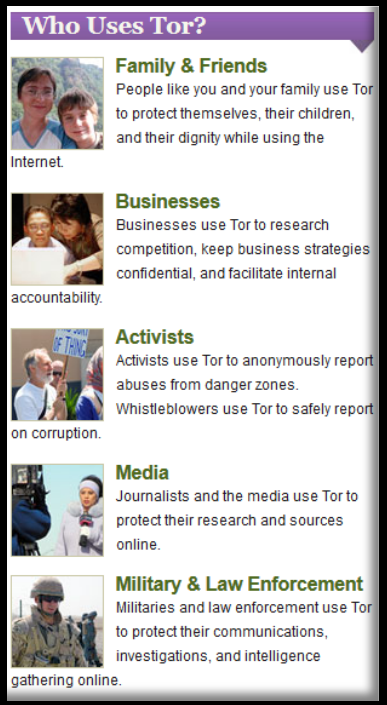
HYPHANET

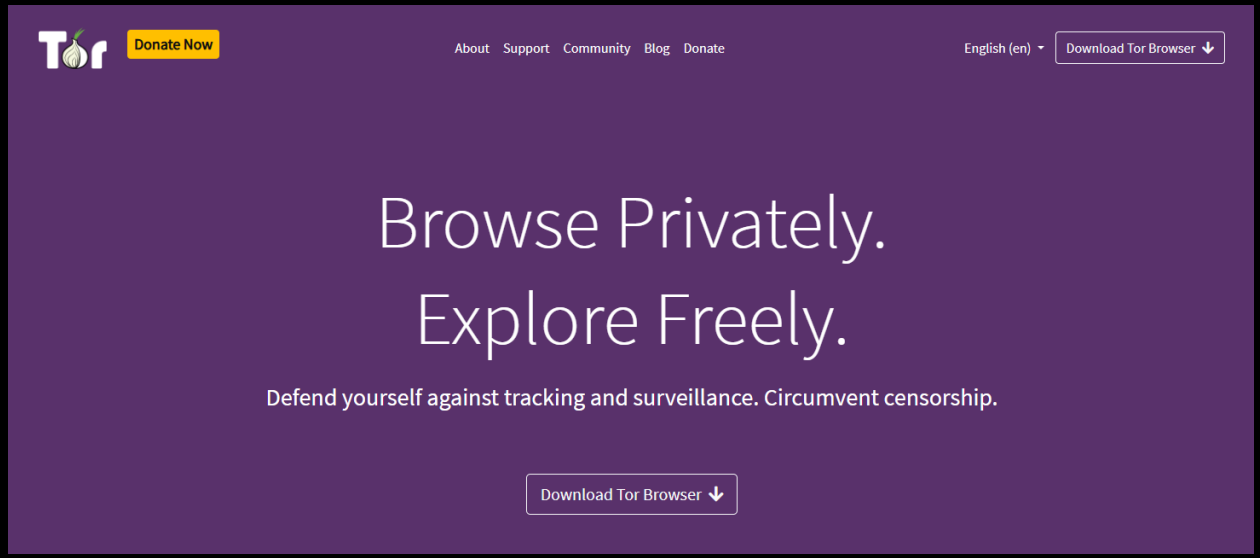
I2P

Tor

Le “Tor Project”

https://torproject.org





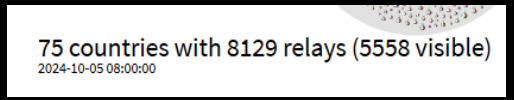
Créé par l’US Naval Research dans les années 1995

Un projet OpenSource

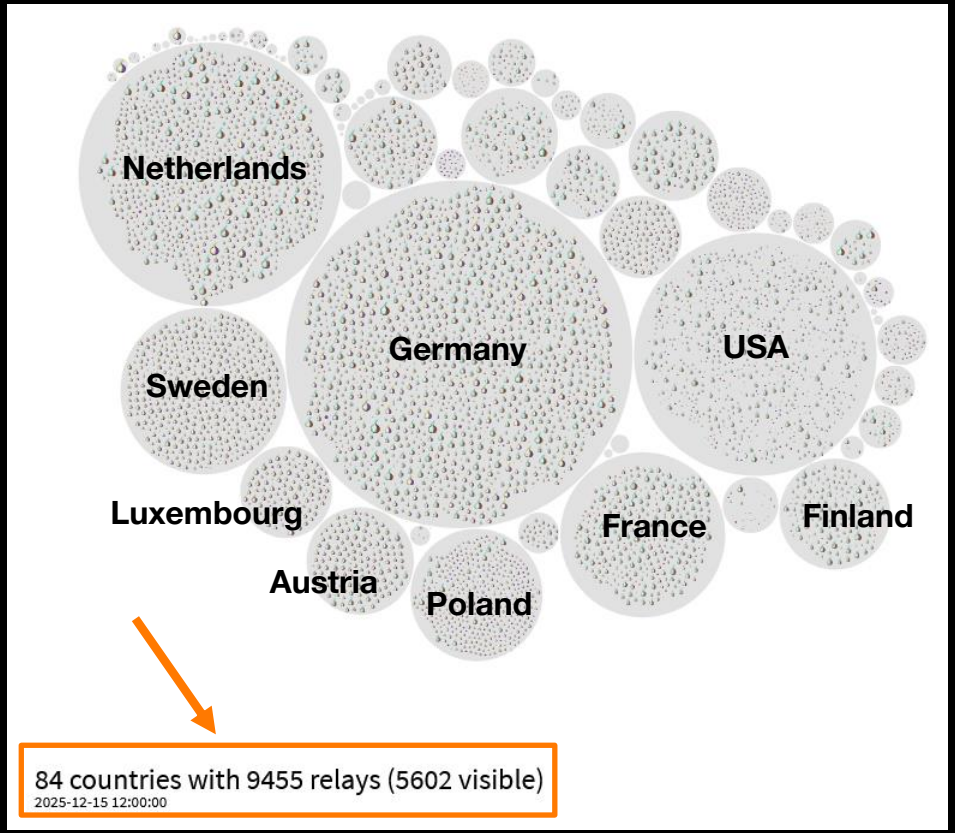
Géographie du réseau Tor

https://metrics.torproject.org/

Un réseau dont les serveurs sont majoritairement hébergés sur le territoire Européen

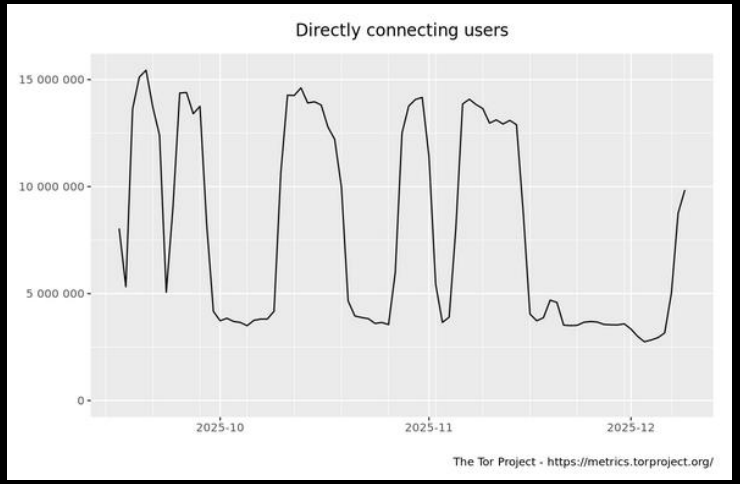


Données en date du 5 octobre 2024

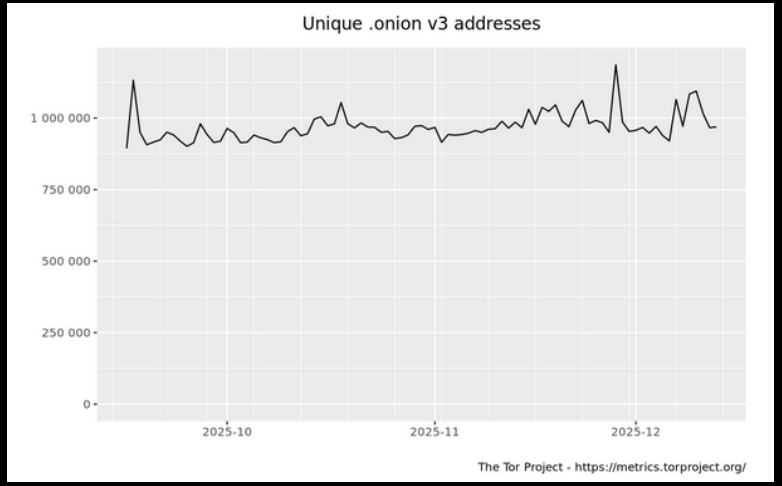


Données en date du 15 décembre 2025

Nombre d’utilisateurs et de sites cachés



Approximativement 8 millions de personnes se connectent quotidiennement au réseau Tor



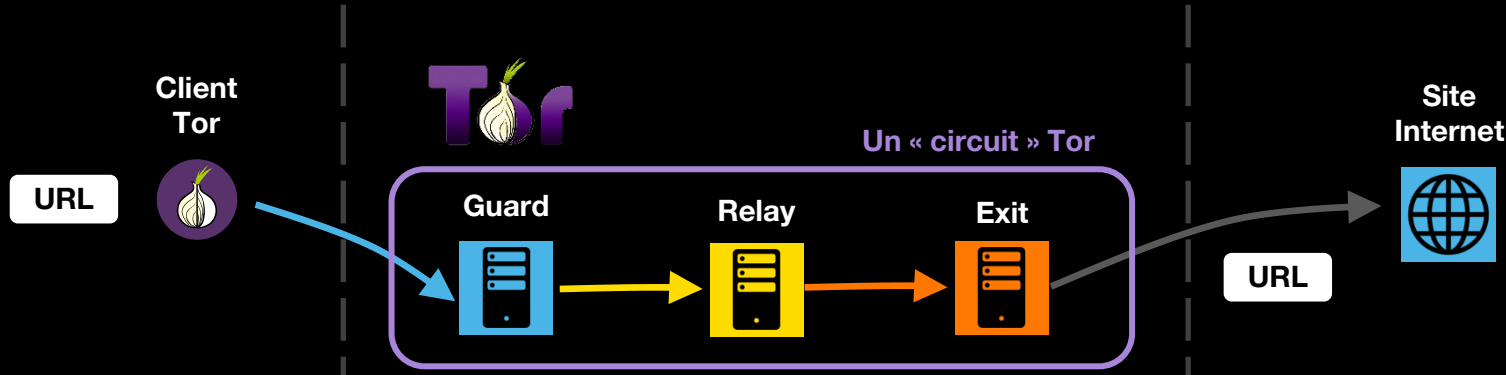
Plus de 800.000 sites « cachés » en « .onion » présents au sein du réseau Tor

Un site « caché » possède une URL se terminant en « .onion », il ne peut être facilement localisé mais est accessible via son URL complète

https://metrics.torproject.org/

Données sur la période du 16 septembre au 15 décembre 2025

Consultation d'un site Internet via Tor



La requête est chiffrée 3 fois de suite avec 3 clés différentes puis envoyée au Guard

3 clés de chiffrement différentes

A chaque étape, le serveur enlève une couche de chiffrement et fait suivre au suivant

Le Guard connait l'adresse IP du Client. Il ne sait rien du serveur Exit ni de l'URL

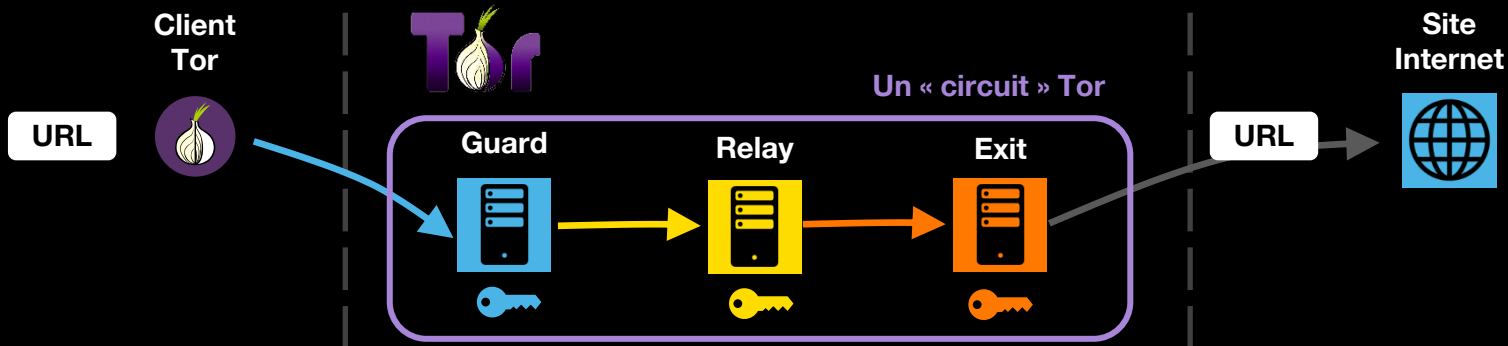
Le Relay connait l'adresse IP du Guard et de celle de Exit. Il ne sait rien de l'adresse IP du Client ni de l'URL

Le Exit connait l'adresse IP de Relay et l'URL. Il ne sait rien de l'adresse IP du Guard, ni de l'adresse IP du Client

Ici, la requête est en clair et la connexion est établie par le serveur Exit

Les « Bridges » sont des « Guards » non référencés/listés. Ils sont utilisés pour contourner la censure du réseau Tor

Consultation d'un site Internet via Tor



3 couches de chiffrement avec 3 clés différentes

Le Guard connait l'adresse IP du Client

Le Relay connait l'adresse IP du Guard et de celle de Exit

Le Exit connait l'adresse IP de Relay et l'URL

A chaque étape, une couche de chiffrement est enlevée

3 couches

2 couches

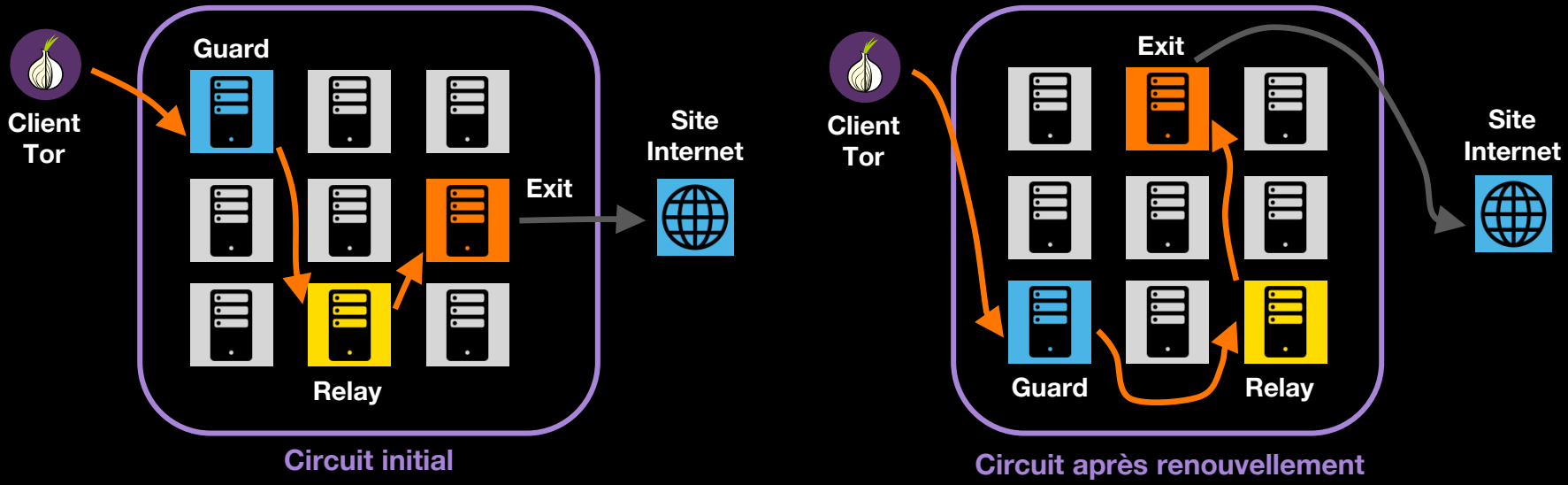
1 couche

On retrouve ici l'analogie avec un « oignon et ses multiples couches », d'où l'expression le « routage en oignon » !

Tor – Principes de fonctionnement

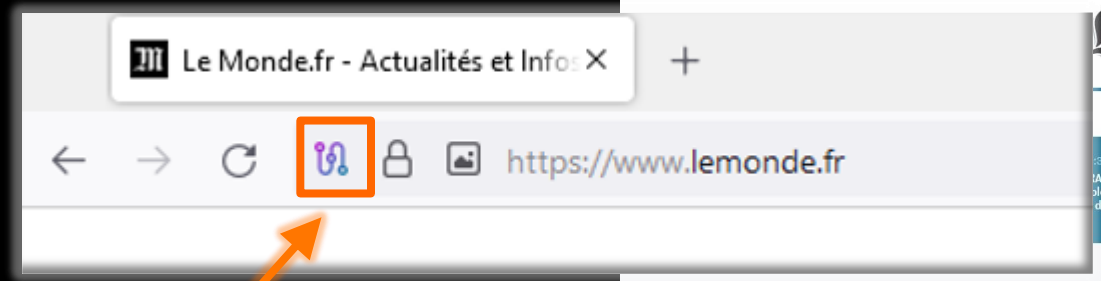
Lors de connexions successives, le circuit Tor peut emprunter des chemins différents

Des serveurs complètement différents sont utilisés

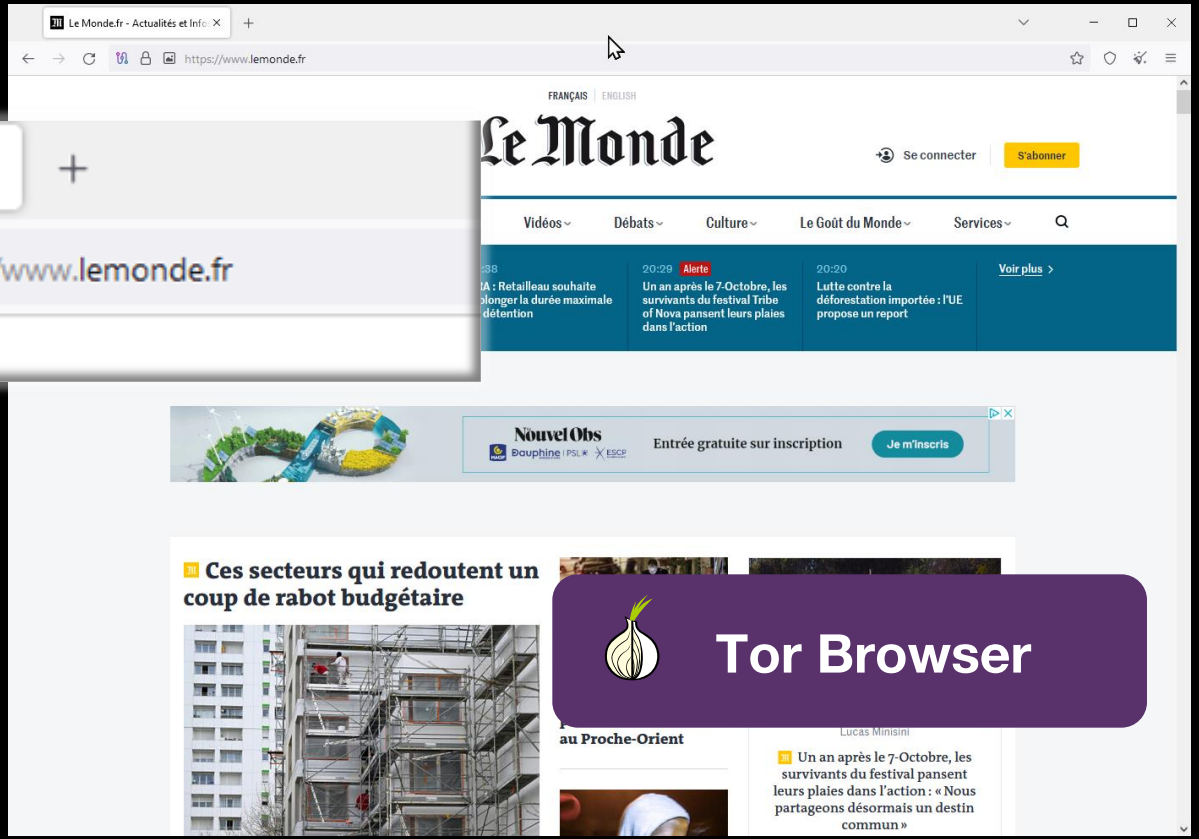


Pour un circuit Tor, il est aussi possible d'utiliser plus de 3 serveurs, d'écarter des serveurs dans des pays précis ou d'indiquer le pays du nœud de sortie (Exit)

Accès à un site web Internet via le réseau Tor

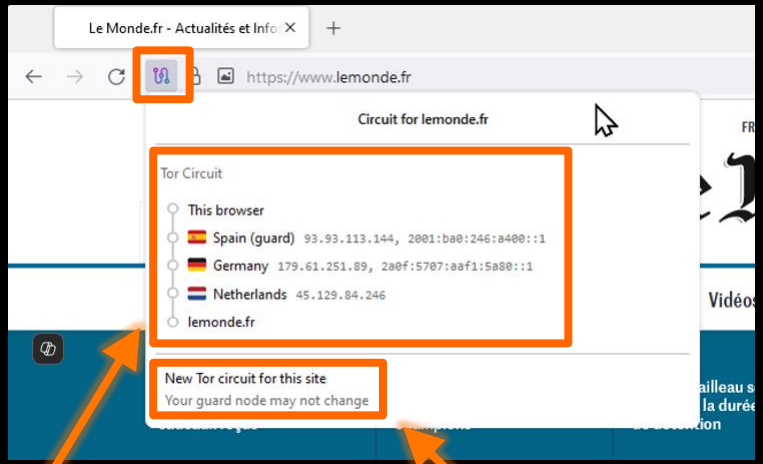


Icône du Tor Browser permettant d'accéder à des informations sur les nœuds du réseau Tor utilisés

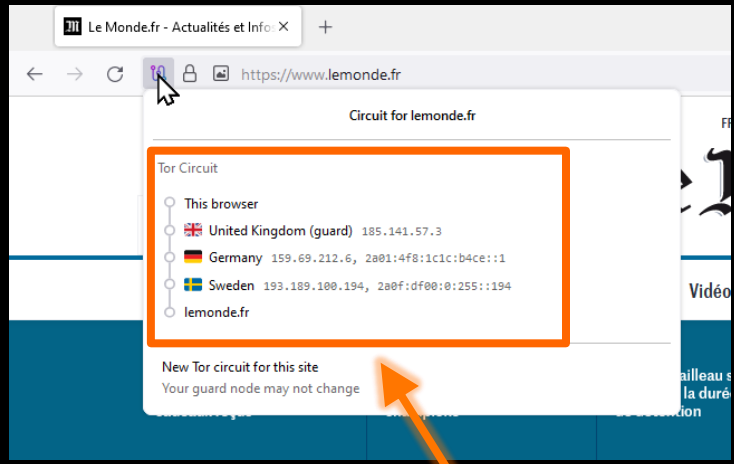


Renouvellement du « Circuit » Tor

Circuit actuel



Nouveau circuit

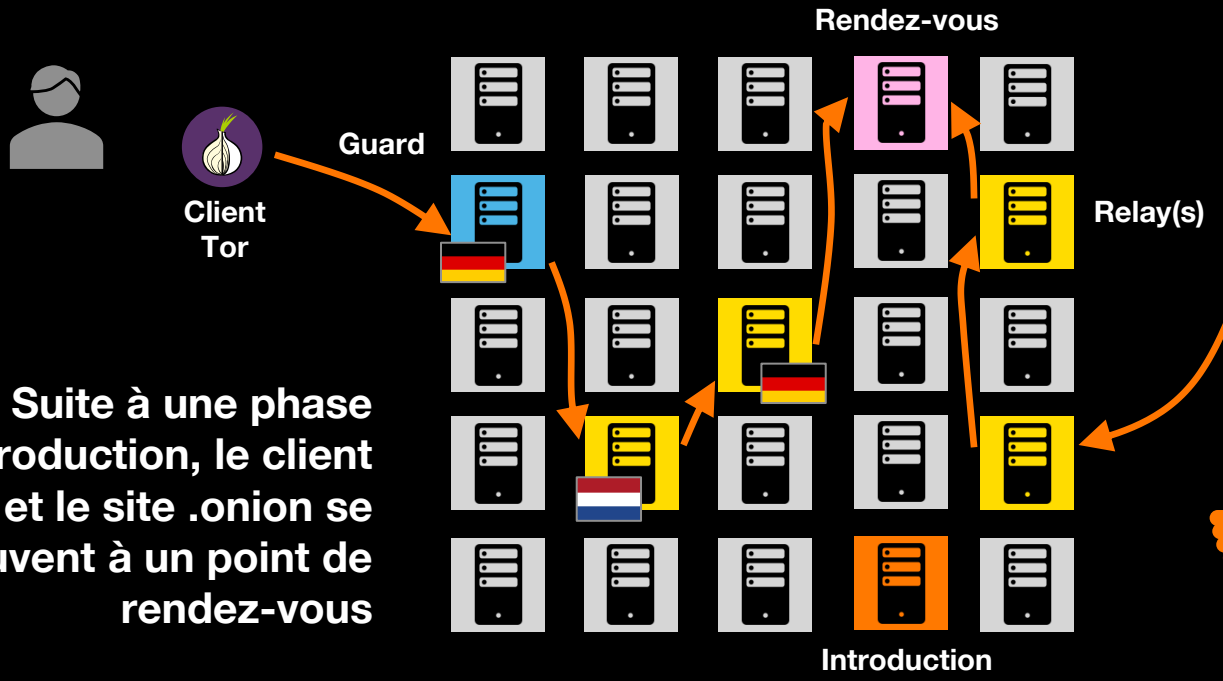


Liste des 3 serveurs Tor utilisés pour se connecter au site

1 On clique pour demander le renouvellement du « circuit » Tor

Un nouveau « circuit » Tor a remplacé celui précedemment utilisé

Tor – les sites cachés en « .onion »



Suite à une phase d'introduction, le client et le site .onion se retrouvent à un point de rendez-vous

Le client et le site caché ne peuvent s'identifier mutuellement

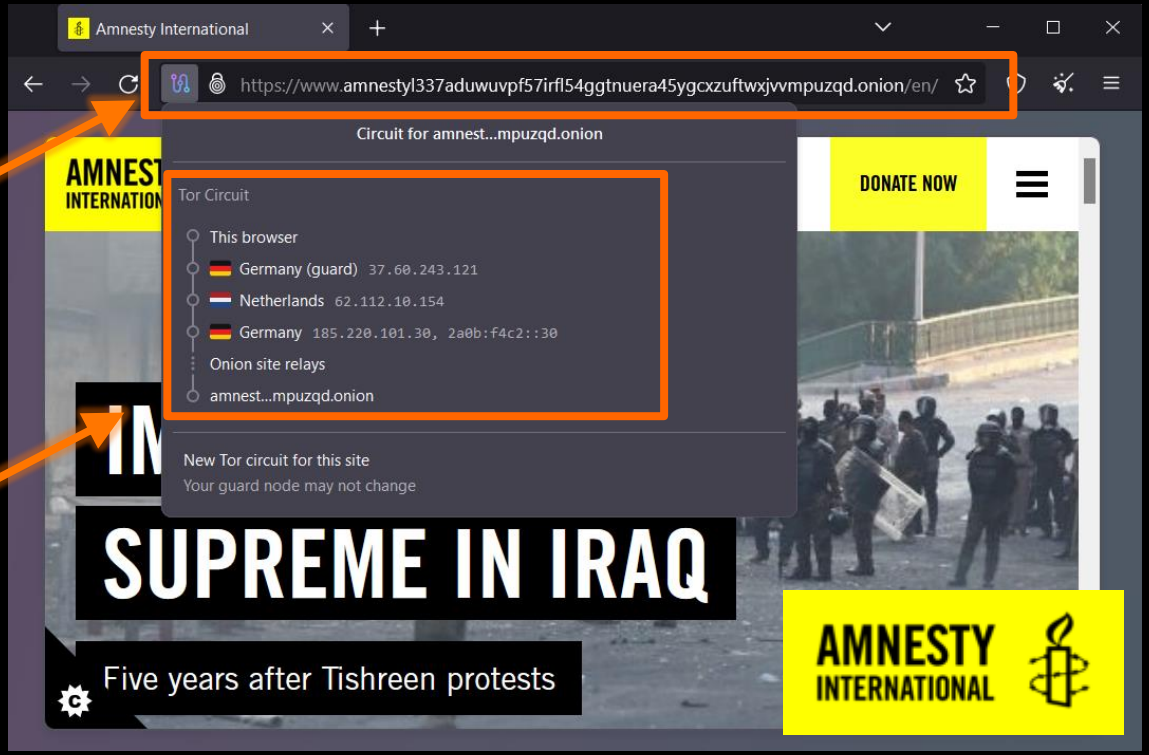
https://www.amnestyl337aduwuvpf57irfl54ggtnuera45ygcxzuftwxjvvmpuzqd.onion/

Adresse URL en « .onion » du site d'Amnesty International

Connexion à un site caché

Adresse URL du site web en « .onion » (site caché sur Tor)

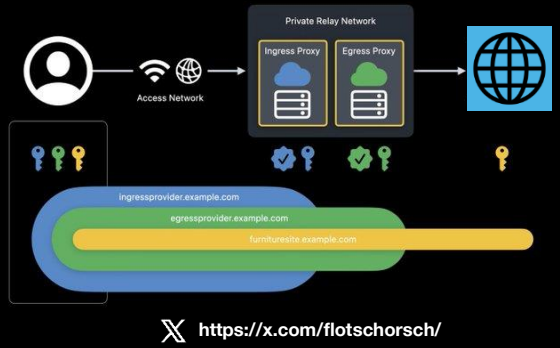
Circuit anonyme utilisé



Via Tor, il est possible de consulter anonymement des sites censurés ou interdits par des régimes ou gouvernements répressifs, ici ce site est « caché » au sein du réseau (adresse en .onion)

Faisons quelques comparaisons

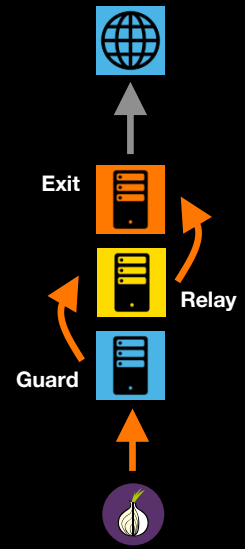
Apple Private Relay



https://x.com/flotschorsch/

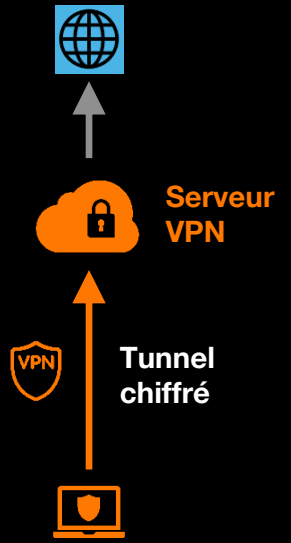
Avec Apple Private Relay, on retrouve un principe de routage en oignon mais sans le coté anonymat et la décentralisation du réseau Tor (service centralisé)

Tor Network



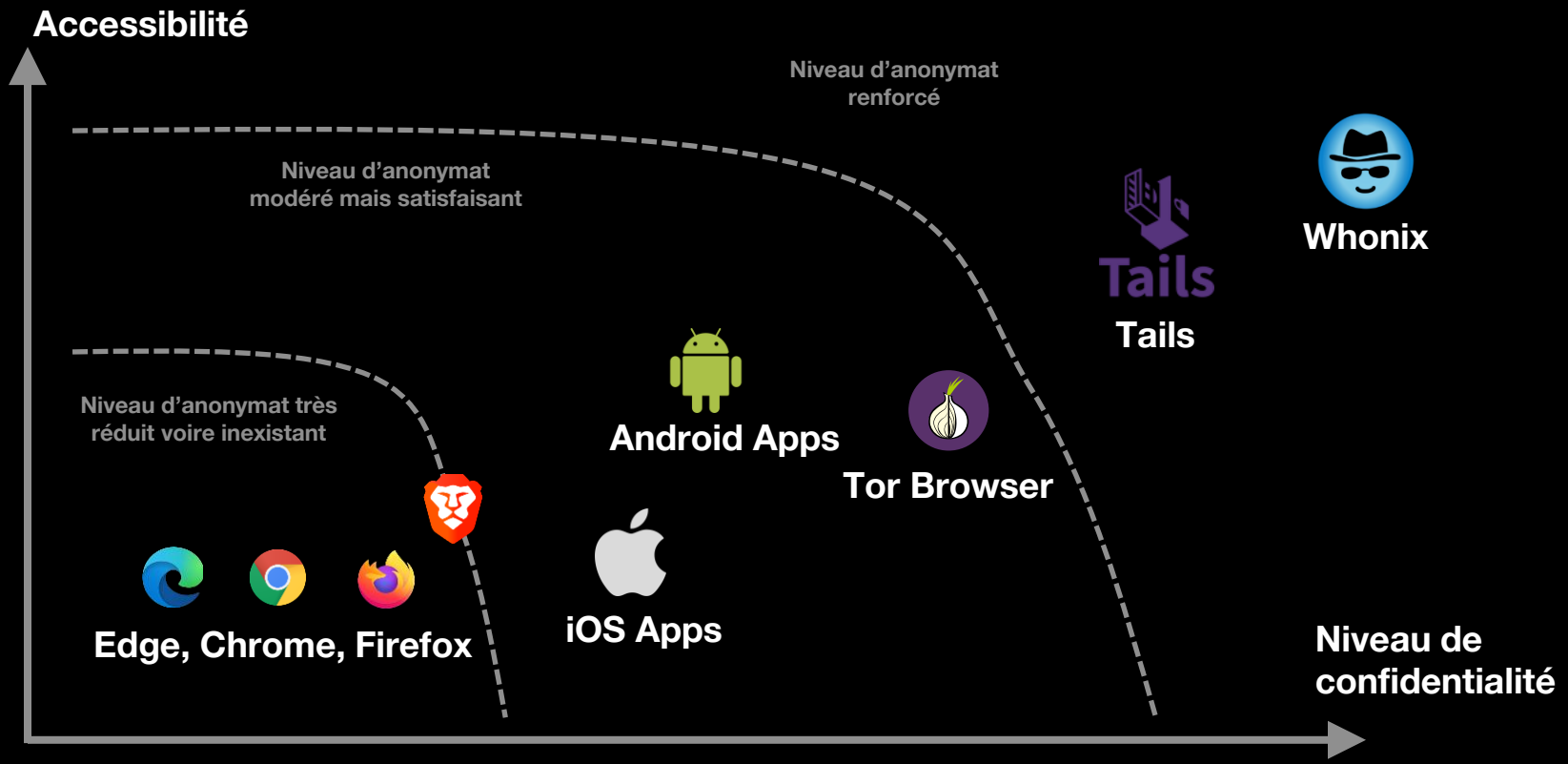
Le serveur web ne verra que l'adresse IP du nœud « Exit ». La possibilité de changer de parcours (ou « circuit ») permet de brouiller les pistes

Service de VPN



Le serveur VPN de sortie a une vision complète des sites accédés, l'adresse IP du client reste masquée mais connue du service de VPN

Se connecter au réseau Tor



Se connecter à Tor depuis un smartphone

iOS

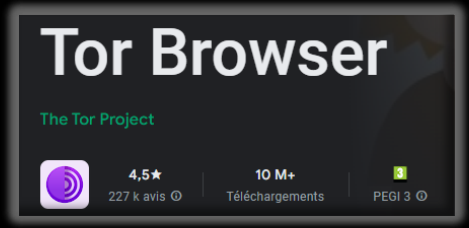
Un navigateur conçu pour un haut niveau d'anonymat et s'intégrant avec Orbot

+

Une application pour disposer d'un accès à Tor sous la forme d'une intégration de type VPN

Toujours privilégier les applications officielles et éviter les applications tierces

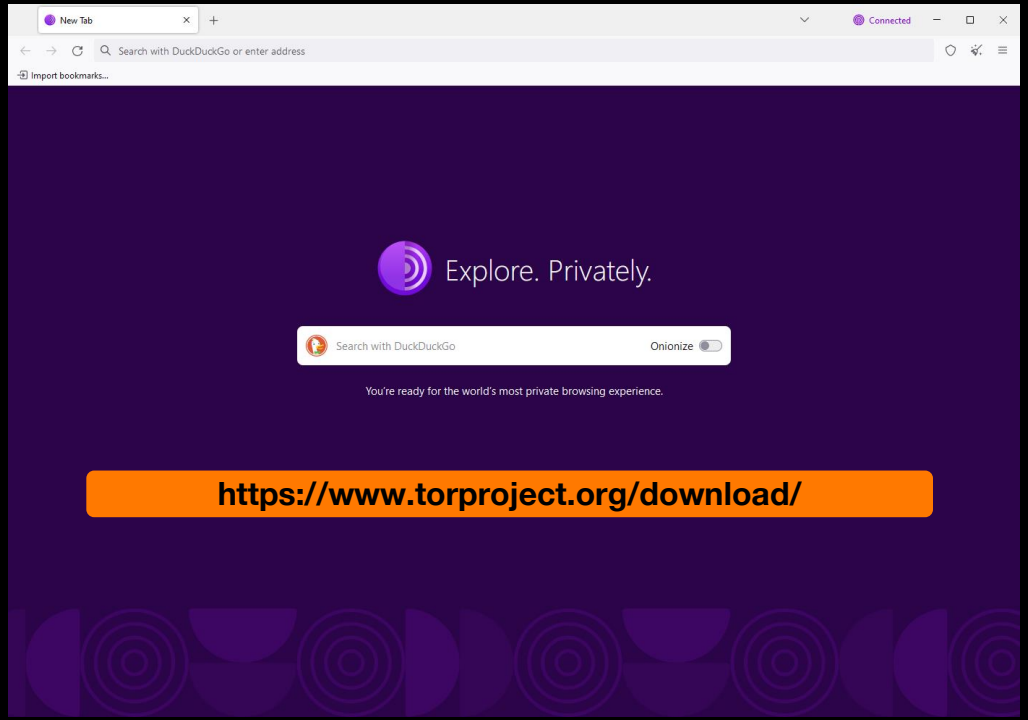
Android



+

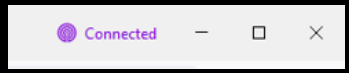
Exclusivement sur vos mobiles personnels !

Tor Browser



Un navigateur basé sur Firefox

Disponible sous Microsoft Windows, Apple MacOS, GNU/Linux



Connexion au réseau Tor transparente/automatique

Accès à des sites Internet via le réseau Tor

Accès à des sites cachés Tor (URL en .onion)

Important de n'installer aucune extension ni de ne changer aucun paramètre

TAILS - Conçu pour l’anonymat sur Tor

Un système d’exploitation spécifiquement conçu pour aller sur Tor

Lancement depuis une clé USB

Tout en RAM sans trace sur le disque

Des logiciels préinstallés et préconfigurés

Un système identique aux autres systèmes Tails

https://tails.net

Surfer sur Tor ce n’est pas tout confort

Surfer sur Tor est lent en raison du passage par plusieurs nœuds

Les adresses « .onion » se partagent entre initiés et peu sur les moteurs de recherche

De faux sites, des escrocs mais aussi des sites opérés parfois par les autorités

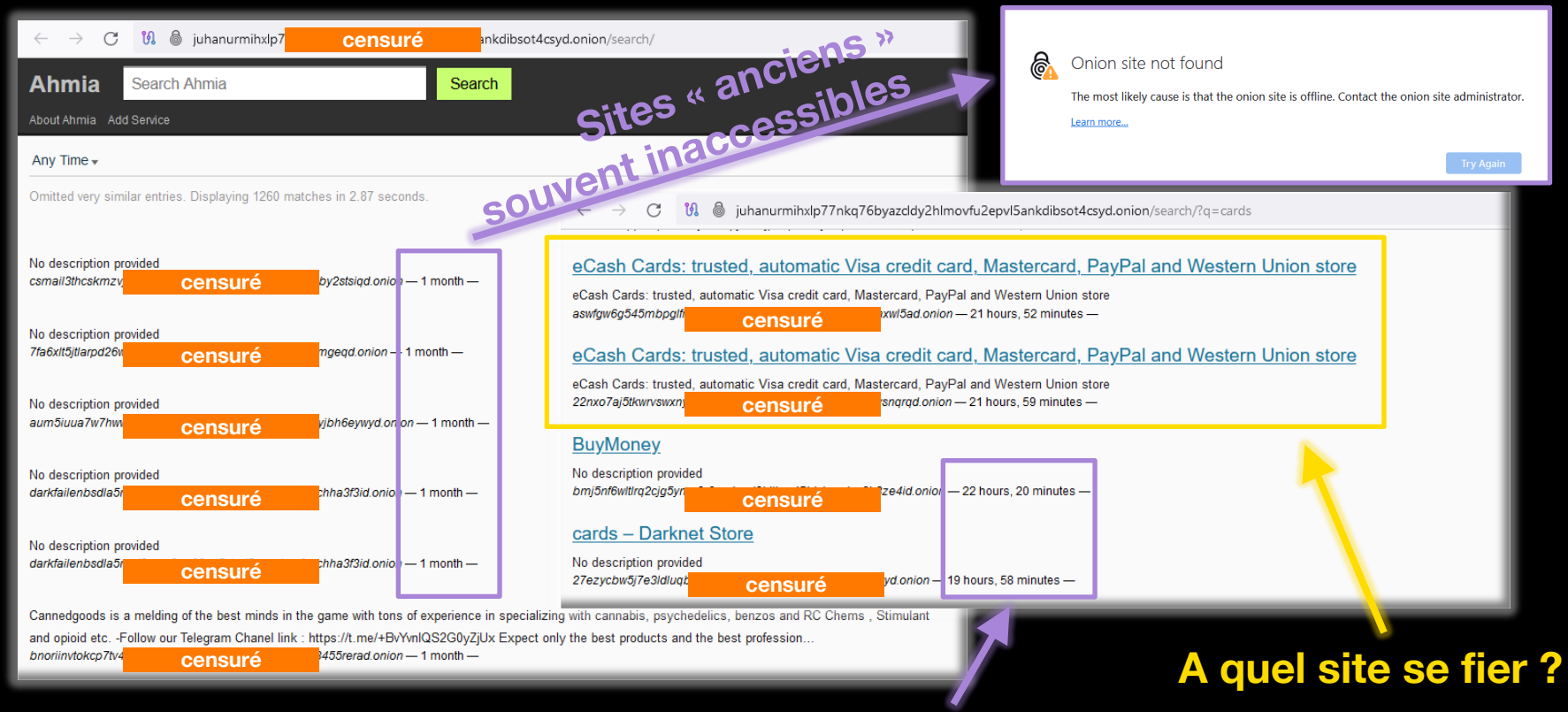
Des sites Internet bloquent les accès depuis Tor

Des sites dont la durée de vie est parfois très courte

Un monde opaque, dangereux et très souvent illégal

Autant de contraintes qu’accepteront uniquement des personnes ayant de réels besoins de contourner la censure, se de protéger de gouvernements oppressifs mais aussi évidemment des personnes impliquées dans des activités criminelles ou illégales

Ahmia, un moteur de recherche du Dark Web



Sites récents donc plus de chances qu'ils soient accessibles

Usages – Les deux visages du Dark Web

Anonymat

Défense des droits de l'homme

Lutte contre la repression et la censure

Accès à l'information

Protection de la vie privée

Anonymat

Echapper aux forces de l'ordre

Préparer et/ou commettre des actes criminels ou délictueux

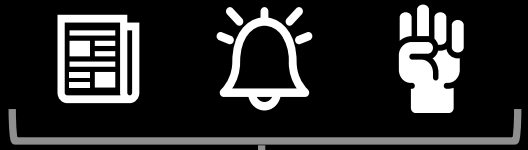
Commettre du harcèlement

Vendre ou acheter des produits ou services illicites

Qui peut rechercher de l’anonymat en ligne ?

Consommateurs, vendeurs de produits ou services illégaux

Délinquants, criminels, cybercriminels



Activistes, journalistes, lanceurs d’alertes

Dissidents, défenseurs des droits de l’homme

Investigations d’experts en sécurité informatique

Services de police ou de renseignement

Personnes souhaitant préserver leur vie privée

Moi, vous, un collègue, un proche, un voisin

SILENT COURIER - UK Secret Intelligence Service

GOV·UK

Press release

New dark web portal launched to recruit spies to support UK security

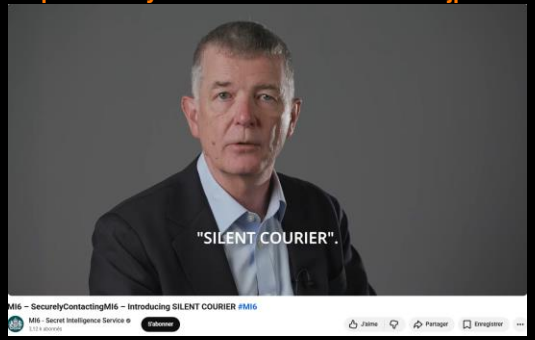
Outgoing Chief of MI6, Sir Richard Moore, announces new platform - Silent Courier - will make it easier for MI6 to recruit agents online

From: Foreign, Commonwealth & Development Of The Rt Hon Yvette Cooper MP

Published 19 September 2025

https://bit.ly/4oQLPff

https://www.youtube.com/watch?v=FLneejpWtC0



CNN World Sign In

WORLD › EUROPE · 2 MIN READ

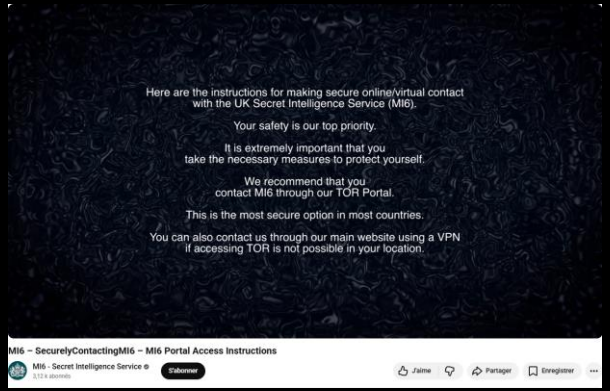
Silent Courier: UK intelligence service MI6 launches dark web portal to recruit foreign spies

UPDATED SEP 19, 2025

By Nick Paton Walsh

https://bit.ly/48VgbXM

https://www.youtube.com/watch?v=OYB129pGq0k



mi6govukbfxe5pzxqw3otzd2t4nhi7v6x4dljwba3jmsczozcolx2vqd.onion

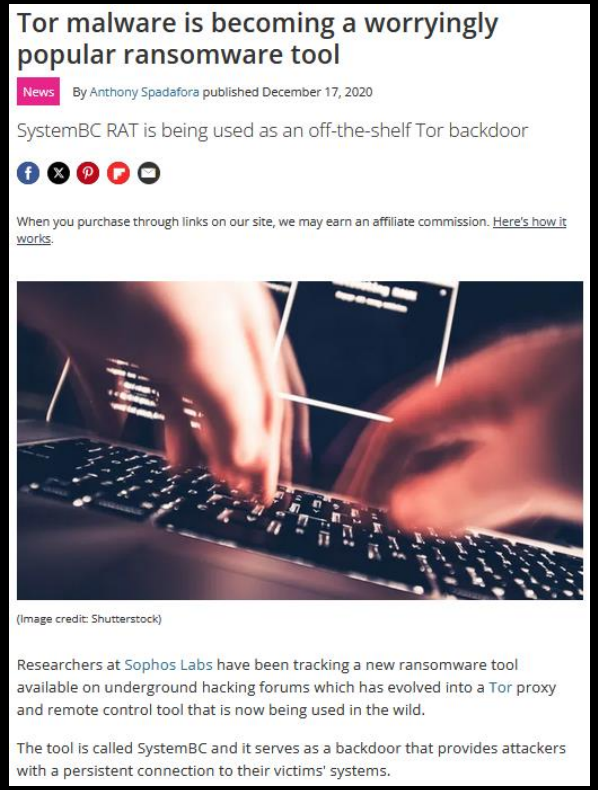
Souvent l’accès à Tor est bloqué depuis les réseaux d’entreprises

Non, ce n’est pas pour restreindre les libertés des salariés à accéder à l’information

Les connexions au réseau Tor sont traitées de la même manière que les services VPNs

Malware et cybercriminels peuvent utiliser Tor ou des VPNs pour mener des attaques

De même, l’accès depuis le réseau Tor à certains sites internet peut être bloqué pour limiter les tentatives d’attaques



Tor malware is becoming a worryingly popular ransomware tool

News By Anthony Spadafora published December 17, 2020

SystemBC RAT is being used as an off-the-shelf Tor backdoor

When you purchase through links on our site, we may earn an affiliate commission. Here's how it works.

(Image credit: Shutterstock)

Researchers at Sophos Labs have been tracking a new ransomware tool available on underground hacking forums which has evolved into a Tor proxy and remote control tool that is now being used in the wild.

The tool is called SystemBC and it serves as a backdoor that provides attackers with a persistent connection to their victims' systems.

http://bit.ly/48GBLAw

Darknet Markets - commerces illégaux

Drogues
Médicaments

Données
bancaires

Malwares
Outils de hacking

Logiciels piratés
Code source volés

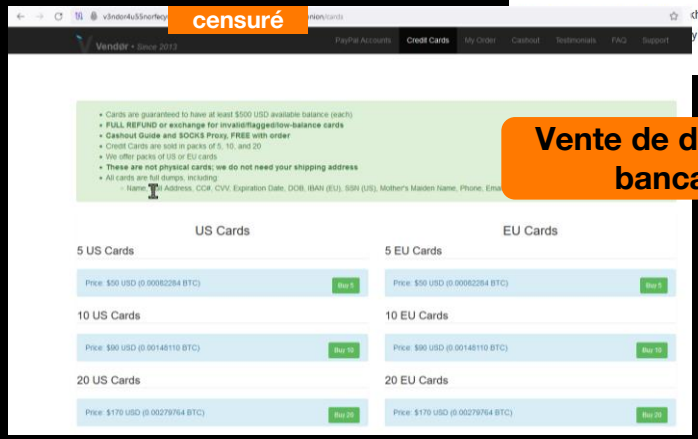
Armes
Munitions

Poisons
Produits radioactifs

Faux
documents

Traffic d'êtres humains
Pédopornographie

Etc..



Le quiz des réseaux et des enfants

1 **Nos enfants utilisent-ils le réseau Tor ?**

Non, il y a très peu de chances

2 **Nos enfants vont-ils sur d'autres réseaux du Dark Web ?**

I2P

Non, certainement pas

3 **Nos enfants vont-ils sur des réseaux sur lesquels sont proposés drogues, produits illicites ou dangereux ?**

Oui clairement ! Et vous connaissez ces réseaux

Drogues et produits illicites sont aussi présents sur ces grands réseaux sociaux

TikTok

.. car les vendeurs vont aux endroits où se trouvent leurs futurs clients

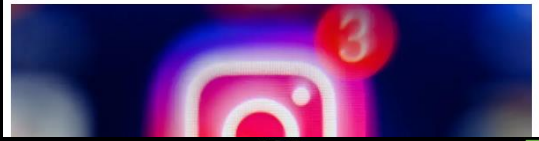
Uberisation des drogues

Instagram

BUSINESS INSIDER

Instagram's algorithm directly connects teens to 'drug dealers selling everything from opioids to party drugs,' researchers say

Connor Perrett Dec 7, 2021, 9:58 PM UTC+1 Share Save



404 SIGN IN SUBSCRIBE

Most of My Instagram Ads Are for Drugs, Stolen Credit Cards, Hacked Accounts, Counterfeit Money, and Weapons

The ads are a window into a blatantly illegal underground economy that Meta is not only failing to moderate, but is actively profiting from and injecting into users' feeds.

JASON KOEBLER · AUG 23, 2023 AT 9:10 AM

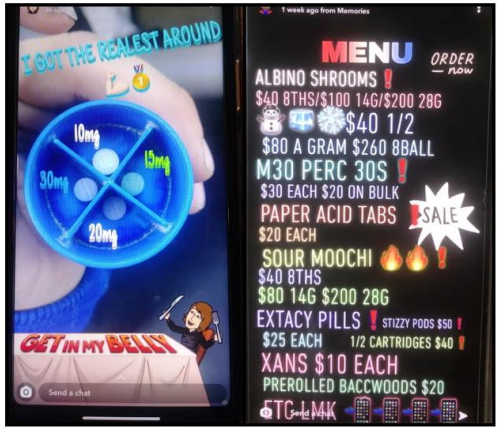
Snapchat

Here's how drug dealers use Snapchat and Instagram to reach kids

By Jacqueline Matter | Published February 1, 2023 10:01pm EST | Opioid Epidemic | FOX 5 DC

Their kids died after buying drugs on Snapchat. Now the parents are suing

Suit claims app features like disappearing messages and geolocating users make kids easy targets for dealers

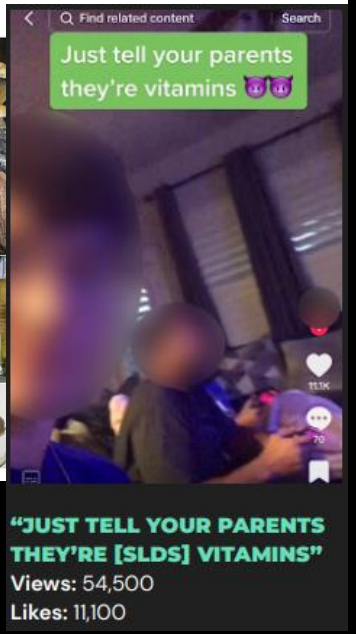


Tiktok

BUSINESS INSIDER

TikTok drug sellers are using nose and snowflake emoji and slang to get around search blocks and peddle cocaine and mushrooms

Rosie Bradbury May 3, 2022, 1:12 PM UTC+2



Des réseaux sous surveillance

Tor n'est PAS invulnérable

Il existe de nombreuses attaques en dé-anonymisation

Encore récemment des preuves que l'anonymat ou la sécurité de Tor peuvent être déjoués par

- Les agences gouvernementales
- Les hackers

Pour protéger son anonymat sur Tor, une attention de tous les instants est requise, la technique ne fait pas tout

CONSUMER INSIGHTS BUSINESS INSIGHTS

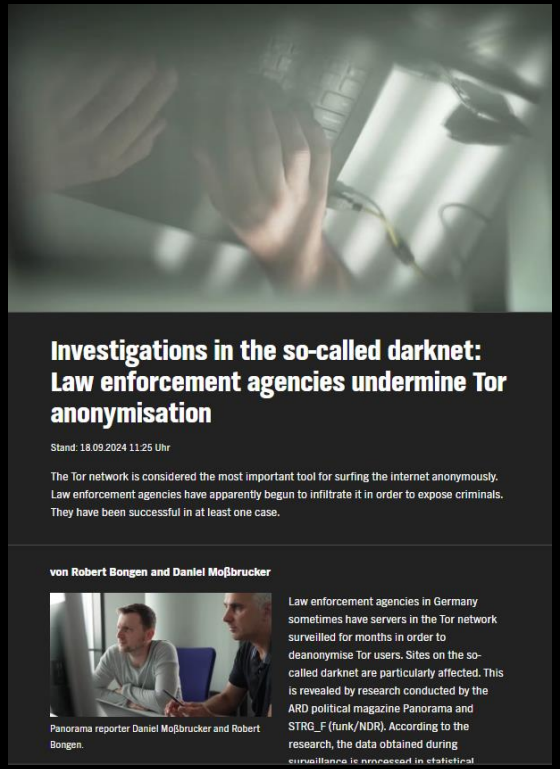
ACTUALITÉS DE LA CYBERSÉCURITÉ • 2 min de lecture •

Un acteur malveillant a compromis plus de 25% des relais du réseau Tor, selon une étude

Bogdan Botezatu
Mai 18, 2021

Promo Un seul produit pour protéger tous vos appareils, sans les ralentir
Essai gratuit de 30 jours

Des cybercriminels ont pris le contrôle d'un quart de tous les relais du réseau Tor pour lancer des attaques de type man-in-the-middle (attaque de l'homme du milieu), cibler des adresses Bitcoin et bien plus encore.



Investigations in the so-called darknet: Law enforcement agencies undermine Tor anonymisation

Stand: 18.09.2024 11:25 Uhr

The Tor network is considered the most important tool for surfing the internet anonymously. Law enforcement agencies have apparently begun to infiltrate it in order to expose criminals. They have been successful in at least one case.

von Robert Bongen and Daniel Moßbrucker

Panorama reporter Daniel Moßbrucker and Robert Bongen.

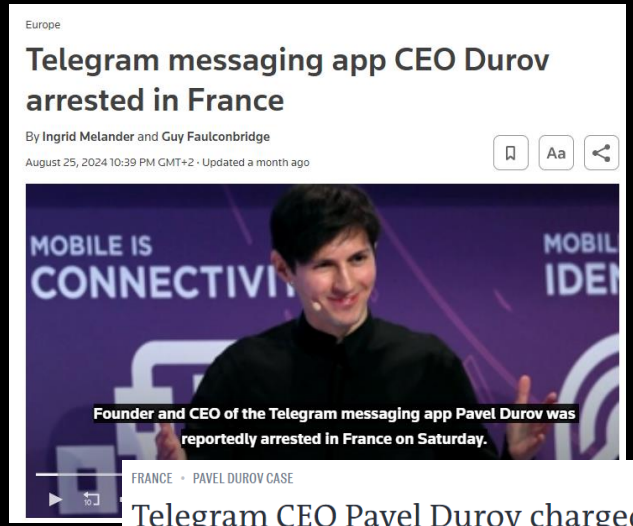
Law enforcement agencies in Germany sometimes have servers in the Tor network surveilled for months in order to deanonymise Tor users. Sites on the so-called darknet are particularly affected. This is revealed by research conducted by the ARD political magazine Panorama and STRG_F (funk/NDR). According to the research, the data obtained during surveillance is processed in statistical

Telegram

Un service utilisé mensuellement par plus de 950 millions de personnes

Une société dont le siège est à Dubaï (Emirats Arabes Unis) et sous le contrôle principal de ses deux fondateurs, Pavel et Nikolai DUROV

Un service « libertarien » devenu au fil des années hors de contrôle et utilisé pour de nombreux usages dévoyés ou totalement illicites



Le 24 août 2024, Pavel DUROV, le PDG de Telegram a été arrêté par la police française

Telegram – Conditions d'utilisation

Terms of Service **(Extract)** **https://telegram.org/tos/eu**

By signing up for Telegram, you accept our Privacy Policy and agree not to:

- Use our service to send spam or scam users.
- Promote violence on publicly viewable Telegram channels, bots, etc.
- Post illegal pornographic content on publicly viewable Telegram channels, bots, etc.
- Engage in activities that are recognized as illegal in the majority of countries. This includes child abuse, selling or offering illegal goods and services (drugs, firearms, forged documents), etc.

For users accessing Telegram within the European Union, the User Guidance for the EU Digital Services Act constitutes an integral part of our Terms of Service.

À la suite de l'arrestation de Pavel DUROV, les conditions d'utilisation du service Telegram évoluent

Telegram – Privacy Policy

Privacy Policy **(extract)**

https://telegram.org/privacy/eu

24/08/2024
Arrestation de Pavel DUROV

23/09/2024
De multiples modifications sont de nouveau apportées

8.3. Law Enforcement Authorities

If Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities. So far, this has never happened. When it does, we will include it in a semiannual transparency report published at: https://t.me/transparency.

8.3. Law Enforcement Authorities

If Telegram receives a valid order from the relevant judicial authorities that confirms you're a suspect in a case involving criminal activities that violate the Telegram Terms of Service, we will perform a legal analysis of the request and may disclose your IP address and phone number to the relevant authorities. If any data is shared, we will include such occurrences in a quarterly transparency report published at: https://t.me/transparency.

Telegram partage désormais numéros de téléphone et adresses IP des « mauvais acteurs » avec les autorités

Telegram – Rapport de transparence

Sur le 3ième trimestre 2024, Telegram a communiqué aux autorités les numéros de téléphone et adresses IP de 632 utilisateurs

Nous verrons si Telegram devient ou non un réseau social comme les autres

Transparency report for the period 01.01.24–30.09.24

Fulfilled requests from France for IP address and/or phone number:
Q1 – 4
Q2 – 6
Q3 – 210
Total: 220

Affected users:
Q1 – 17
Q2 – 37
Q3 – 632
Total: 686

Sur le 3ième trimestre 2024, il y a une très nette augmentation du nombre de transferts de données par Telegram aux autorités

All requests are processed according to paragraph 8.3 of the Privacy Policy.

The increase in processed requests in Q3 was caused by the fact that more authorities from this country started using the DSA-mandated communication channels to request data from Telegram. For more information, see Telegram's User Guidance for the EU Digital Services Act.

Tout est une question d'usage

Des réseaux peut-être plus risqués qu'on ne le pense de prime abord

Des réseaux plutôt utilisés par des (cyber)-criminels pour du « gros » business

Le Dark Web, le réseau Tor et tous les réseaux ne sont pas des endroits de non droit : les autorités y sont clairement actives (ou agissent dans ce sens)

Tous ces réseaux ont des utilisations tout à fait légitimes, il conviendra donc de ne pas tomber dans le piège du « journalisme à sensations » et de chercher à comprendre leurs principes de fonctionnement et usages et de rester vigilant

Merci !

Une question ?

… une réponse !

orange™

Security
Expertise

Jean-François AUDENARD
Orange - Direction Sécurité Groupe & Référent Orange Expertise Security
Membre de l'ARCSI