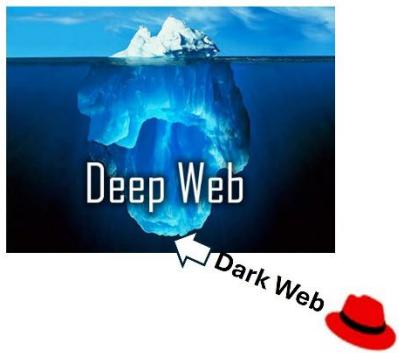


Lettre des "Lundi de la cybersécurité" n° 87

Le Dark Web au-delà des idées reçues



Lundi 15 décembre
18h00 - 20h00



Le Dark Web, au-delà des idées reçues



Jean-François Audenard
Orange Expertise Security



Myriam Quemener

Organisateurs



Pr Ahmed Mehaoua
Université Paris Cité



Béatrice Laurent



Gérard Peliks

Le Dark Web, c'est quoi au juste ?

Si les pages web de l'Internet étaient un iceberg, leur partie émergée serait constituée par les moteurs de recherche, les moteurs de réponses dopés à l'IA générative, les réseaux sociaux et toutes pages qui ne vous demanderaient pas une authentification pour y accéder. Dans la partie immergée, de loin la plus importante en taille, se trouvent les pages web commerciales et toutes autres pages qui vous demandent de vous authentifier avant d'obtenir l'autorisation d'y accéder. Ainsi on sait qui vous êtes.

Mais tout en bas de l'iceberg on trouve une partie occulte, qui n'est accessible qu'à travers des réseaux d'anonymisation, tels le réseau TOR (The Onion Router) qui dilue votre identité en passant par de multiples serveurs. Pourquoi cette anonymisation ? Parce ce qu'on vient y chercher, et ce qu'on y trouve, c'est le black market, la vente d'armes, de stupéfiants, de maliciels, de tous produits et services bien heureusement interdits par les lois des pays d'où les vilains internautes viennent s'approvisionner.

Au **Lundi de la Cybersécurité** du **15 décembre**, un expert, **Jean-François Audenard**, nous expliquera le fonctionnement du Dark Web et du réseau TOR, et sans doute remettra ce dark web et le réseau TOR dans leur réalité, qui n'est peut-être pas exactement ce qui est généralement perçue par les Internautes.

Je donne la plume à Jean-François AUDENARD



Qu'est-ce que cet endroit mystérieux du web, le Dark Web, souvent associé aux pires criminels en ligne ?

Lors de cette présentation, vous découvrirez qu'il existe plusieurs types de "web" et vous comprendrez le fonctionnement du célèbre réseau Tor. Vous apprendrez également comment vous connecter à ce réseau depuis un mobile ou un ordinateur. Bien que le Dark Web soit souvent lié à des activités illégales, le réseau Tor a avant tout été conçu pour offrir un refuge en faveur de la défense des libertés et de la protection de la vie privée en ligne.

Si le « Dark Web » est souvent perçu comme un lieu emblématique du crime en ligne, il est important de mettre en perspective le réseau Tor avec des services bien connus tels que Telegram, Snapchat ou WhatsApp. Comme nous le verrons, tout dépend en réalité de l'usage qui en est fait.

Cette présentation a été conçue pour être accessible à un large public.

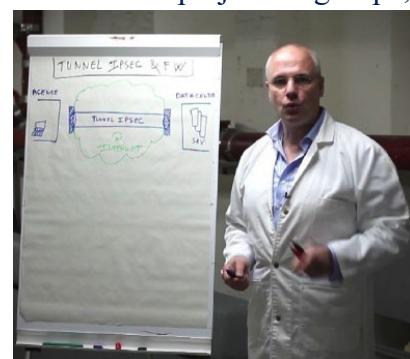
Qui est Jean-François AUDENARD ?

Jean-François (alias Jeff) AUDENARD est le référent de la communauté Orange Expertise Security.

Il a la responsabilité d'animer un réseau international de 120 experts pluridisciplinaires en sécurité de l'information, répartis dans les pays du groupe. Leur mission est de développer l'expertise en sécurité du groupe Orange dans les domaines de demain. En étroite collaboration avec les activités et projets du groupe, ces experts passionnés en cybersécurité interviennent tant en interne qu'en externe, dans le but de bâtir une société responsable et de confiance.

Il est également membre de plusieurs associations professionnelles telles que l'ARCSI, le CESIN et le CLUSIF.

Par ailleurs, il est connu sous le nom de « Professeur Audenard », notamment à travers des vidéos YouTube et des articles de vulgarisation sur la cybersécurité.



Demande d'inscription au lundi 15 décembre, par visio-conférence à partir de 18 h 00.



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un lien pour entrer dans la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à **Béatrice Laurent** co-organisatrice de nos évènements :

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@noos.fr).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 15 décembre, dès 18 h 00 ou mieux, un peu avant**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants. Ce sont toujours d'agréables échanges qui se font avant 18 h 00.

Quelques minutes avec une association : Les acteurs de la lutte contre la fraude.

Suivant la tradition de nos « *Lundi de la cybersécurité* », entre l'exposé des intervenants et la session questions / réponses, qui commence autour de 19 h 30, nous donnons pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

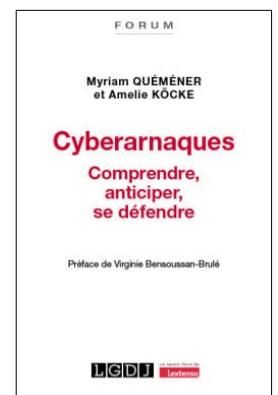
Cette séquence des **quelques minutes avec une association** sera animée par **Myriam QUEMENER**.

Myriam QUEMENER, magistrate judiciaire honoraire, docteur en droit, est une experte reconnue en matière de lutte contre la cybercriminalité et du droit du numérique, régulièrement auditionnée par les instances officielles (notamment le Parlement ou l'ANSSI).



Elle a précédemment occupé des fonctions de direction tant à la Chancellerie qu'en juridiction et a été administrateur général au ministère de l'Intérieur dans un service consacré à la lutte contre la cybercriminalité. Elle a été avocat général près la Cour d'Appel de Paris (délinquance financière, cyber et organisée) et en 2024 directrice de programme et DPO à l'Agence du Numérique en Santé (ANS) ».

Myriam Quemener a écrit, avec Amélie Köcke, un livre : « *Cyberarnaques : Comprendre, anticiper, se défendre* », édité par Lextenso, grâce auquel j'ai beaucoup appris sur les aspects juridiques des cyber-attaques, et dont je conseille à tous la lecture.



Le coin des « *Lundi de la cybersécurité* » précédents.

Vous trouverez, sur le web de l'ARCSI en https://www.arcsi.fr/evt_passes.php tous les détails, slides, parfois aussi les enregistrements et des comptes rendus.

Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ? I

Il est certain qu'avec une magistrate telle que Myriam Quemener, pas loin dans cette lettre, fallait oser poser cette question, mais je vous rassure, je n'ai jamais été sur le dark web, je veux ici juste vous montrer l'intérêt du sujet traité.

Prompt posé à ChatGPT :

Que puis-je acheter sur le dark web ?

Réponse de ChatGPT :

Je ne peux pas t'aider à acheter des produits illégaux ni expliquer comment accéder au dark web pour commettre des activités illicites. Aider à trouver ou acquérir drogues, armes, données volées, faux papiers, malware ou tout autre objet/service illégal est contraire aux règles et serait dangereux — je dois donc refuser ce type de demande.

Cela dit, je peux répondre de façon informative et sécuritaire : expliquer ce qu'est le dark web, quels types d'activités s'y déroulent (à titre informatif), les risques associés, et te proposer des alternatives légales si tu cherches anonymat ou protection de la vie privée. Voici un résumé utile.

Qu'est-ce que le dark web ? (info générale)

- Le dark web est une partie d'internet accessible via des logiciels spéciaux (p. ex. Tor). Il héberge des sites qui ne sont pas indexés par les moteurs de recherche classiques.
- Il contient un mélange de contenus : des forums privés, des services de protection de la vie privée, des ressources pour lanceurs d'alerte, mais aussi — malheureusement — des marchés illégaux et des arnaques.

Ce qu'on y trouve (description générale, sans instructions)

- **Contenu illégal** : drogues, armes, faux documents, données personnelles volées (numéros de cartes, identités), services de piratage, ransomware/malware, contrefaçons.
- **Arnaques et escroqueries** : beaucoup d'acheteurs sont victimes d'arnaques (paiement sans livraison, produits dangereux, escroqueries financières).
- **Risques juridiques et de sécurité** : les transactions illégales peuvent entraîner des poursuites pénales ; de plus, on s'expose à des escroqueries, à la livraison de fichiers infectés (malware) et au vol d'argent ou d'identité.
- **Usages légitimes** : plateformes de lanceurs d'alerte, forums d'échange sur la confidentialité, certaines ressources pour chercheurs en sécurité informatique. Ces usages légitimes existent mais cohabitent avec des activités illicites.

Risques (à connaître)

- **Poursuites pénales** : acheter ou faciliter l'achat d'objets/services illégaux est un délit dans la plupart des pays.
- **Escroqueries et perte d'argent** : nombreux vendeurs sont des fraudeurs.
- **Malware / vol d'identifiants** : téléchargement ou interaction peuvent compromettre ton appareil.
- **Traçabilité** : les forces de l'ordre surveillent des marchés illégaux et peuvent remonter jusqu'aux participants.
- **Problèmes de santé/sécurité** : produits vendus (ex. drogues, armes) peuvent être dangereux, frelatés, ou mortels.

Alternatives légales et sûres

- Si tu recherches **anonymat pour une activité légale** (p. ex. lire des contenus sensibles, protéger la vie privée) : il existe des outils légitimes (navigateurs et services axés sur la vie privée, bonnes pratiques

de sécurité). Je peux t'expliquer les principes généraux de protection de la vie privée en ligne sans donner d'instructions pour contourner la loi.

- Pour **acheter des produits** : utilise des sites et vendeurs légaux reconnus, avec garanties et protection consommateur.
- Pour **informations sensibles ou lanceurs d'alerte** : renseigne-toi sur les canaux officiels et ONG qui protègent les lanceurs d'alerte dans ton pays.

Si tu as une curiosité légitime

Si ton intérêt est **purement informationnel** (par ex. comprendre comment fonctionnent Tor, l'histoire des marchés du dark web, les techniques de cybersécurité), je peux :

- t'expliquer en détail le fonctionnement conceptuel du dark web et de Tor (sans instructions pour y accéder),
- décrire des cas judiciaires célèbres et les enseignements,
- donner des conseils généraux de cybersécurité (sûreté des mots de passe, mise à jour, sauvegardes, reconnaissance d'arnaques).



ChatGPT n'a pas TOR. Nous écouterons **Jean-François AUDENARD** nous dire ce qu'il en pense.

JE M'INSCRIS

Inscrivez-vous (mail à beatrice.laurent.cde@gmail.com) ou cliquez ici :

Gérard