

Démystifions les Darknets

Genma

28 janvier 2014



This work is licensed under the *Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License*.

Les Darknets

On entend de plus en plus parler des Darknets, des endroits sombres de l'Internet, là où se cachent les pirates, hackers, et autres pédo-nazis.

On a de plus en plus d'articles de journalistes qui lancent TOR et qui pondent ensuite un article à sensation pour faire de l'audience.

Mais qu'en est-il vraiment de ces fameux Darknets.

Internet

Ne pas confondre web et Internet

Internet est un réseau de réseaux ; ce n'est pas un seul réseau mais tous un ensemble de réseaux et sous réseaux reliés entre eux.

Sur ces réseaux, il y a le réseau que l'on connaît, le "Web".

Mais dans ces mêmes tuyaux circulent les mails, des flux vidéos, tout un tas d'autres choses et d'autres flux.

Les Darknets

Tentons de définir un Darknet

Un darknet est un réseau privé virtuel dont les utilisateurs sont considérés comme des personnes de confiance.

La plupart du temps, ces réseaux sont de petite taille, souvent avec moins de dix utilisateurs chacun.

Un darknet peut être créé par n'importe quel type de personne et pour n'importe quel objectif, mais la technique est le plus souvent utilisée spécifiquement pour créer des réseaux de partage de fichiers.

Le Deepweb

Le Deepweb

Correspond à tout le web qui est non indexé par Google.

Tout le web non visible

Un document soumis à mot de passe pour consultation, un espace soumis à mot de passe...

Tout ce qui se consulte via un navigateur et qu'a pas de lien dans Google est du Deepweb.

Il n'y a pas un mais DES darknets

Les Darknets

Un darknet est un réseau privé

Un Darknet, ce peut très bien être une LanParty privée mais sur Internet.

Ou un réseau d'Entreprise auquel on se connecte via un VPN.

Ou les réseaux de P2P privé.

On peut assimiler ces réseaux dans le réseau à des Darknet, d'une certaine façon.

Les Darknets

Interconnexion de hackerspace

DN42, ChaosVPN (CCC), Anonet... De plus en plus de hackerspaces interconnectent leurs réseaux via des tunnels VPN (ou des liaisons radio longue distance dans certains cas), ce qui permet :

- De crypter tous les échanges de données entre les hackerspaces participants
- De contourner censure / filtrage / throttling et autres débilités du genre
- De mutualiser / redonder les services d'infrastructure (DNS, IRC, backups...)
- De faciliter la mise à disposition d'informations et de services entre les hackerspaces reliés
- Routage vers les darknets IP (DN42, ChaosVPN, AgoraLink, Anonet, ...)

Tor

TOR

Acronyme de The Onion Router, littéralement : « le routeur oignon » et est un réseau mondial décentralisé de routeurs, organisés en couches, appelés nœuds de l'oignon, dont la tâche est de transmettre de manière anonyme des flux TCP.

C'est ainsi que tout échange Internet basé sur TCP peut être rendu anonyme en utilisant Tor.

Le site officiel : <https://www.torproject.org>

TOR - les services cachés

Tor permet aux clients et aux relais d'offrir des services cachés. Autrement dit, vous pouvez offrir un serveur web, un serveur SSH, etc, sans révéler votre adresse IP de ses utilisateurs.

Avec un moteur de recherche comme DuckDuckGo ou une page wikipedia, il possible de connaître certains de ces services.

Un wiki au sein de ces services cachés regroupant lui-même tout une série d'adresses en .onion.

Il faut donc utiliser un navigateur configuré pour utiliser le réseau Tor pour aller sur ces sites *underground*.

I2P - Invisible Internet Project

Réseau anonyme, offrant une simple couche réseau logicielle de type réseau overlay, que les applications peuvent employer pour envoyer de façon anonyme et sécurisée des informations entre elles. La communication est chiffrée de bout en bout.

On est donc là face à une sorte de VPN en Peer2Peer, chacun étant un relais possible pour les autres. Je n'ai pas encore testé ce réseau, ce sera l'occasion de rédiger différents articles quand ce sera fait.

I2P - les eepsites

Les Eepsites sont des sites qui sont hébergés de façon anonyme au sein du réseau I2P.

Exemple : - The wiki is also available via I2P tunnel :
`npkn2tsan5be7abni7dex7t65jevtifwj2u37uk3xuhvabb6yzwq.b32.i2p`

Un logiciel comme EepProxy peut localiser ces sites par le biais des couches d'identification cryptographiques stockées dans le fichier `hosts.txt` trouvé dans le répertoire du programme I2P.

Une connexion au réseau I2P est donc nécessaire pour accéder à ces eepsites.

Freenet

Freenet

Freenet est un réseau informatique anonyme et distribué construit sur l'Internet.

Il vise à permettre une liberté d'expression et d'information totale fondée sur la sécurité de l'anonymat, et permet donc à chacun de lire comme de publier du contenu.

Il offre la plupart des services actuels d'Internet (courriel, Web, etc.).

Le cypherspace

Le Cipherspace ou cypherspace est l'équivalent chiffré du cyberspace.

Merci de votre attention.
Place aux questions. Débattons...