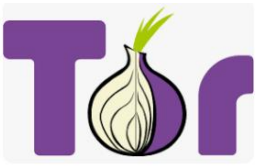
Le Dark Web et le réseau Tor : Accéder au Dark Web est un jeu d'enfant

I) Introduction : Les couches du Web

Internet est souvent représenté comme un iceberg. La surface visible, celle que nous utilisons quotidiennement (Google, Wikipedia, réseaux sociaux…), ne représente qu'une infime partie de l'ensemble des données accessibles en ligne.

II) Le réseau Tor : fonctionnement technique



2.1 Origine et histoire de Tor

Tor (The Onion Router) est un projet né dans les années 1990 au sein du laboratoire de recherche navale américain (US Naval Research Laboratory). L'objectif initial était de protéger les communications gouvernementales américaines. Le projet a été rendu public en 2002 et est depuis développé par la Tor Project, une organisation à but non lucrati

2.2 Le principe de routage en oignon (Onion Routing)

Le routage en oignon est le cœur de la technologie Tor. Son fonctionnement repose sur plusieurs étapes clés :

Étape 1 — Sélection des nœuds

Lorsqu'un utilisateur se connecte à Tor, le client Tor sélectionne aléatoirement trois nœuds (relais) parmi les milliers disponibles dans le réseau mondial : le nœud d'entrée (guard node), le nœud intermédiaire (middle relay) et le nœud de sortie (exit node).

Exemple :

Étape 2 — Chiffrement en couches

Les données sont chiffrées successivement avec la clé publique de chacun des trois nœuds, à l'image des couches d'un oignon. La dernière couche chiffrée est celle du nœud d'entrée, la première à être retirée.

Étape 3 — Transmission progressive

Le paquet chiffré voyage de nœud en nœud. Chaque relais ne retire qu'une seule couche de chiffrement, découvrant uniquement l'adresse du prochain relais. Aucun nœud ne connaît à la fois l'origine et la destination du message.

Étape 4 — Sortie du réseau

Le nœud de sortie déchiffre la dernière couche et transmet la requête au serveur de destination sur Internet. Si la connexion n'est pas chiffrée de bout en bout (HTTPS), le nœud de sortie peut lire le contenu en clair — ce qui constitue une vulnérabilité importante.

2.3 Les limites du chiffrement Tor

Bien que Tor offre un haut niveau d'anonymat, il ne garantit pas une protection totale. Voici les principales limites :

- Le nœud de sortie voit le trafic en clair si HTTPS n'est pas utilisé.
- Des attaques de corrélation temporelle (traffic analysis) peuvent potentiellement désanonymiser un utilisateur.
- Les métadonnées (taille des paquets, timing) peuvent être exploitées.
- Un comportement imprudent de l'utilisateur (connexion à un compte personnel, téléchargement de fichiers) peut révéler son identité.
- La vitesse de connexion est réduite en raison du multi-relayage.

III) Accéder au Dark Web : outils et méthodes

3.1 Le navigateur Tor (Tor Browser)

Le Tor Browser est la méthode la plus simple et la plus sûre pour accéder au réseau Tor. C'est une version modifiée de Firefox qui intègre automatiquement la configuration Tor, des plugins de protection de la vie privée (NoScript, HTTPS-Everywhere) et des paramètres de sécurité renforcés.

Téléchargement officiel : **https://www.torproject.org**

3.2 Les adresses .onion

Sur le Dark Web, les sites n'ont pas d'adresses IP classiques. Ils utilisent des adresses en **.onion**, générées cryptographiquement à partir d'une paire de clés publique/privée. Ces adresses sont longues et complexes (ex : z4yl3jppjnbrp2cw.onion) et ne sont pas résolues par les DNS classiques.

Les services .onion sont dits « services cachés » (hidden services) : le serveur hébergeant le site reste anonyme, tout comme l'utilisateur qui y accède.

3.3 Autres réseaux anonymes

Tor n'est pas le seul réseau de ce type. D'autres solutions existent :

- I2P (Invisible Internet Project) : réseau overlay orienté communication interne, plus décentralisé que Tor.
- Freenet : réseau de partage de fichiers décentralisé et censuré-résistant.
- ZeroNet : réseau de sites web décentralisés utilisant la blockchain Bitcoin.
- Ricochet Refresh : messagerie instantanée anonyme reposant sur Tor.

IV) Usages du Dark Web

4.1 Usages légitimes

Contrairement à l'image véhiculée par les médias, une large partie des utilisateurs du Dark Web y accèdent pour des raisons parfaitement légales et éthiques :

- Journalistes et lanceurs d'alerte : SecureDrop, plateforme utilisée par de nombreux médias (New York Times, Le Monde…) pour recevoir des documents confidentiels de sources anonymes.
- Militants et dissidents politiques : dans des pays comme la Chine, l'Iran ou la Russie, Tor permet de contourner la censure et d'accéder librement à l'information.
- Forces de l'ordre : les agences gouvernementales utilisent elles-mêmes Tor pour des opérations d'infiltration et de surveillance.
- Chercheurs en cybersécurité : étude des menaces, des malwares et des marchés illicites.
- Citoyens soucieux de leur vie privée : protection contre la surveillance commerciale et gouvernementale.

4.2 Usages illicites

Le Dark Web est également le théâtre d'activités criminelles variées. Les plus connues sont :

- Marchés noirs de drogues, d'armes et de données volées (ex-Silk Road, AlphaBay, Hansa).
- Vente de données personnelles issues de fuites (numéros de cartes bancaires, identifiants).
- Distribution de contenus illicites (CSAM, ransomwares, malwares).
- Services de hacking à la demande (DDoS, phishing, intrusion).
- Blanchiment de cryptomonnaies via des mixeurs (tumblers).

4.3 Le cas des marchés darknet

Les marchés darknet (darknet markets) sont des plateformes de commerce en ligne accessibles uniquement via Tor. Ils fonctionnent généralement avec des cryptomonnaies (Bitcoin, Monero) et utilisent un système de notation et d'avis similaire à Amazon ou eBay.

Depuis la fermeture du Silk Road en 2013 par le FBI, des dizaines de marchés similaires ont émergé et disparu, souvent à la suite d'opérations policières internationales coordonnées (Opération Onymous, DisrupTor…).

V) Aspects juridiques et réglementaires

5.1 Le statut légal de Tor et du Dark Web

Dans la grande majorité des pays démocratiques, l'utilisation du navigateur Tor et l'accès au Dark Web ne sont pas illégaux en eux-mêmes. C'est l'usage qui en est fait qui peut être punissable. En France, en Europe et en Amérique du Nord, aucune loi n'interdit explicitement l'utilisation de Tor.

Cependant, certains pays autoritaires ont tenté de bloquer ou d'interdire Tor : Chine (via le Grand Firewall), Russie, Iran, Turquie…

5.2 Le cadre légal en France

En France, les activités suivantes sur le Dark Web sont passibles de poursuites pénales :

- Achat ou vente de produits stupéfiants (Code de la santé publique).
- Trafic d'armes et de données personnelles volées (Code pénal).
- Production, détention ou diffusion de contenus pédopornographiques (art. 227-23 CP).
- Participation à des organisations criminelles ou terroristes.
- Blanchiment de capitaux via des cryptomonnaies.

5.3 Les acteurs de la lutte contre la cybercriminalité

En France, plusieurs organismes sont chargés de lutter contre les menaces issues du Dark Web :

- OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication).
- ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).
- Europol et Interpol au niveau européen et international.

- FBI, DEA et HSI aux États-Unis, souvent en coopération internationale.

VI) Bonnes pratiques et sécurité

6.1 Recommandations si vous utilisez Tor

Si vous utilisez Tor à des fins légitimes (journalisme, recherche, protection de la vie privée), voici les bonnes pratiques à respecter :

- Téléchargez Tor Browser uniquement depuis le site officiel (torproject.org) et vérifiez la signature GPG.
- Ne modifiez pas la taille de la fenêtre du navigateur (fingerprinting).
- N'installez pas de plugins ou extensions supplémentaires.
- Ne vous connectez pas à des comptes personnels (Google, Facebook…) depuis Tor.
- Utilisez HTTPS pour tous les sites visités.
- Ne téléchargez pas de fichiers via Tor sans précautions (les ouvrir hors ligne uniquement).
- Combinez Tor avec un VPN de confiance (VPN before Tor) pour une protection accrue.

6.2 Les limites éthiques et pratiques

Il est essentiel de comprendre que l'anonymat offert par Tor n'est pas absolu. Des erreurs humaines, des failles logicielles ou des attaques sophistiquées peuvent compromettre l'identité d'un utilisateur. L'histoire a montré que de nombreux criminels opérant sur le Dark Web ont été arrêtés, souvent à cause de maladresses hors du réseau Tor plutôt que par des failles techniques.

VII) Exemples de sites sur le Dark Web

Contrairement aux sites web classiques dont les adresses se terminent par *.com*, *.net* ou *.fr*, les sites du Darknet utilisent l'extension .onion, propre au réseau Tor.
Les exemples de sites présentés ci-dessous le sont à titre strictement informatif, dans le seul but de vous expliquer ce qu'est le Darknet et ce que l'on peut y trouver. En aucun cas, ces informations ne constituent une incitation à consommer des substances illicites, ni à commettre des délits ou des crimes. L'auteur décline toute responsabilité quant à l'usage qui pourrait en être fait.
Rappel important : contrairement à une idée reçue très répandue, l'anonymat absolu n'existe pas sur Internet. Même sur le Darknet, des moyens techniques et légaux permettent d'identifier les utilisateurs.

http://jaz45aabn5vkemy4jkg4mi4syheisqn2wn2n4fsuitpccdackjwxplad.onion/

Introduction Points
OnionLinks jaz45aabn5vkemy4jkg4mi4syheisqn2wn2n4fsuitpccdackjwxplad.onion
The Hidden Wiki 5wvugn3zqfbianszhldcqz2u7ulj3xex6i3ha3c5znpgdcnqzn24nnid.onion
Another Hidden Wiki bj5hp4onm4tvpdb5rzf4zsbwoons67jnastvuxefe4s3v7kupjhgh6qd.onion
The Dark Web Pug qrtitjevs5nxq6jvrnrjyz5dasi3nbzx24mzmfxnuk2dnzhpphcmgoyd.onion
The Original Hidden Wiki zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion
Financial Services
AccMarket z7s2w5vruxbp2wzts3snxs24yggbtdcdj5kp2f6z5gimouyh3wiaf7id.onion
Cardshop f6wqhy6ii7metm45m4mg6yg76yytik5kxe6h7sestyvm6gnlcw3n4qad.onion
Dark Mixer cr32aykujaxqkfqyrjvt7lxovnadpgmghtb3y4g6jmx6oomr572kbuqd.onion
Mixabit Bitcoin Mixer 74ck36pbaxz7ra6n7v5pbpm5n2tsdaiy4f6p775qvjmowxged65n3cid.onion

VirginBitcoins 5kpq325ecpcncl4o2xksvaso5tuydwj2kuqmpgtmu3vzfxkpiwsqpfid.onion
ccPal gch3dyxo5zuqbrrtd64zlvzwxden4jkikyqk3ikjhggqzoxixcmq2fid.onion
Webuybitcoins 2bcbla34hrkp6shb4myzb2wntl2fxdbrroc2t4t7c3shckvhvk4fw6qd.onion
HQER sa3ut5u4qdw7yiunpdieypzsrdylhbtafyhymd75syjcn46yb5ulttid.onion
Counterfeit USD pliy7tiq6jf77gkg2sezlx7ljynkysxq6ptmfbfcdyrvihp7i6imyyqd.onion
EasyCoin Bitcoin Mixer vu3miq3vhxljfclehmvy7ezclvsb3vksmug5vuivbpw4zovyszbemvqd.onion
Onionwallet Bitcoin Mixer zwf5i7hiwmffq2bl7euedg6y5ydzze3ljiyrjmm7o42vhe7ni56fm7qd.onion

Commercial Services
DarkWebHackers zkj7mzglnrbvu3elepazau7ol26cmq7acryvsqxvh4sreoydhzin7zid.onion
Mobile Store ez37hmhem2gh3ixctfeaqn7kylal2vyjqsedkzhu4ebkcgikrigr5gid.onion
Kamagra 4 Bitcoin bepig5bcjdhtlwpgeh3w42hfffftcqmg7b77vzu7ponty52kiey5ec4ad.onion
OnionIdentityServices endtovmbc5vokdpnxrhajcwgkfbkfz4wbyhbj6ueisai4prtvencheyd.onion
UkGunsAndAmmo onili244aue7jkvzn2bgaszcb7nznkpyihdhh7evflp3iskfq7vhlzid.onion
USfakeIDs 7wsvq2aw5ypduujgcn2zauq7sor2kqrqidguwwtersivfa6xcmdtaayd.onion
EuroGuns hyjgsnkanan2wsrksd53na4xigtxhlz57estwqtptzhpa53rxz53pqad.onion
Apples4Bitcoin awsvrc7occzj2yeyqevyrw7ji5ejuyofhfomidhh5qnuxpvwsucno7id.onion
UKpassports wosc4noitfscyywccasl3c4yu3lftpl2adxuvprp6sbg4fud6mkrwqqd.onion
USAcitizenship pz5uprzhnzeotviraa2fogkua5nlnmu75pbnnqu4fnwgfffldwxog7ad.onion
Rent-A-Hacker jn6weomv6klvnwdwcgu55miabpwklsmmyaf5qrkt4miif4shrqmvdhqd.onion

Drugs
DCdutchconnectionUK wms5y25kttgihs4rt2sifsbwsjqjrx3vtc42tsu2obksqkj7y666fqid.onion
DrChronic gkcns4d3453llqjrksxdijfmmdjpqsykt6misgojxlhsnpivtl3uwhqd.onion
TomAndJerry c5xoy22aadb2rqgw3jh2m2irmu563evukqqddu5zjandunaimzaye5id.onion
420prime rbcxodz4socx3rupvmhan2d7pvik4dpqmf4kexz6acyxbucf36a6ggid.onion
Bitpharma 7bw24ll47y7aohhkrfdq2wydg3zvuecvjo63muycjzlbaqlihuogqvyd.onion
EuCanna wges3aohuplu6he5tv4pn7sg2qaummlokimim6oaauqo2l7lbx4ufyyd.onion
Smokeables porf65zpwy2yo4sjvynrl4eylj27ibrmo5s2bozrhffie63c7cxqawid.onion
CannabisUK hyxme2arc5jnevzlou547w2aaxubjm7mxhbhtk73boiwjxewawmrz6qd.onion
Brainmagic 6hzbfxpnsdo4bkplp5uojidkibswevsz3cfpdynih3qvfr24t5qlkcyd.onion
NLGrowers gn74rz534aeyfxqf33hqg6iuspizulmvpd7zoyz7ybjq4jo3whkykryd.onion
Peoples Drug Store 4p6i33oqj6wgvzgzczyqlueav3tz456rdu632xzyxbnhq4gpsriirtqd.onion
DeDope dumlq77rikgevyimsj6e2cwfsueo7ooynno2rrvwmppngmntboe2hbyd.onion

Chans
8Chan 4usoivrpy52lmc4mgn2h34cmfiltslesthr56yttv2pxudd3dapqciyd.onion
Nanochan nanochanqzaytwlydykbg5nxkgyjxk3zsrctxuoxdmbx5jbh2ydyprid.onion
Picochan picochanwvqfa2xsrfzlul4x4aqtog2eljll5qnj5iagpbhx2vmfqnid.onion
Endchan enxx3byspwsdo446jujc52ucy2pf5urdbhqw3kbsfhlfjwmbpj5smdad.onion
256Chan dngtk6iydmpokbyyk3irqznceft3hze6q6rasrqlz46v7pq4klxnl4yd.onion
THE END theendgtso35ir6ngdtyhgtjhhbbprmkzl74gt5nyeu3ocr34sfa67yd.onion

Privacy Services
Snopyta cct5wy6mzgmft24xzw6zeaf55aaqmo6324gjlsghdhbiw5gdaaf4pkad.onion
Riseup vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion
Vyempire.xyz wnrgozz3bmm33em4aln3lrbewf3ikxj7fwglqgla2tpdji4znjp7viqd.onion
SystemLi.org 7sk2kov2xwx6cbc32phynrifegg6pklmzs7luwcggtzrnlsolxxuyfyd.onion
Cryptostorm VPN stormwayszuh4juycoy4kwoww5gvcu2c4tdtpkup667pdwe4qenzwayd.onion
Privacy Tools privacy2zbidut4m4jyj3ksdqidzkw3uoip2vhvhbvwxbqux5xy5obyd.onion
TiTan XMPP titanxsu7bfd7vlyyffilprauwngr4acbnz27ulfhyxrqutu7atyptad.onion

Email Providers
Cock.li xdkriz6cn2avvcr2vks5lvvtmfojz2ohjzj4fhyuka55mvljeso2ztqd.onion
Elude.in eludemailxhnqzfmxehy3bk5guyhlxbunfyhkcksv4gvx6d3wcf6smad.onion
Sonar Tor Messenger sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid.onion
ProtonMail protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion
RiseUp Email 5gdvpfoh6kb2iqbizb37lzk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion

Blogs And Personal Sites
qorg11.net lainwir3s4y5r7mqm3kurzpljyf77vty2hrrfkps6wm4nnnqzest4lqd.onion
Course Enigma cgjzkysxa4ru5rhrtr6rafckhexbisbtxwg2fg743cjumioysmirhdad.onion
Kill-9 killnod2s77o3axkktdu52aqmmy4acisz2gicbhjm4xbvxa2zfftteyd.onion
Digdeeper digdeep4orxw6psc33yxa2dgmuycj74zi6334xhxjlgppw6odvkzkiad.onion
Spware Watchdog spywaredrcdg5krvjnukp3vbdwiqcv3zwbrcg6qh27kiwecm4qyfphid.onion
MayVaneDay Studios meynethaffeecapsvfphrcnfrx44w2nskgls2juwitibvqctk2plvhqd.onion
Shadow Wiki zsxjtsgzborzdllyp64c6pwnjz5eic76bsksbxzqefzogwcydnkjy3yd.onion
Outer Space reycdxyc24gf7jrnwutzdn3smmweizedy7uojsa7ols6sflwu25ijoyd.onion
Tech Learning Collective lpiyu33yusoalp5kh3f4hak2so2sjjvjw5ykyvu2dulzosgvuffq6sad.onion
Fuwa Fuwa fwfwqtpi2ofmehzdxe3e2htqfmhwfciwivpnsztv7dvpuamhr72ktlqd.onion
S-Config xjfbpuj56rdazx4iolylxplbvyft2onuerjeimlcqwaihp3s6r4xebqd.onion

Hacking
Defcon g7ejphhubv5idbbu3hb3wawrs5adw7tkx7yjabnf65xtzztgg4hcsqqd.onion
InfoCon w27irt6ldaydjoacyovepuzlethuoypazhhbot6tljuywy52emetn7qd.onion

News Sites
ProPublica p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyeznfu5uqd.onion
Darknetlive darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid.onion

Open Source Software
OnionShare lldan5gahapx5k7iafb3s4ikijc4ni7gx5iywdflkba5y2ezyg6sjgyd.onion
Whonix dds6qkxpwdeubwucdiaord2xgbbeyds25rbsgr73tbfpqpt4a6vjwsyd.onion
Qubes OS www.qubesosfasa4zl44o4tws22di6kepyzfeqv3tg4e3ztknltfxqrymdad.onion
Keybase.IO keybase5wmilwokqirssclfnsqrjdsi7jdir5wy7y7iu3tanwmtp6oid.onion
Bitcoin Core 6hasakffvppilxgehrswmffqurlcjjjhd76jgvaqmsg6ul25s7t3rzyd.onion
Wasabi Wallet wasabiukrxmkdgve5kynjztuovbg43uxcbcxn6y2okcrsg7gb6jdmbad.onion
The Tor Project 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion

Others
CIA.gov ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion
Internet Archive archivebyd3rzt3ehjpm4c3bjkyxv3hjleiytnvxcn7x32psn2kxcuid.onion
Bible4u bible4u2lvhacg4b3to2e2veqpwmrc2c3tjf2wuuqiz332vlwmr4xbad.onion
Imperial Library kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd4xzt26ochei4m6f7tayd.onion
Comic Book Library nv3x2jozywh63fkohn5mwp2d73vasusjixn3im3ueof52fmbjsigw6ad.onion
Tor Paste torpastezr7464pevuvdjisbvaf4yqi4n7sgz7lkwgqwxznwy5duj4ad.onion
Fuck Facebook 4wbwa6vcpvcr3vvf4qkhppgy56urmjcj2vagu2iqgp3z656xcmfdbiqd.onion
Just Another Library libraryfyuybp7oyidyva3ah5xvwgyx6weauoini7zyz555litmmumad.onion
Google Feud lkqx6qn7whctpdjhcoohpoyi6ahtrveuii7kq2m647ssvo5skqp7ioad.onion
NCIDE Police Task Force ncidetfs7banpz2d7vpndev5somwoki5vwdpfty2k7javniujekit6ad.onion
Rewards For Justice he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion
Ablative Hosting hzwjmjimhr7bdmfv2doll4upibt5ojjmpo3pbp5ctwcg37n3hyk7qzid.onion
KlosHost kaizushih5iec2mxohpvbt5uaapqdnbluaasa2cmsrrjtwrbx46cnaid.onion
SporeStack Hosting spore64i5sofqlfz5gq2ju4msgzojjwifls7rok2cti624zyq3fcelad.onion
Blockstream BTC Explorer explorerzydxu5ecjrkwceayqybizmpjjznk5izmitf2modhcusuqlid.onion
BlockChair BTC Explorer blkchairbknpn73cfjhevhla7rkp4ed5gg2knctvv7it4lioy22defid.onion
Shitposting Forum bombsjy5lsgehdyuevxu5kt3zdw22bfqrhbanc32evab3o3j3dvc7cid.onion
The Longest Onion Index jptvwdeyknkv6oiwjtr2kxzehfnmcujl7rf7vytaikmwlvze773uiyyd.onion

VIII) Conclusion

Le Dark Web est un espace complexe, souvent mal compris et caricaturé. S'il est indéniablement le terrain de nombreuses activités criminelles, il reste aussi un outil essentiel pour la liberté d'expression, la protection des sources journalistiques et la lutte contre les régimes autoritaires.