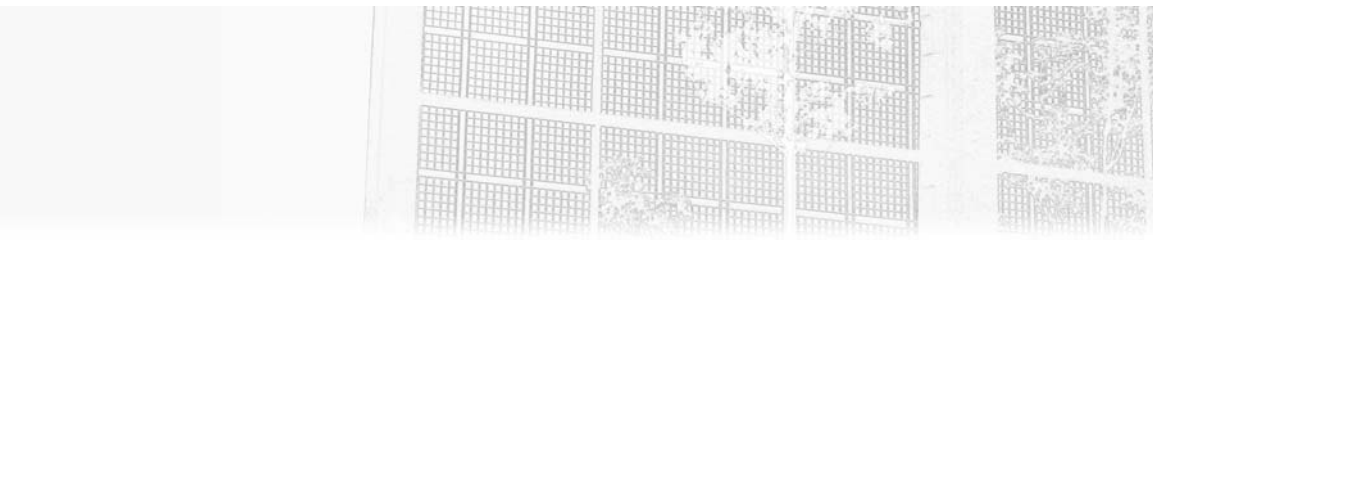




Chapitre 3

Black Market

1. Introduction

La prise en compte du Black Market dans un plan global lié à la sécurité informatique est devenue une obligation pour une entreprise soucieuse de protéger, sécuriser ses actifs et sa pérennité économique, sans oublier ses clients et son image. Bien évidemment, ce chapitre n'a pas pour mission de vous inviter à participer à ces Black Market en vendant ou en achetant les contenus commercialisés (bases de données piratées, identités numériques usurpées, etc.). Notre mission : vous permettre d'être un veilleur attentif de ce marché noir 3.0 de l'illicite.

Ce chapitre vise à expliquer pourquoi il est indispensable de réaliser une veille de cet environnement et à vous faire découvrir ce qu'est le Black Market : pourquoi ne faut-il pas le confondre avec le Dark Web/Deep Web ? Ce que l'on peut y trouver, son fonctionnement, ce qui est vendu et acquis, et comment orchestrer une veille efficace dans cet étrange milieu informatique.

2. Deep Web, Dark Web, Darknet, Black Market

Dès que l'on commence à parler du Black Market, le vocabulaire, sa situation géographique numérique, sa présence fantasmée ou non se mélangent. Il n'est pas rare de lire que le Black Market se cache dans le Deep Web. Que les pirates commercialisent leurs forfaits dans un Dark Web caché dans un *darknet* qui protège leur business. Si dans la forme ce raccourci peut sembler logique, dans le fond, nous sommes à mille lieues de la réalité.

En 2024, selon le FBI, le chiffre d'affaires global des marchés noirs numériques aurait dépassé 8 milliards de dollars, toutes plateformes confondues. À lui seul, Hydra Market (Russie, fermé en 2022) brassait 1,3 milliard \$ par an. Le site BreachForums, administré par des Français brassait entre 50 000 et 60 000 € par mois. Il est toujours actif mais, en janvier 2026, la base de données complète du forum (environ 324 000 utilisateurs) a été divulguée publiquement ce qui a entraîné une crise de confiance pour ce site dans la communauté criminelle.

D'abord, le Deep Web n'a rien de dangereux et de trouble. Il s'agit ni plus ni moins des données qui ne sont pas référencées sur le Web. Par exemple, une base de données qui gère votre site ; ce blog qui n'est destiné qu'à votre famille ; ces courriels que vous envoyez et recevez ; ce forum qui réclame des identifiants de connexion pour accéder à ses contenus, etc. Tout ceci n'a pas pour mission d'être référencé. Les moteurs de recherche qui parcourent la toile avec leurs robots (*spider*) fouineurs n'ont pas la possibilité de les cataloguer pour les retrouver à la première demande. Bref, ces données sont dans le Deep Web.

Avant de nous lancer dans cette visite du Black Market et de son utilisation dans une politique de veille, revenons rapidement sur les différentes couches du Web. D'abord, le plus connu, le Web « commun », le Clear Web. Facebook, Twitter, YouTube en font partie. Il se trouve en quelques secondes via l'ensemble des moteurs de recherche du globe.

Ensuite, le Web de surface. Lui aussi est simple d'accès, mais on y trouve des contenus plus « underground » comme Reddit, jetable.org (permet de créer une adresse mail à durée limitée) ou tout simplement des bases de données SQL, l'hébergeur de votre blog, l'intranet de votre entreprise, etc. En ce qui concerne le darknet, même confusion. Le darknet est un réseau de communication de personne à personne (*friend-to-friend*). Il n'a rien de dangereux ou d'illégal. C'est son utilisation à des fins malveillantes qui perturbe sa compréhension. C'est un peu comme dire que la voiture est dangereuse car des individus l'utilisent à l'occasion d'un braquage de banque.

Dans un troisième temps, le Bergie Web, le lien entre le Web et le Deep Web. On y croise par exemple The Pirate Bay. Le moteur de recherche de TPB dirige les utilisateurs vers le Deep Web, où se trouvent les liens torrent. Les forums anonymes 4chan, ou encore des serveurs FTP en font aussi partie.

Quatrième couche, le Web profond, le fameux Deep Web dans lequel se trouvent plusieurs autres sous-niveaux dont celui qui nous intéresse dans ce chapitre, celui des markets et autoshops du Black Market.

Un monde en constante évolution, créant des « métiers » de la malveillance. Par exemple, les « *Initial Access Brokers* (IAB) ». Ces spécialistes vendent l'accès à des réseaux d'entreprise, prélude aux attaques ransomware ou la possibilité, en toute discrétion d'accéder aux données de l'entreprise comme ont pu le connaître en 2024 : France Travail, SFR, FREE. Viennent ensuite les « *Ransomware-as-a-Service* » (RaaS). Nous parlons ici de la location de kits de ransomware, assistance technique incluse. Des groupes comme Lockbit, démantelés en 2025, avait pendant 5 ans attiré des dizaines de clients dans cette location d'outil pirate. La vente de faux documents, même si elle n'est pas nouvelle, attire de plus en plus de fraudeurs KYC. L'émergence de faux documents « numériques » générés par l'IA pour passer les contrôles d'identité se professionnalise. Les deux derniers exemples de ces « nouveaux métiers » pirates, il en existe d'autres à découvrir sur ZATAZ.COM : l'exfiltration d'API. Le pirate spécialisé vol et vent des clés API (OpenAI, AWS, Google...) à usage frauduleux. Enfin, les arnaqueurs « AI scam » : usurpation d'identité audio/vidéo via IA générative pour extorquer des proches (deepfake voice, etc.).

Les marketplaces se sont « Uberisés » avec des systèmes de notation vendeur/acheteur, des garanties de remboursement, des SAV, du cashback et même des campagnes promo (Black Friday, etc.).

3. Black Market, entre le visible et l'invisible

Le Black Market tente de se retrouver dans cet espace invisible, du moins pourrions-nous le penser au premier abord. Ce Web invisible est apparu pour la première fois dans le vocabulaire informatique en 1994, de la bouche de l'écrivain Jill H. Ellsworth. Le Black Market évolue dans le Deep Web, et plus précisément dans le Dark Web, le Dark Web étant lui-même une partie du darknet. Le darknet regroupe toutes les activités numériques organisées par un nombre limité de personnes n'évoluant pas obligatoirement dans le Dark Web, le Dark Web demandant obligatoirement un affichage de pages web. Compliqué ?

Le Dark Web est une infime partie de ce qui se cache dans le Deep Web sous forme de pages web accessibles via des outils comme Tor, Freenet, IP2, etc.

Le Dark Web ne se référence pas via un moteur de recherche ; du moins, normalement. Nous en reparlerons plus loin dans ces pages. Dans le darknet, on retrouve donc, par exemple, des mails chiffrés de pirate à pirate ou encore des boutiques du Black Market. Des boutiques qui, pour vivre, doivent évoluer dans le Dark Web, seul endroit où elles peuvent exister.

Bref, s'il fallait faire simple, le Black Market n'est rien d'autre qu'une boutique proposant des données piratées comme des bases de données volées sur un site web infiltré, des clones de cartes bancaires, des faux documents administratifs (de la fiche de paie en passant par des permis de conduire et autres fausses factures), des produits stupéfiants, des modes d'emplois et logiciels dédiés au piratage informatique sous la forme de pages web. Pour les plus extrêmes de ces boutiques, armes et munitions peuvent être acquises. L'idée étant bien évidemment que cela se passe de la façon la plus anonyme possible.

Il existe plusieurs « tailles » de Black Market. La simple boutique est tenue par une seule personne. Elle est baptisée « autoshop ». Cet espace propose un type précis de produits : drogue, faux documents, etc. Le « marketplace » regroupe quant à lui plusieurs « auto-shops » comme pourrait le faire une galerie marchande dans un hypermarché que nous trouvons dans nos villes. Sauf que les galeries marchandes du Black Market ne commercialisent que de l'illégal.

4. Fonctionnement

Un portail du Black Market fonctionne comme les boutiques que vous croisez sur la toile : des produits, des clients, des vendeurs et des transactions financières. Pour attester de leur fiabilité, des systèmes de notation s'affichent comme sur eBay. Dans votre veille, le fait qu'un vendeur soit crédité d'un certain nombre de ventes, avec des clients satisfaits, doit vous faire tendre l'oreille sur l'authenticité des données qu'il commercialise. Il est fiable si son pourcentage de satisfaction dépasse les 80 %. Les notes des acheteurs attesteront de son efficacité et de la qualité des produits : les bases de données vendues sont-elles inédites ? Le contenu est-il intéressant ? La vitesse de fourniture ? Etc.

Les « shops » les plus connus proposent même des garanties. La donnée bancaire achetée ne fonctionne pas ? Le remboursement et/ou le remplacement sont orchestrés. Malheur aux vendeurs qui tenteraient de fournir des informations et des produits périmés car le Black Market est un milieu criminel qui fonctionne avec de nombreux intermédiaires dont les principaux acteurs sont baptisés les « escrows ».

La mission de l'escrow ? C'est un intermédiaire qui contrôle et vérifie la transaction entre le vendeur et l'acheteur. Il réceptionne l'argent et verse la somme au vendeur une fois le produit réceptionné par l'acquéreur. L'escrow prend un pourcentage du prix fixé (entre 2 et 10 % selon les boutiques). Autant dire que le vendeur a tout à perdre en cas de problème. Un tiers, escrow ou boutique, qui conserve l'argent d'une transaction est baptisé « exit scam ». Il existe aussi des robots escrows. Ils font l'intermédiaire entre un acheteur et un vendeur et sont censés ainsi éviter les arnaques. L'escrow « automatique multi-sig » contrôle que chaque transaction est signée avec une clé privée afin de bloquer les tentatives d'exit scam. Selon le niveau de confiance, il est possible de rencontrer des Finalize Early (FE) : le vendeur étant connu et reconnu, il reçoit l'argent avant la réception de la commande.

Les paiements se font dans la grande majorité sous forme de monnaies dématérialisées comme le Bitcoin, le XMR ou encore l'Ethereum. Côté communication, les plus professionnels des Black Markets imposent le chiffrement des conversations entre interlocuteurs soit avec un système propriétaire, soit par le biais de clés PGP.

Fonctionnement : plus pro que jamais

Les sites « pirates » sont de plus en plus professionnels. Des interfaces utilisateur au design comparable à celui de plateformes comme Amazon ou Vinted. Des boutiques personnalisables, chat en ligne, gestion de panier, recommandations, plugins Telegram/Discord. Des paiements renforcés par la généralisation du Bitcoin, XMR (Monero, star de l'anonymat), Ethereum. Certains espaces pirates font encore payer les achats via des coupons Amazon ou Apple. Plus facile à blanchir, mais moins simple à manier. Depuis 2023, adoption partielle de cryptomonnaies stables (USDT, USDC) pour contourner la volatilité.

La prolifération des escrows (banquier) automatiques multisig (vérification multiclés) permet de sécuriser les transactions pirates. La tendance à la plateformesation est apparue en 2024. Certains Black Markets proposent même des API pour les vendeurs ! Finissons avec le passage massif vers des messageries chiffrées (Telegram, Signal) pour prise de contact, livraison de données ou SAV. Telegram, après l'arrestation par la France de son cofondateur, aura vu des dizaines de pirates se faire « attraper » par les autorités. Le 28 août 2024, Pavel Durov a été mis en examen pour une quinzaine d'infractions, placé sous contrôle judiciaire en France (interdiction de sortir du territoire, obligation de se présenter deux fois par semaine à la police, caution de plusieurs millions d'euros). Il a été remis en liberté en 2025. Les enquêteurs reprochent à Telegram, et donc à son fondateur, de laisser circuler librement sur sa plateforme des contenus illicites (pornographie infantile, drogues, blanchiment...) et de ne pas fournir les données demandées lorsqu'ils en faisaient la requête.

Depuis Telegram répond. Global 2024 : 893 demandes adressées à Telegram, concernant 2 072 utilisateurs. Dernier trimestre 2024 : 673 demandes par la justice française pour 1 386 utilisateurs. Cela signifie que 75 % des requêtes et profils ciblés l'ont été sur les trois derniers mois de l'année 2024. Le chiffre de **+30 % d'augmentation** reflète un contexte post-arrestation, marquant un tournant pour Telegram en France.

5. Anonymat des boutiques

Les boutiques du Black Market peuvent être contactées via de nombreuses méthodes : par cooptation, des liens qui se passent de main à la main... La plus simple, et surtout devenue la tendance, est un moteur de recherche qui permet de trouver une information ou un produit précis en tapant une requête comme sur Yahoo!, Qwant ou Google. Le site de Black Market peut avoir la forme d'un forum ou tout simplement d'une boutique avec offres, prix, boutons d'achat. Méfiez-vous des forums. Le plus généralement, ce sont des nids de vipères, quand il ne s'agit pas tout simplement d'arnaques pures et simples. Le Black Market via Google n'est pourtant pas impossible bien que risqué et illégal. Nous y reviendrons un peu plus loin dans ce chapitre.

La grande majorité de ces boutiques évoluent via des adresses en .onion. Comme le rappelle Wikipédia, le .onion **indique une adresse anonyme accessible par l'intermédiaire du réseau Tor** (<https://www.zataz.com/infiltration-pirate-via-un-noeud-tor/#axzz4gUQFI5Ji>).

Comprenez qu'une URL sous la forme de « adresse.onion » ne fonctionnera pas sur Internet, via votre navigateur habituel tel que Chrome, Edge, etc. Cette adresse .onion ne pourra être lue qu'à partir du réseau Tor, ses proxies et son navigateur dédié, Tor Browser. L'adresse générée pour évoluer sur Tor est aléatoire, même s'il est possible de lui donner un sens pour connaître sa destination. Un espace .onion a offert pendant un temps la possibilité d'acquérir des noms de domaine en .onion. Plusieurs millions d'adresses furent vendues en bitcoins comme freakbugfpaynode.onion (Freak Bug-F Paynode), qui fut cédée pour 5 bitcoins, soit plus de 7 000 €.

En ce qui concerne Tor, c'est un formidable outil proposé par le Tor Project, Inc (<https://fr.wikipedia.org/wiki/.onion>). Tor signifie *The Onion Router*. C'est un réseau informatique décentralisé qui fait appel à des millions d'ordinateurs dans le monde servant de nœuds de connexion. Bilan : Tor permet de cacher la trace de l'utilisateur ou du site .onion visité. Les communications étant chiffrées, Tor permet d'anonymiser l'origine des connexions TCP. C'est un outil génial utilisé par des centaines de journalistes, blogs prônant la liberté d'expression ou simples internautes ne souhaitant pas être suivis par le marketing et les traceurs des géants de l'Internet, Google en tête.

Les concepteurs de boutiques du Black Market profitent aussi de cet anonymat pour empêcher la localisation de leurs serveurs, un serveur pouvant être logé chez un hébergeur ayant pignon sur rue, tout à fait légal. Des boutiques peuvent aussi être cachées via Ip2, Freenet, mais Tor et .onion restent majoritaires car plus simples d'accès. Le système Tor permet aussi à ces boutiques du Black Market de « protéger » leurs visiteurs, l'IP de connexion des acheteurs/vendeurs n'apparaissant pas. Prudence cependant avec ce détail d'anonymisation.

Même si l'incontournable Electronic Frontier Foundation (EFF), fondation qui tente de protéger la vie privée sur Internet, propose Tor comme solution de sécurisation de ses connexions, des cas ont démontré que l'outil n'était pas infaillible (<https://www.torproject.org/>). Sarah Jamie Lewis, chercheuse en informatique, a lancé le projet OnionScan. Sa mission : permettre de trouver, de remonter des failles et des bugs découverts dans Tor. OnionScan (<https://github.com/s-rah/onionscan>) permet de numériser automatiquement les vulnérabilités et les erreurs communes qui peuvent bloquer la possibilité d'être anonyme sous Tor. **« La vie privée est importante. Même si certaines personnes utilisent Tor pour faire des choses illégales, il y a beaucoup de sites privés et des blogs politiques hébergés dans le Dark Web, et les propriétaires doivent se sécuriser »** (<http://www.extremetech.com/internet/226106-onionscan-tests-dark-web-sites-to-see-if-they-really-are-anonymous>).

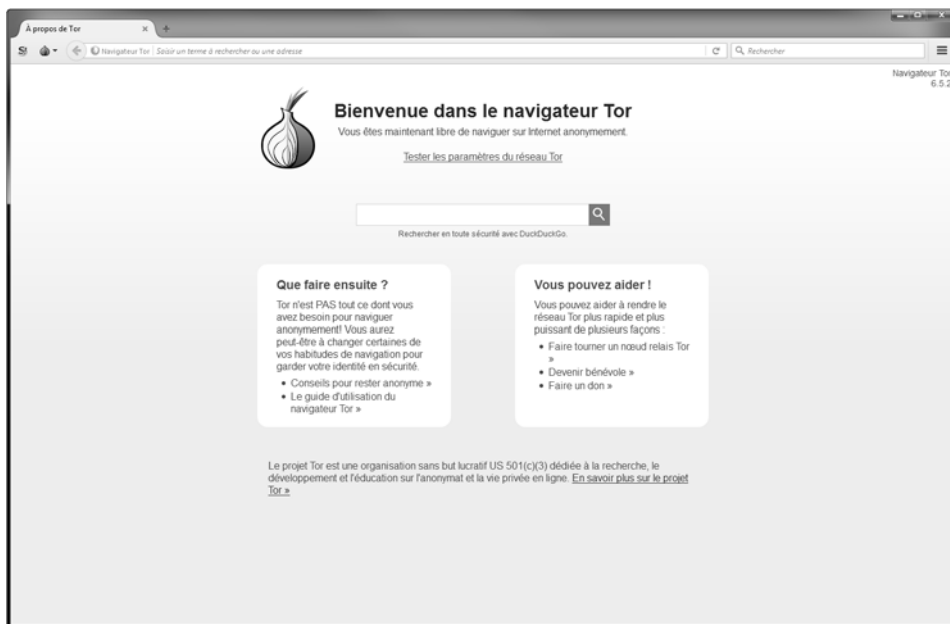
6. Mode d'emploi de Tor

Pour mettre en place votre veille et visiter les espaces proposés dans le Black Market en passant par les adresses en .onion, l'installation de Tor et l'utilisation de Tor Browser sont indispensables. Les sections qui suivent détaillent la façon de l'installer et de l'utiliser.

6.1 Installation

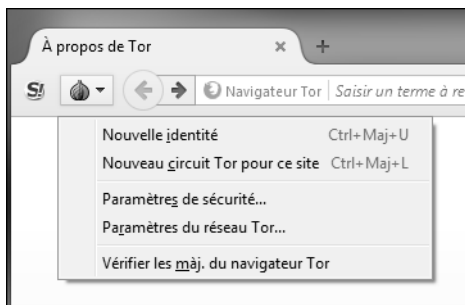
L'installation est simple.

Après avoir téléchargé Tor via le site officiel <https://www.torproject.org>, il suffit de l'installer sur votre ordinateur en suivant la procédure proposée par le logiciel.



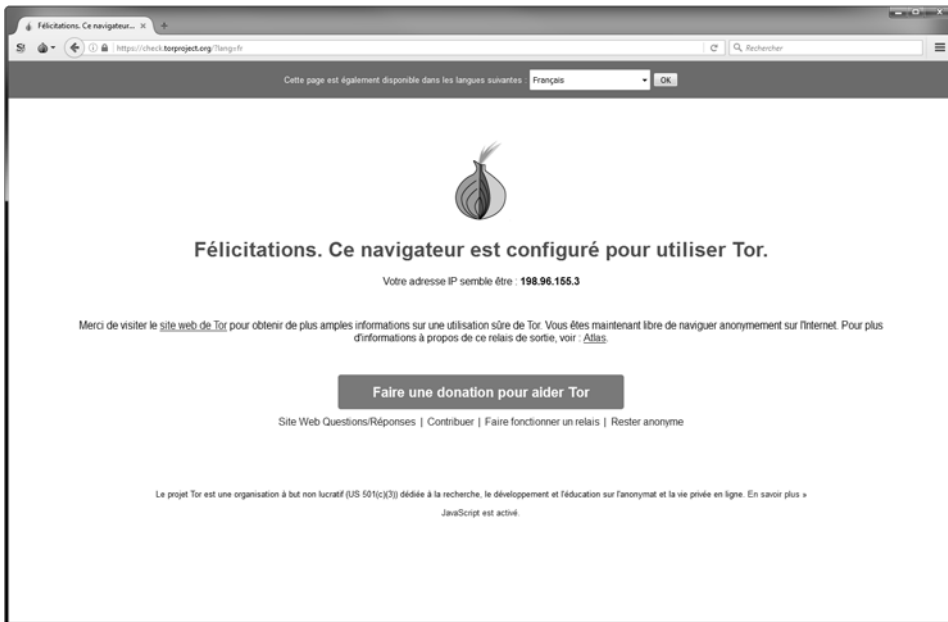
6.2 Configuration de la sécurité

► Dans l'onglet en forme d'oignon, en haut à gauche du navigateur, paramétrez votre Tor Browser.



6.3 Vérification de l'adresse IP

Vous pouvez vérifier votre adresse IP en cliquant sur le lien **Tester les paramètres du réseau Tor**. Le lien <http://www.mon-ip.com/localiser-adresse-ip.php> va vous permettre de comparer votre véritable adresse IP avec votre adresse IP une fois Tor mis en fonction sur votre connexion. Les deux adresses IP doivent être différentes lorsque vous vous connectez via Tor.



6.4 Navigation

Pour naviguer sur Tor, il suffit de rentrer l'URL .onion ou web dans la barre du navigateur. Les sites web recevront l'adresse IP que proposera Tor et non pas votre adresse IP officielle. Vous pouvez, en haut à droite dans le menu représenté par trois lignes horizontales, créer des règles pour les sites que vous souhaitez visiter car empêcher certaines requêtes limite les risques d'espionnage entre l'utilisateur et son point de connexion. Cela réduit fortement les possibilités d'interception.