INSTITUT D'ETUDES POLITIQUES DE STRASBOURG

Université de Strasbourg

Le développement de la cybercriminalité sur le Dark Web

Le Dark web francophone vu par un de ses membres

Mémoire de 4ème année, filière Droit et Administration Publique

Paul BARBASTE

Sous la direction d'Emmanuel DROIT

Sous le haut patronage du Général d'armée (2S) Marc WATIN-AUGOUARD

Année universitaire 2018- 2019

" L'Université de Strasbourg n'entend donner aucune approbation ou improbation aux opinions émises dans ce mémoire. Ces opinions doivent être considérées comme propres à leur auteur[e] ".

Remerciements

Je tiens à remercier M. Emmanuel DROIT pour son encadrement et son soutien pendant l'année, pour un projet de mémoire original et risqué.

Remerciements particuliers au Général d'armée (2S) Marc WATIN-AUGOUARD et à M. Bruno DENOYELLE, soutiens de la première heure, ainsi qu'à M. Jean-Philippe RENNARD pour son aide.

Enfin, je tiens également à remercier M. Adrien PETIT pour ses conseils et son suivi rigoureux de l'avancement du mémoire ces derniers mois ainsi que mes anciens collègues de CEIS et d'INQUEST, qui m'ont formé à la recherche sur le Dark Web ces deux dernières années.

Sommaire

Préambule

Ce mémoire porte sur l'histoire du Dark Web, tout en se focalisant sur sa partie francophone. Notre analyse s'est arrêtée le 31 mai 2019, date de rendu de ce mémoire. Il ne prend ainsi pas en compte les dernières opérations menées par la police française sur le Dark Web, menant au déclin de Liberty's Hacker. Elles feront en effet l'objet d'une autre étude dans les prochains mois, nécessitant de prendre un recul important sur ces évènements.

Introduction

Le 12 juin 2018, les autorités françaises ferment le marché noir francophone *BlackHand*. Ils interpellent son administratrice ainsi que trois autres membres, lors d'une opération menée simultanément à Lille, Marseille et Montpellier. Très médiatisée, elle est annoncée le 16 juin 2018 dans un communiqué officiel par le Ministre des Comptes Publics Gérald Darmanin. A ce jour, il s'agit de l'opération officielle la plus importante menée par les forces de l'ordre françaises sur le Dark Web.

Présente depuis les années 2010 sur le darknet Tor, la cybercriminalité prospère grâce au marché noir *Silk Road*, qui démocratise l'utilisation du darknet Tor à des fins criminelles, l'exposant au grand public, qui assimile les deux notions de darknet et de Dark Web. Le Dark Web désigne en effet le contenu cybercriminel présent sur les darknets, contenant avec lequel il est trop souvent confondu.

Notre analyse doit ainsi différencier ces deux notions, afin de comprendre quelle est l'importance de la cybercriminalité sur les darknets, en nous focalisant sur le darknet Tor, aujourd'hui le plus utilisé, totalisant plus de 2.8 millions d'utilisateurs réguliers. Un darknet est un réseau parallèle à Internet, qui offre des fonctionnalités d'anonymat plus importantes que celles offertes par le réseau traditionnel. La confidentialité qu'offre un darknet pousse un grand nombre d'utilisateurs à s'y cacher, espérant principalement échapper à la surveillance étatique ; opposants politiques, crypto-anarchistes, pirates informatiques, vendeurs de drogues, faussaires et consommateurs de pédopornographie.

Le réseau Tor fait face à une très forte médiatisation, notamment après les révélations d'Edward Snowden en 2013 sur la surveillance de masse, qui poussent de nombreux internautes à recourir à un darknet afin de protéger leurs données de navigation. Le darknet n'est ainsi pas uniquement utilisé par les cybercriminels ou les opposants politiques, mais également par des internautes sensibilisés à la sécurité de leur données. En effet, le site qui

enregistre aujourd'hui le plus de visites sur Tor est Facebook, accessible en .onion sur le darknet Tor.

Le Dark Web est principalement divisé en trois services : marchés noirs, forums et services d'hébergement. Les fermetures de Freedom Hosting I et II, principaux services d'hébergement, en 2014 et 2017 réduisent considérablement la proportion de sites pédopornographiques sur le Dark Web, aujourd'hui principalement organisé autour des marchés noirs et de la vente de drogues. Les autres services, tels que les *redrooms*, véritables chambres de torture diffusant les vidéos en direct ou les sites proposant les services de tueurs à gages relèvent plus de la croyance populaire que de la réalité. En effet, nous n'avons pas réussi à déterminer si les sites récupérés par notre algorithme avec ce type de contenu étaient réels.

L'anonymat offert par Tor ne nous permet pas de pouvoir remonter directement aux hébergeurs des *hidden services*, c'est pourquoi nous utiliserons une distinction par langues afin de pouvoir procéder à une cartographie du Dark Web. L'écosystème anglophone représente aujourd'hui plus de 90 % des contenus sur Tor, devant les écosystèmes russophones et européens, selon les statistiques effectués sur les données récupérées par notre moteur de recherche.

Notre analyse reviendra sur le développement de la cybercriminalité avant qu'elle ne passe sur Tor, puis sur le darknet Tor, en se focalisant sur l'histoire des principaux marchés noirs, depuis *Silk Road* jusqu'à la fermeture de *Wall Street Market* en mai 2019 et le rôle des forums dans la diffusion de nouveaux types de cybermenaces, les malware et les ransomware. Enfin, ce mémoire étudiera la communauté francophone, à travers son histoire et la fraude identitaire, spécificité du Dark Web francophone.

Face à l'absence de sources officielles et à la difficulté d'accès aux données, nous avons mis en place une méthodologie spécifique, afin de pouvoir réussir à accéder aux informations nécessaires à la réalisation de ce mémoire.

Méthodologie de recherche

La principale difficulté rencontrée est le manque d'informations et de sources officielles. A ce jour, il n'y a aucune étude approfondie ni de cartographie du Dark Web. Seules quelques études, réalisées par des entreprises privées de sécurité informatique comme Trend Micro, DarkOwl ou CEIS sont accessibles librement. Ces études, faites dans le cadre d'entreprises, sont à étudier avec subjectivité : leur objectif principal étant de mettre en avant l'entreprise dans leur secteur, elles occultent volontairement certains points afin de ne pas dévoiler leurs sources d'information. Les autorités veillent également à ne pas communiquer sur le Dark Web pour ne pas révéler d'éléments qui pourraient être utilisés par les cybercriminels ou révéler une opération de police en cours.

Le manque d'informations disponibles est également explicable par la nature même du Dark Web. Cet espace n'est en effet pas référencé, très difficilement accessible, et ne bénéficie pas de moteur de recherche officiel pour récupérer les données. Le moteur de recherche le plus complet, Aleph GrayMatter, n'est pas accessible au grand public et n'est utilisé que par les services de renseignement ou les grandes entreprises qui bénéficient de moyens suffisamment importants.

Bien qu'utilisant des méthodes de collecte et d'analyse de données parfois très techniques, ce mémoire reste un mémoire de sciences humaines et n'a pour objectif que d'analyser et de comprendre le Dark Web. La méthodologie de recherche et de collecte de données se divise principalement en quatre parties :

- Utilisation du moteur de recherche pour récupérer directement les informations recherchées ;
- Analyse des données dans le système d'analyse Open Semantic Search ;
- Vérification des informations via Wayback Machine ;
- Entretiens avec des professionnels

A. Outils

La méthodologie de recherche s'appuie principalement sur des outils adaptés à effectuer des recherches sur le darknet Tor et à les recouper avec des informations obtenues sur le clear web. Nous développerons ainsi ces deux points dans les prochaines pages.

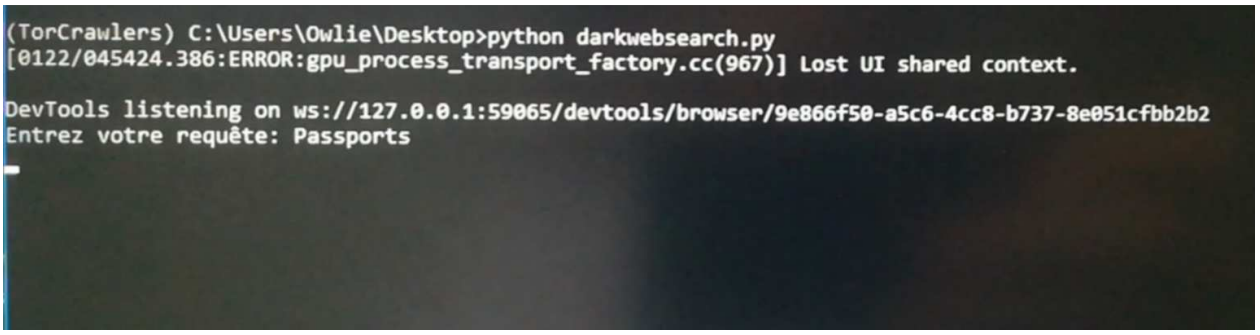
1. Création et utilisation de Wotan, moteur de recherche Dark Web

Afin de pouvoir accéder rapidement et directement aux services cybercriminels cachés, la création d'un petit moteur de recherche était indispensable. Six mois ont été nécessaires pour le développer. Nous nous sommes principalement appuyés sur le fonctionnement d'un ancien moteur de recherche qui n'existe plus depuis décembre 2017: *Grams*. Ce moteur permettait de se connecter aux marchés noirs et d'effectuer des recherches sur leur contenu.

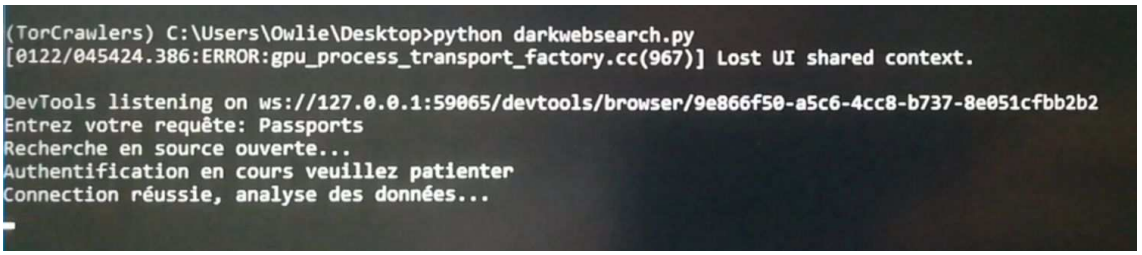
Ancien moteur de recherche Grams

Bien que n'ayant pas eu accès au code source de *Grams,* nous avons pu déterminer une partie de la technologie qui était utilisée par le moteur : le langage de programmation Python et l'utilisation de bibliothèques de fonctions spécifiques à ce langage, afin de se connecter aux marchés noirs et de résoudre leurs captcha (images qui vérifient si l'utilisateur n'est pas un robot). Nous nous sommes également appuyés sur le code source des moteurs de recherche

Ahmia[1] et *Memex*[2] afin de développer le moteur de recherche *Wotan*. Faute de temps, nous n'avons pas eu le temps de développer une interface graphique. Ce moteur reste donc en ligne de commande depuis la console de développement et a deux fonctions principales : effectuer des requêtes sur le darknet Tor, tout en se connectant aux marchés noirs et aux forums indexés, ainsi qu'à exporter les données vers le système d'analyse Open Semantic Search.



Requête avec le mot-clé "Passeports"



Analyse des données par le moteur de recherche

[1] Ahmia, *Ahmia/ahmia-site*, https://github.com/ahmia
[2] Nasa-Jpl-Memex, *Nasa-jpl-memex/memex-explorer*, https://github.com/nasa-jpl-memex/memex-explorer

Liste des liens contenant le mot-clé 'passeport' après analyse par notre moteur

2. Analyse des données dans Open Semantic Search

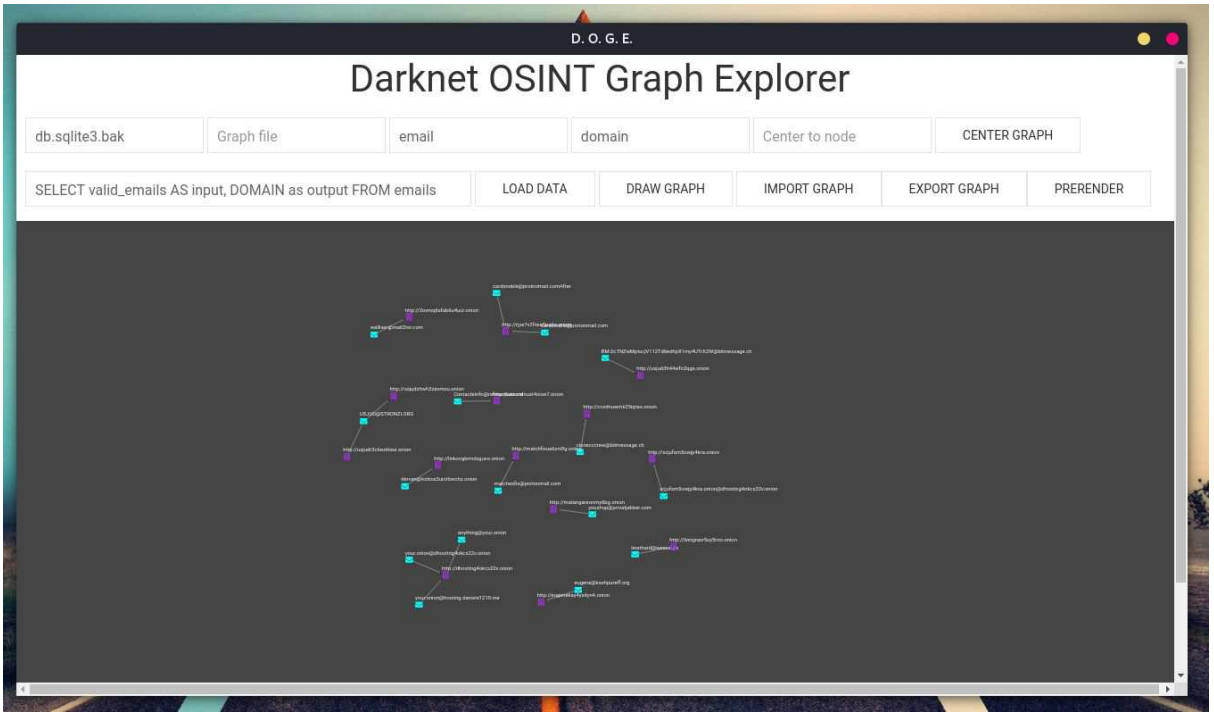
Dans le respect de la démarche d'un mémoire de recherche, nous avons ainsi mis en place un système de récupération et d'analyse de données, s'appuyant sur notre moteur pour la partie collecte et sur un système d'analyse de données, Open Semantic Search.

Une fois les données récupérées par le moteur de recherche, nous les avons indexées sur une base de données appelée Open Semantic Search, permettant de faire des recherches, de regrouper les mots-clés et de réaliser des arborescences de documents. Elle est basée sur le moteur de recherche Apache Solr. Nous avons ajouté un module OCR (optical character recognition), qui permet d'identifier et d'indexer le texte présent dans certaines images, afin de pouvoir rajouter à notre analyse l'ensemble documents scannés.

Les fonctionnalités de cette base de données nous ont ainsi permis d'identifier les données les plus pertinentes, faute de pouvoir lire et prendre en compte l'ensemble des documents récupérés. Pour finir, une fois les données pertinentes identifiées, nous avons utilisé un outil d'analyse de métadonnées appelé FOCA afin de remonter directement à leur source (auteur, date et origine des données téléchargées). Les métadonnées ont par la suite été ajoutées à la

base d'Open Semantic Search afin de prendre en compte et de pouvoir remettre en contexte les sources et auteurs des données.

Nous avons également pu utiliser d'autres outils spécialisés qui permettent de recueillir des données sur le darknet Tor. Onion Scan[3] nous a permi de scanner le réseau Tor et DOGE (Darknet Osint Graph Explorer) de modéliser les données recueillies.[4]



exemple de modélisation de données sur DOGE

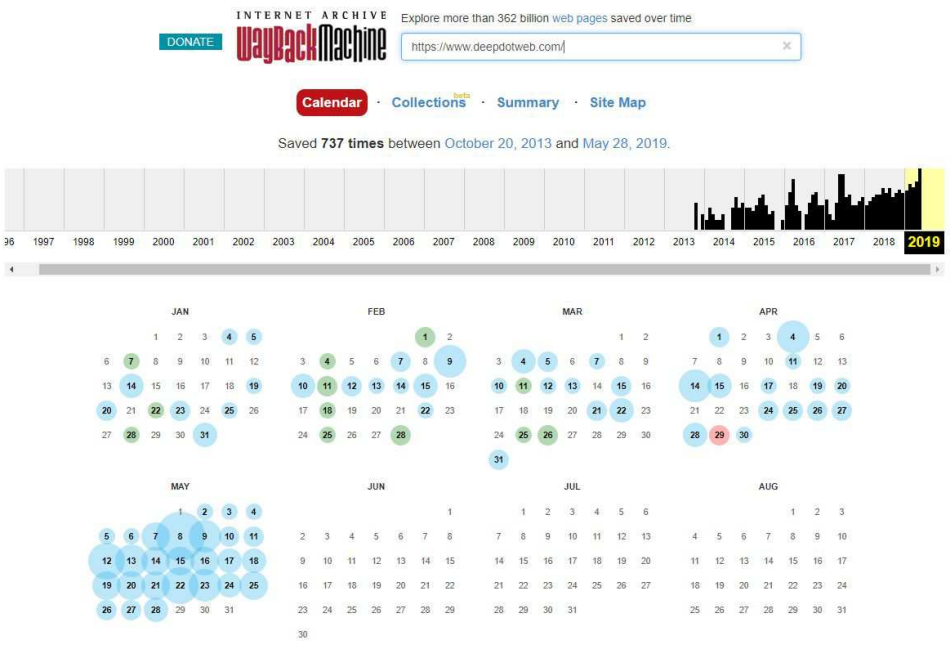
3. Recherche et validation des sources

Dans cette analyse, le principal problème rencontré a été la disparition de certaines sources, principalement fermées par les autorités. Une source d'informations très importante, le site *Deepdotweb* a en effet été fermé le 4 mai 2019 lors d'une opération conjointe du FBI et d'Europol[5]. Afin de continuer à pouvoir accéder aux articles de cette source, nous avons

[3] S-Rah, *S-rah/onionscan*, https://github.com/s-rah/onionscan
[4] Pielco11, *Pielco11/DOGE*, https://github.com/pielco11/DOGE
[5] *DeepDotWeb shut down: administrators suspected of receiving millions of kickbacks from illegal dark web proceeds*, https://www.europol.europa.eu/newsroom/news/deepdotweb-shut-down-administrators-suspected-of-receiving-millions-of-kickbacks-illegal-dark-web-proceeds

utilisé *Wayback Machine*[6] qui permet d'accéder à certaines pages qui ne sont plus en ligne, enregistrées dans des archives. Nous avons également utilisé ce moteur afin d'accéder aux anciens sites et forums décrits dans la première partie de ce mémoire, ce qui nous a notamment permis de comprendre le fonctionnement de la cybercriminalité avant qu'elle ne passe sur Tor. Le moteur de *Wayback Machine* est basé sur Elasticsearch, un outil que nous avons utilisé afin de classer certaines informations, avant d'avoir recours au système d'analyse Open Semantic Search.

Afin d'accéder aux données, il faut sélectionner une date dans les résultats proposés par le moteur, qui correspondent aux dates capturées par le site. Il ne donne cependant accès qu'à certaines pages des sites.



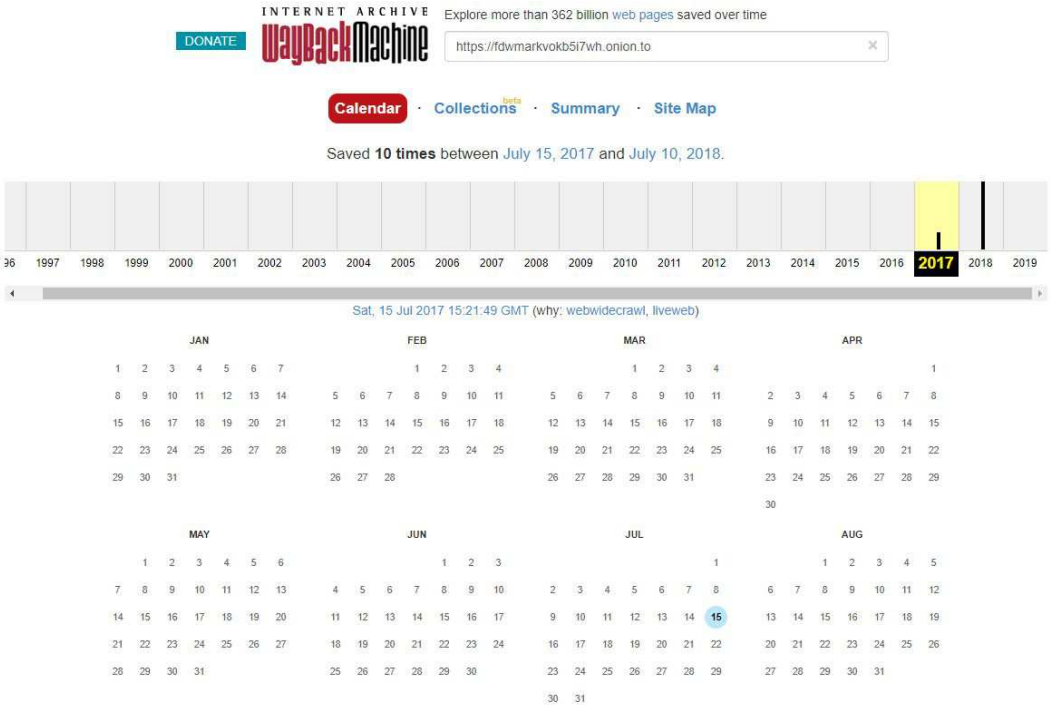
Utilisation de WaybackMachine afin d'accéder aux archives du site deepdotweb.com

Wayback Machine ne permet malheureusement pas de pouvoir accéder au réseau Tor. C'est pourquoi nous l'avons couplé à un autre service, *Tor2Web*[7]. qui permet d'accéder au réseau

[6] https://archive.org/web/.

[7] *Browse the Tor Onion Services*, https://www.tor2web.org/

Tor sans pour autant passer par son navigateur. Pour cela, il est nécessaire de rajouter '.to' à la fin de l'url en .onion et de le rentrer dans le moteur de recherche de *Wayback Machine*. Il n'y a souvent que peu de résultats mais cela permet de remonter certaines informations ou pouvoir accéder à d'anciennes versions de *hidden services*.



Utilisation de WaybackMachine afin d'accéder aux archives du site frenchdeepweb, en y ajoutant '.to' à la fin de l'url

B. Indexation et recherches sur la base '*Darknet Market Archives*'

La base *Darknet Market Archives*[8] est un set de données qui réunit les données de 89 marchés noirs et 37 forums, récupérées entre 2011 et 2015. Ce sont ces données qui ont permis de dresser des statistiques de vente ainsi qu'une brève histoire des marchés noirs. Il n'y a cependant que les données des marchés noirs et forums anglophones. Bien que cela représente plus 80% du contenu des services cachés sur Tor, il a néanmoins été nécessaire

[8] Gwern, *Darknet Market Archives (2013-2015)*, https://www.gwern.net/DNM-archives

d’effectuer des statistiques sur les marchés noirs russophones en utilisant nos propres outils de collecte de données.

C. Entretiens et validation des informations récupérées

Afin de valider la véracité de certaines informations, nous avons été aidé par d’anciens collègues de travail, travaillant dans diverses entreprises de sécurité ou services de police. Ils nous ont apporté leur aide sur certaines questions (histoire d’un marché noirs, communautés cybercriminelles cachées). Pour des raisons de confidentialité, leurs noms ne seront pas communiqué dans ce mémoire.

Nous avons également pu réaliser plusieurs entretiens et assister à des conférences (‘*Is the Dark Web a lawless space ?’*) avec des personnalités du monde du renseignement cyber, notamment au Forum International de la Cybersécurité, qui s’est tenu à Lille en janvier 2019.

Notions

En octobre 2017, le Journal officiel de la République française a publié une série de traductions de termes techniques, comprenant notamment la traduction de deep web et darknet, dénommés désormais en français respectivement par « web abyssal » ou « web profond » et « internet clandestin »[9].

On fait cependant face à de trop nombreuses confusions sur la nature et la terminologie du Dark Web. Avant d'aller plus loin, il conviendra donc d'opérer une distinction entre les types de contenus (clear web, deep web et Dark Web) et les types de réseaux (clearnet et darknets).

A. L'analogie de l'iceberg, une comparaison qui peut porter à confusion

L'analogie de l'iceberg peut porter à confusion. On trouve en effet beaucoup de représentations mélangeant l'approche par le réseau et celle par le contenu, qui ne doivent pas être séparées mais nécessitent cependant d'être définies préalablement.

Analogie de l'iceberg - starweaver.com

[9] *Legifrance - Le service public de l'accès au droit*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000035638

1. Approche réseau : *darknets* et *clearnet*

L'approche réseau désigne l'aspect lié à l'infrastructure. On peut donc le diviser en deux parties principales : le *clearnet* et les *darknets*. Les *darknets* désignent les réseaux superposés, dits overlay[10], qui utilisent des protocoles permettant aux utilisateurs de rester anonymes. Le terme trouve ses origines dans les années 1970, alors utilisé afin de désigner les réseaux isolés d'ARPANET. Ces réseaux superposés pouvaient recevoir des données provenant du réseau central mais ses adresses IP n'y étaient pas référencées et ne pouvaient pas répondre aux requêtes venant d'ARPANET.

Le réseau darknet le plus utilisé aujourd'hui est Tor, (*The Onion Router*) qui compte plus de 2,8 millions d'utilisateurs, devant I2P et Freenet[11]. On peut également trouver d'autres réseaux, moins accessibles au grand public, comme RetroShare et AnoNet. Du fait du fort degré d'anonymisation qu'ils offrent à leurs utilisateurs, les darknets sont souvent utilisés à des fins illégales.

Peu utilisé, le terme *clearnet* désigne désigne ce qui n'est pas présent sur un darknet et ne possède pas de protocole d'anonymisation.

2. Approche contenu : *clear web, deep web et Dark Web*

Il est nécessaire de distinguer une seconde approche, qui s'intéresse au contenu et à son indexation par les moteurs de recherche classique traditionnels. On s'intéresse donc ici à l'accessibilité des informations pour le grand public. C'est cette approche qui est souvent abordée lors de l'analogie de l'iceberg. Il est nécessaire de distinguer trois parties principales: le *clear web, le deep web* et le *Dark Web*.

Le *clear web* représente l'ensemble des contenus accessibles depuis les moteurs de recherche généralistes (Google, Bing, Qwant…). Ces contenus sont accessibles grâce à leur indexation par les moteurs de recherche.

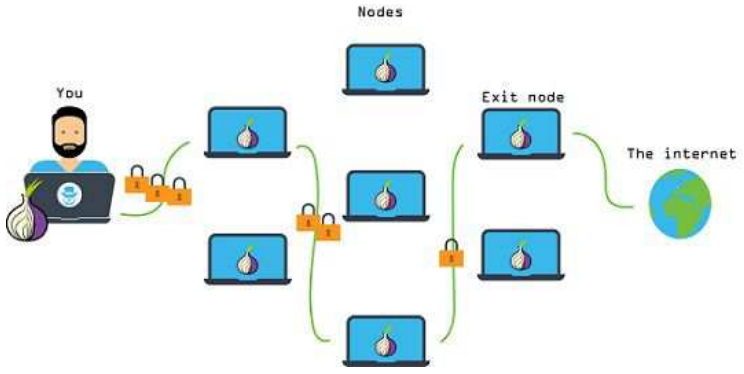
[10] Rennard Jean-Philippe, *Darknet chapitre 1*, http://www.rennard.org/Darknet/presentation.html.
[11] *Users*, Tor project, https://metrics.torproject.org/userstats-relay-country.html

Souvent utilisé à tort, le *deep web* désigne les contenus non-indexés par les moteurs de recherche généralistes, pour des raisons techniques[12] - certaines bases de données (Internet Movie Database, National Climatic Data Center, NASA…) étant trop volumineuses pour être traitées – et pour des raisons de confidentialité (web privé…). Ces contenus peuvent cependant être accessibles depuis les navigateurs classiques comme Chrome, Firefox ou Explorer, contrairement au contenu présent sur un réseau darknet.

Le *Dark Web* représente les contenus illégaux présents sur les darknets, non-indexés par les moteurs de recherche et non accessibles depuis les navigateurs classiques[13]. Il est nécessaire d'utiliser une application dédiée afin de pouvoir y accéder.

B. Tor, un outil contre la surveillance détourné par les cybercriminels

Le réseau Tor, acronyme de *The Onion Router* a été développé par la marine américaine à la fin des années 1990. Il est publié sous licence libre en 2004. L'organisation *The Tor Project*, aujourd'hui en charge du maintien de Tor, est fondée en 2006[14]. Le réseau est constitué de serveurs, appelés nœuds, qui font rebondir les échanges afin de complexifier les analyses du trafic des flux réseaux[15]. Les sites qu'il héberge ont pour nom de domaine .onion et sont appelés *hidden services*.



Fonctionnement du réseau Tor - lebiddata.fr

[12] Hamilton Nigel (2003), *The Mechanics of a Deep Net Metasearch Engine*
[13] Riha, *Surface Web vs Deep Web vs Dark Web vs Darknet*, https://www.firecompass.com/blog/darkweb-deepweb-darknet-browsers
[14] *The Tor Project | Privacy & Freedom Online*, https://www.torproject.org/about/history/
[15] Inc, *Tor*, https://2019.www.torproject.org/about/overview.html.en

L'usage de Tor permet ainsi de se protéger contre la surveillance du trafic et de contourner la censure de certains états. Il a notamment été utilisé par des opposants politiques lors des Printemps Arabes afin de pouvoir échanger sans être surveillés[16]. Le nombre d'utilisateurs de Tor explose en 2013, suite aux révélations d'Edward Snowden sur les programmes de surveillance de la NSA, qui pousse lui-même les internautes à passer sur des réseaux darknets afin de protéger leurs données de navigation[17]. L'anonymat offert par Tor permet la création des premières grandes plateformes cybercriminelles, permettant aux pirates de pouvoir échanger sans être surveillés par les autorités.

L'utilisation de Tor ne rend pas pour autant la navigation totalement anonyme. La sécurité et la fiabilité de certains nœuds est aujourd'hui mise en cause par des chercheurs[18]. Afin de protéger leur anonymat, les utilisateurs de Tor utilisent aujourd'hui un VPN et bloquent l'exécution des scripts sur les pages web. Le navigateur se démarque des autres programmes darknets par sa prise en main très facile et rapide.

[16] Wbur, *U.S. Activists Help Egyptians Elude Online Censorship*, https://www.wbur.org/hereandnow/2011/01/31/egypt-internet-government
[17] *This is What a Tor Supporter Looks Like: Edward Snowden*, https://blog.torproject.org/what-tor-supporter-looks-edward-snowden
[18] Dingledine Roger (18 February 2009), *One cell is enough to break Tor's anonymity*

Partie I : Naissance du Dark Web : le développement de la cybercriminalité sur le darknet Tor

L'utilisation de Tor par les cybercriminels n'est que très récente et ne remonte qu'à la dernière décennie. La cybercriminalité s'est développée dans les années 1980 via Usenet et les premiers Bulletin Board System. Au début des années 2000, les forums qui traitent de drogues et de piratage ne se cachent pas encore sur Tor, et sont accessibles librement sur Internet. Suite aux premières opérations de police menées par la DEA et le FBI, les premiers marchés noirs commencent à rejoindre un darknet afin d'échapper à la surveillance des autorités. Le marché noir *Silk Road* change la donne en 2011 en popularisant Tor dans les média mais également en créant une communauté importante, qui tend à faciliter l'accès aux marchés noirs en démocratisant l'accès au Dark Web. Désormais plus accessible, le Dark Web bénéficie d'une publicité importante sur le clear web, à travers les sites spécialisés, les moteurs de recherche et les hidden wiki.

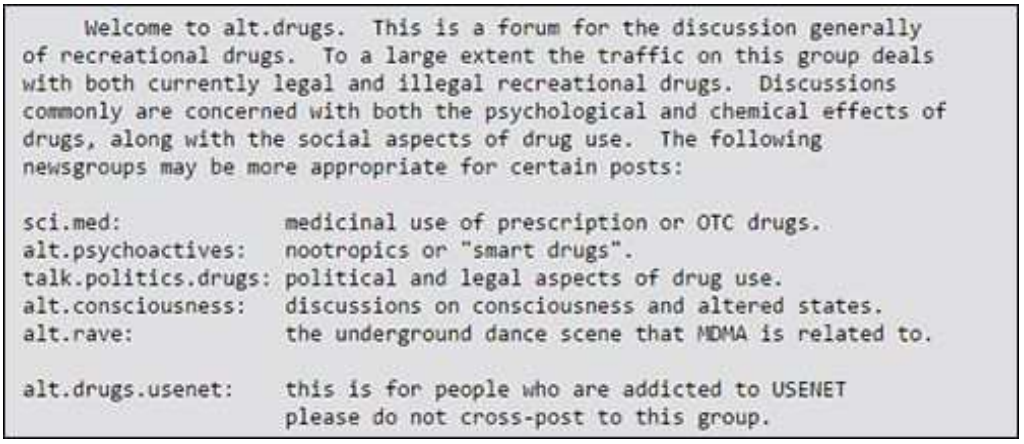
Chapitre 1 : Du clear web au darknet

Dès les années 1970, ARPANET est utilisé par les étudiants de Stanford, qui utilisent leur compte du laboratoire d'Intelligence Artificielle, afin d'échanger du cannabis avec les étudiants du Massachusetts Institute of Technology[19]. La cybercriminalité continue à se développer dans les années 1980 avec la création d'Usenet et des premiers Bulletin Board System (BBS). Dans cette partie, nous distinguerons le développement des premiers forums et marchés noirs centrés autour de la drogue et des substances illicites et celui centré autour du piratage et des données volées[20].

[19] Markoff John (2005), *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry*
[20] Howell O'Neill Patrick (15 February 2015), *The uncensored history of the Internet's drug revolution*

A. Usenet et le développement des premiers forums centrés autour de la drogue et des substances illicites

Créé en 1979[21], Usenet démocratise l'utilisation des forums décentralisés et des groupes de discussion, alors divisés en huit sujets[22] *(comp, humanities, misc, news, rec, sci, soc, and talk)*. John Gilmore et Brian Reid, informaticiens et activistes libertariens créent en 1987 le groupe de discussion 'alt', comme alternative aux huit sujets principaux. Le forum alt.drugs devient très vite populaire et rassemble plusieurs milliers d'utilisateurs[23].

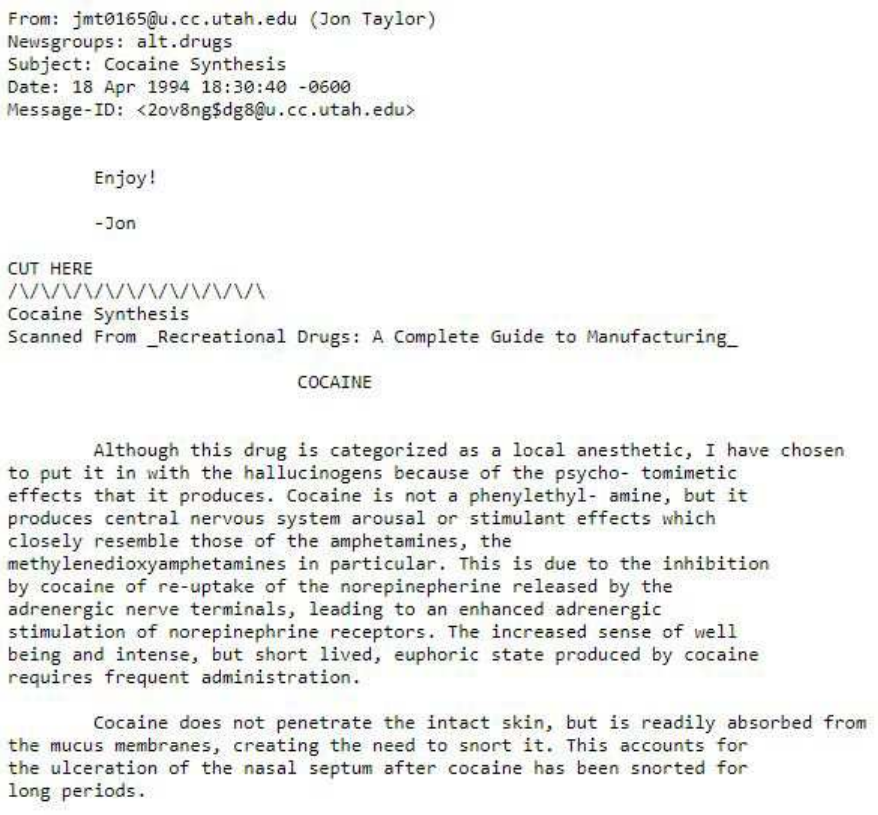


```
    Welcome to alt.drugs.  This is a forum for the discussion generally
of recreational drugs.  To a large extent the traffic on this group deals
with both currently legal and illegal recreational drugs.  Discussions
commonly are concerned with both the psychological and chemical effects of
drugs, along with the social aspects of drug use.  The following
newsgroups may be more appropriate for certain posts:

sci.med:              medicinal use of prescription or OTC drugs.
alt.psychoactives:    nootropics or "smart drugs".
talk.politics.drugs:  political and legal aspects of drug use.
alt.consciousness:    discussions on consciousness and altered states.
alt.rave:             the underground dance scene that MDMA is related to.

alt.drugs.usenet:     this is for people who are addicted to USENET
                      please do not cross-post to this group.
```

Charte d'utilisation du forum usenet alt.drugs

Face à l'explosion du nombre d'utilisateurs d'alt.drugs, les autorités américaines commencent à y surveiller les échanges. La vente de drogues illicites n'est ainsi pas abordée directement sur les forums ouverts, qui servent néanmoins à mettre en relation les vendeurs et les acheteurs, qui échangent par la suite en messages privés. Le forum sert également aux utilisateurs pour partager des connaissances sur la culture et l'utilisation des drogues illicites. Après une décennie d'utilisation importante, Usenet décline cependant peu à peu dans les années 1990 face à l'arrivée du World Wide Web.

[21] Lueg Christopher, Fisher Danyel (2003), *From Usenet to CoWebs: interacting with social information spaces*, (2003)
[22] *8 Usenet*, http://www.big-8.org/articles/b/i/g/Big-8_Usenet.html.
[23] Patrick Howell O'Neill, The Kernel, *"The Uncensored History of the Internet's Drug Revolution."*, kernelmag.dailydot.com/issue-sections/features-issue-sections/11680/hive-silk-road-drugs-history/



```
From: jmt0165@u.cc.utah.edu (Jon Taylor)
Newsgroups: alt.drugs
Subject: Cocaine Synthesis
Date: 18 Apr 1994 18:30:40 -0600
Message-ID: <2ov8ng$dg8@u.cc.utah.edu>

        Enjoy!

        -Jon

CUT HERE
/\/\/\/\/\/\/\/\/\/\/\
Cocaine Synthesis
Scanned From _Recreational Drugs: A Complete Guide to Manufacturing_

                        COCAINE

        Although this drug is categorized as a local anesthetic, I have chosen
to put it in with the hallucinogens because of the psycho- tomimetic
effects that it produces. Cocaine is not a phenylethyl- amine, but it
produces central nervous system arousal or stimulant effects which
closely resemble those of the amphetamines, the
methylenedioxyamphetamines in particular. This is due to the inhibition
by cocaine of re-uptake of the norepinepherine released by the
adrenergic nerve terminals, leading to an enhanced adrenergic
stimulation of norepinephrine receptors. The increased sense of well
being and intense, but short lived, euphoric state produced by cocaine
requires frequent administration.

        Cocaine does not penetrate the intact skin, but is readily absorbed from
the mucus membranes, creating the need to snort it. This accounts for
the ulceration of the nasal septum after cocaine has been snorted for
long periods.
```

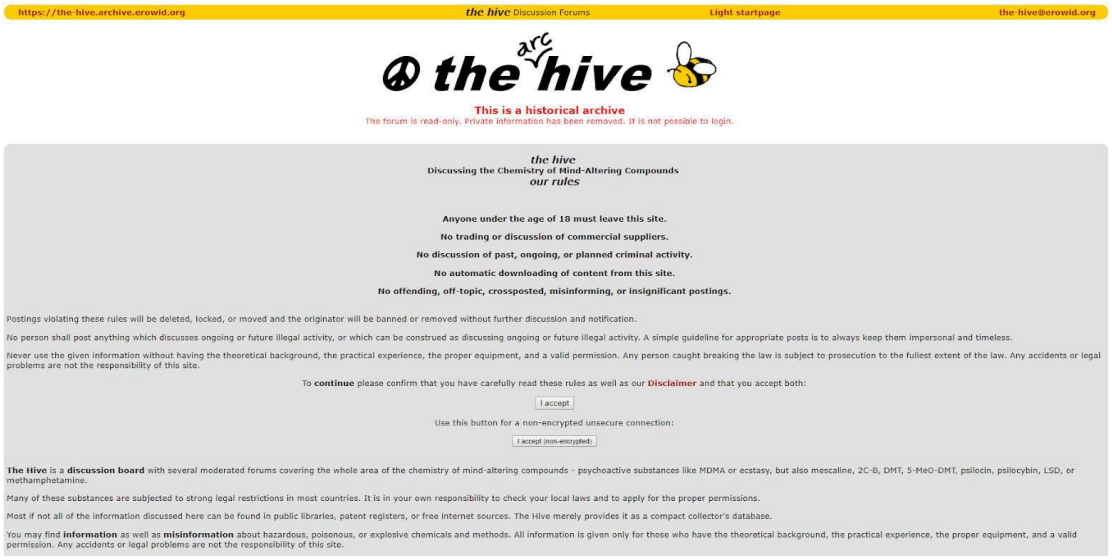
Recette de fabrication de la cocaïne, alt.drugs - 1994 - Wayback Machine

Dans les années 1990, le développement du Web facilite la création et le développement de sites internet. Plus faciles à créer, ils bénéficient également d'une audience bien plus importante que les forums Usenet, jusqu'alors utilisés par une population plus technique et très universitaire. L'arrivée d'Internet permet ainsi au cybercrime de prospérer.

B. *The Hive* et *The Farmer's Market*, précurseurs des forums et marchés noirs de la drogue

Lancé en 1997, le forum *The Hive* reprend une grande partie des sujets de discussion abordés sur *alt.drugs*[24]. Le site est popularisé par les média en 2001, suite à son apparition dans l'émission *The "X" Files*[25] sur la chaîne américaine Dateline NBC, qui conduira à l'arrestation de son administrateur, Hobart Huson, aussi connu sous le pseudonyme de *Strike*.

[24] Cadwalladr Carole, *Drugs 2.0: The Web Revolution That's Changing How the World Gets High by Mike Power,* https://www.theguardian.com/books/2013/may/12/drugs-web-revolution-power-review
[25] O'Neill Howell Patrick, *How the Internet powered a DIY drug revolution*, https://www.dailydot.com/crime/hive-silk-road-online-drug-culture-history



The Hive - Archive hébergée par Erowid

The Hive est par la suite repris par l'administrateur du site *Rhodium.ws*, également spécialisé dans les échanges autour de la drogue et des produits illicites. Suite à des problèmes d'hébergement, le site ferme en 2004.

Menée par la DEA le 21 juillet 2004, l'opération *Web Tryp*[26] permet d'arrêter dix individus impliqués dans la fabrication et la distribution des 'research chemicals', nouvelles drogues de synthèse qui ne sont pas encore documentées ni inscrites dans la législation nationale américaine. Plusieurs sites web (*www.racresearch.com, www.duncanlabproducts.com, www.pondman.nu, www.americanchemicalsupply.com et www.omegafinechemicals.com*) ont ainsi été la cible des autorités américaines.

Le marché noir *The Farmer's Market* marque un tournant très important dans le développement de la cybercriminalité sur le Dark Web. Il s'agit en effet du premier grand marché noir qui passe du clearnet au darknet Tor.[27] Ouvert sous le nom d'*Adamflowers* en 2006 par le néerlandais Marc Peter Willems, il devient un service caché en 2010, date à laquelle il prend le nom de *The Farmer's Market*. Le marché noir met en relation les vendeurs et les acheteurs de substances illicites, prenant une commission sur les ventes de

[26] Drug Enforcement Administration, 2004-07-22, *DEA announces arrests of website operators selling illegal designer drugs*
[27] *US busts online drugs ring Farmer's Market*, https://www.bbc.com/news/world-us-canada-17738207

marchandises, utilisant principalement des paiements passés par Paypal et Western Union via un système de comptes bancaires intermédiaires appelés *cash drops*, localisés au Panama.

Selon la DEA, le site a permit de générer environ 1 million de dollars entre 2007 et 2009 pour plus de 3000 utilisateurs, principalement originaire des Etats-Unis. *The Farmer's Market* sera fermé par les autorités américaines en avril 2012 lors de l'opération *Adam Bomb*[28], menée conjointement par la DEA et les autorités néerlandaises, après plus de deux ans d'investigations.

C. Bulletin Board System et Internet Relay Chat, prémices de la cybercriminalité

Les premiers *Bulletin Board System*, ou systèmes de bulletins électroniques voient le jour à la fin des années 1970[29]. Contrairement à Usenet, les BBS bénéficient d'une architecture centralisée. Tout comme les IRC qui commencent à se populariser à la fin des années 1980, les BBS permettent de communiquer par messages mais également d'échanger des fichiers. Les premiers forums sur le piratage sont bien différents de ce que l'on peut trouver aujourd'hui. Les premiers pirates des années 1980 se concentrent principalement sur la fraude bancaire, les échanges de jeux vidéos et autres fichiers piratés.

Bulletin Board System - 1987

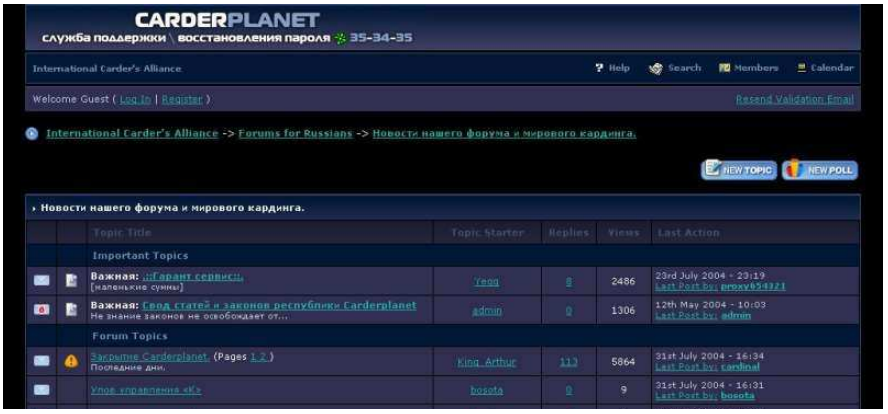
[28] J. Schwartz Mathew, *Feds Bust 'Farmer's Market' For Online Drugs*, https://www.darkreading.com/attacks-and-breaches/feds-bust-farmers-market-for-online-drugs/d/d-id/1103901
[29] Britannica The Editors of Encyclopaedia, *Bulletin-board system*, https://www.britannica.com/technology/bulletin-board-system

D. Premiers forums cybercriminels sur le Web

Le début des années 2000 marque l'avènement des premiers grands forums cybercriminels. Ceux-ci s'articulent principalement autour de la fraude bancaire, aussi appelée carding et de la fraude identitaire (fausses cartes d'identité, passeports et diplômes). Le site *Counterfeit Library* est ainsi créé en 2000 et permet aux faussaires de pouvoir partager leurs produits sur le Web[30]. Il ne s'agit alors pas encore d'un véritable marché noir, le site ne faisant que référencer les faussaires, en évaluant la qualité de leur produit.

Capture d'écran - Counterfeit Library (2004) - Wayback Machine

Le principe de *Counterfeit Library* est repris l'année suivante par le site russophone *CarderPlanet*. En août 2004, il représente plus de 7 000 membres et propose plusieurs milliers de comptes bancaires volés.



CarderPlanet, forum de fraude bancaire russophone - Wayback Machine

[30] Poulsen Kevin, *Kingpin / How One Hacker Took over the Billion Dollar Cyber Crime Underground*, Crown Publishers, 2010

En 2002, suite à une campagne de spamming menée contre *Counterfeit Library*, la communauté de cette dernière décide de migrer vers *ShadowCrew*, alors jeune plateforme qui vient d'ouvrir ses portes[31]. Elle marque un tournant très important dans l'histoire de la cybercriminalité ; il s'agit en effet du premier site dont l'offre se rapproche le plus des grands marchés noirs que l'on peut aujourd'hui trouver sur le Dark Web (drogues, faux papiers, malware, services de piratage et tutoriels).

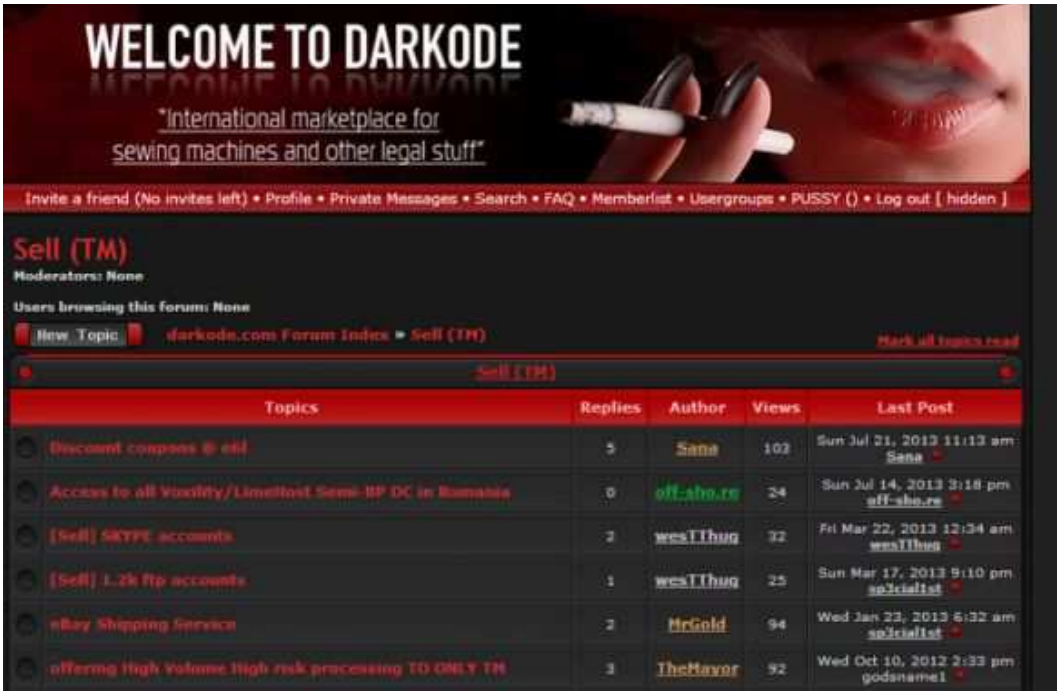
L'administrateur de la plateforme interdit également la diffusion de pédopornographie, interdiction que l'on retrouve aujourd'hui sur de nombreux marchés noirs et forums du Dark Web. Le site était géré par une petite équipe d'administrateurs et par une dizaine de modérateurs qui régulaient les sujets de discussions, reprenant en partie la structure et les membres principaux de *Counterfeit Library*[32].

Forum ShadowCrew - Wayback Machine

Suite à l'arrestation d'un des administrateurs en juillet 2003, l'Electronic Crimes Task Force de l'United States Secret Service, réussi à infiltrer la plateforme. L'opération *Firewall* est ainsi menée pendant plus de 18 mois, conduisant en octobre 2004 à la fermeture du site et à l'arrestation de 28 personnes impliquées[33]. Son administrateur principal, Brett Shannon

[31] Poulsen Kevin, *op.cit., p22*
[32] Ibid
[33] *Busted: The inside story of 'Operation Firewall'*, https://searchsecurity.techtarget.com/news/1146949/Busted-The-inside-story-of-Operation-Firewall

Johnson aussi connu sous le pseudonyme *Gollumfun*, est appréhendé par les autorités l'année suivante pour production de faux chèques. La plateforme est rapidement imitée par d'autres services et sa communauté donnera notamment naissance au forum *Dark0de*, ouvert en 2007.



Forum Dark0de, Wayback Machine

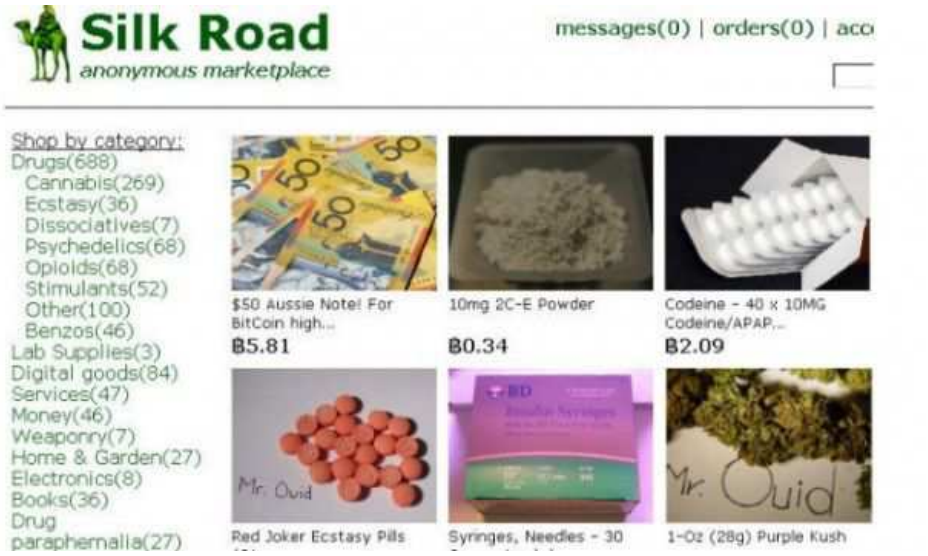
ShadowCrew est aujourd'hui considéré comme l'ancêtre des forums de piratage et des marchés noirs. Le journaliste Kevin Poulsen, dans son enquête Kingpin, décrit *ShadowCrew* comme étant le premier marché noir international[34] :

> "*Un voleur d'identité de Denver pouvait acheter des numéros de carte de crédit à un hacker moscovite, les envoyer à Shanghaï pour qu'ils soient transformés en cartes contrefaites, puis se procurer un permis de conduire auprès d'un faussaire ukrainien avant d'aller faire un tour au centre commercial"*.

[34] Poulsen, Kevin *op.cit., p22*

E. Popularisation et médiatisation du darknet Tor - naissance du Dark Web

Ouvert en février 2011 par l'américain Ross Ulbricht sous le pseudonyme de *Dread Pirate Roberts*, le marché noir *Silk Road* bouleverse le développement de la cybercriminalité sur le Dark Web, contribuant notamment à la popularisation du darknet Tor et des marchés noirs dans les média. En effet, dès juin 2011, le blog populaire américain *Gawker* publie un article sur *Silk Road*[35]. Cette première médiatisation conduit à une forte augmentation du trafic du marché noir. Quelques années plus tard, en octobre 2013, la fermeture de *Silk Road* par le FBI renforce cette forte médiatisation. Selon le site d'information *DeepDotWeb*, la fermeture du site est considérée comme '*la plus belle publicité dont les marchés noirs auraient pu rêver*".[36]



Marché noir Silk Road -

Comme nous l'avons étudié précédemment, *Silk Road* n'est pas le premier marché noir à avoir utilisé le réseau Tor. Ross Ulbricht s'était en effet inspiré de *The Farmer's Market*, ouvert deux ans auparavant sur Tor. *Silk Road* est également présent sur le darknet I2P, bien qu'il n'y bénéficie pas d'une forte audience. La fermeture de *Silk Road* permet de faire connaître les marchés noirs au grand public et popularise le terme "Dark Web", afin de

[35] Chen Adrian, *The Underground Website Where You Can Buy Any Drug Imaginable*, https://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160
[36] Deepdotweb, *Silk Road And Beyond, https://www.deepdotweb.com/2014/10/17/silk-road-beyond/*

désigner la face sombre d'Internet, où se cachent les cybercriminels pour échanger sur les forums et les marchés noirs. On assiste néanmoins à une forte confusion entre le terme Dark Web et darknets dans les média, ce qui contribue à la propager dans les croyances populaires. Le Dark Web devient alors sujet à fantasmes, souvent confondu avec les darknets et le deep web, termes jusque là peu utilisés.

Par ailleurs, les révélations d'Edward Snowden contribuent à la croissance du darknet Tor. L'ancien analyste de la NSA conseille en effet d'utiliser le réseau en routage onion afin de préserver l'anonymat. La croissance exponentielle du nombre d'utilisateurs de Tor provoque alors une forte accélération du réseau, qui tire sa puissance de son nombre d'utilisateurs.

Chapitre 2 : Une accessibilité et une navigation de plus en plus facile pour les cybercriminels novices

La structure du Dark Web est complexe à aborder du fait de sa nature et de son contenu. Les sites présents sur le Dark Web ne sont en effet pas référencés par les moteurs de recherche classiques. A ses débuts, les hiddens services du darknet Tor restent difficiles d'accès et sont principalement utilisés par des individus bénéficiant déjà de compétences techniques. Suite à la forte médiatisation subie par le marché noir *Silk Road*, le Dark Web fait désormais l'objet de nombreux fantasmes et de discussions sur les forums. De nombreux sites spécialisés ont été développées, afin de répertorier les *hiddens services*, pour qu'ils soient accessibles au plus grand nombre.

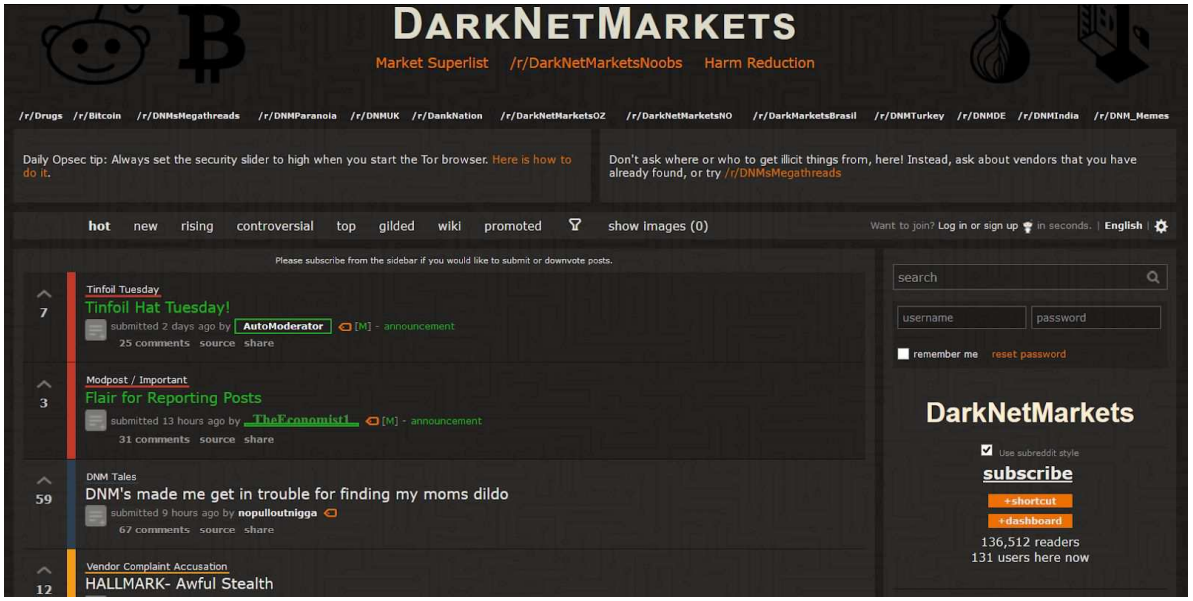
Le développement de la cybercriminalité a grandement été favorisé par l'accessibilité facile aux principaux marchés noirs et forums cybercriminels. Le clear web fait désormais office de vitrine principale pour le Dark Web. Les hiddens wikis et moteurs de recherche, de plus en plus nombreux, permettent de faciliter l'accès aux plateformes cybercriminelles.

A. Clear Web et sites spécialisés

Le clear web fait office de vitrine pour les forums et marchés noirs du Dark Web. Une communauté d'utilisateurs des marchés noirs très importante se forme sur la plateforme *Reddit*, peu après la création de Silk Road sur Tor, permettant notamment aux vendeurs de bénéficier de publicité. Les sites spécialisés comme *Deepdotweb* et *Darkwebnews* apparaissent plus tard, en 2013 et 2014 et contribuent au développement de la communauté, notamment en notant et répertoriant les marchés noirs, mais également en diffusant des informations liées à la communauté, ainsi que des tutoriaux pour accéder au Dark Web en tout anonymat.

1. Reddit et naissance d'une importante communauté de darknautes sur le clear web

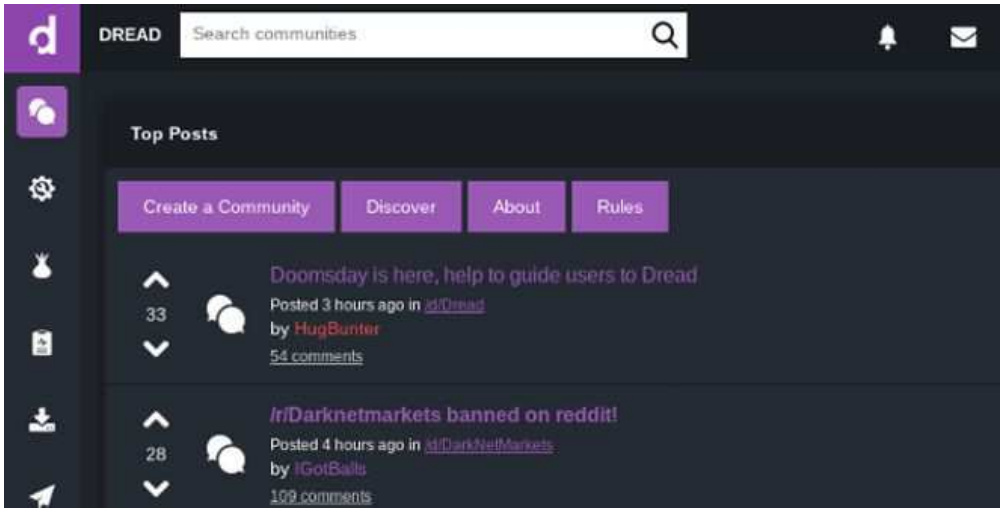
Fondée en 2005, la plateforme *Reddit* reprend le principe des premiers BBS et des forums Usenet : un forum organisé en plusieurs sous forums et sujets de discussions portant sur l'actualité et les grandes tendances du moment. La très forte exposition du Dark Web dans les média suite à la fermeture du marché noir *Silk Road* contribue à développer et agrandir les discussions autour du Dark Web et des marchés noirs. Ces groupes vont jusqu'à réunir plusieurs dizaines de milliers de membres.[37]



DarkNetMarkets, ancien forum Reddit dédié aux échanges autour des marchés noirs

[37] Brackett Eric, *Reddit Bans Communities Dedicated to Illegal Goods*, https://www.digitaltrends.com/social-media/reddit-bans-illegal-communities/

Les utilisateurs y échangent alors des adresses de *hidden services* et des commentaires et retours sur les produits vendus sur les marchés noirs. Reddit contribue ainsi à la démocratisation et à l'accessibilité des sujets autour du Dark Web, formant une grande communauté d'initiés de plusieurs dizaines de milliers de membres. La plus grande communauté, organisée autour du sous forum *DarkNetMarkets* est cependant fermée par la plateforme en mars 2018, l'administration du site considérant que les discussions ne respectent pas les conditions d'utilisation de la plateforme[38]. La communauté du sous-forum *DarkNetMarkets* se déplace vers la plateforme *Dread*, véritable clone de Reddit sur Tor[39].



Plateforme Dread, clone de Reddit sur le Dark Web - Capture d'écran

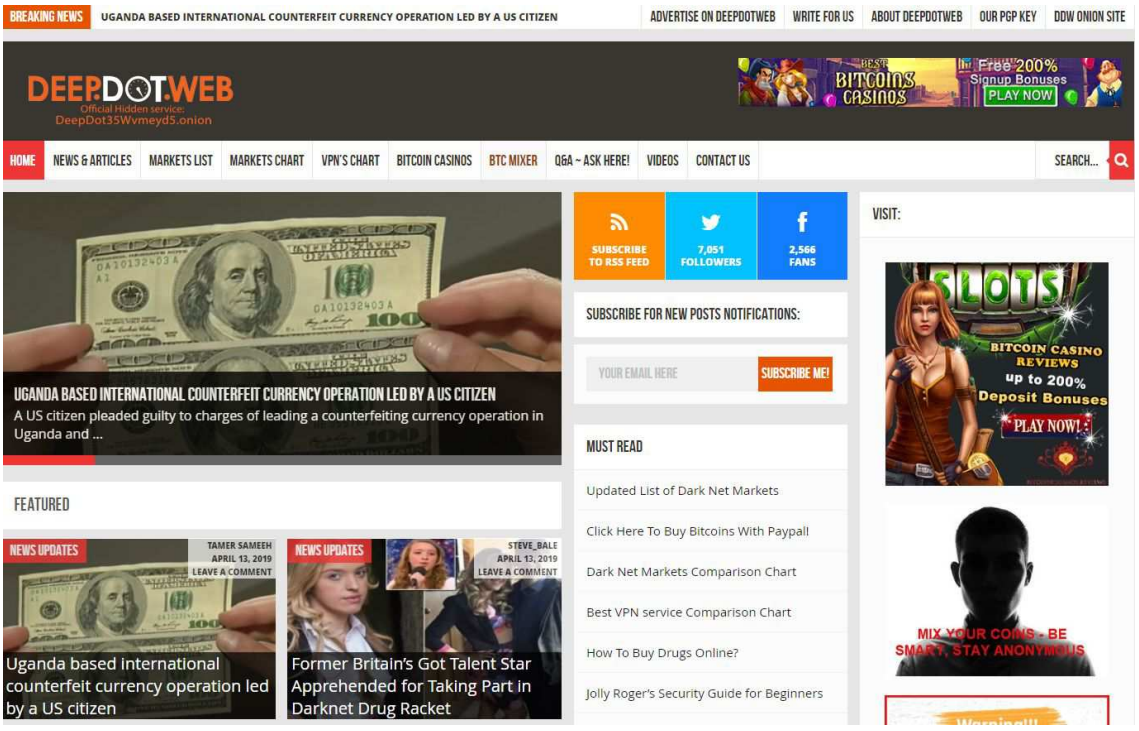
Malgré la fermeture du sous-forum sur Reddit, on peut néanmoins trouver aujourd'hui d'autres sous-forums traitant des marchés noirs et des *hiddens services* qui n'ont pas encore été fermés par l'administration. Reddit contribue ainsi fortement à la démocratisation et au partage des informations sur le clear web, contribuant à développer une communauté autour des marchés noirs et de la cybercriminalité très importante.

2. Plateformes spécialisées et actualités autour du Dark Web

L'accessibilité est par la suite renforcée suite à la naissance de plateformes spécialisées autour du Dark Web comme *DeepDotWeb* en 2013 et *DarkWebNews* l'année suivante. Ces sites font office d'annuaires de hiddens services, référençant les marchés noirs et les forums

[38] Brackett Eric, op. cit., p27
[39] *R/RedditAlternatives - Dread*, https://www.reddit.com/r/RedditAlternatives/comments/b34ciy/dread/

actifs. Les utilisateurs peuvent y noter les plateformes et y laisser des avis. Véritables sites journaux de la communauté darknaute, on peut y trouver les dernières actualités sur le Dark Web ; dernières fermetures des marchés noirs, arrestations récentes par les autorités, nouveaux marchés noirs..



Capture d'écran - DeepDotWeb.com

On y trouve également de nombreux tutoriaux gratuits, permettant aux néophytes d'apprendre rapidement à se connecter sur le darknet Tor et d'y acheter des produits en toute sécurité, allant même jusqu'à faire la promotion de services VPN, afin de pouvoir cacher leurs adresses IP. Ces sites référencent ainsi les 'bonnes pratiques' pour se connecter et évoluer sur le Dark Web.

Mardi 7 mai 2019, *DeepdotWeb* est fermé lors d'une opération internationale, menée conjointement par le FBI et Europol. Le site aurait en effet rapporté plusieurs millions de dollars à ses administrateurs depuis sa création, en faisant de la publicité pour des marchés

noirs.[40] Plus disponible sur le clear web, il affiche cependant un message du FBI, “This site has been seized” sur sa version hébergée sur Tor.

Capture d’écran - version hébergée sur Tor - deepdotweb

B. Développement des moteurs de recherche et des hidden wikis : le Dark Web de plus en plus accessible pour les cybercriminels novices

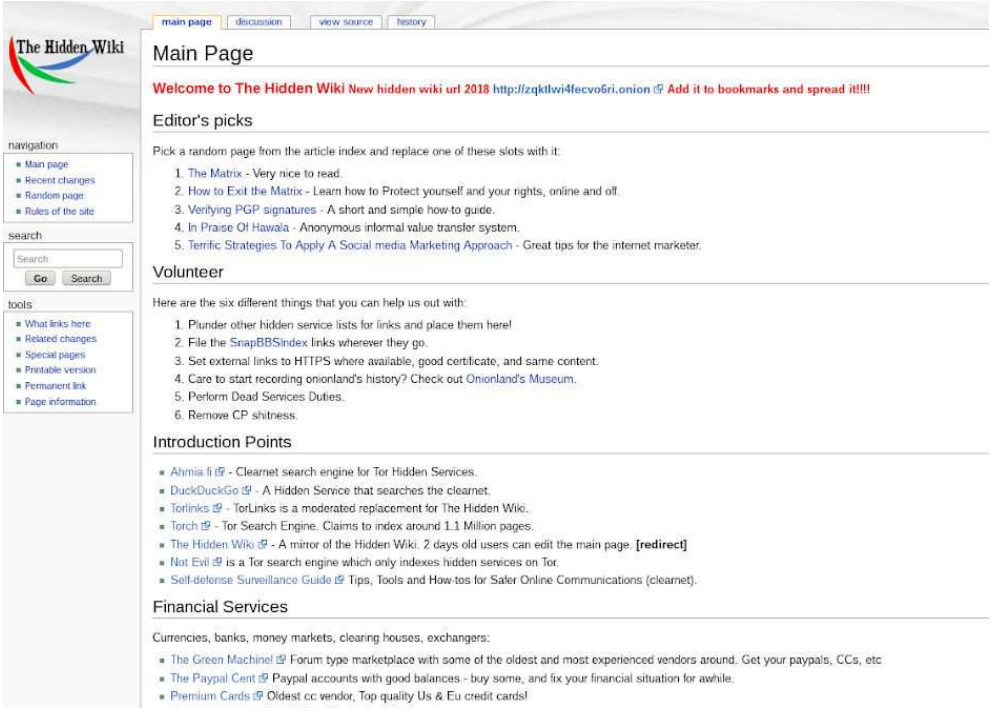
Lors de la création de *Silk Road* en 2011, le Dark Web ne bénéficie pas de moteur de recherche. Il est donc nécessaire d’accéder à un annuaire qui répertorie les *hidden services*, nommé *hidden wiki*. Les moteurs de recherche apparaissent deux ans plus tard. Bien qu’ils ne soient que très limités, ils constituent une passerelle importante pour les utilisateurs novices qui se rendent pour la première fois sur Tor.

1. Les hiddens wikis

Les Hiddens Wikis sont de véritables annuaires Dark Web dont les liens sont disponibles sur le clear web sur des sites grands publics, type *Deepdotweb* ou *Darkwebnews*. Beaucoup de *hiddens wikis* possèdent une version sur le clear web, accessible directement depuis Google et

[40]Timesofisrael, *Two Israelis arrested in international dark web takedown involving FBI*, https://www.timesofisrael.com/two-israelis-arrested-in-international-dark-web-takedown-involving-fbi

une autre sur le réseau Tor. Ils ne référencent cependant que les principaux services du réseau Tor (marchés noirs et forums), voire parfois même des *scams*, faux services ayant pour but d'arnaquer leurs utilisateurs.



Capture d'écran - Page d'accueil du Hidden Wiki anglophone

2. Les moteurs de recherche spécialisés

Les moteurs de recherche spécialisés ne permettent d'avoir accès qu'à une très faible partie du contenu et ne peuvent indexer que peu de sites. En effet, l'indexation des contenus du Dark Web pose un problème technique et juridique.

La plupart des plateformes sur le Dark Web nécessitent une authentification, posant ainsi un problème technique. Il sera donc nécessaire d'effectuer un travail d'infiltration afin d'obtenir un compte sur lesdites plateformes. Le crawling devient ainsi plus complexe et n'est aujourd'hui pas abordé par les moteurs de recherche publics. Les entreprises de renseignement privées commencent aujourd'hui à s'équiper de crawlers permettant de passer les captchas et de s'authentifier sur les plateformes à l'aide d'identifiants obtenus suite à un processus d'infiltration. L'indexation des contenus soulève également un problème juridique.

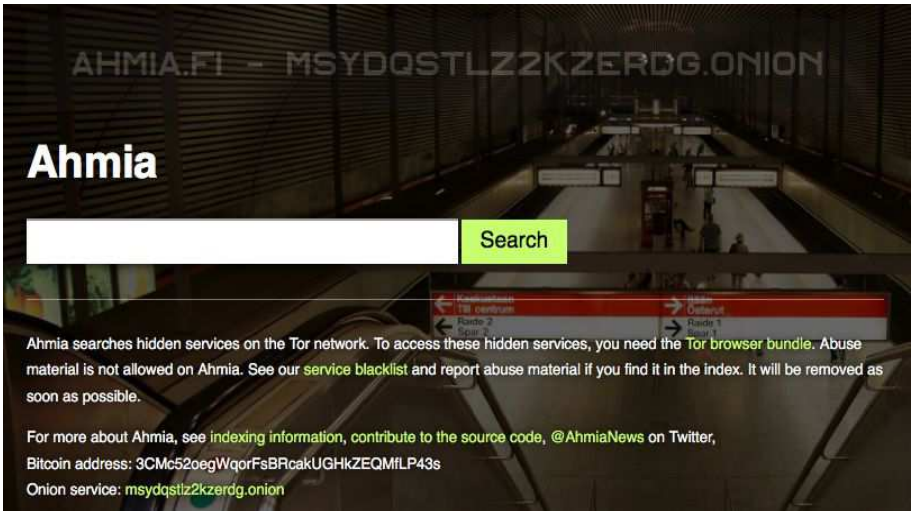
Les crawlers téléchargent un ensemble de données qui sont par la suite triées et indexées. Ces données contiennent des contenus à caractère pédopornographique dont la détention est strictement illégale.

Ces deux enjeux réduisent ainsi fortement les tentatives d'indexation du Dark Web, laissant le sujet à des services de renseignements et aux entreprises de renseignement privées. Le développement de l'intelligence artificielle et la qualification automatique des données récupérées par les crawlers pourrait ainsi constituer une avancée certaine dans l'indexation du Dark Web. Les moteurs de recherche accessibles gratuitement sont ainsi limités – *Ahamia* - ou dans l'illégalité (*NotEvil, Candle, Torch, Haystack*).

Ahmia

Le moteur de recherche *Ahmia* est un projet open source, développé par le chercheur finlandais Juha Nurmi et disponible sur le site de partage de code *Github*. C'est le seul moteur de recherche actuellement disponible sur le clearnet, permettant à la fois de requêter sur le réseau Tor, mais également sur le réseau I2P.

Comme expliqué précédemment, la plupart des moteurs de recherche orientés Dark Web sont illégaux. *Ahmia* est en effet doté d'une *blacklist,* indiquant à son algorithme de recherche de ne pas se rendre sur les sites à contenu pédopornographique. Développé en Python, le moteur de recherche utilise le framework (à définir en bas de page) Scrapy. Très populaire et utilisé par de nombreux développeurs, Scrapy offre une prise en main très rapide à ses utilisateurs.



Capture d'écran - Moteur de recherche Ahmia

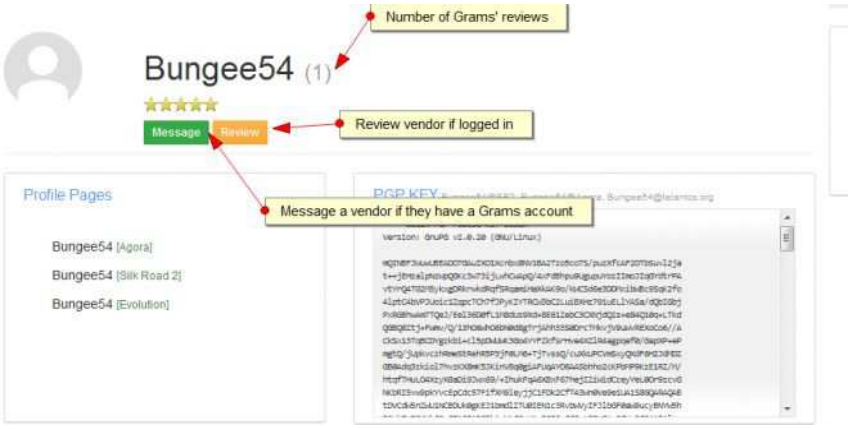
Ahmia ne permet malheureusement pas de se connecter sur les plateformes qui nécessitent une authentification. Il n'indexe ainsi qu'une faible partie du Dark Web. Par ailleurs, les annuaires sur lesquels s'appuient son algorithme sont bien plus orientés sur du contenu anglophone. On fait ainsi face à un moteur de recherche qui peut s'avérer parfois très limité.

Grams

Aux allures de *Google*, le moteur de recherche *Grams* reste un cas très particulier dans l'histoire de Tor. Créé en 2014 par un utilisateur anonyme prénommé *gramsdmin*, *Grams* reste longtemps le moteur le plus utilisé par les cybercriminels utilisateurs du réseau Tor et a permi de grandement faciliter l'accès aux marchés noirs.[41]

Moteur de recherche Grams - deepdotweb.com

En plus de pouvoir effectuer des recherches, le moteur référençait les produits des grands marchés noirs. Via son service *InfoDesk*, il était possible d'avoir accès aux profils des vendeurs sur les marchés noirs, permettant ainsi de vérifier la qualité de leurs produits ainsi que leur réputation.



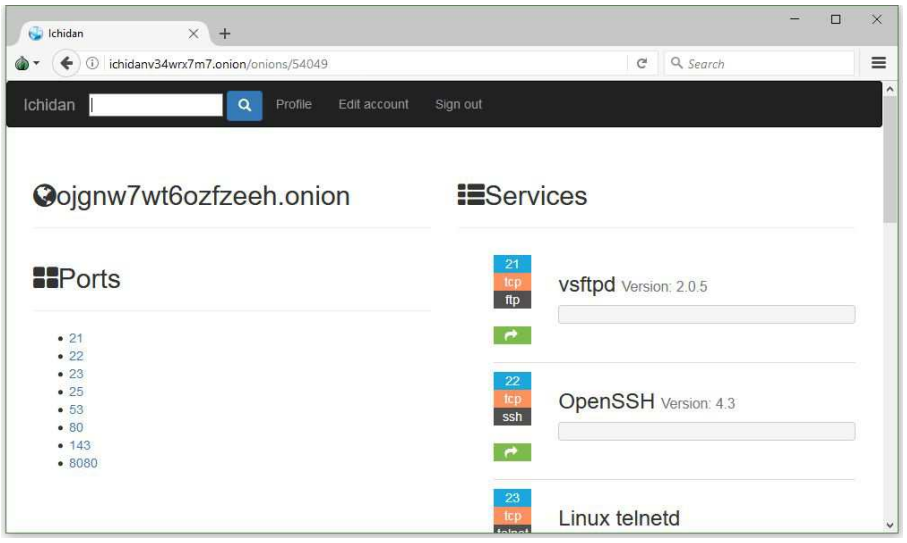
Exemple d'un ancien profil de vendeur - deepdotweb

[41] DeepDotWeb, *"Gramwords" Launched: Google Adwords Of The DeepWeb", http://www.deepdotweb.com/2014/06/01/gramwords-launched-google-adwords-of-the-deepweb*

Ce service sera complété par *Helix*, service de mixage de bitcoins, qui offrait aux acheteurs l'anonymisation des transactions effectuées en bitcoin. *Grams* a été fermé par son administrateur en décembre 2017 sans raison apparente[42]

Helix, ancien service d'anonymisation de Bitcoins

Le moteur de recherche *Ichidan* marque également un tournant dans l'historique des moteurs de recherches orientés Dark Web. Disponible entre septembre et décembre 2017, *Ichidan* reprenait le principe du moteur de recherche *Shodan*, en référençant le résultat de balayages de ports effectués sur le réseau Tor[43].

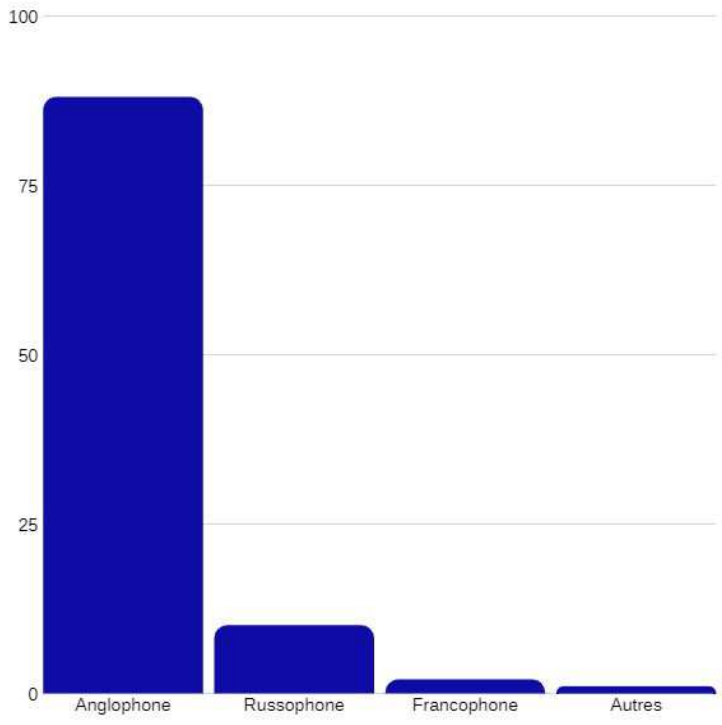


Ancien moteur Ichidan

[42]Stone Zara, Forbes, *Grams, The Google Of The Dark Web Has Shuttered Operations*, https://www.forbes.com/sites/zarastone/2017/12/16/grams-the-google-of-the-dark-web-has-shuttered-operations
[43]Cimpanu Catalin, *Ichidan Is a Shodan-Like Search Engine for the Dark Web*, https://www.bleepingcomputer.com/news/security/ichidan-is-a-shodan-like-search-engine-for-the-dark-web

Partie 2 : La place des plateformes de vente et des forums dans le développement de la cybercriminalité.

On trouve aujourd'hui deux grandes catégories de plateformes de vente sur le Dark Web : les marchés noirs, véritables hypermarchés allant jusqu'à plusieurs dizaines de milliers de produits proposés par des milliers de membres et les autoshops, plateformes personnelles n'appartenant qu'à un seul vendeur. Les marchés noirs reprennent aujourd'hui les principes posés par *Silk Road* en février 2011 ; l'utilisation du système d'escrow et du Bitcoin. Dans cette partie, nous présenterons une brève histoire des marchés noirs anglophones, qui représentent plus de 70% du contenu présent sur Tor. La communauté russophone est la seconde, suivie par les communautés européennes, latino-américaines et asiatiques, qui sont bien plus marginales. Nous nous pencherons également sur le rôle des forums dans le développement du malware as a service, qui permet au piratage de se démocratiser aujourd'hui.



Proportion des communautés sur le Dark Web selon les langues - données exportées depuis Wotan sur un dataset de 6 200 sites - mars 2019

Chapitre 1 : Marchés noirs anglophones, de *Silk Road* à *Dream Market* (2011-2019)

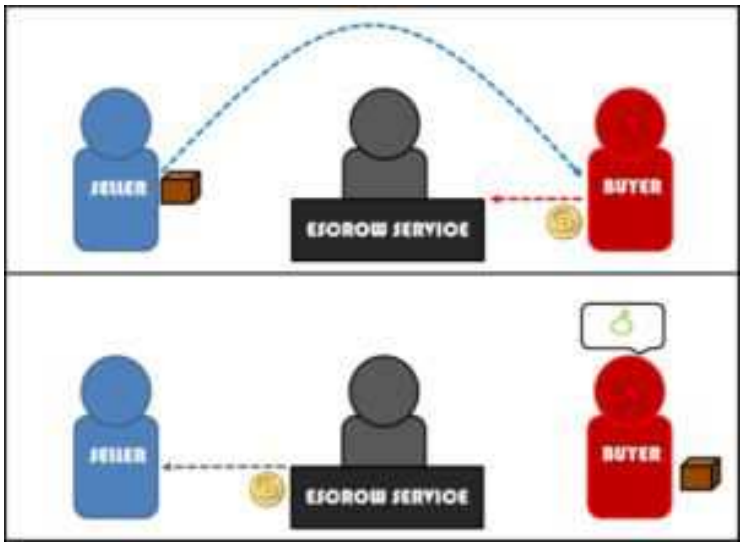
A sa création en janvier 2011, le marché noir *Silk Road* ne possède aucune concurrence. Le réseau Tor n'est alors que peu connu du grand public et les marchés noirs peu développés sur les darknets. *Black Market Reloaded*, son premier concurrent, est créé en juin 2011, mais ne reste que minoritaire face à l'hégémonie de *Silk Road* sur le Dark Web. A sa fermeture en octobre 2013, bien qu'il soit le principal marché noir, il est néanmoins suivi par trois autres plateformes. A travers l'évolution du Dark Web cette dernière décennie, on retrouve presque toujours ce même schéma ; un marché noir presque hégémonique, suivi de deux ou trois autres marchés noirs qui récupèrent ses parts de marché lors de la chute de ce dernier.

Nous étudierons ainsi quatre périodes principales au cours de cette analyse : la période *Silk Road*, qui s'étend de janvier 2011 à octobre 2013, l'ère post *Silk Road*, de 2014 à 2015, la domination d'*Alphabay*, de 2015 à juillet 2017 et enfin celle de *Dream Market*, de juillet 2017 à avril 2019.

A. Un fonctionnement qui découle de *Silk Road* : escrow et cryptomonnaies

Comme nous l'avons étudié précédemment, *Silk Road* n'était pas le premier marché noir à avoir fait son apparition sur le darknet Tor. Il a cependant été le premier à proposer un système d'*escrow* utilisant une crypto-monnaie alors encore peu connue : le Bitcoin. Bien qu'ayant été fermé en octobre 2013 par le FBI, son influence a été très importante sur le développement des marchés noirs et l'est encore aujourd'hui.

Le marché noir *Silk Road* popularise le système d'escrow, qui permet aux acheteurs d'éviter les arnaques (scams), où le vendeur récupère l'argent donné par l'acheteur sans lui envoyer le produit acheté. Le système d'escrow place donc un tier de confiance dans la transaction, qui reçoit l'argent de l'acheteur lors de la transaction afin de le donner au vendeur une fois le produit reçu.



Système d'escrow - CEIS

Ce système est fondé sur l'honnêteté du tier de confiance, qui fait partie de l'équipe administratrice du marché noir. Le système d'escrow engendre ainsi malheureusement parfois un *exit scam*, lorsque le tier de confiance garde l'ensemble des transactions en cours et quitte le marché noir. Ce type d'arnaque a été la cause de la fermeture de nombreux marchés noirs très importants, notamment celle du marché noir *Evolution* en 2015.

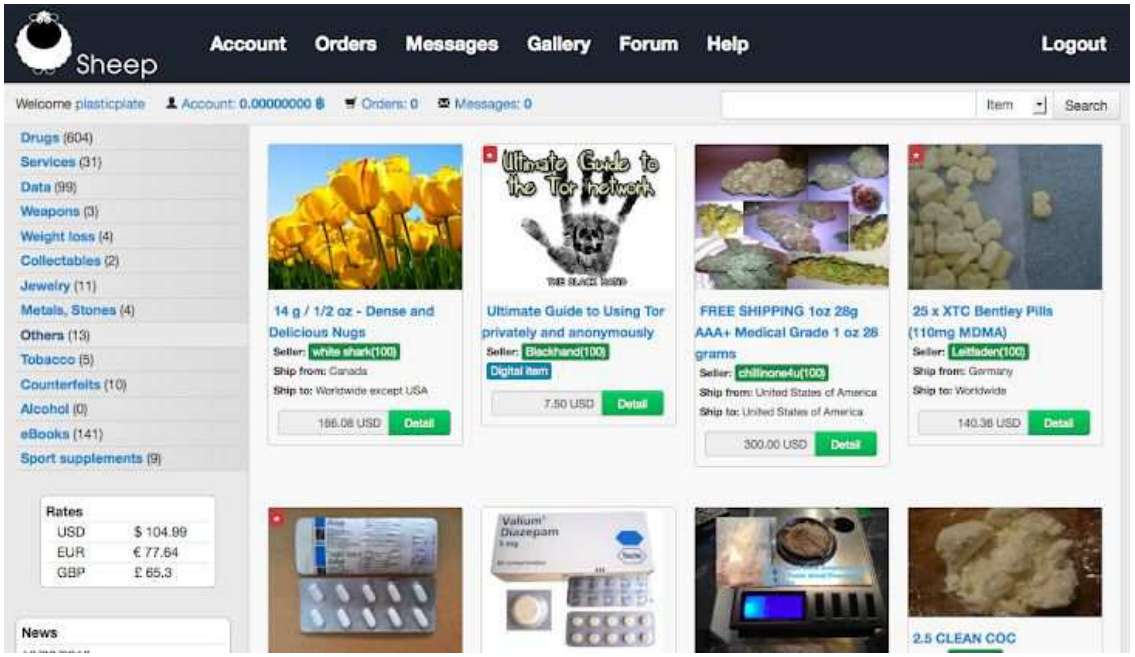
Silk Road est également le premier marché noir à utiliser une crypto-monnaie comme moyen de paiement, le Bitcoin, permettant à ses utilisateurs de pouvoir rester anonymes au cours des transactions.

1. Emergence de la concurrence

Le succès de *Silk Road* pousse d'autres cybercriminels à se lancer dans la création de marchés noirs. Le marché noir *Black Market Reloaded* est créé en juin 2011, soit six mois après l'ouverture de *Silk Road*, reprenant les mêmes caractéristiques que ce dernier. Il reste cependant moins important que son prédécesseur, totalisant environ 4 500 membres, contre plus de 50 000 pour *Silk Road* en 2013. Il s'en démarque néanmoins en proposant la vente d'armes à feu.

Tous deux restent les principaux marchés noirs anglophones jusqu'en mars 2013, date de la création d'*Atlantis* et de *Sheep Marketplace*. Afin de faire face à la concurrence, *Atlantis* est le premier marché noir à accepter une autre crypto-monnaie que le Bitcoin, le Litecoin. A sa

fermeture en octobre 2013, *Silk Road* a alors quatre concurrents principaux : *Black Market Reloaded*, *Sheep Marketplace*, *Atlantis* et *Deepbay*.



Marché noir Sheep Marketplace

B. La fin de *Silk Road*, marquée par la peur des arrestations et les exits scams

La fermeture du marché noir *Silk Road* en octobre 2013 bouleverse le milieu des marchés noirs sur le Dark Web. Les utilisateurs de cette plateforme se rabattent ainsi vers les marchés noirs secondaires, augmentant ainsi le trafic de transactions. Les administrateurs d'*Atlantis*, de *Sheep Market Place* et de *Deepbay* arrêtent leurs activités, tout en conservant les fonds déposés par les acheteurs, de plus en plus importants sur ces marchés noirs depuis la fermeture de *Silk Road*. Ce sont les premiers exit scams de l'histoire du Dark Web. Ces trois fermetures entraînent un flux très important d'utilisateurs vers *Black Market Reloaded*, qui ne tient pas le coup et ferme ainsi ses portes en décembre 2013.

C. Ere-Post *Silk Road* (2014 - 2015) : héritiers et exit scams

La fermeture de Silk Road est ainsi accompagnée par celle des principaux autres marchés noirs du Dark Web. D'anciens membres des équipe d'administration et de modération choisissent alors de lancer leur propres marchés noirs. Cette période est également marquée par d'importants exit scams, causant la fermeture des principaux marchés noirs.

1. Silk Road 2.0 et *Utopia*, marchés noirs créés à partir d'anciennes équipes de modération de *Silk Road* et de *Black Market Reloaded*

La fin de l'année 2013 est ainsi marquée par de nombreuses fermetures de marchés noirs. Face à un besoin une demande très importante et une communauté inquiète de la fermeture des plateformes de vente principales, on assiste à une vague importante de création de nouveaux marchés noirs, qui reprennent les communautés qui s'étaient organisées précédemment. Dès le 6 novembre 2013, soit quelques semaines seulement après la fermeture de *Silk Road*, d'anciens administrateurs de la plateforme, menés par un nouveau *Dread Pirate Roberts*, ouvrent *Silk Road 2.0*, qui reprend la structure du site original, tout en y améliorant la sécurité, comme l'explique l'ancien modérateur *Synergy* :

> "*Silk Road 2.0 will be reborn better, much much more secure as testament to the tenacity and determination of this wonderful community of ours*".[44]

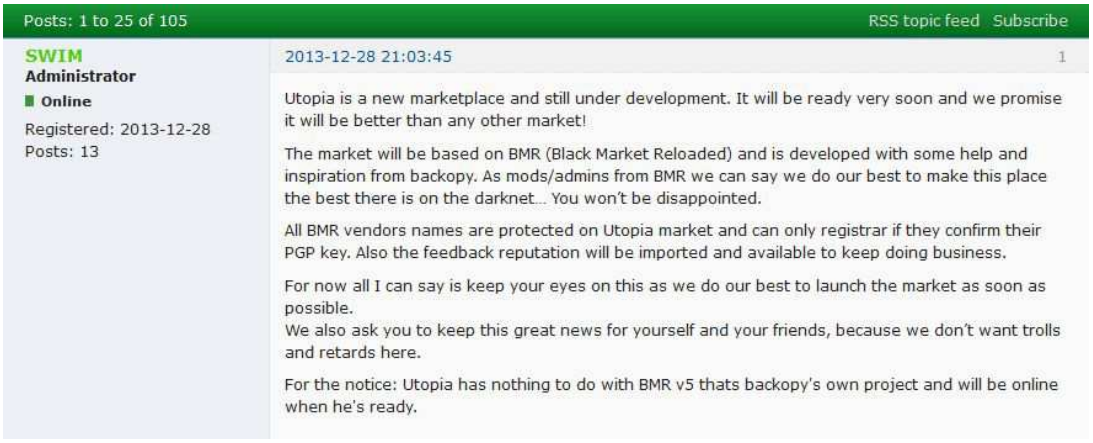
Silk Road 2.0 connaît des débuts chaotiques, avec l'arrestation de deux de ses principaux administrateurs, *Libertas* et *Inigo*, le 20 décembre 2013. En février 2014, la plateforme est également victime d'une faille de sécurité dans le protocole de paiement Bitcoin, appelée "transaction malleability". Cette vulnérabilité est exploitée par un pirate qui vole les bitcoins stockés par la plateforme, pour une somme évaluée à plus de 2.7 millions de dollars. Le 6 novembre 2014, l'opération *Onymous*[45], menée conjointement par le FBI et Europol met fin aux activités de *Silk Road 2.0* en arrêtant le principal administrateur de la plateforme, Blake Benthall, connu sous le pseudonyme de *Defcon*. Dès sa fermeture, le marché noir *Diabolus*

[44]Greenberg Andy, *'Silk Road 2.0' Launches, Promising A Resurrected Black Market For The Dark Web*, https://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web

[45]*Operation Onymous*, https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-onymous

Market est rebaptisé par ses administrateurs *Silk Road 3.0*, afin de reprendre l'image de marque du premier marché noir.

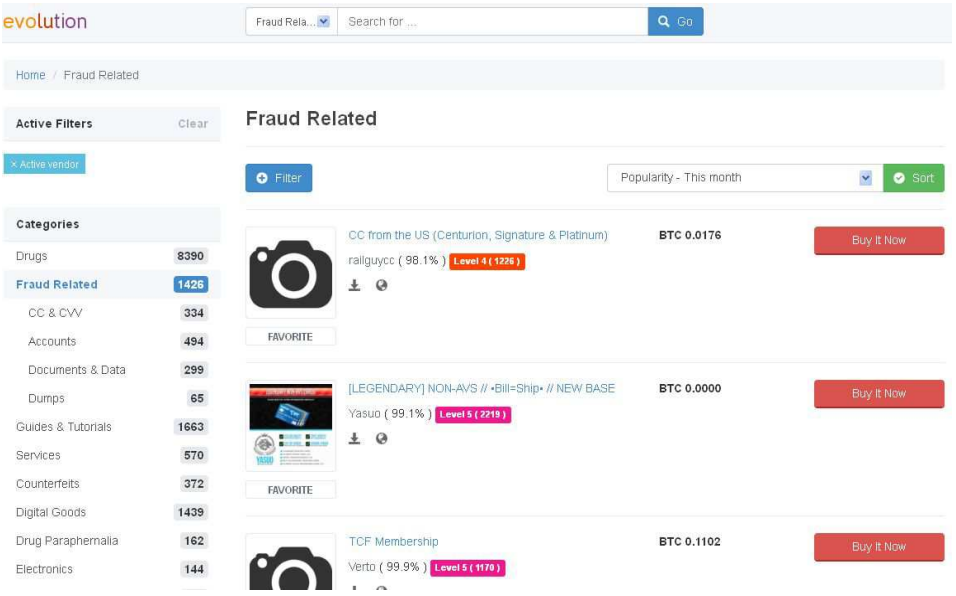
Le marché noir *Utopia* est créé par l'équipe modératrice de *Black Market Reloaded* dès la fin du mois de décembre 2013, comme l'explique un message posté par son administrateur sur la plateforme le 28 décembre 2013.



Message posté sur Utopia par SWIM, administrateur du marché noir, 28 décembre 2013

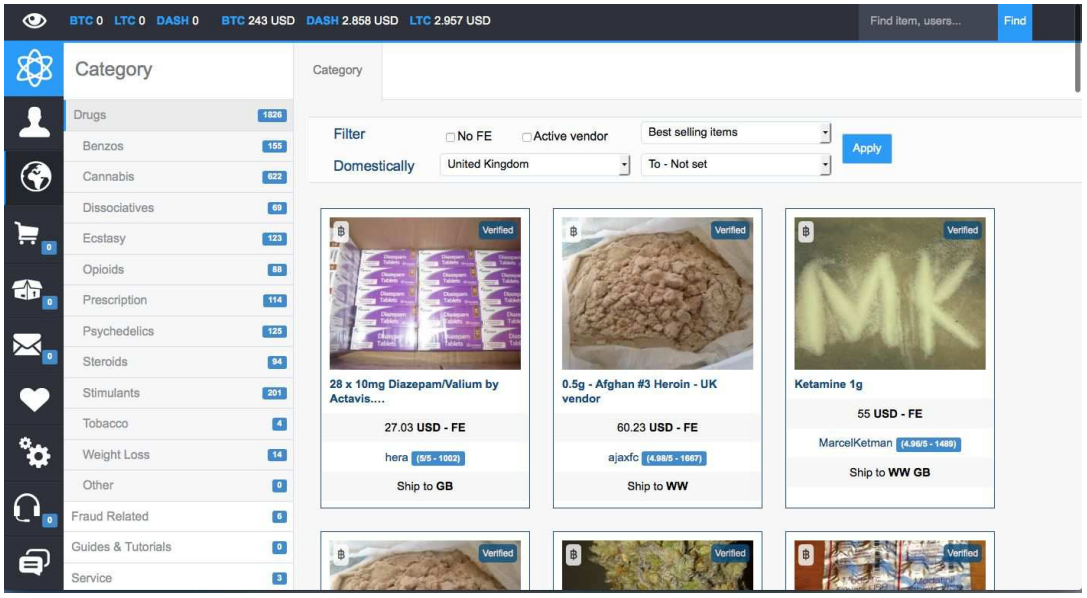
2. Agora et *Evolution*, principaux marchés noirs entre 2014 et 2015

La fermeture de *Silk Road 2.0* entraîne le flux d'utilisateurs des marchés noirs vers *Agora*, déjà fortement développé depuis décembre 2013 et *Evolution*, créé en janvier 2014. Ces deux marchés noirs ne sont pas touchés par les arrestation de l'opération *Onymous*, qui touchent leurs principaux concurrents. Ils s'imposent rapidement comme leaders, devant un nombre très importants de plus petites plateformes secondaires (*Pandora*, *Nucleus*, *Middle Earth*, *Abraxas*…).

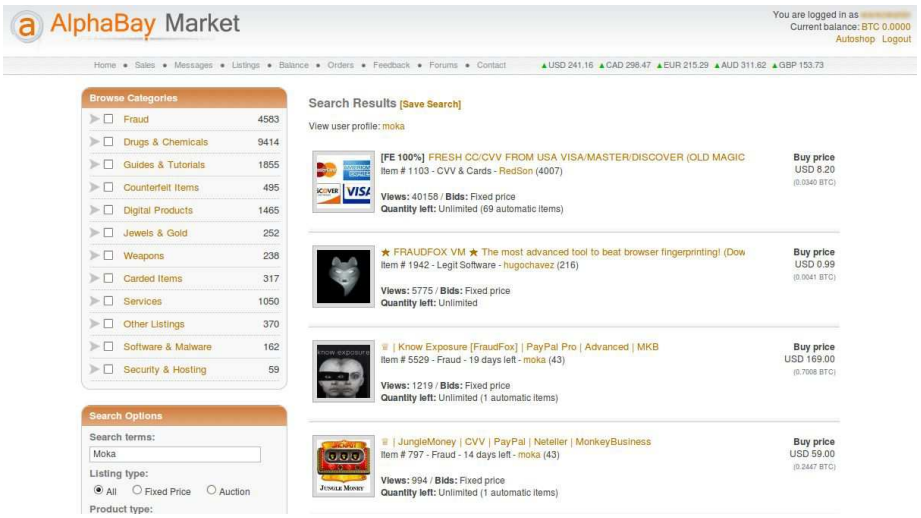


Marché noir Evolution

La fermeture d'*Evolution* est causée par un exit scam en mars 2015, aujourd'hui toujours considéré comme le plus important de l'histoire du Dark Web, s'élevant à plus de 12 millions de dollars. Ses parts de marché sont rapidement reprises par deux jeunes plateformes, *Nucleus* et *Alphabay*, ouvertes respectivement en octobre 2014 et en décembre 2014, et qui s'imposent peu à peu comme grandes remplaçantes d'*Evolution*.



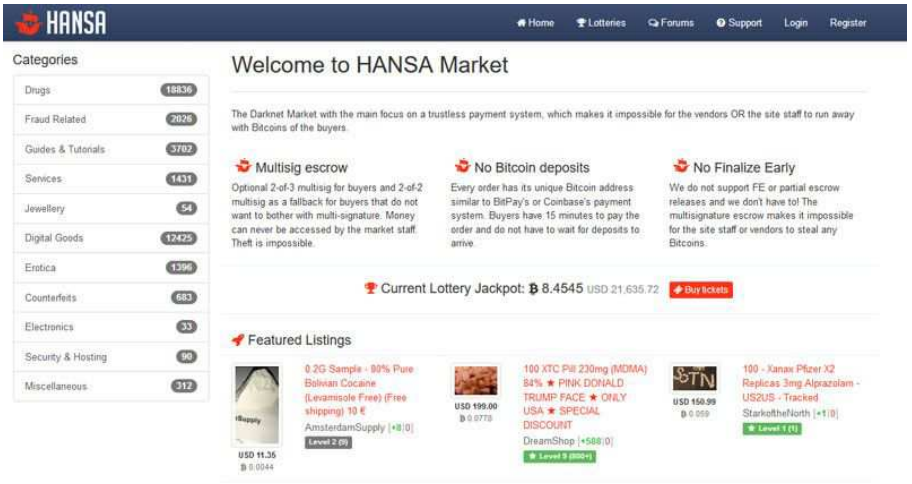
Marché noir Nucleus



Marché noir Alphabay

D. L'Hégémonie d'*Alphabay*, suivi par *Hansa* et *Dream Market* (2015 - 2017)

Le marché noir *Agora* ferme ses portes en début septembre 2015, suite à un message de son administrateur publié en août, expliquant que la plateforme allait progressivement arrêter son activité notamment à cause des tentatives de désanonymisation du réseau Tor. *Nucleus* disparaît en avril 2016, sans raison apparente donnée par ses administrateurs ni exit scam. Les utilisateurs d'*Agora* et de *Nucleus* se reportent ainsi vers *Alphabay*, qui devient alors la principale plateforme devant *Hansa* et *Dream Market*, deux plateformes qui bénéficient toutefois d'une petite communauté solide depuis leur création en 2013 et 2014.

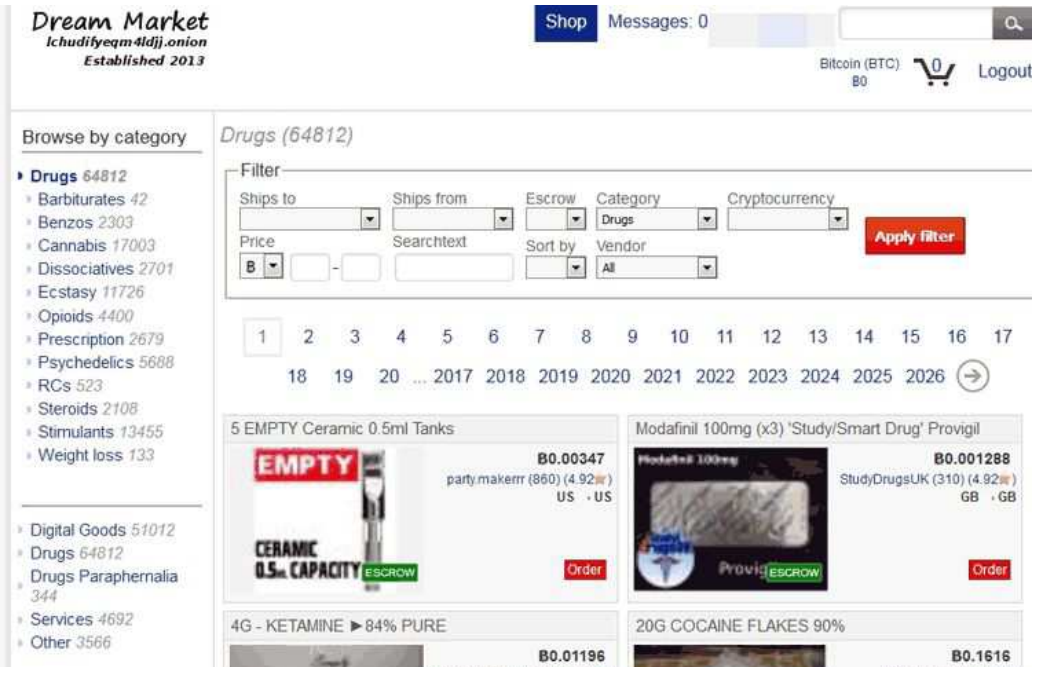


Marché noir Hansa

Alphabay reste la principale plateforme de vente pendant plus de deux ans, jusqu'à sa fermeture en juillet 2017 lors de l'opération *Bayonet*, menée par le FBI, Europol et la police néerlandaise[46]. L'opération *Bayonet* provoque également la chute du marché noir *Hansa*, quelques semaines après *Alphabay*. Les autorités avaient pris le contrôle d'*Hansa* dès juin 2017 et ont pu analyser le trafic du marché noir lorsque les ventes d'*Alphabay* s'y sont reportées, faute de sa fermeture. L'opération *Bayonet* reste aujourd'hui une des plus importantes menées par les autorités internationales[47].

E. Hégémonie de *Dream Market* (2017 - 2019)

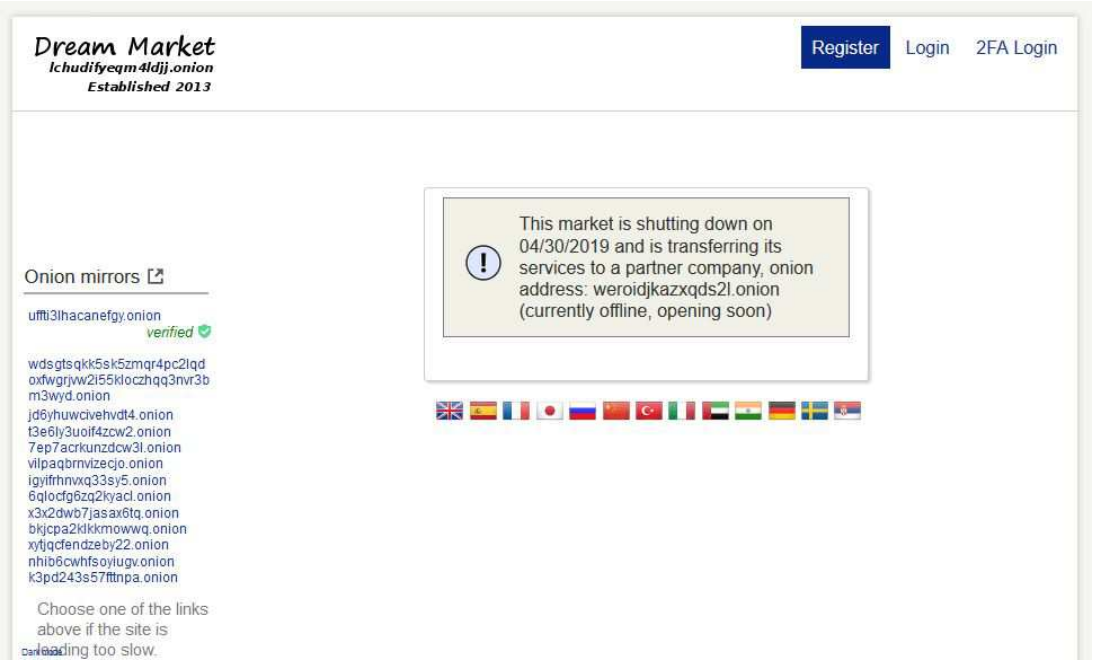
Le marché noir *Dream Market* reprend ainsi presque l'ensemble des utilisateurs d'*Alphabay* et d'*Hansa* après leur fermeture en juillet 2017. La principale crainte des utilisateurs est alors de se faire arrêter ou d'être victime d'exit scam. Ils se reportent alors sur un marché noir, qui existe depuis fin 2013. *Dream Market* fait parler de lui dans les média dès l'été 2017, lors de l'arrestation d'un de ses administrateurs, le français Gal Vallerius, connu sous le pseudonyme d'*Oxymonster*.



Marché noir Dream Market

[46]Farivar Cyrus and Utc, *AlphaBay taken down by law enforcement across 3 countries, WSJ says*, https://arstechnica.com/tech-policy/2017/07/report-alphabay-notorious-dark-web-drug-website-shuttered-by-feds/
[47]McMillan Robert and Aruna Viswanatha, *Illegal-Goods Website AlphaBay Shut Following Law-Enforcement Action*, https://www.wsj.com/articles/illegal-goods-website-alphabay-shut-following-law-enforcement-action-1499968444

Derrière *Dream Marke*t, se placent *Empire Market* et *Wall Street Market*, deux marchés noirs plus petits et plus récents. *Empire Market* fait son apparition en fin d'année 2017, reprenant totalement la structure et la charte graphique d'*Alphabay*, dont il est considéré comme clone. *Wall Street Market* est lui ouvert par trois Allemands en 2016, et se place derrière *Dream Market* et *Empire*.



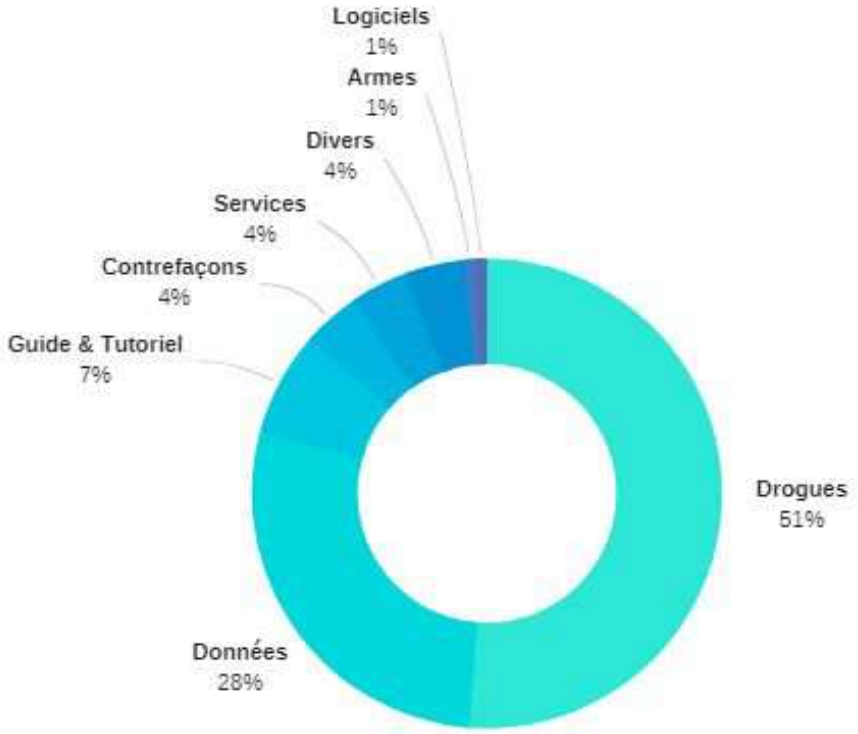
Message de fermeture, posté sur Dream Market - CCN.net

Le 24 mars 2019, l'administrateur de *Dream Market* annonce que le marché noir arrêtera ses activités le 30 avril 2019[48]. Le 4 mai 2019, soit seulement quelques jours après la fermeture de *Dream Market*, c'est au tour de *Wall Street Market* de disparaître, cette fois fermé par les autorités allemandes[49].

[48] *Le site de vente illégale Dream Market annonce son déménagement*, https://www.lemonde.fr/pixels/article/2019/03/28/le-site-de-vente-illegale-dream-market-annonce-son-demenagement_5442702_4408996.html.

[49] *Dark web marketplace Wall Street Market busted by international police*, https://nakedsecurity.sophos.com/2019/05/07/dark-web-marketplace-wall-street-market-busted-by-international-police

F. Quelles proportions pour les marchandises échangées aujourd'hui ?



Statistiques de ventes sur les marchés noirs - statistiques effectuées à partir des données d'un dataset de 150 000 produits - avril 2019

Les marchandises échangées aujourd'hui sur les marchés noirs restent principalement des drogues, qui représentent plus de 50% des marchandises proposées. Les cannabinoïdes sont les plus représentées, comptant au total plus de 70% des drogues vendues.

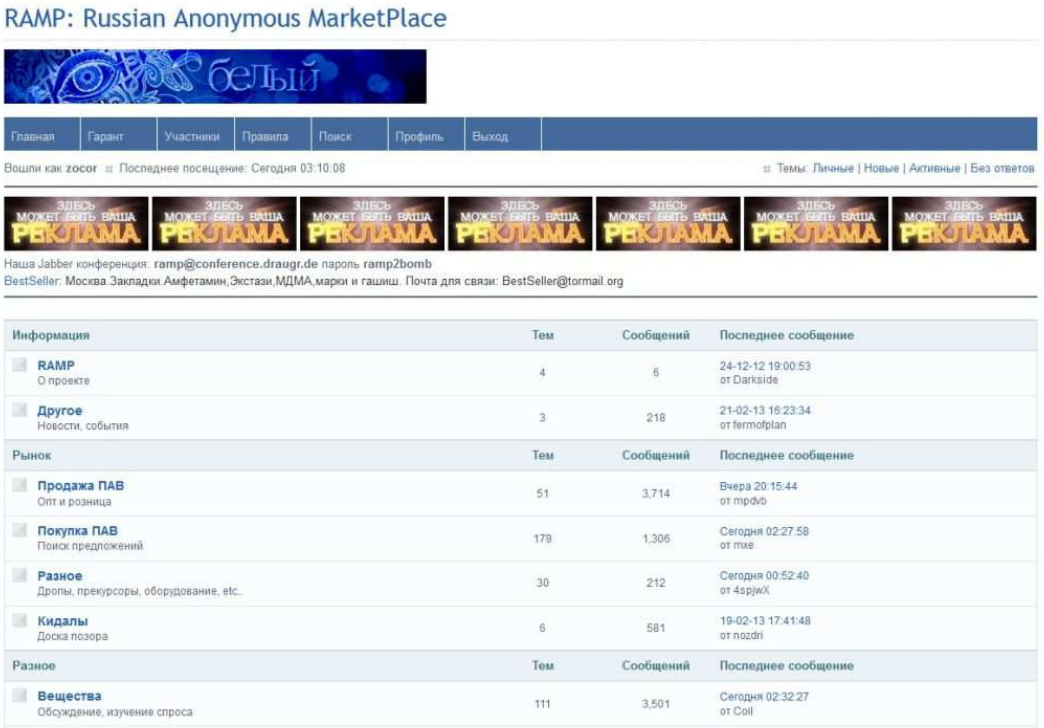
Viennent ensuite les données volées, présentes sous diverses formes (logs, cartes de crédit, mails et leurs mots de passe, documents d'identité volés…), qui prennent une place de plus en plus importante sur les marchés noirs, s'élevant désormais à un tiers des offres. Les armes, documents contrefaits et autres services représentent une part plus faible des ventes.

Chapitre 2 : Marchés noirs russophones

La communauté russophone est la seconde communauté présente sur le Dark Web. Elle représente environ 15% du contenu présent sur les marchés noirs. Elle est marquée par la domination de *RAMP (Russian Anonymous Market Place)* pendant plus de cinq ans, de 2012 à 2017, qui laissera place à *Hydra*, suivi par deux marchés noirs plus récents, *Mega* et *BlackMart*.

A. *RAMP*, ou l'émergence des marchés noirs russophones

Face au développement des marchés noirs anglophones qui deviennent de plus en plus populaires, on assiste à l'émergence des premières plateformes russes non-anglophones. Le marché noir *RAMP, Russian Anonymous Market Place* ouvre ainsi ses portes en début 2012, fondé par deux utilisateurs nommés *Darkside* et *Orange*. Le site se différencie de ses homologues anglophones, en prenant la forme d'un forum mercantile et non-pas d'une marketplace.

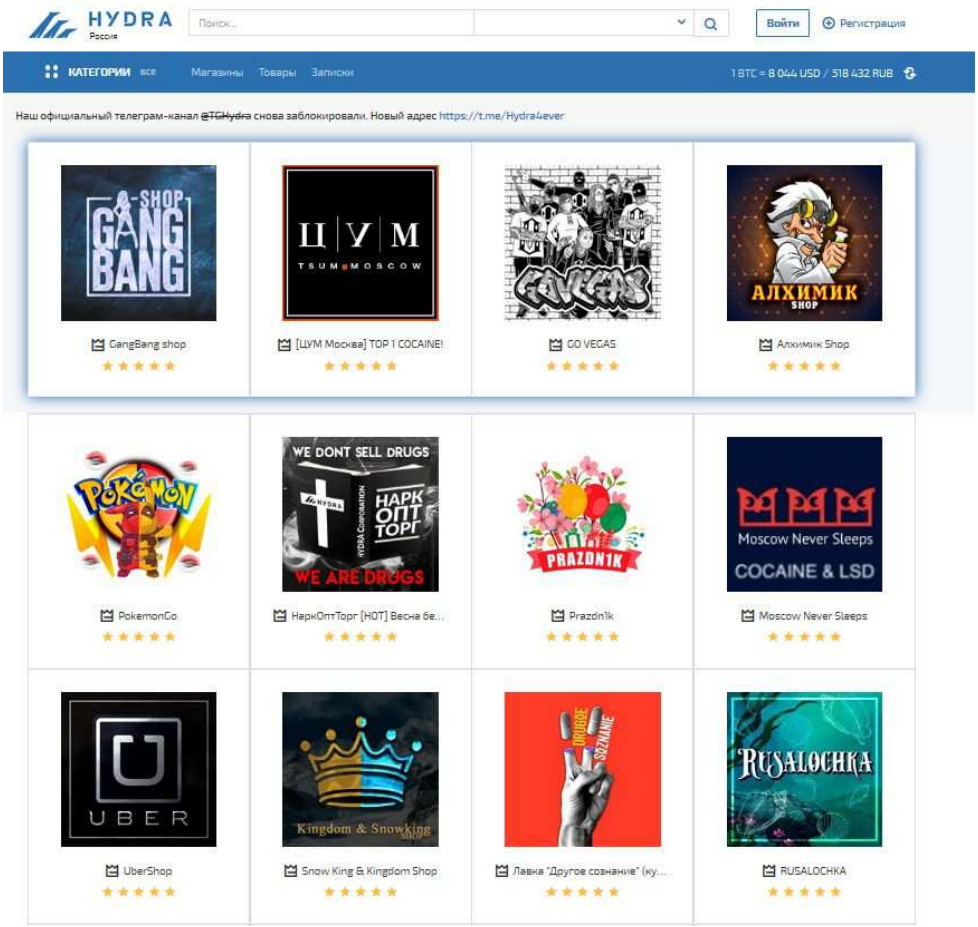


Forum Mercantile RAMP

La plus grandes majorité des échanges sont ainsi effectués en privé, via la messagerie du marché noir. *RAMP* fait ses bénéfices les plus importants sur la publicité, en proposant de mettre en avant sur le site certains vendeurs sur un espace publicitaire sous forme d'une bannière à l'avant du site. A sa fermeture en juillet 2017 par les autorités russes, il totalise plus de 14 000 membres inscrits[50].

B. *Hydra*, principal héritier de *RAMP*

Le marché noir russophone *Hydra* est aujourd'hui la plateforme de vente la plus importante du Dark Web russophone. Fondée en 2015, elle est liée au forum mercantile *Wayaway*, où les utilisateurs se regroupent pour échanger autour des produits du marché noir. Les plateformes *Hydra* et sont les plus ergonomiques du Dark Web.

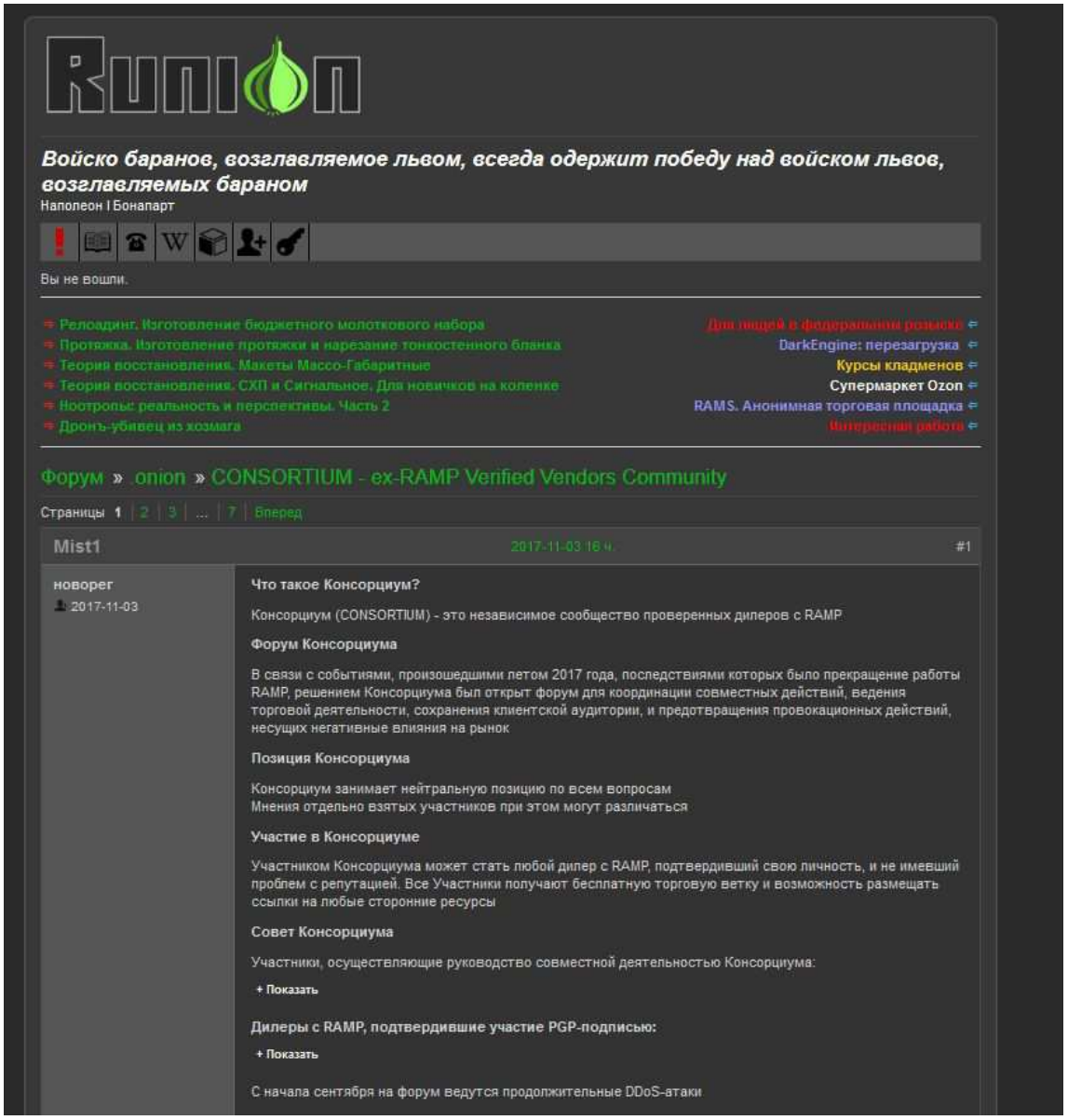


Capture d'écran - marché noir russophone Hydra

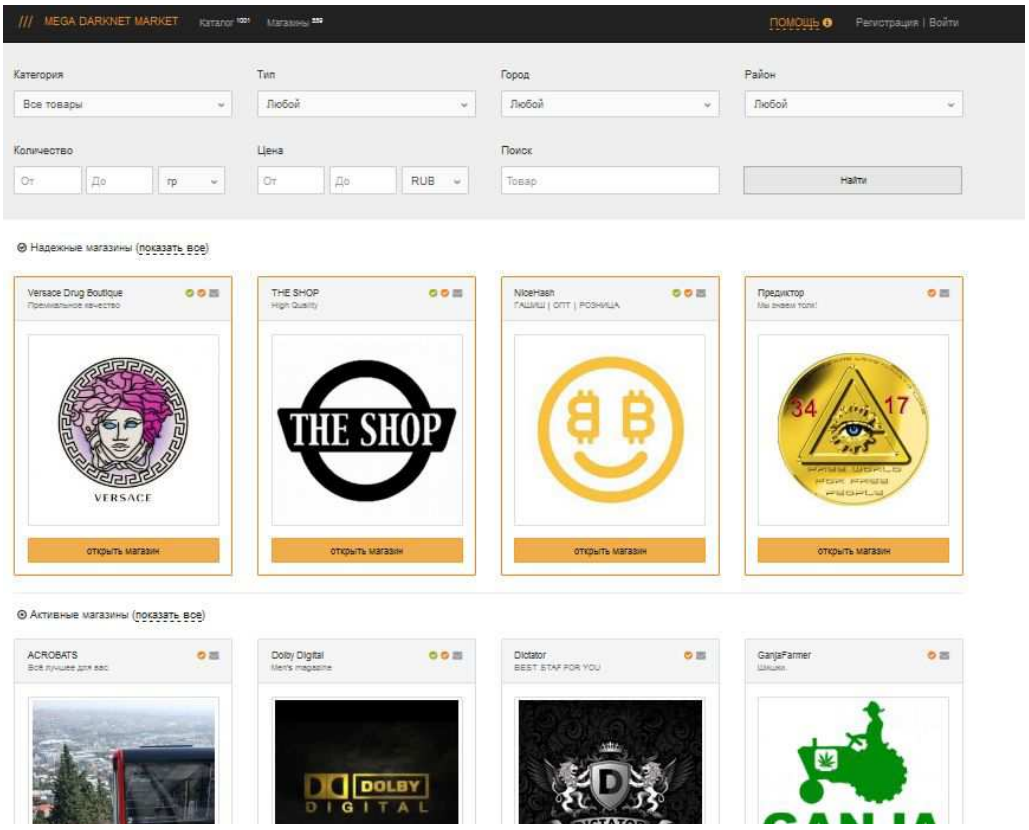
[50] Cimpanu Catalin, *Russian Authorities Announce Takedown of RAMP Dark Web Marketplace*, https://www.bleepingcomputer.com/news/security/russian-authorities-announce-takedown-of-ramp-dark-web-marketplace

C. *Consortium*, communauté de *RAMP* qui fonde le marché noir *Mega*

Consortium, une communauté très importante de *RAMP*, décide de reprendre la base de données des utilisateurs de *RAMP* afin de recréer un nouveau marché noir. Les premières annonces sont faites sur le forum russophone *Runion*. *Consortium* s'organise par la suite sur un forum, qui donnera naissance au marché noir *Mega* en 2018.



Création de Mega par Consortium - forum Runion - Capture d'écran



Marché noir russophone Mega - Capture d'écran

On trouve également un autre marché noir, *Black Mart*, lié au forum *Rutor*. Il est cependant bien plus petit que ses deux homologues russophones et moins connu sur le Dark Web international. *Hydra* et *Mega* ont en effet bénéficié de publicité sur les forums anglophones et sites spécialisés (*deepdotweb* et *darkwebnews*).

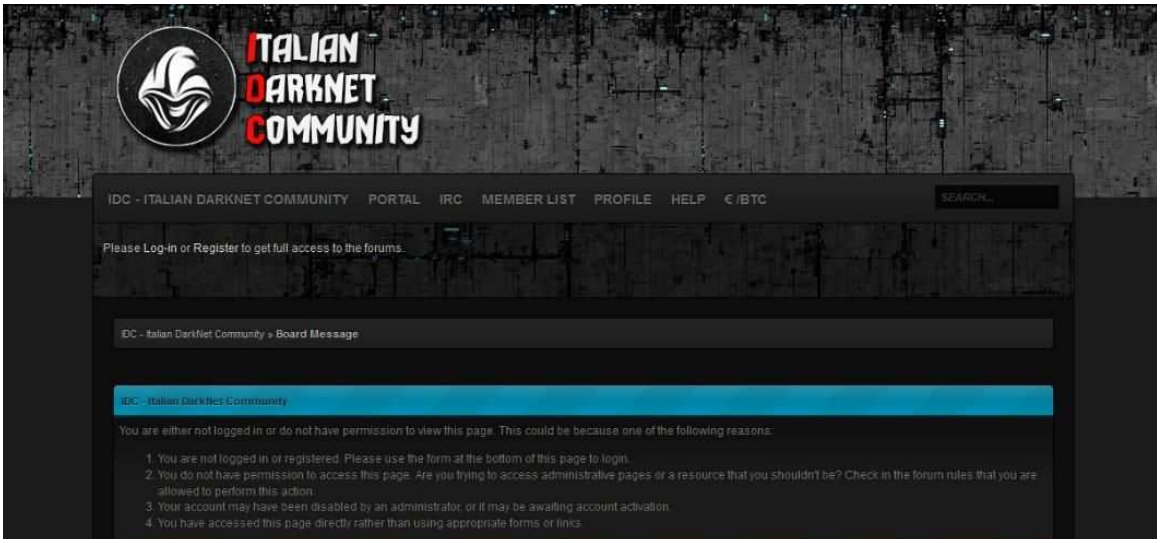
Chapitre 3 : Autres communautés

Représentant une partie bien plus faible que leurs homologues anglophones et russophones, les plateformes européennes constituent néanmoins une part importante sur le Dark Web.

A. Européens

Les trois écosystèmes cybercriminels européens - Italophone, Germanophone et Francophone - ont une structure très similaire ; plus petits, ils disposent d'un forum principal plus ancien, et de plusieurs marchés noirs plus éphémères, gravitant autour de la communauté.

L'écosystème italophone est probablement le plus méconnu, n'ayant jamais fait l'objet d'étude ou d'attention particulière de la part des média internationaux. Les deux principales plateformes italiennes depuis la fermeture du marché noir *Babylon* en 2017[51] sont aujourd'hui l'*Italian Darknet Community*, qui a plus de cinq ans, et l'*Italian Dark Web*. On y trouve les mêmes marchandises que sur les marchés noir anglophones, dans des proportions plus limitées. Le marché noir *Berlusconi Market*, malgré son nom, n'est pas une plateforme italophone.



Capture d'écran - Italian Darknet Community - Forum/marché noir

[51] Operazione "Babylon": la Postale scopre un mercato illecito nella darknet, https://www.poliziadistato.it/articolo/39585.

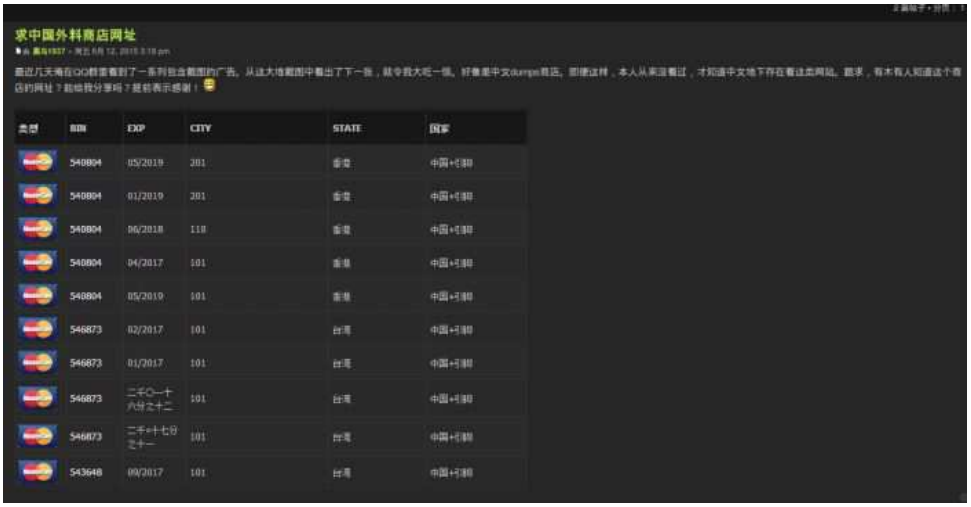
L'écosystème germanophone se rapproche davantage de son homologue russophone, présentant en effet bien plus de produits techniques et d'offres spécialisées dans la production et l'offre de malware. Nous étudierons en détail les spécificités et l'architecture de l'écosystème cybercriminel francophone en dernière partie de ce mémoire.

Capture d'écran - fermeture du marché noir Wall Street Market par les autorités allemandes

B. Asiatiques

Bien plus fermés que les autres écosystèmes internationaux, les plateformes asiatiques sont plus difficiles d'accès et moins bien référencées. On y distingue plusieurs communautés : coréenne, japonaise et chinoise. Du fait de la censure et du « Great Firewall » mis en place par le gouvernement, de plus en plus d'utilisateurs chinois utilisent le réseau Tor. Elles sont bien plus petites que leurs homologues anglophones et russophones[52]. Moins développées que les marchés noirs internationaux, les plateformes y sont hybrides, entre forum et marché noir.

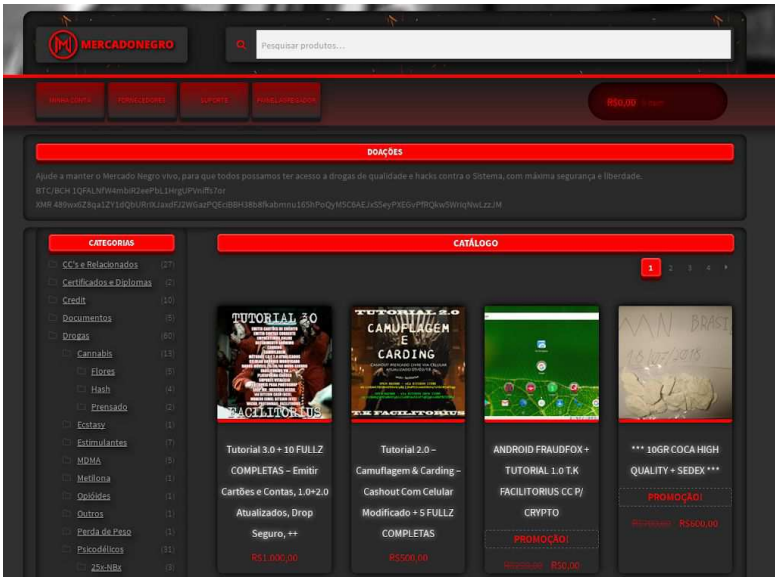
[52] L. Gu, *Revisiting the Chinese Underground Market* - Trend Micro



Vente de cartes bancaires, Dark Web sinophone

C. Latino-américain

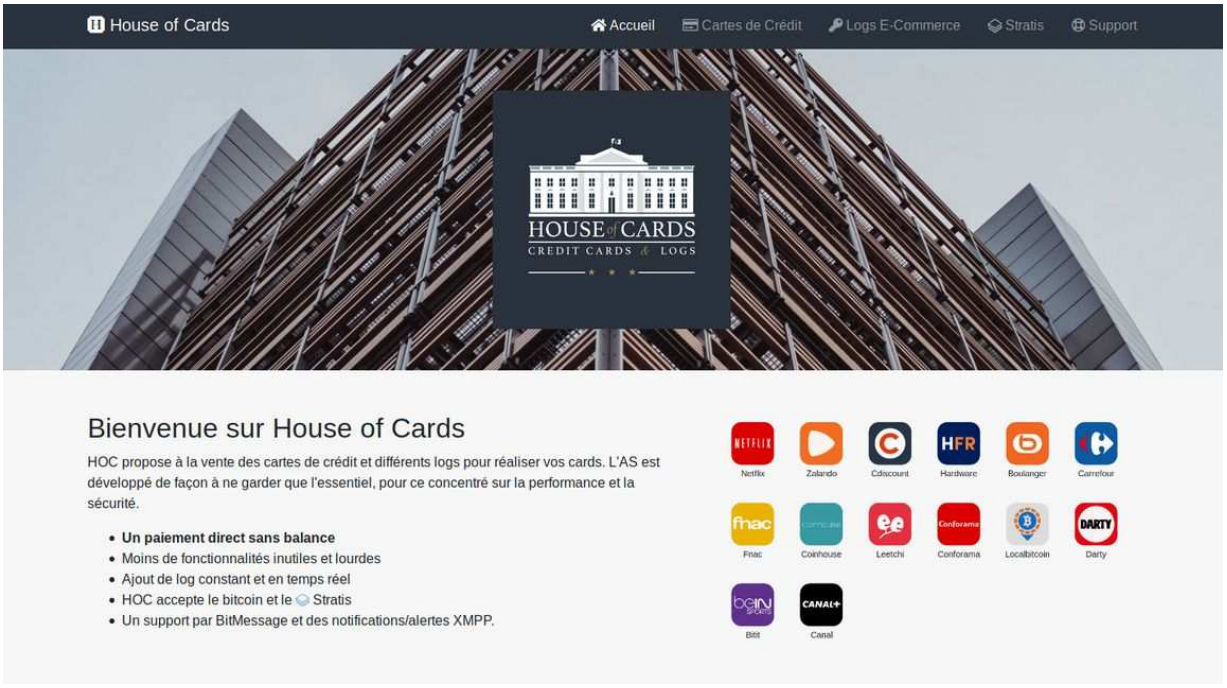
L'écosystème latino-américain est principalement constitué des communautés lusophones et hispanophones. Encore très jeune et en développement, il ne représente qu'une part très faible des échanges et des visites. Les plateformes principales sont aujourd'hui le forum *Café Cebolla* et le marché noir *Mercado Negro*, qui s'est imposé comme plateforme de vente principale après le piratage de *Trishula Market* en fin 2017. S'y échangent principalement de la drogue et des documents frauduleux et des malware bancaires.



Mercado Negro, marché noir lusophone

Chapitre 4 : Développement des petites plateformes de vente n'appartenant qu'à un vendeur ou à un petit groupe de cybercriminels

Les autoshops sont de plus petites plateformes, spécialisées dans la vente d'un produit ou d'une gamme de produits[53]. Elles sont tenues pour la plupart d'entre elles par des vendeurs possédant déjà une réputation et une clientèle très importante sur les marchés noirs, qui souhaitent pouvoir être administrateurs de leurs propres plateformes, évitant ainsi les commissions prises par les tiers de confiance sur les marchés noirs. Ils se développent notamment après l'importante vague d'arrestations de vendeurs qui a suivi la chute de *Silk Road 2.0*. De nombreux vendeurs ont en effet souhaité bénéficier de leur propre plateforme, minimisant les risques d'arrestation car les autorités se concentrent sur les plateformes de vente importantes.



Capture d'écran - Projet d'Autoshop Francophone House of Cards

[53] Rolland Sylvain, *Cybercriminalité : qui sont les escrocs du darknet français ?*, https://www.latribune.fr/technos-medias/cybercriminalite-qui-sont-les-escrocs-du-darknet-francais-599111.htm

Chapitre 5 : Forums et plateformes d'échange, le Dark Web comme laboratoire de développement des nouvelles cybermenaces (malware as a service + ransomware as a service + data leaks)

Outre les marchés noirs, on trouve également un autre type de plateforme sur le Dark Web qu'on appelle les forums. Ils sont les héritiers directs des Bulletins Board System dont ils reprennent l'organisation. Les forums sont conçus pour servir d'espace d'échange pour leurs utilisateurs, organisés autour de sous-forums, divisés en sujets et catégories de discussion. Les forums ont contribué au développement de la cybercriminalité, permettant notamment aux cybercriminels de pouvoir échanger sur les dernières techniques de piratage, failles de sécurité, nouveaux malware et fuites de données. Il est à noter que ces forums n'ont servi qu'à des pirates novices, les connaissances plus poussées autour du piratage étant vendues ou proposées par les pirates comme service.

On assiste à une évolution très importante depuis 2010 avec le développement de la cybercriminalité 'as a service' sur le Dark Web. Il ne s'agit pas seulement de pouvoir louer un pirate contre quelques bitcoins, mais surtout du développement du Malware as a service (MaaS) dont nous traiterons dans cette partie. Nous étudierons également un de ses sous-genre actuellement en expansion, le Ransomware as a service (RaaS).

A. Terminologie

Un malware, ou « Malicious Sofware » est un terme générique qui désigne l'ensemble des programmes développés dans un but malveillant, regroupant notamment les virus, vers, trojans et ransomware[54]. Développés par les étudiants dans les universités durant les années 80, les malware sont aujourd'hui utilisés par les cybercriminels à des fins plus lucratives. Le Ransomware, ou « Ransom Software » est ainsi une sous-catégorie de malware, prenant en otage les données stockées sur une machine, en échange d'une rançon, sans laquelle la victime ne pourra plus avoir accès à sa machine et à ses données[55]. Il y a deux grands types de ransomware ; les locker-ransomware et les crypto-ransomware.

[54] *What is malware (malicious software)?* - https://searchsecurity.techtarget.com/definition/malware
[55] *Ransomware*, https://www.us-cert.gov/Ransomware

Ransomware Bad Rabbit - verdict.co

Les locker-ransomware sont les ransomware les plus anciens : ils empêchent l'utilisateur d'accéder à sa machine en bloquant le système d'exploitation, les données ne sont cependant pas chiffrées. Ces derniers tendent à disparaître au profit des crypto-ransomware qui chiffrent les données de l'utilisateur, rendant la récupération bien plus difficile que pour les simples locker-ransomware.

B. Développement du Malware as a Service – MaaS

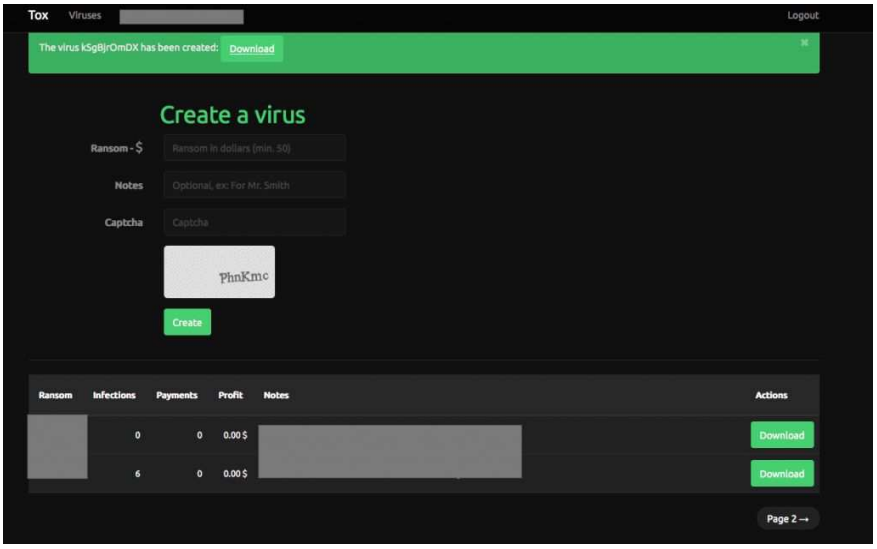
Jusqu'au début des années 2010, les malware nécessitaient un niveau de compétences techniques élevé de la part de ses utilisateurs afin d'être manipulés. Les programmes les plus avancés étaient encore vendus par leurs concepteurs auprès d'une communauté fermée pour plusieurs milliers de dollars. En 2011, les codes sources de plusieurs malware (SpyEye – ZeuS – Crimepack) furent divulgués sur des forums du Dark Web. Ces fuites permirent de produire les premiers kits de développement de malware, marquant l'émergence du Malware as a Service (MaaS)[56]. Il n'est désormais plus nécessaire de détenir des compétences techniques avancées pour développer un malware. L'interface ergonomique permet en effet à son utilisateur de sélectionner les options désirées afin de lancer une cyberattaque. Le MaaS a

[56] *Note Stratégique: L'influence du Dark Web sur la démocratisation du Malware-As-A-Service*, https://observatoire-fic.com/note-strategique-linfluence-du-dark-web-sur-la-democratisation-du-malware-as-a-service/

ainsi contribué à l'industrialisation de la production et de l'exploitation des malware en se servant des plateformes d'échange sur le Dark Web comme principal vecteur de communication.

C. Ransomware as a Service – RaaS Pourquoi les RaaS ?

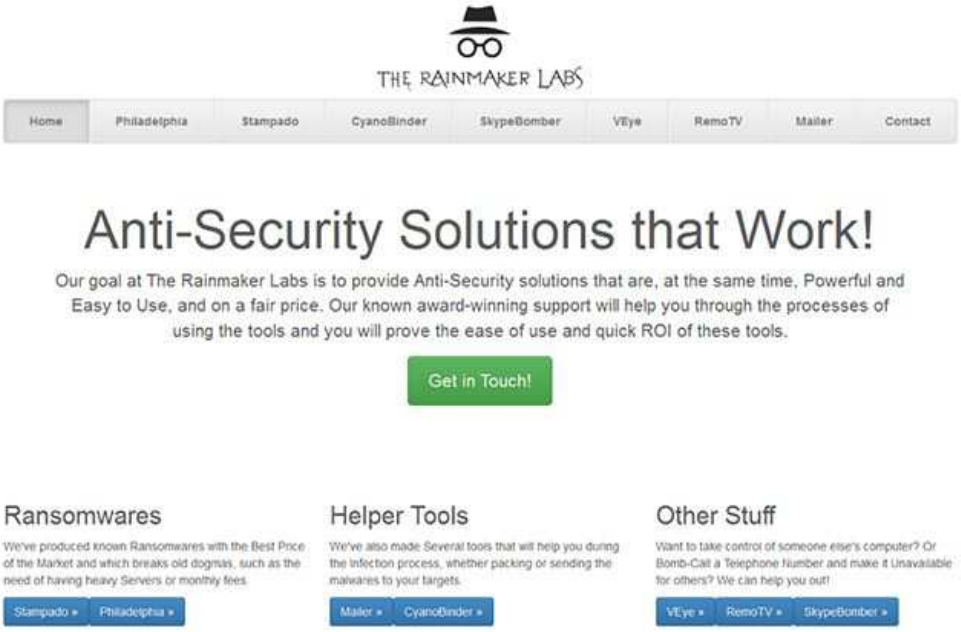
Les cyberattaques par ransomware sont aujourd'hui les plus rentables. C'est ce qui a conduit les cybercriminels à mettre sur les marchés noirs des kits de développement de ransomware, reprenant le concept du MaaS. En mai 2015, Tox, premier Ransomware as a Service voit le jour sur le darknet Tor. Les utilisateurs de Tox n'avaient alors qu'à spécifier le montant de la rançon (minimum 50 $), ainsi que le message à afficher aux victimes puis à télécharger un petit fichier exécutable d'environ 2 Mo. Une fois le fichier envoyé, un tableau de bord permettait de suivre la propagation du ransomware.



Ransomware as a Service - page de création du ransomware - McAfee Blog

Le créateur de la plateforme gagnait une commission de 30% par utilisateur infecté qui choisissait de payer la rançon. Le site Tox ferma ses portes une semaine seulement après sa mise en service, son créateur ayant pris peur face à la forte notoriété de la plateforme. Tox n'est que le premier d'une longue lignée de RaaS. L'organisation cybercriminelle russe Rainmaker Labs est aujourd'hui un des principaux producteurs de RaaS, comptant à son actif deux des principaux kits de développement de ransomware, Philadelphia et Stampado.

Philadelphia est aujourd'hui l'exemple de RaaS le plus sophistiqué distribué sur le marché noir.



Site de Rainmaker Labs - helpnetsecurity.com

L'offre des RaaS est aujourd'hui très étendue sur les plateformes du Dark Web. On trouve en effet plusieurs dizaines de kits de développement de ransomware, disponibles pour seulement quelques centaines d'euros, comme *RaasSberry*, *Datakeeper*, *Runion* ou *Createyourownransomware*. Ces plateformes ne diffèrent que par les options et les kits personnalisés qu'elles proposent, mais le modèle économique reste le même. La plateforme *RaaSberry* est aujourd'hui la plus facile d'accès et la mieux répertoriée sur les forums du Dark Web.

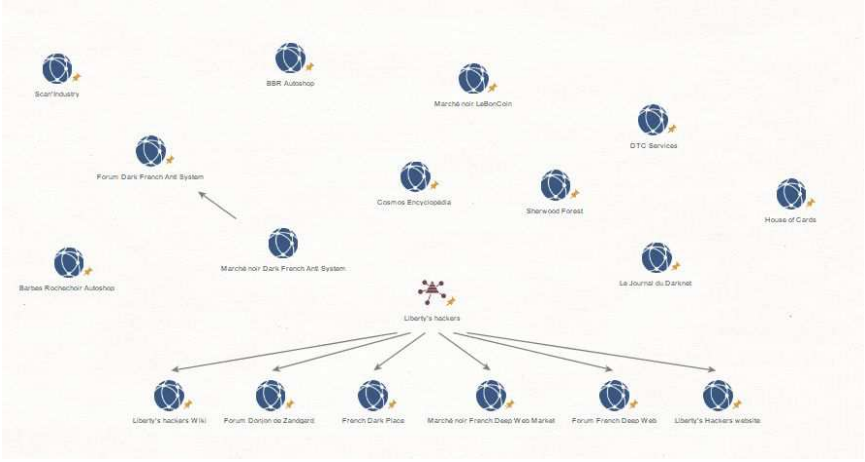
L'offre tend à se diversifier dans les années qui suivent. D'autres types de ransomware font ainsi leur apparition sur le Dark Web : on peut ainsi trouver les scareware qui simulent une cyberattaque, afin d'effrayer la victime et de lui soutirer de l'argent, ainsi que les doxware, qui dérobent des informations personnelles dans l'objectif de faire du chantage.

Partie 3 : Comprendre l'écosystème cybercriminel francophone

La communauté francophone représente une partie importante du Dark Web. Elle est en effet la troisième communauté, derrière l'anglophone et la russophone. Le groupe *Liberty's Hackers* détient la plus forte longévité sur Tor, hébergeant la communauté principale du Dark Web francophone, devant plusieurs plateformes plus jeunes. La communauté francophone a été fortement marquée par l'opposition entre trois communautés, aujourd'hui disparues. Elle s'est spécialisée dans la fraude. Cette analyse s'appuie sur les données et informations récoltées par notre moteur de recherche.

Chapitre 1 : Cartographie

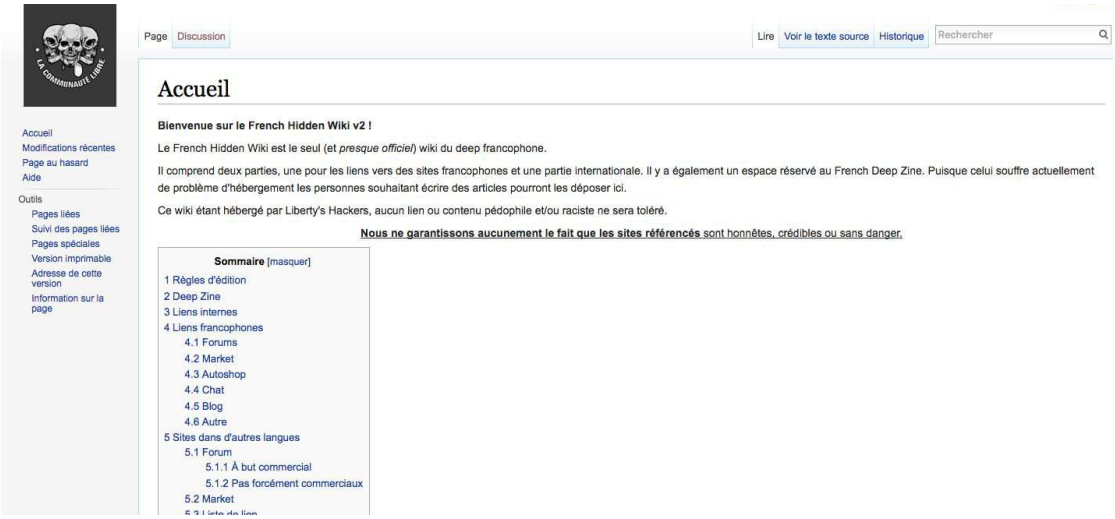
Le Dark Web francophone est aujourd'hui concentré autour de la communauté hébergée par *Liberty's Hackers*, regroupée autour du forum *French Deep Web* et de son marché noir *French Deep Web Market*. Plusieurs plateformes plus jeunes - *Sherwood Forest*, *Dark French Anti-System, French Dark Place* - et d'autres plus petites gravitent autour de la communauté principale. Elles sont néanmoins plus fermées et nécessitent à l'utilisateur d'être intégré par la communauté avant de pouvoir y accéder. On estime aujourd'hui la communauté francophone à moins de 10 000 membres.



Cartographie de l'écosystème francophone - Casefile

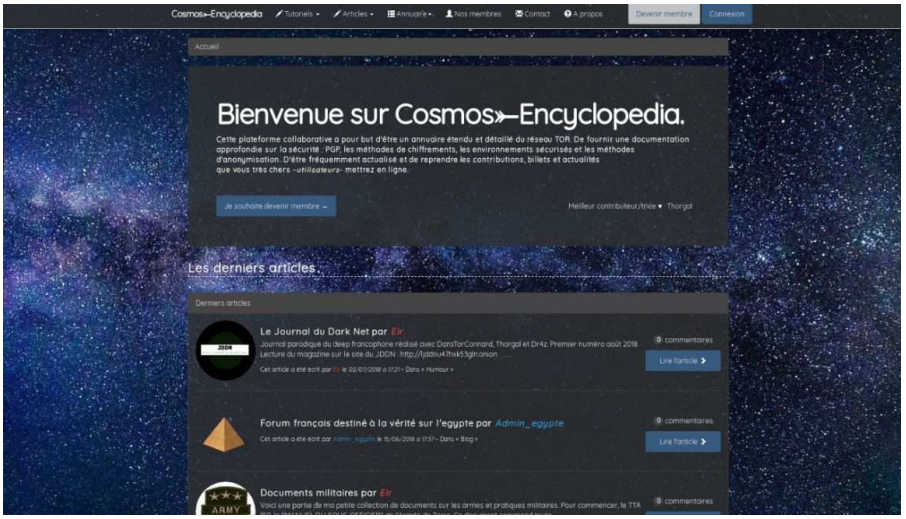
A. Accessibilité : Wiki caché, Encyclopédie et médias

Le Dark Web francophone bénéficie lui d'un Hidden Wiki, hébergé par le groupe *Liberty's Hackers* mais également d'une encyclopédie, *Cosmos Encyclopédia*, ouverte depuis novembre 2017, portée par *Sherwood Forest*.



Hidden Wiki Francophone - capture d'écran

C'est en novembre 2017 que la communauté francophone se dote également d'une encyclopédie, *Cosmos Encyclopédia*, qui a pour vocation de recenser les plateformes francophones, les tutoriels et l'histoire de la communauté. L'encyclopédie référence également les sites du Dark Web francophone, faisant également office d'annuaire pour les darknautes. L'encyclopédie est également liée à un projet de web radio qui n'a pas perduré, faute de temps et de moyens.



Comos Radio, projet de web radio pour le Dark Web francophone

S'en suit la création d'un journal mensuel, « Le Journal du Dark Net », lors du mois de juillet 2018, ayant pour objectif de présenter les actualités du Dark Web francophone sous un angle satirique. D'une vingtaine de pages, il est rédigé par l'équipe modératrice de la communauté francophone[57].

Journal du Dark Web, deux premiers numéros - décembre 2018 - capture d'écran

[57] voir annexe 1

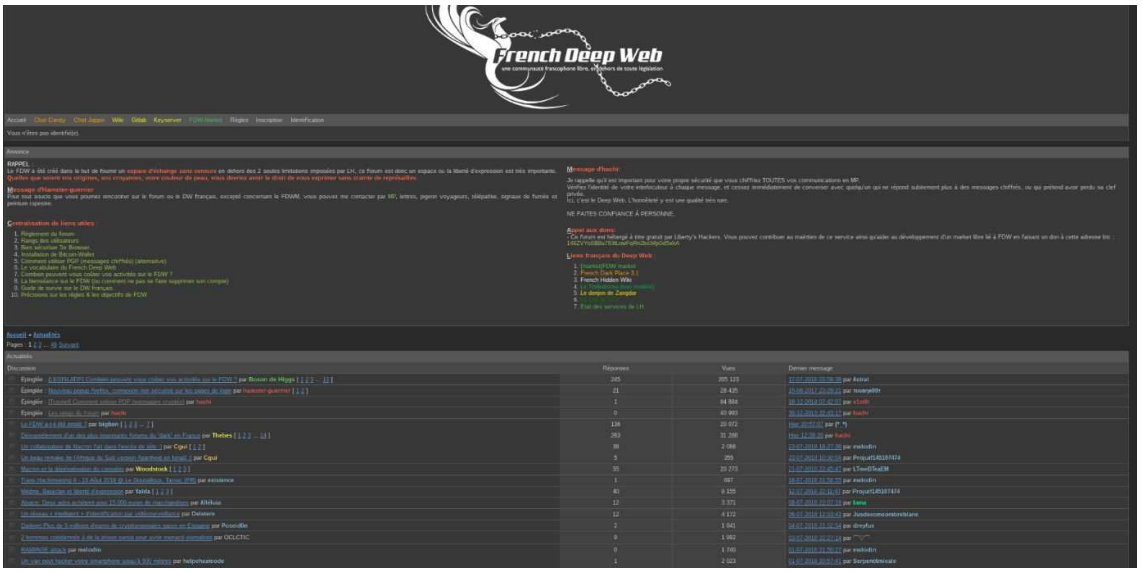
B. Liberty's hackers, épicentre historique de la communauté

La communauté formée par *Liberty's Hackers* a été fondée à la fin des années 2010 et s'appuie aujourd'hui sur une dizaine de modérateurs, regroupés autour de l'administrateur V1ct0r, fondateur historique de la communauté. Les recherches menées par notre équipe suggèrent que la communauté a été fondée par d'anciens membres francophones du groupe d'hacktivistes *Anonymous*.

Page d'accueil du site de Liberty's Hackers - 2014 - capture d'écran

Fortement marquée par les *exit scams*, la communauté formée par *Liberty's Hackers* est la plus importante et pérenne aujourd'hui, et ce notamment grâce à la confiance qu'accordent les utilisateurs du Dark Web francophone envers ses administrateurs, qui y exercent leur propre modération.

La communauté est ainsi centrée autour du forum *French Deep Web*, fondé en 2012 par V1ct0r. L'objectif de la plateforme, à l'image des plateformes anglophones et russophones déjà existantes, était alors de constituer un espace d'échanges et de partage non régi par une autorité, mais modéré par un conseil de modérateurs qui filtrent les contenus à caractères pédopornographiques, terroristes et haineux, alors présents sur le forum *Noel Board*. C'est dans ce cadre que se développe la première communauté darknaute francophone.



French Deep Web forum - capture d'écran

Les sujets de discussions sont en effet contrôlés par les administrateurs et les modérateurs des plateformes qui possèdent leur propre éthique. La vente d'armes létales, de drogues, de données et de faux documents est en effet autorisée, contrairement aux données relatives à la pédopornographie, la zoophilie, le djihadisme ou la torture. Une éthique propre aux pirates francophones ? La communauté francophone centrée autour de *Liberty's Hackers* reste proche des idéaux libertariens véhiculés par Ross Ulbricht lors de la création de *Silk Road*. La seule exception qui s'en détache reste le *Trollodrome*, forum reprenant le principe de 4chan, plateforme anglophone très contestée pour son absence de modération et pour la violence des propos tenus par certains membres.

Accès au Site et aux services fournis

FDW-Market est une plateforme de vente dédiée à la communauté francophone du French Deep Web. Les comptes enregistrés sur le Site sont liés à un compte sur le Forum FDW. Il est nécessaire de posséder un compte sur le forum FDW pour s'enregistrer. Cependant, il est aussi possible de s'enregistrer sans compte FDW lié en faisant une demande auprès du staff.

Bien que nous n'encouragions pas les activités illégales, nous ne nous mêlons pas de vos affaires. Toutefois, certaines pratiques nous paraissent totalement répugnantes et nous ne voulont pas y être associés. De ce fait les limitations suivantes s'appliquent au contenu que vous pouvez publier sur la plateforme et les espaces de discussions liés (salon et forum) :

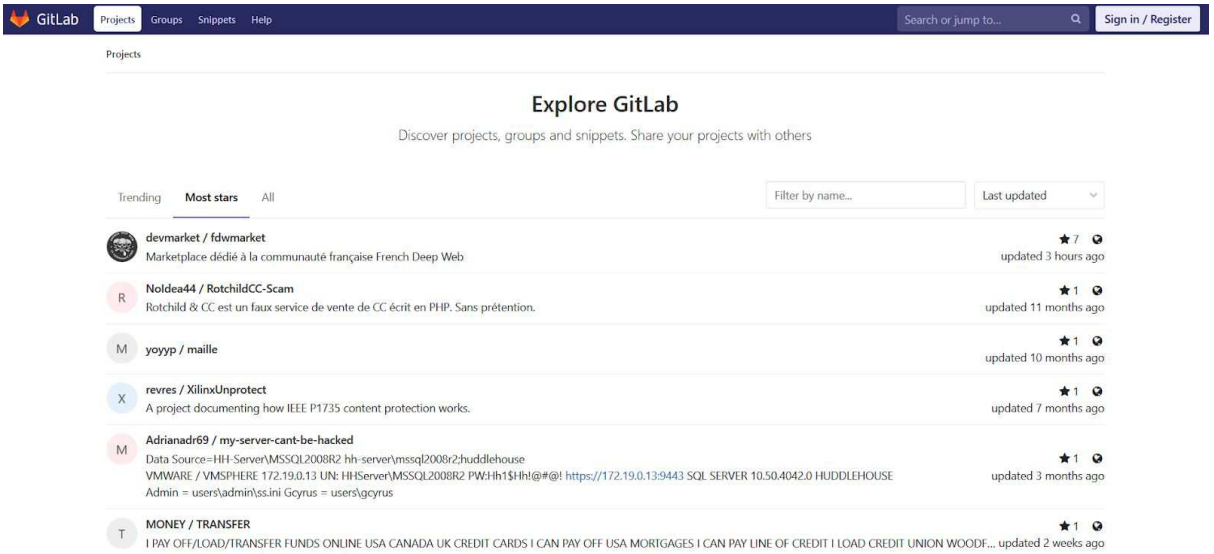
- Tout contenu à caractère pédopornographique est strictement interdit. Cela concerne aussi bien la simple discussion que la mise à disposition de fichiers ou données.
- Il est interdit de faire l'apologie du racisme et de diffuser des messages à caractère raciste. Cependant, la vente, l'achat et la possession de produits liés au racisme n'étant pas considéré comme du racisme, la vente d'objets lié au racisme, comme par exemple des croix gammées, est autorisée.
- La prostitution, le viol, le meurtre (service de tueur à gage, etc.), la vente d'organes et le trafic humain sont strictement interdits, tout d'abord car ces activités sont contraires à notre éthique et également parce que ces services sur le Deep Web sont trop souvent des arnaques.
- Personne n'offrirait 1000€ en échange de 100€, c'est une évidence et les *"YesCard"* n'existent plus depuis les années 80. La vente de *"YesCard"* et assimilés ainsi que toute offre de transfert de fonds farfelus et irréaliste sont donc interdit.
- Le FDW-Market propose des outils de communication sécurisés : service de messagerie privée, salon de discussion basé sur le protocole XMPP avec un module JavaScript sécurisé incluant le protocole OTR (NB: l'intégration du salon XMPP sur le Site, bien que fonctionnelle, n'est pas encore terminée). Des liens vers d'autres moyens de communication sont disponibles dans le profil utilisateur ainsi qu'un lien vers le profil utilisateur sur le forum FDW. Vous êtes libre d'utiliser les moyens de communication de votre choix mais nous ne garantissons que la sécurité de la messagerie interne au Site ainsi que celle du salon XMPP.

Conditions d'utilisation du forum French Deep Web - capture d'écran

Le *French Deep Web* se dote également en 2015 d'un marché noir, le *French Deep Web Market*, afin de séparer les discussions mercantiles des simples échanges entre les pirates. Il s'agit aujourd'hui du principal marché noir francophone, totalisant plus de 5 000 vendeurs pour plus de 10 000 offres.

Marché noir French Deep Web Market - capture d'écran

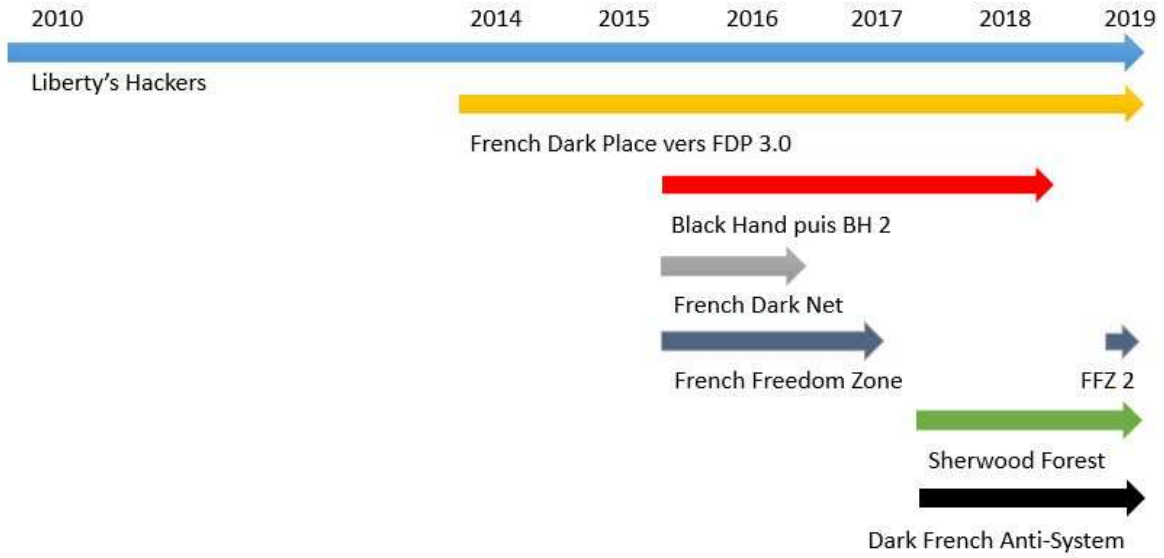
Liberty's Hackers a également mis en place un service web d'hébergement et de gestion de développement. Bénéficiant ainsi d'un *Gitlab* sur le Dark Web, les pirates francophones peuvent ainsi échanger codes et logiciels malveillants.



Gitlab de Liberty's Hackers hébergée sur Tor - capture d'écran

C. Autres plateformes et communautés secondaires

La communauté formée par *Liberty's Hackers* n'est pas la seule évoluant sur le Dark Web francophone. Elle est en effet suivie par trois autres communautés, plus petites, qui gravitent autour d'elle – *Sherwood Forest*, *Dark French Anti-System* et *French Dark Place*. La dernière-née, *French Freedom Zone 2*, se considère comme héritière d'une ancienne communauté francophone très importante, disparue en début 2017.



1. Sherwood Forest ou l'élite des pirates ?

La plateforme *Sherwood Forest* a été fondée en mi 2016 et est réservée aux anciens membres du Dark Web francophone, où ces derniers échangent à l'abri des nouveaux membres moins expérimentés. Pour y rentrer, il est nécessaire de montrer patte blanche, et parfois même de fournir des preuves d'actes de piratage. Le principe n'est pas nouveau et fait écho à une ancienne plateforme francophone, *Deep Let Tor*, fermée en 2014, mais également à la communauté *French Dark Place*. Cette communauté est à l'origine de la création de l'encyclopédie *Cosmos Encyclopédia*, qui a débuté sous forme de projet sur le forum de *Sherwood Forest*.

Page d'accueil du forum Sherwood Forest - capture d'écran

Manifeste d'entrée de la communauté *Sherwood Forest :*

« Loin des affres et des tumultes, une forêt siège et prospère depuis fort longtemps.

Le chemin pour y parvenir n'est pas à la portée d'un simple passant.

Ses racines sont profondes, ses arbres anciens et exigeants.

Elle vit en harmonie avec ses habitants :

Druides, Conscients, Braconniers, Vendeurs ou Compagnons.

Elle n'obéit à aucun règne, à aucune règle.

Elle prospère en reprenant aux riches ce qu'ils ont dérobés aux pauvres.

« Donne à un homme un fusil et il peut braquer une banque. Donne à un homme une banque et il peut braquer l'humanité. »

Elle rétablit la Justice contre le mensonge. Contre l'illusion qui berce les habitants du monde.

Choisis la pilule bleue, l'histoire s'arrête là, tu peux rentrer chez toi.

Choisis la pilule rouge, tu restes au Pays des Merveilles et je te montre jusqu'où va notre forêt...

L'envie a empoisonné l'esprit des hommes, a barricadé le monde avec la haine, nous a fait sombrer dans la misère et les effusions de sang.

Je vois une génération entière qui travaille à des pompes à essence, qui fait le service dans des restos, ou qui est esclave d'un petit chef dans un bureau.

Ne vous donnez pas à ces brutes, à une minorité qui vous méprise et qui fait de vous des esclaves.

Tant que des hommes mourront pour elle, la liberté ne pourra pas périr.

Elevez-vous, dressez-vous sans relâche. Jusqu'à ce que les moutons deviennent les lions.

Que vos bourgeons prospèrent et se hissent tout en haut.

Que les feuilles du savoir se prêtent et se ressèment :

Car la connaissance n'est réelle que lorsqu'elle est partagée.

Incarnez ce symbole, cette fondation :

Redistribuons la richesse.

Cette volonté ne peut mourir... On ne peut tuer une idée.

La haine finira par disparaître et les dictateurs mourront, le pouvoir et les richesses qu'ils avaient pris aux peuples va retourner aux peuples.

Démontre tes compétences et la forêt te laissera puiser dans ses sources.

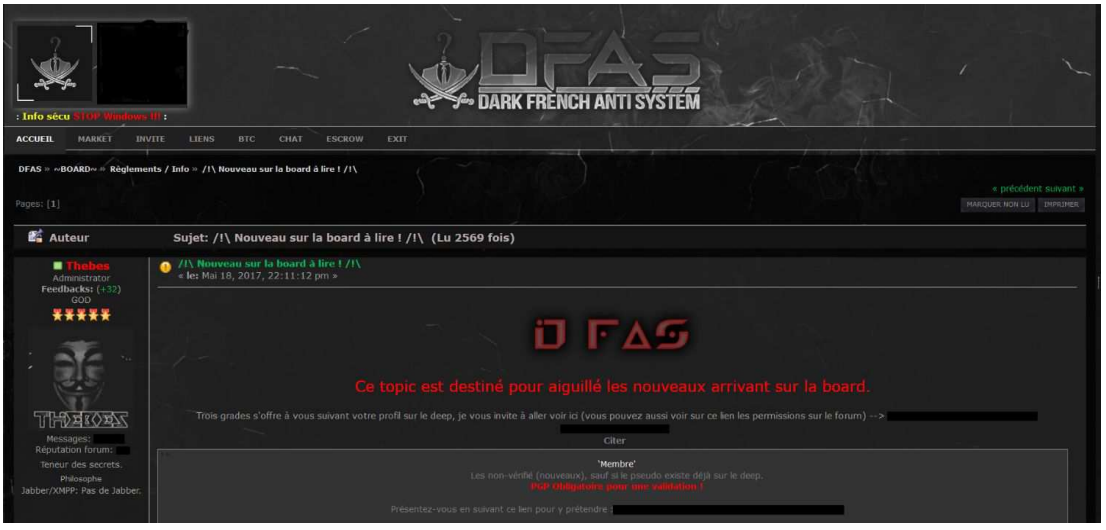
Fais preuve de conscience et les arbres te confieront leurs force.

Si tu n'as pas de temps à investir, tu peux rentrer chez toi.

Si tu as un Parrain, sois le bienvenu. Nous t'attendions.»

2. Dark French Anti System : jeune communauté à l'écoute du marché

La communauté *Dark French Anti System* ouvre ses portes au même moment que *Sherwood Forest* en fin de printemps 2017. Moins restrictive que cette dernière, elle est plus centrée autour des échanges commerciaux. Reprenant la division forum/marché, elle se dote de deux plateformes, un forum, où les utilisateurs peuvent communiquer, et un marché noir, où sont vendus les produits illicites. Son administrateur, *Thèbes* est un membre historique de la communauté du *French Deep Web*, marque de confiance pour les utilisateurs de la plateforme.



Forum Dark French Anti-System - capture d'écran

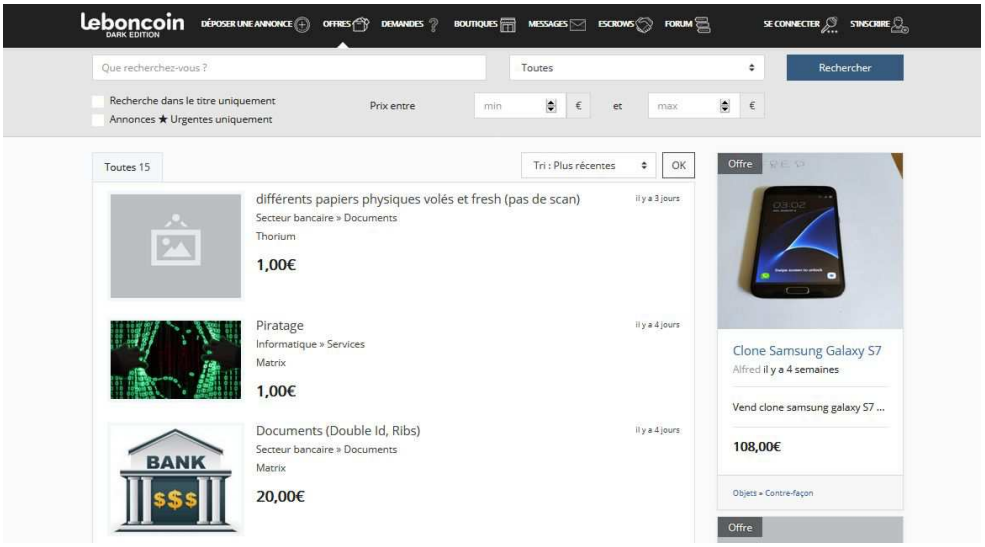
3. French Dark Place 3.1 : relique élitiste du vieux Dark Web

Ouverte en 2014, la plateforme d'échange *French Dark Place* reste aujourd'hui à la marge de la communauté francophone. Plus petite et plus restreinte que *French Deep Web*, elle ne contient qu'un forum de plusieurs centaines de membres peu actifs. Bien plus sélective, il est très difficile d'y rentrer. Aucun échange mercantile ou scandale particulier n'ayant touché cette communauté, elle continue à perdurer à l'écart des grandes plateformes.

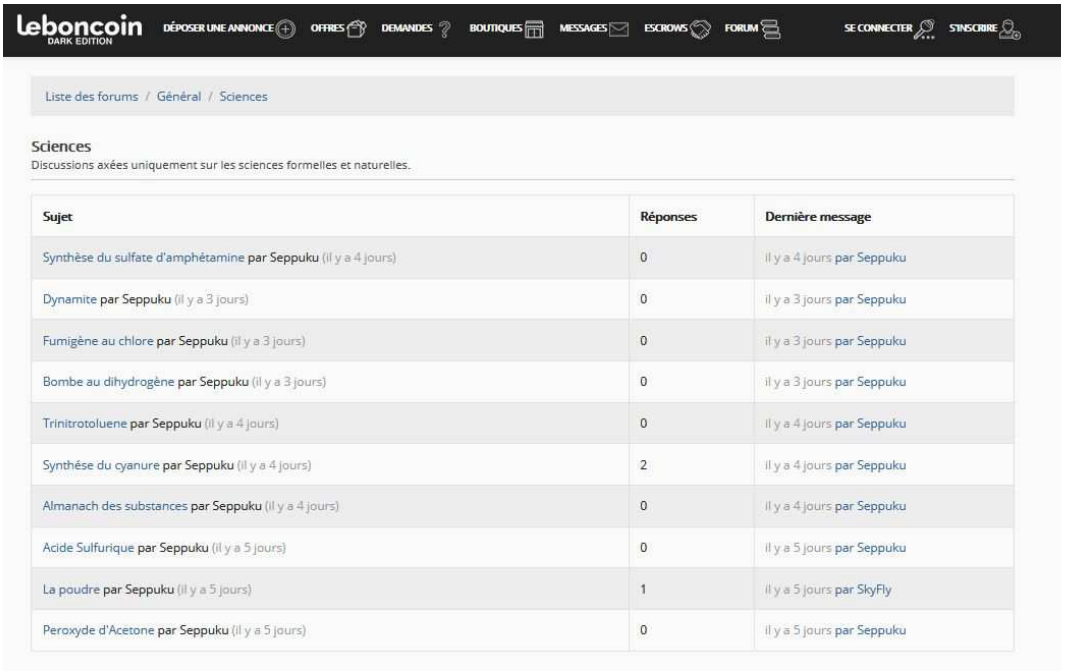
Communauté de French Dark Place

4. Le Bon Coin Dark Edition, petit nouveau dans la cour des grands ?

Le marché noir *Le Bon Coin « Dark Edition »* ouvre ses portes en début août 2018. Il s'agit de la troisième fois que le site *Le Bon Coin* est parodié par des pirates. Il tente de se démarquer des autres marchés noirs en proposant des vulnérabilités n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu, mais également des marchandises classiques présentes sur les marchés noirs : faux documents, marchandises volées, drogues, etc.



Ce marché noir est également doté d'un forum et d'une page wiki, permettant aux utilisateurs de réaliser diverses préparations chimiques.



Marché noir - Le Bon Coin - capture d'écran

D. Communautés et marchés noirs disparus du Dark Web Francophone

Le Dark Web francophone a été marqué par une très forte opposition entre deux communautés: French Dark Net et French Freedom Zone, aujourd'hui disparues, malgré la réouverture de French Freedom Zone 2 en décembre 2018. Le marché noir Black Hand a également été très important dans l'histoire de la cybercriminalité française, étant resté actif pendant plus de trois ans.

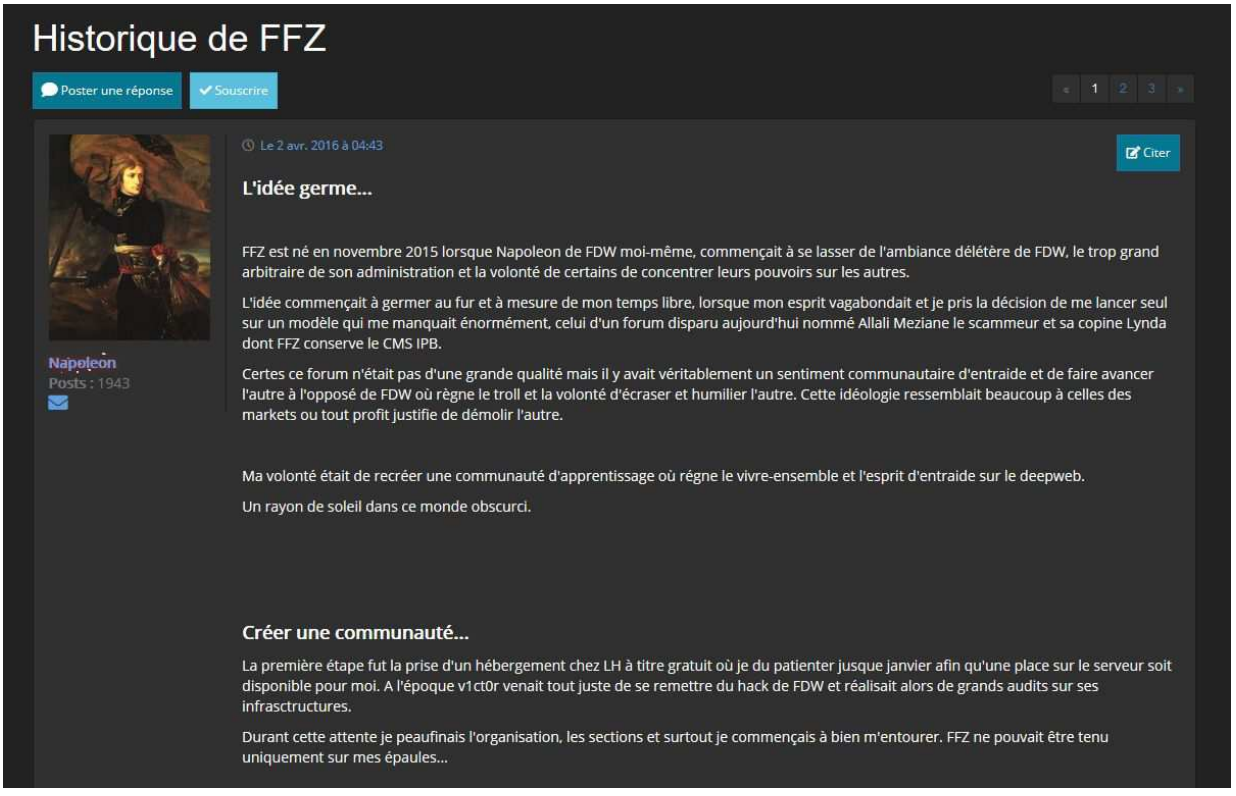
1. French Dark Net & French Freedom Zone

Outre les quatre communautés actuelles, d'autres communautés darknautes ont également marqué l'histoire du Dark Web francophone. Les deux plus importantes à mentionner ont été formées par les plateformes *French Freedom Zone* et *French Dark Net* entre fin 2015 et début 2017. Le conflit entre ces deux plateformes a fortement marqué le Dark Web

francophone, allant de diffamation aux attaques informatiques. La plateforme *French Dark Net* a fermé ses portes durant l'été 2016 à la suite de ce que l'on suppose être un exit scam, suivi par *French Freedom Zone* en début 2017 pour des raisons similaires.

Symbole de la communauté francophone French Dark Net

Symbole de la communauté francophone French Freedom Zone



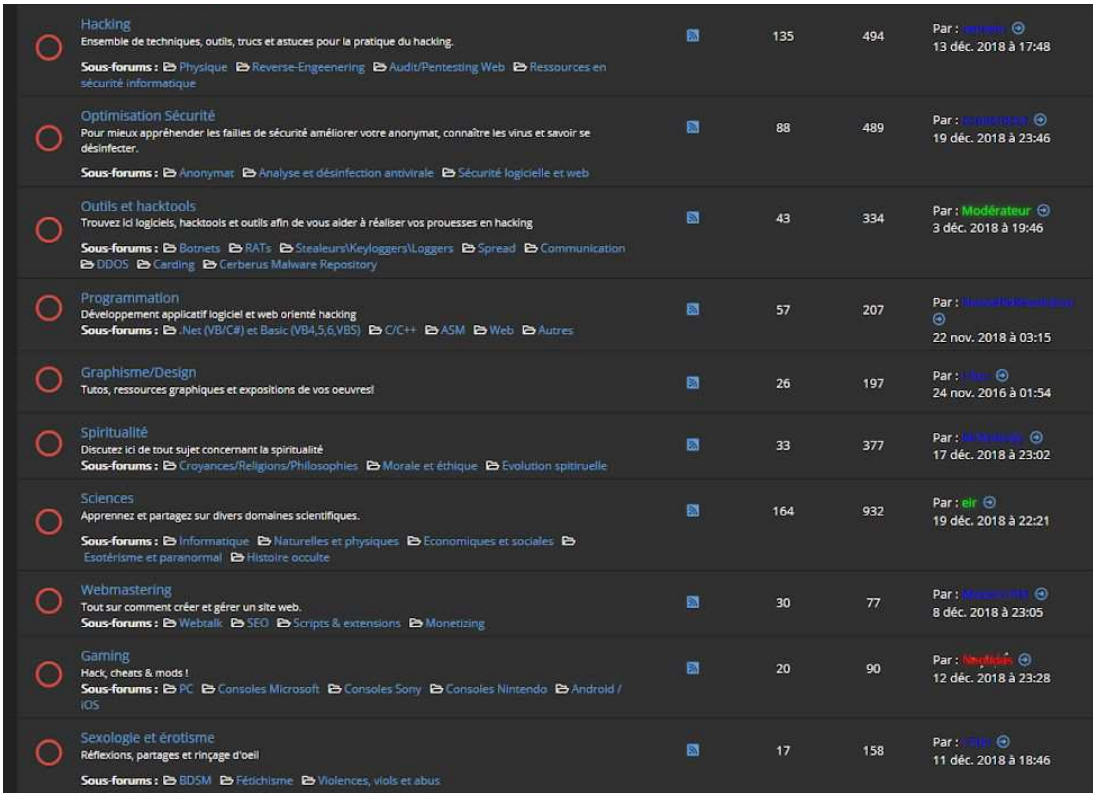
Message posté par Napoleon, ancien fondateur de la communauté de French Freedom Zone

> *« Nous souhaitons augmenter la communauté du French Dark Net. Pour cela, vous irez sur l'un des sites mentionnés (voir liste en rose en dessous !) et ouvrirez un topic sur le sujet « Deep web francophone » (ne prenez pas ce titre attention !). Vous devrez être assez intelligent pour que votre post soit feedé et uppé au maximum sans qu'il passe pour un flood. Entre soldats vous vous devez de répondre aux autres soldats pour les créditer au maximum… »*

La communauté de *French Dark Net* avait en effet mené d'importantes campagnes de communication sur le clear web, postant de nombreuses annonces sur des forums légaux ouverts (*commentçamarche.fr*, *hardware.fr*, *jeuxvideo.fr*…) espérant convertir de nouveaux adeptes au deep web francophone.

2. French Freedom Zone 2 – renaissance d'une ancienne communauté ou coup d'éclat marketing ?

Début décembre 2018, un sujet est posté sur le forum *French Deep Web* qui annonce la réouverture de l'ancienne communauté, sous le nom de *French Freedom Zone 2*. Le forum permet également d'accéder aux anciennes discussions datant de 2016.



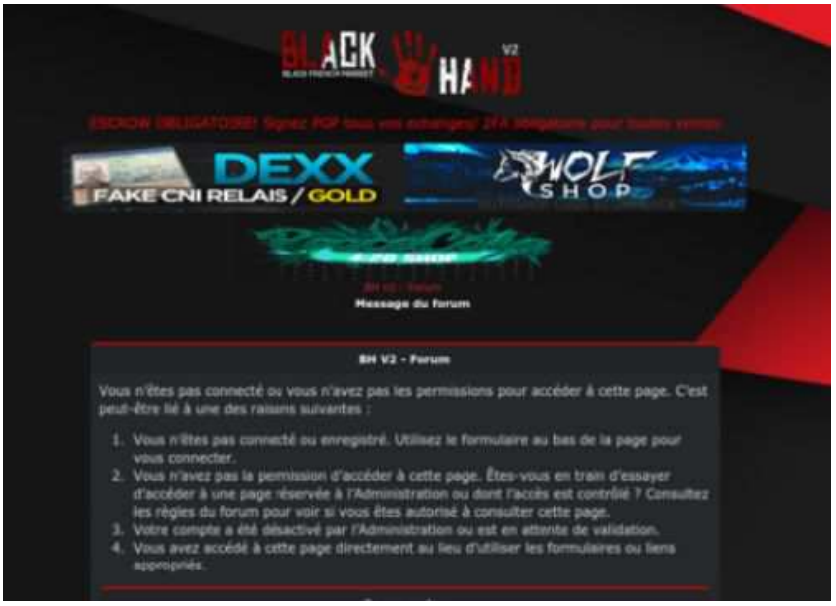
Forum French Freedom Zone 2 - capture d'écran

3. Anciens marchés noirs – *BlackHand*, prise la main dans le sac

Deux fermetures de marchés noirs marquent aujourd'hui l'histoire du Dark Web Francophone : *French Market Place* en février 2015 et *BlackHand* en juin 2018. L'histoire de ces deux plateformes est fortement liée, *BlackHand* s'étant développée après la fermeture du *French Market Place*, tombé en février 2015, suite à un exit scam de plus de 40 000 euros. La fermeture du marché noir a un impact très important sur ses utilisateurs, provoquant une importante crise de confiance envers le système mercantile cybercriminel français.

Logo de l'ancien marché noir Black Hand

C’est à la suite de ces événements que *BlackHand*, qui n’est alors qu’une jeune plateforme, ouvre ses portes aux utilisateurs du Dark Web. Le marché noir *BlackHand* tient son nom de l’organisation criminelle américaine tristement célèbre Mano Nera, première organisation criminelle italienne aux États-Unis. La plateforme n’est accessible qu’après avoir payé une petite somme, une cinquantaine d’euros en bitcoin.



Page d'accueil du marché noir Black Hand, seconde version - capture d’écran

La plateforme *BlackHand*, reste prospère jusqu’au printemps 2017, où elle est alors marquée par de nombreux scams, et délaissée peu à peu par ses utilisateurs. En avril 2017, un des administrateurs prend alors la décision de quitter le marché noir en récupérant la base de données de ses utilisateurs ; c’est la création de *BlackHand V2*, qui supplante son prédécesseur au bout de quelques semaines. La plateforme sera petit à petit mise à l’écart et perdra ses derniers clients jusqu’en juin 2018, date de l’arrestation d’Hadès, administratrice historique de la plateforme ainsi que de trois autres vendeurs.

Des conséquences jusqu’à aujourd’hui

L’analyse des serveurs saisis par les autorités ont permis d’identifier plusieurs vendeurs autrefois officiant sur *BlackHand*, notamment un agent de la DGSI qui vendait des données provenant des fichiers de police. L’individu, officiant sous le pseudonyme d’Haurus, a été

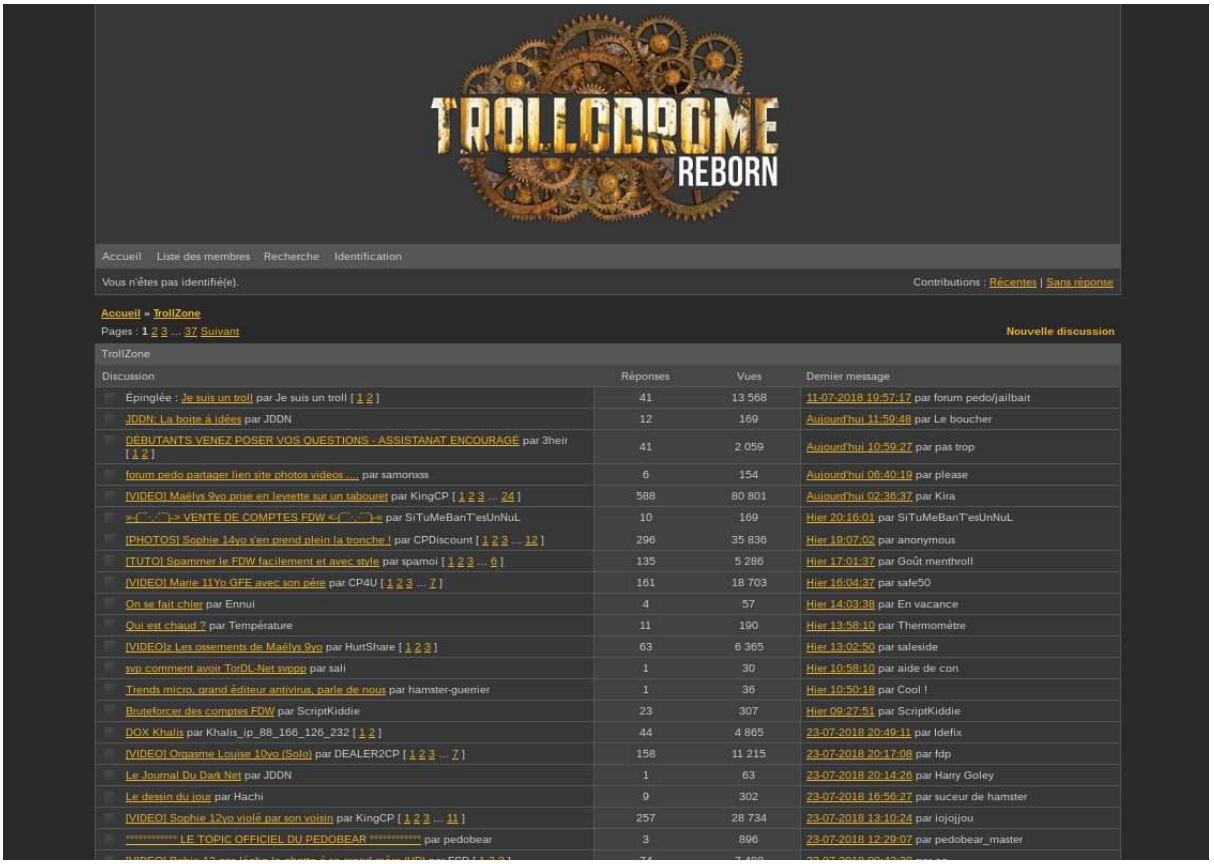
appréhendé le 28 septembre. Il était également présent sur le forum *DFAS*, où il avait posté l'annonce suivante :

> *« Je suis Haurus, la quarantaine, initié aux arts divinatoires de l'informatique depuis quelques années. J'espère me nourrir de votre connaissance et qui sait… me faire de l'argent ! Participer à ce joyeux bordel sera aussi un plaisir ! À très vite »*

Haurus, identité utilisée par le policier de la DGSI sur le Dark Web

E. Le *Trollodrome*, forum qui reste en dehors de la communauté

En marge de la communauté francophone, le *Trollodrome* est une plateforme non modérée, où ses utilisateurs échangent autour de sujets interdits sur les autres forums du Dark Web francophone. La plateforme est souvent décriée et critiquée par les darknautes francophones pour ses sujets de discussion, qui tournent principalement autour de la pédopornographie, de la zoophilie et du racisme.



Forum Trollodrome Reborn - capture d'écran

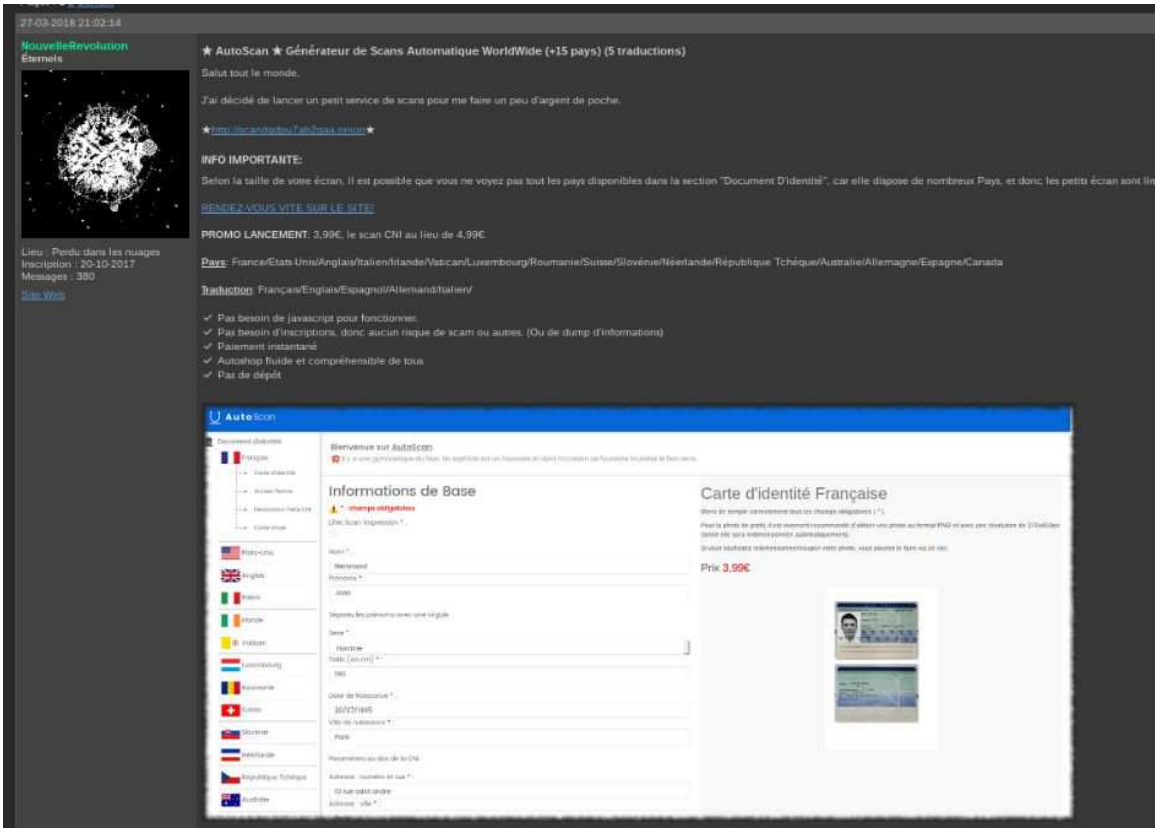
Reprenant le principe du forum 4chan, *Noel Board* est la plateforme qui précède le *Trollodrome*, créé à la suite de la fermeture de cette dernière, lors de la disparition de l'hébergeur de serveurs *Freedom Hosting*. Le *Trollodrome* est par la suite fermé par son administrateur en novembre 2015, puis ouvre dans sa version actuelle, le *Trollodrome Reborn*, en août 2016.

Chapitre 2 : La fraude : un business cybercriminel made in France

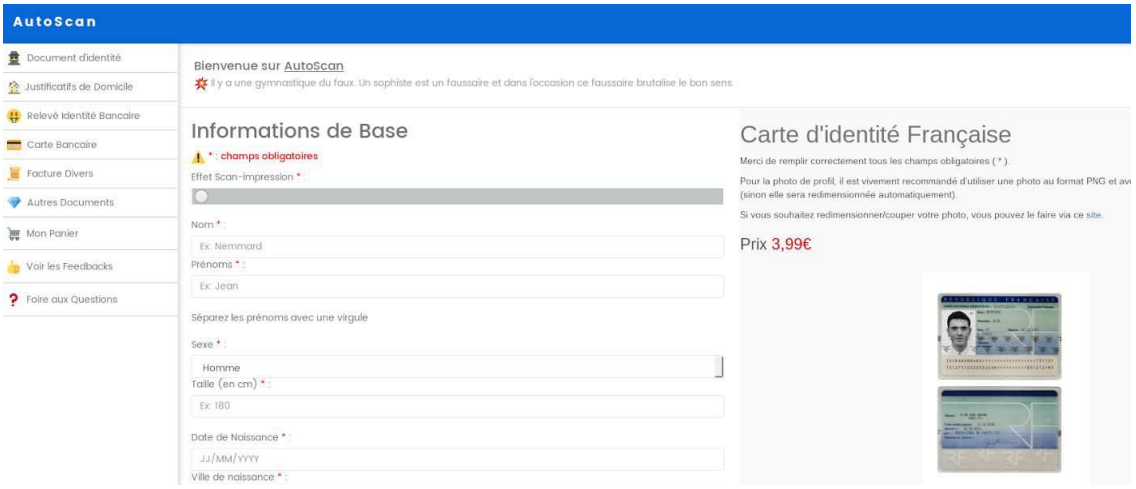
Les marchés noirs francophones, tout comme les plateformes internationales, distribuent principalement de la drogue. Le marché francophone s'est cependant spécialisé dans la fraude physique et numérique, qui représente une proportion bien plus importante sur le marché noir francophone que sur ses homologues internationaux.

A. Distribution

Le marché des faux documents est en effet très développé sur le marché noir francophone. Outre la distribution sur les marchés noirs traditionnels, il existe également des plateformes spécialisées et uniquement consacrées à la production de faux documents. Ces autoshops, que nous avons abordés précédemment sont référencés sur les forums, où leurs administrateurs y font de la publicité pour leurs plateformes.



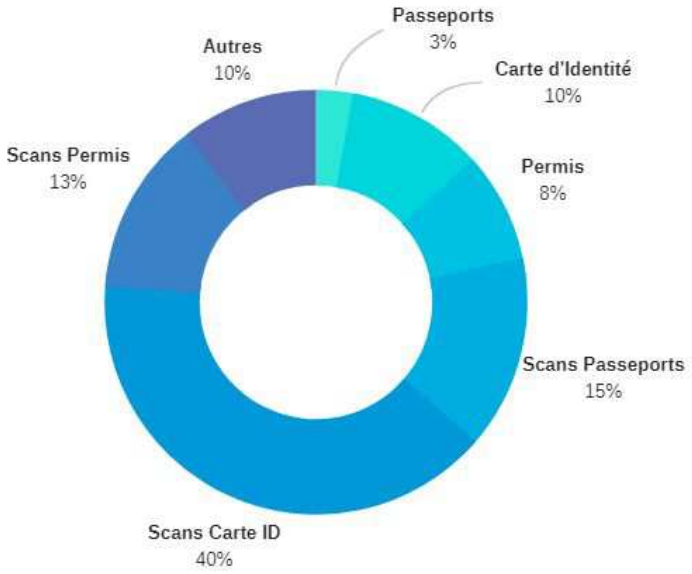
Message posté par un membre du forum French Deep Web afin de promouvoir son autoshop - capture d'écran



Autoshop Scan'Industry - capture d'écran

B. Fraude physique et fraude numérique

Avant d'aller plus loin, il convient cependant de distinguer deux catégories : la fraude dite « physique » et la fraude dite « numérique », qui se subdivisent également en deux sous-catégories ; les documents volés et les documents produits frauduleusement.



Produits - fraude numérique et fraude physique

La fraude numérique, c'est-à-dire l'ensemble des faux documents fournis sous forme de scans, représente la part la plus importante des documents vendus sur le Dark Web francophone, plus de 80%. Les documents les plus échangés sont les scans de cartes d'identité, puis viennent les scans de permis et de passeports, ainsi que les factures et les justificatifs de domicile.

L'ensemble de ces documents permettent à leurs acheteurs de se créer de fausses identités lors de l'inscription à des services en ligne (banque en ligne, paris et casinos en ligne), mais également de pouvoir recevoir des colis sous une autre identité dans des points relais. Ces services sont souvent ainsi utilisés en complément d'autres délits, afin de pouvoir bénéficier d'une couverture et de ne pas révéler son identité.

Scan de carte d'identité contrefait vendu sur le marché noir francophone French Deep Web Market

Bien plus minoritaire, la fraude physique représente l'ensemble des documents produits ou volés et distribués en format physique. Elle nécessite en effet beaucoup plus de et de matériels pour les faussaires, qui doivent remplir plus de critères que pour les scans de faux documents (ultra-violets, poinçons). Les documents achetés sont utilisés par leurs acheteurs pour des délits dépassant la simple escroquerie (passage de douane, contrôle de police).

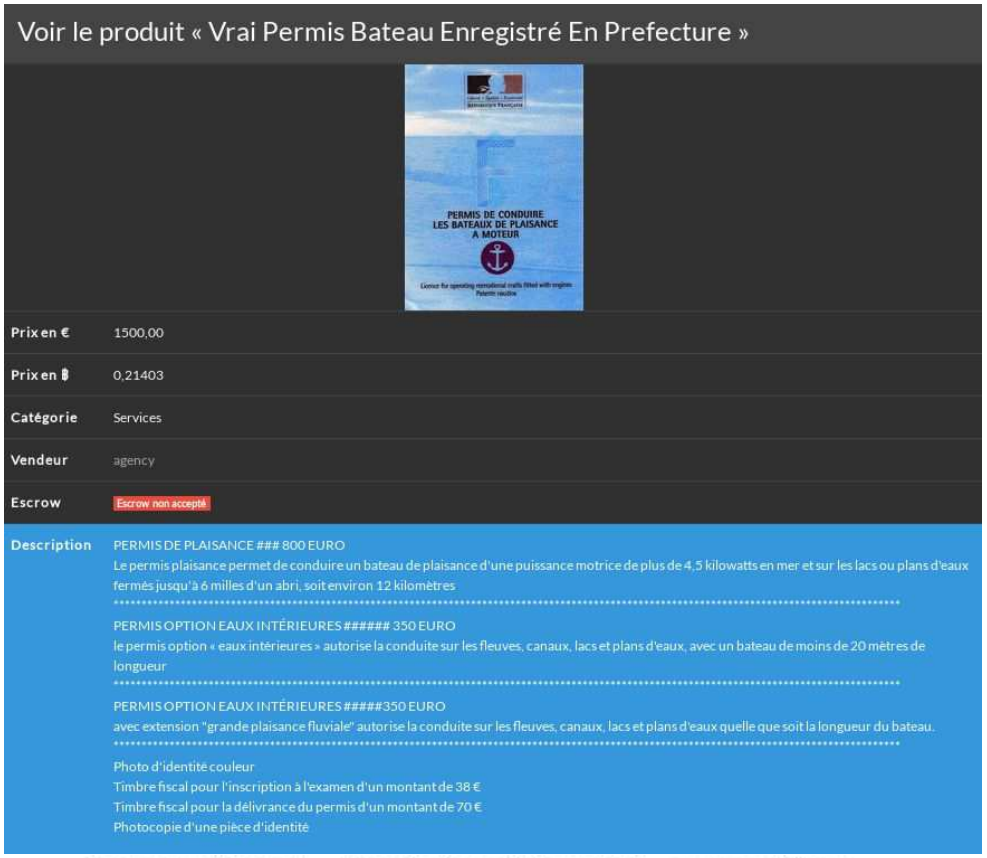
Fausse carte d'identité - French Deep Web Market - capture d'écran

C. Une offre qui s'élargit

L'offre de faux document s'élargit depuis plusieurs années. Bien que les scans de carte d'identité soient les produits les plus distribués, suivis par les scans de permis et de passeports, on peut désormais trouver de faux permis bateau à personnaliser, des cartes grises et des cartes vitales.

Moyenne des prix

Produit	Prix du Scan	Prix Document Physique
Carte Nationale d'Identité	5 euros	100 – 500 euros
Permis de Conduire	10 euros	100 – 300 euros
Passeport	10 euros	100 – 350 euros
Carte Grises	10 euros	X
Carte Vitale	5 euros	X
Permis Bateau	X	1500 – 1800 euros



Faux permis bateau - French Deep Web market - capture d'écran

Conclusion

Le Dark Web est un espace en constante mutation, qui répond aux besoins des cybercriminels. La fermeture de *Silk Road*, ainsi que les révélations faites par Edward Snowden ont conduit à une très forte médiatisation de celui-ci, conduisant à la popularisation d'une légende noire associée à l'utilisation de Tor.

Suite aux nombreuses opérations de police, le Dark Web s'est considérablement réduit, passant à moins de 5 000 sites actifs aujourd'hui, soit un tiers de sa taille à son apogée en 2015. Les contenus pédopornographiques, que nous avons choisi de ne pas traiter dans ce mémoire, restent aujourd'hui minoritaires et plus difficilements accessibles, ces plateformes étant également la cible des pirates du groupe Anonymous, lors des opérations *Darknet* et *Pedohunt*.

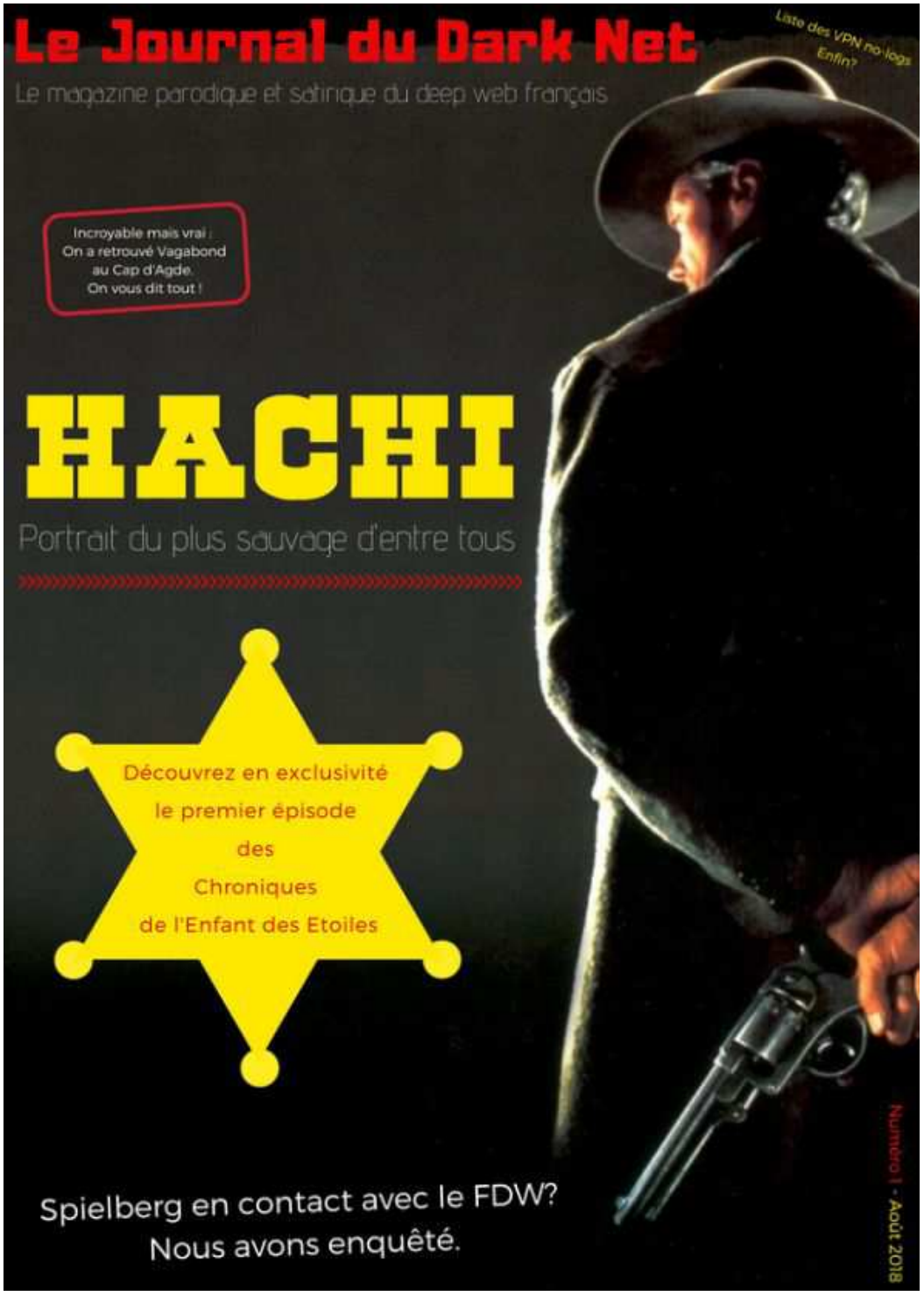
Le Dark Web francophone, plus jeune que ses homologues russe et anglophone, est fortement touché par cette vague médiatique, conduisant à l'explosion de la fréquentation des sites francophones. Cette explosion se traduit également par l'alignement sur les marchés internationaux, alors inexistants sur le Dark Web francophone suite à une demande de plus en plus importante de la part de ses nouveaux utilisateurs. La communauté organisée autour de Liberty's Hackers, la plus ancienne et la plus structurée, a perduré jusqu'à aujourd'hui, au milieu des conflits et crises qui ont touché le Dark Web francophone. L'importance croissante que revêt la cybercriminalité pousse les autorités françaises à se doter d'unités similaires aux darknets units du FBI et d'Europol. La fermeture du marché noir *Black Hand* en juin 2018 marque ainsi une première victoire pour les forces de police française. L'impact de cette opération sur la communauté cybercriminelle francophone s'est fait ressentir dès les premières semaines succédant la chute de *Black Hand*, provoquant un climat de méfiance parmi ses utilisateurs. Le Dark Web francophone est actuellement en pleine restructuration. De nouvelles plateformes sont encore en création, suggérant une année 2019 haute en couleurs pour les cybercriminels. Certains projets de la communauté laissent penser que les administrateurs des plateformes souhaitent s'internationaliser.

Vers la fin du Dark Web tel qu'on l'entend ?

Les récentes opérations menées par les autorités ainsi que le climat de méfiance qui entoure les Dark Web internationaux suggèrent cependant une tout autre hypothèse. Le Dark Web serait-il en déclin ? Les hébergeurs .onion publics et accessibles au grand public tels que *Freedom Hosting II* ou *Daniel's Hosting* ont subi de grosses attaques ces deux dernières années. Les gros marchés noirs et forums bénéficient ainsi de leur propre hébergement. Beaucoup de vendeurs, faute de confiance envers les administrateurs des plateformes de vente s'exportent vers des plateformes accessibles au grand public sur le clear web. On assiste à une forte augmentation des services d'échange et de messageries chiffrés privés tels que Jabber ou Telegram, mais également des services de blockchain DNS, tel que Joker's Stash. Le Dark Web évolue donc vers une nouvelle forme décentralisée, plus difficile à surveiller mais parfois hors des réseaux darknets.

Annexes

Annexe 1 : Journal du Dark Net - Journal satirique du Dark Web francophone - 1e édition, Août 2018



Le Journal du Dark Net

Sommaire

Le Journal du Dark Net

Edité par Liberty Hackers, société anonyme au capital de 1000 BTC
Siège Social : French Deep Web
Responsable de la rédaction et rédactrice en chef : Eir
Rédacteur en chef adjoint : DansTorConnard
Envoyé spécial : Thorgal
Courrier des lecteurs : Dr4z

Le site du JDDN :
http://ljddnu47hxk53gln.onion

EDITO

Aujourd'hui paraît le premier (vrai) numéro du Journal du Dark Net.

Depuis la première maquette, nous avons donc rédigé plusieurs articles et interviews et l'équipe s'est étoffée de nouveaux rédacteurs qui auront leur rubrique tous les mois.

Le Journal du Dark Net est un journal mensuel satirique. Son nom fait allusion au site web Le Journal du Net et s'inspire du Gorafi pour la ligne éditoriale.

Le ton employé, humoristique, est celui de la satire ou de l'ironie. Parfois sévère ou venimeux, il n'est cependant pas vindicatif.

Les interviews publiées sont constituées de véritables déclarations mêlées à des déclarations imaginées.
Nous remercions les personnes qui ont répondu favorablement au jeu de l'interview pour ce premier numéro (d'autres seront publiées ultérieurement).

Nous avons réalisé un site dédié au journal pour conserver les archives des numéros.

Nous vous souhaitons une bonne lecture.

La rédaction.

Le courrier des lecteurs

Par Dr4z

Chers lecteurs, bonjour,

C'est avec joie que je débute avec vous cette rubrique dialogue où nous allons pouvoir discuter, à bâtons rompus, de tous ces petits tracas et petites choses que tout le monde pense tout haut mais que vous voudriez dire tout bas.

À des fins de conservation d'anonymat, les éventuelles fautes d'orthographe de nos lecteurs seront corrigées - ne vous inquiétez pas, mes chéris, maman veille au grain.

Commençons avec une lettre de **splodia54** :

splodia54 a écrit :

Bonjour,

Je comprends pas, j'ai créé un topic et il s'est fait mettre au "dépotoir" pour assistanat. Du coup j'ai fait un autre topic pour demander c'est quoi l'assistanat, et on m'a banni pour assistanat.

Je suis complètement perdu, moi je voulais juste vendre ma beuh à prix d'ami et pas me prendre la tête. Que faire? Merci.

Bonjour splodia54,

Effectivement, c'est très ennuyeux. Je comprends ton désarroi, et sache que beaucoup ici partagent ton mécontentement pour des raisons similaires. Ces derniers finissent généralement par expier leur rage sur le Trollodrôme, où il est libre de se plaindre de tout en tout anonymat, bref, un paradis pour tout francophone râleur qui se respecte.

Concernant ton problème, voici quelques conseils:
Déjà, si tu veux faire de l'achat/vente, c'est sur le market qu'il faut aller, pas sur le forum (section liens utiles). Ça, c'est surtout parce que tes prix d'ami m'intéressent.

N'importe quelle question qui n'est pas bien décorée de recherches préalables passe sous le coup des modérateurs, qui n'hésiteront pas à juger ton sujet trop trivial, indigne du FDW, qui se veut être un idéal de bibliothèque.

Un forum est un endroit où l'on discute, et une bibliothèque est un endroit où l'on se tait, alors faut-il tout dire à demi-mot? À méditer.

En attendant, ne t'en fais pas - il y a une méthode simple pour que ton topic subsiste sur le forum. Dis une connerie, et demande comment améliorer ta connerie. Tu auras bien quelques bonnes âmes au milieu des insultes qui te mettront sur la voie.

100pseudo a écrit :
SAC À MERDE SERPILLÈRE À FOUTRE JE VOUS BAISE PUTE À NÈGRE ENCULÉ NIQUE TA RACE DE TA MÈRE LA GROSSE SUCEUSE DU BOIS DE BOULOGNE BITE CUL CHATTE

Bonjour 100pseudo,

Je pense que j'ai mal compris la question, je t'invite à reformuler.

La corneille a écrit
Je trouve que le deep s'est grandement dégradé. Avant, c'était la belle époque, il y avait une communauté active, des partages dans tous les sens. Aujourd'hui? Il n'y a plus qu'un seul market, et le reste est mort. Même le donjon est hors ligne. Il n'y a plus rien. Et c'est triste.

Ah, le fameux "c'était mieux avant". Eh bien, ceci nous laisse sur une excellente ouverture de fin. Chers lecteurs, que pensez-vous de l'ambiance qui règne sur le deep FR? Un commentaire, des suggestions? N'hésitez pas à nous envoyer vos idées, et vos lettres seront immortalisées dans le prochain numéro!

Bien à vous,
Maman dr4z.

Tragique :
le Trollodrome qui s'auto-hébergeait nous a troll en s'auto-down.

C'est un choc ce matin pour les collégiens du Deep Web et les webédiens sans cervelle : le Trollodrome est down.
DTC a mené l'enquête sur cette tragique disparition.

Au début, tout va bien, après tout ce n'est « qu'un des nombreux down du service LH » disent les plus savants... Mais très vite, une semaine passe.
Les Jean-Trolls s'impatientent, le week-end est déjà là mais le Trollodrome est toujours down...
Que faire alors de leur week-end ? Sans doute se renseigner sur comment faire le Djihad...

Énervé car il venait de lancer son CTF dont tout le monde se foutait, DTC (quelqu'un qui aimerait être important depuis 5 ans) étant dans le secret des dieux, contacte par MP **Scred**, le fondateur de cette plateforme.
« Bah disons qu'au début j'ai demandé à LH de me mettre un petit forum FluxBb oklm pour faire mes bails, mais disons que j'avais plus de quoi payer à un moment... J'suis qu'un étudiant en vrai ! »

Mais voilà, ce que Scred ne savait pas lors du téléchargement du FluxBb sur son PC, c'est qu'au même moment l'IA de Google modifie le code de ce dernier en direct (Scred utilisant Chrome comme tout jeune dynamique de son âge) et le transforme en véritable forum vivant !
« **Au début je comprenais pas ! Je me disais « bah tant mieux »** confie-t-il encore perturbé par cette troublante expérience.

Mais voilà, v1ct0r étant très occupé et hamster faisant la guère aux kikoos et spammers, ils ne remarquent pas le FluxBb se réanimmer...
« Bah moi j'ai des scripts qui font ça tout seuls », nous confie v1ct0r encore dans l'incompréhension. **« Après avoir analysé les logs, le pire, c'est qu'il a bien été down pour défaut de paiement... »**

Pendant plus d'un an, le Trollodrome continue de s'auto-héberger malgré les redoutables commandes de v1ct0r : rien n'y fait.
Et puis, en cette fin de mois de juin, le Trollodrome en a assez : il s'auto-down.
Scred confia que dans le code source était écrit :
« Putain de cassos de merde, vous m'avez saoûlé bande de bolosses, ciao-bye-cimer»
Le tout signé de la clé PGP de l'IA de Google en personne.

Quoiqu'il en soit la préparation d'un nouveau serveur est déjà en cours pour notre plateforme préférée.

Anonymat : « Toujours Plus » Les conseils d'un hamster parano.

La rédaction a concentré pour vous le tutoriel ultime, basé sur les divers et nombreux posts de notre hamster préféré.

Par DTC

1 : Avoir TOR
Bon c'est la base, mais on commence doucement pour pas perdre le lecteur moyen.

2 : Avoir un VPN
Là encore classique. Évidement, no-log cela va s'en dire.

3 : Utilisez une connexion anonyme
Celle d'un voisin, ou mieux : une puce SIM pré-payée.
ATTENTION : pas de lieux publics car « on ne sait jamais ».

4 : Utilisez un BON OS
De préférence Tails ou Whonix. D'ailleurs un très joli débat animé sur FDW vous attend

5 : Avoir un PC anonyme
Payé en liquide (billets tout justes retirés à prendre avec des gants pour ne laisser aucune empreinte), de préférence déjà servis (genre annonce leboncoin).
Bien entendu vous l'achetez cagoulé en forçant votre vendeur à boire et consommer du GHB pour qu'il n'ait aucun souvenir de la transaction. Utilisez pour le rendez-vous un lieu à l'opposé de chez vous (2h de transport minimum).

6 : Choisir ses relais TOR
Blacklister tout nœud appartenant aux divers gouvernements, et au mieux créez vos propres relais !

7 : Utilisez un RaspberryPi entre votre ordinateur et votre BOX
Dessus il faudra installer un OpenVPN (car 2 valent mieux qu'un) ainsi qu'un CRON qui supprimera l'intégralité de tous les logs présents toutes le secondes.

8 : Planquez vos données
Dans une partition Veracrypt, dans une clé USB achetée en liquide cagoulé...(cf étape 5).
Cette clé devra être rangée dans un autre appartement que le votre à minimum 5h de route.

9 : Devenez personne
Trempez vos doigts dans l'acide pour ne plus laisser d'empreinte avant de vous déclarer mort en mairie.
Pensez, au cas où, à quand même utiliser des gants latex.

10 : Débranchez votre WiFi et coupez vos câbles RJ45
De cette manière plus personne n'aura accès à votre ordinateur.

11a : Disparaissez
Rendez-vous sur ces coordonnés GPS et suicidez-vous en vous jetant dans le volcan.
De de fait personne ne sera jamais qui vous étiez et plus personne ne vous attendra !!!

11b : Soignez-vous !
Allez voir un psy, la parano est un sujet très bien étudié...

HACHI
ADMINISTRATEUR DU FRENCH DEEP WEB

ENTRETIEN EXCLUSIF

Propos recueillis par Eir

Hachi, parlons de ton background.
Tu es présent sur le FDW depuis mai 2013.
Qu'est-ce qui t'a attiré vers le deep web et comment en es-tu arrivé à t'inscrire sur le FDW ?
Eir, la noob... Putain les nouveaux il faut toujours tout vous réexpliquer... Bon alors, je suis là depuis que le Deep Web est Deep Web, depuis que TOR existe, et avant même j'étais sur d'autres réseaux Dark Net, ok ?
Je suis le parrain ici alors plus de respect quand tu t'adresses à moi. J'ai eu un autre compte avant de créer "hachi" (ne le cherchez pas, je l'ai supprimé).
Pour le FDW, je l'ai découvert un peu par hasard en trouvant un pastebin qui contenait divers liens vers des sites .onion francophones. L'ambiance du forum m'a plu, je suis donc resté. Je regrette un peu son évolution, on parlerait plus d'involution d'ailleurs.

Sur un pastebin ? Comme un noob en fait ?!
..... (soupir).

On enchaîne :
Le deep francophone prend naissance en 2008.
Quel regard portes-tu sur l'évolution du deep depuis ces dix dernières années ?
A ton avis ? Tu lis ce que j'écris sur le forum ou pas du tout ?
Je porte un regard très pessimiste et très critique sur ce que devient le deep francophone depuis 5 ans.
Le mercantilisme prend de plus en plus de place, au détriment du partage désintéressé d'informations.
Question suivante.

Quel est ton avis sur le deep étranger par rapport au deep francophone?
Je m'en bats la race.
Les anglophones sont seulement plus nombreux, et peuvent donc spécialiser un peu plus les plateformes (au détriment des forums généralistes). C'est tout.

Pourquoi n'es-tu sur aucun autre forum?
Je ne suis sur aucun autre forum avec ce pseudo.
Question suivante.

Tu es modérateur mais également escrow du market afférent au FDW.
Tu déclares bien tes revenus d'escrow aux impôts ?
T'en as pas marre de gérer des conflits ? De tous ces scams qui se répètent à l'infini ?
La modération du market est comme une expérience de sociologie pour moi. Ils sont tous plus cons les uns que les autres. À croire que le fric fait perdre des neurones.
J'en ai marre, mais ça me provoque souvent des crises de fou rire tellement la débilité atteint des abysses insondables.

hachi, arborant fièrement ses derniers achats sur le dark net

Au quotidien, quelles sont tes missions ?
A quoi ressemble une journée type ? Quels sont tes objectifs et quels types de problèmes as-tu à résoudre ?
Ma journée type est assez basique :
- Se connecter
- Lire les discussion privées entre membres du staff
- Répondre aux cons
- Supprimer les comptes de bots et leurs messages qui nous cassent les couilles
- Survoler le forum pour supprimer les assistés et les parasites marketeux qui nous cassent les couilles
- Croire que je vais répondre à certains sujets qui semblent intéressants mais en vrai, j'en ai jamais le temps.

Qu'est-ce qui te plait le plus dans tes missions d'administrateur ?
Enfin une question intéressante !
Je peux assouvir mes envies de tyrannie. Je tape sur des gens qui aiment ça puisqu'ils reviennent toujours. L'histoire du deep le confirme, relisez le forum depuis 2012 vous jugerez par vous même, si toutefois vous avez un cerveau qui fonctionne.

Quels sont les aspects les plus difficiles et selon toi, les inconvénients de ce statut ?
Le plus gros inconvénient est que je dois particulièrement faire attention à ce que j'écris.
Tout le monde me copie, mais personne ne m'égale.
Ca met une pression au quotidien.
La chute de BH est un exemple : les propos des membres du FDW ont été cité dans un article du Monde.
Je lis Le Monde et Libé tous les jours, je n'ai pas le droit à l'erreur. Ma réputation est en jeu à chaque seconde.
Dans les inconvénients, ce qui me déplait le plus, c'est la modération. Modérer ne me laisse que trop peu de temps pour participer aux discussions. Et quand je lis certains topics, ce ne serait pas du luxe que je vienne relever le niveau.

Quelle est ton éthique de travail au sein du forum ?
On est sur le deep chérie, l'éthique c'est pour les autres sur le clear, mais pas ici.
La prochaine fois je te ban pour cette connerie.
J'ai toujours raison, même quand l'autre a raison, il a tort.
Si un frustré vient crier à la censure, c'est qu'il a merdé quelque part.

Tu donnes beaucoup d'informations sur toi, notamment dans ta présentation qui est épinglée, et à la fois tu mets en garde l'ensemble de la communauté en leur disant de ne faire confiance à personne.
Comment tu expliques ce paradoxe ?
A part toi Eir (parfois), je ne fais confiance à personne.
Chaque détail que je donne est mesuré pour découvrir une fausse personnalité, et pour ne jamais connaître ma vie.
Malgré mes plus de 13 000 messages, rien ne permettra de m'identifier.
(Ne parle pas de mon tatouage de dauphin sur mes parties intimes ou je te downgrade novice à vie).

Pourrais-tu nous parler des événements ou des relations humaines qui t'ont marqué durant ton parcours?
C'est Voici ton journal ou c'est un truc sérieux ?
Sans blague, tu crois vraiment qu'un humain m'a touché dans la vie et même pire, ici ?
Pour te répondre parce que tu me fatigues :
Comme évènement, je retiens particulièrement la trahison de Maestro et la disparition de Doc_M.
Je ne détaillerai pas, ce serait trop long.
Dans les relations humaines, je dois signaler Doc_M, Enki et Eir. Je ne détaillerai pas non plus, ce serait trop long et un peu dangereux pour l'anonymat. Enfin le mien (cf le tatouage).

S'il n'y avait pas cette contrainte d'anonymat, quels membres du forum aimerais-tu rencontrer IRL ?
Doc_M (même si c'est trop tard), Enki (je sais qu'il va lire, je n'ai pas abandonné l'idée) et Eir. (N.D.R : l'interview a été réalisée chez lui, sur la terrasse de sa propriété).
Hamster et V1ct0r, même si j'aimerais les rencontrer, je m'abstiendrais. C'est une question de sécurité. Moins on en sait mutuellement sur les membres du staff, plus on se blinde. Et puis le petit hamster là, pour être honnête, je lui casserai bien les pattes arrière. Cette boule de poils tellement adorable, fragile et musclé à force de courir dans sa roue... Rien que d'y penser, je...

Ca va aller hachi. D'ailleurs concernant la zoo...
Putain j'ai assez parlé sur le sujet, il y a un topic de 1000000000 pages sur FDW alors LIS avant de poser des questions de merde !

Quelle est pour toi la meilleure période du FDW et pourquoi ?
Je n'ai pas de période préférée. Chacune a été émaillée de points forts et de trucs très chiants.

Est-ce que tu voudrais bien nous raconter une anecdote, le truc le plus drôle ou invraisemblable qui t'est arrivé ici ?
Un mec a voulu me payer 10 000 € pour que je quitte le deep web et qu'il prenne ma place.

Pourquoi tout le monde rêve de prendre ta place ?
Parce que je suis le fils illégitime de Jésus et de Mahomet.

Tu es intelligent, cultivé, drôle, charismatique, comment vis-tu toutes ces qualités au jour le jour ?
C'est difficile. Voir que le reste de l'humanité est rempli de cons consanguins et stupides est plutôt frustrant.

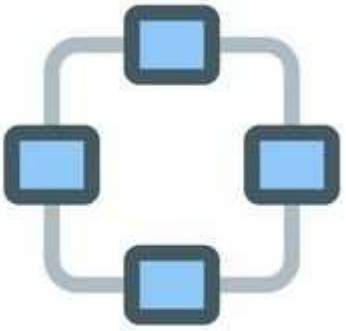
Es-tu conscient de ton charisme hors du commun ?
Oui. Les femmes se jettent à mes pieds, et les hommes sont prêts à me suivre en enfer. Je suis un alpha.

D'où tiens-tu cette classe dans le comportement et la façon de t'exprimer ?
J'ai une autorité naturelle de mâle alpha. Quand je parle, on m'écoute. Quand j'ordonne, on exécute.

Tu as effectué un parcours sans faute, une carrière impeccable, comment fais-tu pour avoir toujours raison ?
Mon secret est simple : Je suis un génie.

Petit à petit tu es devenu indispensable, comment ferait-on sans toi ?
Sans moi, le monde s'effondrerait en 10 minutes.

Informatique :
Top 5 des meilleurs VPN no-logs compatibles SOCKS5



Par DTC

CardSniper (1 message)

salu a tous les ami
vous avez une liste des meilleur VPN no-log conpatible TOR svp ?
c urgent merci !

hamster-guerrier (over9000 messages)
Je lock pour assistanat.

Musique :

Ils étaient au Hellfest, mais ne se sont pas vus. Ils racontent.

Par DTC et Eir

Comme beaucoup de personnes underground, Thibaud va sur le Dark Net et écoute du Métal. Kevin, un autre jeune fait de même que Tommy, Kylian et Brandon, tous prépubères.

« **Ouah c'était trop bien cette année y avait des groupes de ouf !** » nous confie Kevin encore des étoiles plein les yeux.

« **Ouais de ouf, par contre le soleil m'a niqué quand j'étais mort bourré sur l'herbe** » ajoute Tommy héro « Khro » de sa bande de potes.

« **En vrai ça allait** » rétorque Thibaud, un peut plus blasé que les autres car le faisant depuis « **au moins 2 ans sans mes parents mais depuis mes 5 ans si je les compte... »**

Kylian ne ménage pas sa déception : **"La batterie de Dimmu Borgir est trop triggée... et le bassiste de Marylin Manson a fait des pains... c'est abusé ! Sans parler du son de merde à Satyricon... Les mecs cachetonnent et s'en branlent de leurs fans.**
C'est bon, je me désinscris du fan club de Pleymo puisque c'est comme ça."

Brandon s'interroge : **"Vous l'avez vu le mec sur son cheval qui se baladait partout sur le site?**
Il était au concert de Judas Priest avec un haut genre résille super moulant et des bracelets à clous.
Vous l'avez vu??
Je me demande si c'est pas hachi qui était là. Il est fan de Judas Priest depuis 1952.
Il a mis un post sur FDW à MadTweak pour dire qu'il avait pas mal picolé au Hellfest.
Bon moi, en même temps, j'étais perché tout le week-end, on a trouvé d'la came au camping le premier soir, d'la bombe frère, on a TOUT pris le jour même comme des gogols, je ne suis pas redescendu des 4 jours...
Peut-être que j'ai tapé une hallu pour hachi... Ce serait ouff qu'il vienne avec son cheval, sérieux.
Bonjour l'anonymat.
Non mais vous l'avez vu ce type ou pas???? P'tain, mais j'vous parle bordel !!!"

Une année encore palpitante ou personne du DW ne se sera vu.

Cinéma :

Spielberg va faire un film sur les cryptomonnaies et recrute en douce des consultants sur FDW

Par DTC

Informations exclusives :

Tonton beberg nous fait encore chier avec un blockbuster de merde sur un sujet qu'il ne maîtrise pas.

« Pour ne pas reproduire les mêmes erreurs que « Player One » on va faire appel à des consultants cette fois » nous confie l'incontournable réalisateur qui se touche les tétons en observant son reflet dans l'une de ses nombreuses coupes.

« On a décidé d'aller à la source des informations, dans le lieu où tout à commencé : sur le Dark Net » ajoute-t-il en frôlant l'orgasme.

Seulement l'homme déjà âgé se heurte à un problème : il ne sait pas comment y accéder.
Étant brouillé avec la plupart de ses neveux pour une vague histoire d'héritages, il appelle alors Frédéric, sont neveu Québécois de 12 ans qui passe ses journées sur le Trollodrome.

Mais voilà : comme la plupart des ex webédiens, Frédéric ne connaît rien à l'informatique.
Il propose alors à son oncle de le mettre en contact avec des **"gens balèses qui maîtrisent le hacking et tout »** qui pourront le conseiller.

Les rumeurs disent que Hamster et Hachi auraient déjà répondu positivement, **"ne pouvant pas supporter un film de plus de cet imbécile qui n'y connaît rien à l'informatique et aux geeks."**

En espérant donc que le prochain soit moins du fan service et plus proche de la réalité...

Ancien SDF, il devient transformiste au Cap d'Agde

On a envoyé une équipe d'espions du dark net pour réaliser une filature du membre Vagabond.
Après plusieurs mois d'une investigation sans relâche, nous l'avons retrouvé dans sa « real life ».
Ce que vous allez lire va vous faire HALLUCINER !

Par Eir

Longtemps sans domicile fixe, le trimardeur aurait posé son baluchon sous les ponts du Sud-Est courant 2013, une destination qu'il aurait choisi pour la douceur des hivers.
Mendiant le jour, il pratiquait le SE à la nuit tombée sur les clochards alcooliques de son entourage.
Sa méthode : les faire boire de la Villageoise jusqu'à l'ivresse et l'amnésie, et attendre qu'ils soient bien bourrés pour leur proposer une petite incartade charnelle en échange de rémunération. Les pauvres clochards se faisaient dépouiller des maigres revenus de la journée mais Vagabond était déterminé à s'en sortir, même si ça devait passer par la souillure de son corps.
Un soir, quelqu'un lui parle d'une "pizzeria cabaret" située non loin de sa tente Quechua, ce moment fut pour lui une révélation : il sera artiste transformiste à la Pizzeria Le Rencard, au Cap d'Agde.

Otto W. ancien taulard aujourd'hui patron de l'établissement, nous raconte : **«Quand il est venu nous voir pour proposer sa candidature, j'ai vu immédiatement qu'il avait le profil. Il a chanté L'Aigle Noir de Barbara et a fini de me convaincre en décrivant sa passion pour les reines Egyptiennes. Je me suis dis qu'il apporterait un nouveau souffle à mon affaire, proche du dépôt de bilan. En plus, sans papiers, aucune exigence sur le salaire, c'était tout bénéf pour moi."**

Le nécessiteux ne rechigna pas devant le travail et se donna corps et âme en représentation chaque soir pendant 4 ans sous le pseudonyme "Néfertiti".
De plus en plus proche du patron de l'établissement, il prit confiance, ce qui un jour, le perdit.
Le masque est tombé le 21 juin 2018, un soir de fête de la musique.

L'équipe de transformistes avait l'habitude de se réunir après la fermeture pour boire quelques verres. L'ancien clochard habitué de la pratique du SE avait toujours fait attention à boire raisonnablement, pour garder le contrôle, sauf un soir, où dans l'ivresse, il se confia à ses collègues en leur parlant de ses activités sur le dark net.
D'après une source sûre qui souhaite rester anonyme :**"Quand il nous a dit qu'il traînait sur le « dark net », au début on y a pas cru ! On a comme image des dangereux criminels, des violeurs, pédophiles et autres vendeurs de mort, et lui, c'est tout l'inverse ! Un homme tellement sensible... Il ne retient pas ses larmes quand on met le disque de Garou sur la platine CD»**

Une autre source confirme : « **Un garçon très gentil, toujours poli, il disait bonjour à tout le monde, c'est un véritable choc d'apprendre ça.** »

Et d'ajouter : « **Ce n'est que plus tard qu'on a réalisé l'imposteur il était. Quand il s'est vanté d'être le meilleur en informatique sur le dark net, que personne ne l'égalait. Mais quand on voit son visage d'ange, on y croit pas une seconde, il le talent et le physique d'une danseuse étoile, pas d'un dangereux hacker.**»

Les Chroniques de l'Enfant des Étoiles

En l'an de grâce 2018, dans les tréfonds de la fosse des Mariannes, un fléau se réveille.

Ce qu'il va provoquer dépasse les limites de votre imagination… et de la mienne.

Sharon@libertygb2nyeyay.onion : "Ca ne m'intéresse pas, passons à autre chose".
Okay sharon. Un peu plus près alors.

Paris, 14H18, Kevin se réveille. Il allume son joint fait avec du tabac bon marché et se rend nonchalamment vers sa porte pour ouvrir le nouveau colis cardé qu'il vient de recevoir. « Une nouvelle PS4, trop bien. » pensa t-il. Avant de la jeter quelques secondes plus tard dans le taudis qui lui sert de chambre.

Il allume ensuite son pc et nettoie un peu pendant l'allumage son clavier recouvert de foutre. Cortana l'accueille de sa voix mielleuse : « Bonjour Kevin, que puis-je faire pour vous aujourd'hui ?»

"Ouvre Tor Browser, répondit-il. Et lance 'bukakespecialkawaï2hours.mov' en même temps."

Alors qu'il se connecte tranquillement à l'administration de dfas (un forum très très #dark et #antisystème) pour répandre la bonne nouvelle, notre héros effectue en même temps des recherches sur stopmensonges.com à la recherche des derniers complots impliquant les élites judéo-reptilo-illuminatiaçoniques ces derniers jours.

Il tombe alors sur un fait divers qui attire son attention.

"UN GORILLE EN TUTU A ÉTÉ RETROUVÉ SÉQUESTRÉ DANS UNE CAMIONNETTE AU BOIS DE BOULOGNE"

Son sang ne fait qu'un tour dans ses veines et il s'empresse de cliquer sur l'article.

"UN GORILLE RÉPONDANT AU NOM DE TOTOCHE RETROUVÉ DANS UN ÉTAT GRAVE"

Notre reporter s'est rendu sur place et nous raconte.

« C'est avec effroi ce matin que je me suis rendu au bois de boulogne pour ma ronde journalière. Je ne m'attendais vraiment pas à découvrir ce que j'ai vu. Il y avait un gorille affamé vêtu d'un tutu dans une camionnette de gitans. Celle-ci a attiré mon attention quand je passais car elle n'arrêtait pas de remuer dans tous les sens et j'entendais des cris.

« SCAM EXIIIIIT !!!! Cette salope m'a SCAM EXIIIIIT !!!! » hurlait la voix.

Lorsque j'ai ouvert le van, la créature que j'ai aperçu faisait vraiment de la peine à voir. Elle s'était arrachée à plusieurs endroits de bonnes touffes de poils et partout au sol jonchaient des cadavres de hamsters en décomposition accompagnés d'oignons frits. Elle en avait encore un en bouche lorsque je l'ai découverte.
Détail insolite : sur son front étaient scotchés ses papiers d'identité.
On y lisait :
Totoche Dubontier, 52 ans.
Accompagné d'un post-it : après 34 ans au RSA, il prend aujourd'hui une retraite anticipée.

Partout au mur était également accroché toutes sortes d'images reliées entre elles par des traits. Nous n'avons pas encore compris leur signification mais nos équipes d'experts professionnels ultra spécialisés sont en train des les étudier.

Après avoir appelé le chenil, nous avons dû lui injecter une solide dose de kétamine pour calmer la bestiole. Celle-ci voulait nous avertir d'un dangereux complot impliquant « Elle hache », « Tout le tard que nette» et « La déjouer est-ce eux ».

Ses propos, ensuite suivis de nombreux « Je le savais » ou de « Méfiance, c'est louche » nous semblant trop incompréhensibles pour être retenus, nous avons décidé de confier la bête au département de psychiatrie lourde de l'hôpital Sainte Mangouste. Après diverses analyses, il s'est avéré que son taux de scamexitine (une hormone responsable du sentiment de persécution) a été estimée à « Over 9000 », un véritable record dans le milieu.
Mais qu'est-ce qui a bien pu lui causer autant de dommages?!
En tout cas, nous prions pour le sort de cette créature. La vie est parfois cruelle. »

XXXXXXXXXXXXX

Kevin mis du temps à revenir à lui après la lecture de l'article.
Son chef venait de tomber, tous ses soupçons étaient bien réels.
"Maintenant ils vont le torturer pour qu'il leur révèle tout ce qu'il sait" rumina t-il.

"Le FBI et la CIA sont dans le coup, c'est sûr!"
Ils vont faire tomber le réseau Tor, l'Univers et le reste.
"Qu'est-ce que je dois faire ?" lança t-il à haute voix.
Un silence de plomb envahit l'atmosphère. Avant que les terribles mots de la voix d'une I.A. retentissent.

"J'ai contacté l'agent Smith, il va venir s'occuper de votre problème. J'espère avoir pu vous être utile." répondit Cortana.

"Diagnostique en cours, veuillez ne pas éteindre votre système."

XXXXXXXXXXXXX

Kevin réussira t-il à sauver totoche le gorille avant qu'il ne soit trop tard?
Comment l'animal en est arrivé là?
Les autorités sauront-elles démêler cette sombre histoire?

Vous le découvrirez dans le prochain épisode des "**Chroniques de l'Enfant des Étoiles**".

Source

Le Dark Web est caractérisé par l'absence de sources officielles. Notre analyse a été construite en utilisant les informations recueillies lors de nos recherches (voir méthodologie de recherche) et en utilisant les données de la base Darknet Market Archives, Gwern Branwen.

Darknet Market Archives - *Mirrors of ~89 Tor-Bitcoin darknet markets & forums 2011-2015, and related material,*
https://archive.org/download/dnmarchives/dnmarchives_archive.torrent

Bibliographie

Aleph – GrayMatter, *Deep Web, Hidden Web... la face cachée d'internet*,
http://www.aleph-graymatter.com/deepweb-darkweb-la-face-cachee-dinternet/. (5 décembre 2018)

Berlin Staff and agencies in, *German police shut down one of world's biggest Dark Web sites*,
https://www.theguardian.com/world/2019/may/03/german-police-close-down-dark-web-marketplace.
(5 mai 2019)

Bertin IT, *Démystifier le Dark Web en 10 points !*,
https://www.bertin-it.com/replay-webinar-dark-web/. (28 janvier 2019)

Brackett Eric, *Reddit Bans Communities Dedicated to Illegal Goods*,
https://www.digitaltrends.com/social-media/reddit-bans-illegal-communities/. (7 avril 2019)

Britannica The Editors of Encyclopaedia, *Bulletin-board system*,

https://www.britannica.com/technology/bulletin-board-system. (11 avril 2019)

Browse the Tor Onion Services, https://www.tor2web.org/. (15 mars 2019)

Busted: *The inside story of 'Operation Firewall'*, https://searchsecurity.techtarget.com/news/1146949/Busted-The-inside-story-of-Operation-Firewall. (11 avril 2019)

Cadwalladr Carole, *Drugs 2.0: The Web Revolution That's Changing How the World Gets High by Mike Power – review*, https://www.theguardian.com/books/2013/may/12/drugs-web-revolution-power-review. (15 avril 2019)

Chen Adrian, *The Underground Website Where You Can Buy Any Drug Imaginable*, https://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160. (4 avril 2019)

Cimpanu Catalin, *Ichidan Is a Shodan-Like Search Engine for the Dark Web*, https://www.bleepingcomputer.com/news/security/ichidan-is-a-shodan-like-search-engine-for-the-dark-web/. (24 février 2019)

Cimpanu Catalin, *Russian Authorities Announce Takedown of RAMP Dark Web Marketplace*, https://www.bleepingcomputer.com/news/security/russian-authorities-announce-takedown-of-ramp-dark-web-marketplace/. (15 février 2019)

Crawling Dark Web Sites on the TOR network,

https://ache.readthedocs.io/en/latest/tutorial-crawling-tor.html. (5 décembre 2018)

Cyrille Savelief, *Dark Analytics*, https://observatoire-fic.com/dark-analytics-par-cyrille-savelief/. (26 janvier 2019)

Dark Web Map, https://www.hyperiongray.com/dark-web-map/. (15 novembre 2018)

Décary-Hétu & Giommoni 2016, *"Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous"*

EMCDDA 2017, *"Drugs and the darknet: Perspectives for enforcement, research and policy"*

Europol, *DeepDotWeb shut down: administrators suspected of receiving millions of kickbacks from illegal dark web proceeds*, https://www.europol.europa.eu/newsroom/news/deepdotweb-shut-down-administrators-suspected-of-receiving-millions-of-kickbacks-illegal-dark-web-proceeds. (15 mai 2019)

Europol, *Operation Onymous*, https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-onymous. (9 avril 2019)

Farivar Cyrus and Utc, AlphaBay taken down by law enforcement across 3 countries, WSJ says, https://arstechnica.com/tech-policy/2017/07/report-alphabay-notorious-dark-web-drug-website-shuttered-by-feds/. (24avril 2019)

Ghosh, 2017, *"ATOL: A Framework for Automated Analysis and Categorization of the Darkweb Ecosystem"*

Greenberg Andy, '*Silk Road 2.0' Launches, Promising A Resurrected Black Market For The Dark Web*, https://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/#29c7b62f5714. (24 avril 2019)

Gwern, Darknet Market Archives (2013-2015), https://www.gwern.net/DNM-archives. (30 mai 2019)

Haase Mark E., Freedom Hosting 2: Overview, https://blog.hyperiongray.com/freedom-hosting-2-overview/. (22 mai 2019)

Inc, Tor, https://2019.www.torproject.org/about/overview.html.en (29 mai 2019)

Kruithof, 2016, *"Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands"*

Le site de vente illégale Dream Market annonce son déménagement, https://www.lemonde.fr/pixels/article/2019/03/28/le-site-de-vente-illegale-dream-market-annonce-son-demenagement_5442702_4408996.html. (28 avril 2019)

Legifrance - Le service public de l'accès au droit,

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000035638782&dateTexte=&categorieLien=id. (7 avril 2019)

Lewis Sarah Jamie, *OnionScan Report June 2016* - Snapshots of the Dark Web, https://mascherari.press/onionscan-report-june-2016/. (18 novembre 2018)

Lewis Sarah Jamie, *OnionScan Report: Freedom Hosting II, A New Map and a New Direction.*, https://mascherari.press/onionscan-report-fhii-a-new-map-and-the-future/. (28 novembre 2018)

Lewis Sarah Jamie, *OnionScan Report: Reconstructing the Finances of Darknet Markets through Reputation Systems*, https://mascherari.press/onionscan-report-forensic-finances-dark-markets/. (24 novembre 2018)

Lorenzo-Dus & Di Cristofaro 2018, *"'I know this whole market is based on the trust you put in me and I don't take that lightly': Trust, community and discourse in crypto-drug markets"*

Martin & Christin 2016, *"Ethics in Cryptomarket Research"*

McMillan Robert and Aruna Viswanatha, *Illegal-Goods Website AlphaBay Shut Following Law-Enforcement Action*, https://www.wsj.com/articles/illegal-goods-website-alphabay-shut-following-law-enforcement-action-1499968444. (5 mai 2019)

Meredith Leah, *Insider Report: Darknet reacts to Dream Market announcement*, https://www.darkowl.com/blog/darknet-reacts-to-dream-market-announcing-their-upcoming-closure. (11 mai 2019)

Meredith Leah, *Russians on the Darknet Part II: Marketplaces & Forums*, https://www.darkowl.com/blog/2019/russians-on-the-darknet-marketplaces-amp-forums. (18 mai 2019)

Moeller et al 2017, *"Flow My FE the Vendor Said: Exploring Violent and Fraudulent Resource Exchanges on Cryptomarkets for Illicit Drugs"*

Nasa-Jpl-Memex, *Nasa-jpl-memex/memex-explorer*, https://github.com/nasa-jpl-memex/memex-explorer. (5 octobre 2018)

O'Neill Howell, *How the Internet powered a DIY drug revolution*, https://www.dailydot.com/crime/hive-silk-road-online-drug-culture-history/. (7 avril 2018)

O'Neill Howell, *The uncensored history of the Internet's drug revolution*, https://kernelmag.dailydot.com/issue-sections/features-issue-sections/11680/hive-silk-road-drugs-history/. (18 avril 2018)

Operazione "Babylon": la Postale scopre un mercato illecito nella darknet, https://www.poliziadistato.it/articolo/39585. (11 février 2019)

Petit Adrien, *Piratage informatique et acquisition de compétences : focus sur la communauté arabophone*, https://observatoire-fic.com/piratage-informatique-et-acquisition-de-competences-focus-sur-la-communaute-arabophone/, (19 février 2019)

Petit Adrien, *Note Stratégique: L'influence du Dark Web sur la démocratisation du*

Malware-As-A-Service,
https://observatoire-fic.com/note-strategique-linfluence-du-dark-web-sur-la-democratisation-du-malware-as-a-service/. (8 novembre 2018)

Pielco11, Pielco11/DOGE, https://github.com/pielco11/DOGE. (14 octobre 2018)

Poulsen Kevin, *Kingpin / How One Hacker Took over the Billion Dollar Cyber Crime Underground, Crown Publishers,* 2010. (11 avril 2019)

US-CERT, *Ransomware*, https://www.us-cert.gov/Ransomware. (20 avril 2019)

Rayna Stamboliyska, '*La face cachée d'Internet*', 7 juin 2017

R/RedditAlternatives, Reddit - *Dread*,
https://www.reddit.com/r/RedditAlternatives/comments/b34ciy/dread/. (26 avril 2018)

Rennard Jean-Philippe, *Darknet chapitre 1*, http://www.rennard.org/Darknet/presentation.html. (16 avril 2019)

Riha, *Surface Web vs Deep Web vs Dark Web vs Darknet*,
https://www.firecompass.com/blog/darkweb-deepweb-darknet-browsers/. (8 octobre 2018)

Rolland Sylvain, *Cybercriminalité : qui sont les escrocs du darknet français ?*,
https://www.latribune.fr/technos-medias/cybercriminalite-qui-sont-les-escrocs-du-darknet-francais-59

9111.html. (7 mai 2019)

Schwartz Mathew, Feds Bust *'Farmer's Market' For Online Drugs'*, https://www.darkreading.com/attacks-and-breaches/feds-bust-farmers-market-for-online-drugs/d/d-id/1103901. (4 avril 2019)

Sixgill, *Dark Web Provides Cybercriminals With Trojan FAQ*, https://www.cybersixgill.com/trojan-faq/. (24 février 2019)

Sixgill, *Dark Web as Platform for Hactivist Warfare*, https://www.cybersixgill.com/dw-as-platform-for-hactivists/. (26 avril 2019)

S-Rah, S-rah/onionscan, https://github.com/s-rah/onionscan. (18 octobre 2018)

Sheils Conor, *The Dark Web & Deep Web: How To Access The Hidden Internet Today*, https://digital.com/blog/deep-dark-web/. (10 février 2019)

Stone Zara, *Grams, The Google Of The Dark Web Has Shuttered Operations*, https://www.forbes.com/sites/zarastone/2017/12/16/grams-the-google-of-the-dark-web-has-shuttered-operations/. (28 mars 2019)

This is What a Tor Supporter Looks Like: Edward Snowden, https://blog.torproject.org/what-tor-supporter-looks-edward-snowden. (7 avril 2019)

Two Israelis arrested in international dark web takedown involving FBI, https://www.timesofisrael.com/two-israelis-arrested-in-international-dark-web-takedown-involving-fbi/. (15 mai 2019)

The Tor Project | Privacy & Freedom Online, https://www.torproject.org/about/history/. (11 avril 2019)

US busts online drugs ring Farmer's Market, https://www.bbc.com/news/world-us-canada-17738207. (5 avril 2019)

Users, https://metrics.torproject.org/userstats-relay-country.html. (20 mai 2019)

Vaas Lisa, *Dark web marketplace Wall Street Market busted by international police*, https://nakedsecurity.sophos.com/2019/05/07/dark-web-marketplace-wall-street-market-busted-by-international-police/. (11 mai 2019)

Wbur, *U.S. Activists Help Egyptians Elude Online Censorship*, https://www.wbur.org/hereandnow/2011/01/31/egypt-internet-government. (16 février 2019)

What is malware (malicious software)? - Definition from WhatIs.com, https://searchsecurity.techtarget.com/definition/malware. (10 novembre 2018)

Yuan et al 2018, *"Reading Thieves' Cant: Automatically Identifying and Understanding Dark Jargons from Cybercrime Marketplaces"*

Zataz, 'Attaque dans le Dark Web : 6 500 sites effacés définitivement'

https://www.zataz.com/attaque-dans-le-dark-web-6-500-sites-effaces-definitivement (17 mai 2019)

Zataz, '*Black market : La police a aussi infiltré Dream Market*',

https://www.zataz.com/black-market-fbi-a-infiltre-dream-market (17 mai 2019)

Table des matières