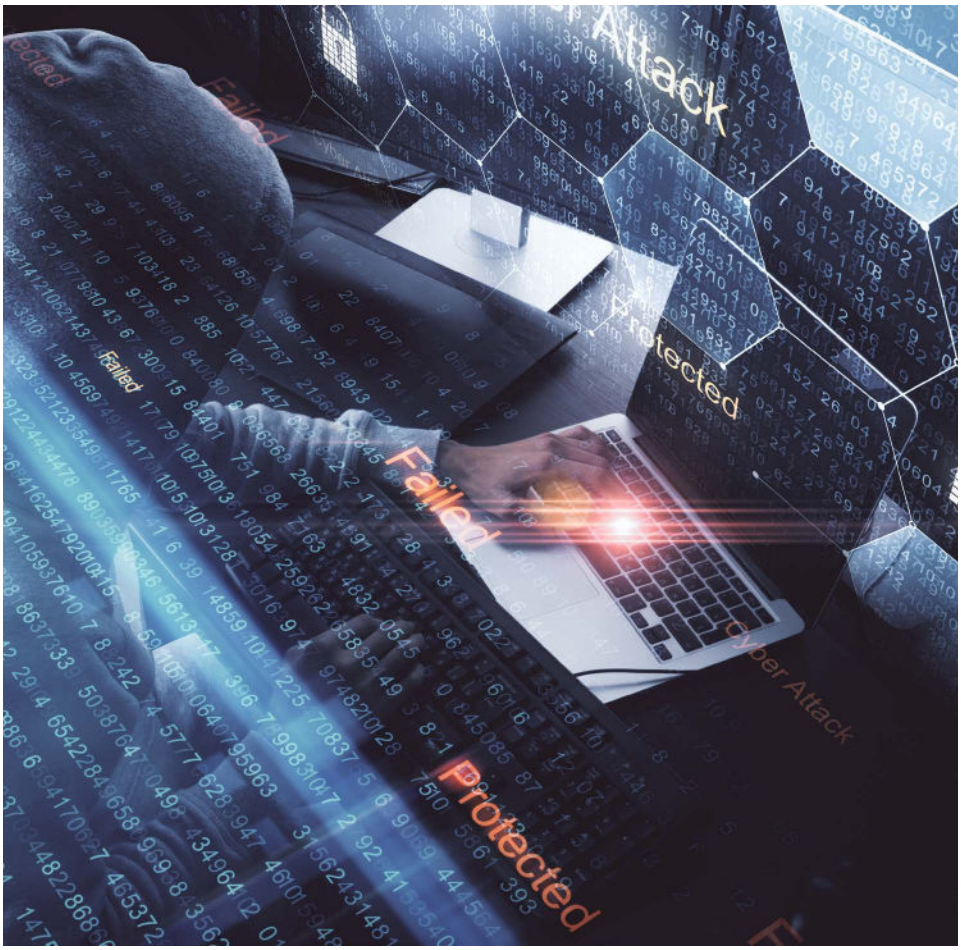
Livre blanc

TOUJOURS PLUS DE LUMIÈRE SUR LE DARK

Tome 2



ALEPH

Avant-propos

Après le succès et les retours positifs de nos lecteurs sur le tome 1 " Le livre blanc qui éclaire le dark ", nous avons le plaisir aujourd'hui de vous présenter le tome 2 : " Toujours plus de lumière sur le dark ".

L'équipe Aleph remercie ses lecteurs pour leurs questions pertinentes et leurs remarques constructives, auxquelles nous tentons de répondre dans ce nouveau tome. Vous nous avez demandé d'aller plus en profondeur et d'entrer dans le contenu-même du dark web. Ce second tome vous entrainera à travers le dark web pour vous permettre de mieux appréhender la nature des activités qui s'y trouvent.

Tout comme le premier tome, ce livre blanc a été rédigé par les experts Aleph grâce à leur connaissance du dark web, de ses communautés, de ses sinuosités et de ses pièges.

Mettons encore plus de lumière sur cette zone obscure...

Nous vous souhaitons un très bon moment de lecture !

Précisions importantes

- De très nombreux escrocs sévissent sur le dark web. Il est donc tout à fait possible que certains sites que nous mentionnons soient des arnaques pures et simples.
- Ce livre blanc n'a pas pour vocation de faire la promotion des sites du dark web. Elle n'a pas davantage vocation à procurer des conseils pour faire des transactions en toute sécurité sur ces sites. Il s'agit ici uniquement de décrire les types de biens et services qui sont proposés à la vente dans le périmètre du dark web. Pour cette raison, nous ne donnons aucune adresse de site et toutes les coordonnées de contact pouvant figurer sur les captures d'écran sont floutées.

Sommaire

#1 Introduction p4

#2 Qu'est-ce que le dark web d'un point de vue technique et pratique ? p5

#3 Les communautés sur le dark web (Hackers) p8

#4 Les ransomwares sur le dark web p12

#5 Les places de vente dans le dark web : p18

#5.1 Vente d'armes et de stupéfiants p18

#5.2 Les contrefaçons p23

#5.3 Les opérations financières p28

#5.4 Raretés et légendes urbaines p33

#6 Conclusion p38

ALEPH

01

Introduction

La réputation sulfureuse du dark web est-elle méritée ?

Si depuis ces vingt dernières années le web est devenu un outil de traçage et de partage de données dans notre société, et ce quels que soient les domaines d'activité et les profils utilisateurs, la crise COVID a encore renforcé et accéléré ce phénomène.

En effet, le télétravail, les VPN, les applications téléphoniques, le tout numérique a permis au dark web d'évoluer en terme de contenus et d'usages. Si initialement le dark web avait des objectifs sociétaux (liberté d'expression, activisme...), il est aussi devenu la plateforme, le réceptacle d'une multitude d'activités illégales.

Par exemple, la quasi-totalité des acteurs du Ransomware distribue les données volées au sein du dark web et anime son activité dans cette enceinte.

C'est donc dans sa grande diversité que nous souhaitons vous introduire dans le dark web.

Ce livre blanc tentera de vous sensibiliser aux cybermenaces mais aussi aux autres activités présentes dans cet environnement varié et étonnant.

Souvenez-vous, nous avons dessiné dans le premier tome la structure générale du dark web. L'objectif de ce deuxième tome est de vous présenter les différents réseaux qui le constituent. Nous allons également décrire certaines communautés exerçant et s'exprimant dans le dark web, ainsi que les places de vente qui y ont élu domicile et y font leurs affaires...

Saisissez une lampe torche et laissez Aleph vous guider.

Qu'est-ce que le dark web d'un point de vue technique et pratique ?

L'émergence de réseaux dans le réseau

C'est au début des années 2000 qu'un besoin de technologies permettant une forme d'anonymat sur internet émerge. Quelques rares pionniers s'y attèlent et la solution envisagée est de créer un **'réseau dans le réseau'.**

Tout d'abord, Ian Clark lance la première version de **Freenet**, qui propose un réseau totalement distribué permettant de stocker de l'information de manière anonyme. En 2003, le développeur zzz lance la première version de **I2P** (Internet Invisible Protocol), qui va proposer un réseau décentralisé pour permettre des communications anonymes. Puis enfin **Tor**, issu de recherches effectuées dans les années 90 sera disponible dans sa première version publique en 2004.

https://freenetproject.org

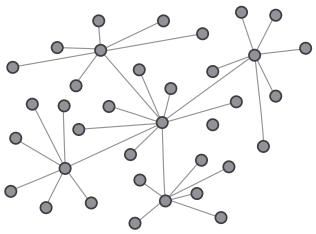
https://geti2p.net

https://www.torproject.org

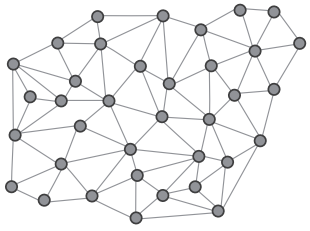
Le dark web est ainsi né autour de ces trois technologies. Il allait alors se différencier techniquement du web standard par l'apport d'une technologie d'anonymisation by design. **Ces 3 technologies proposent chacune des fonctionnalités différentes.**

	Freenet	I2P	TOR	Web
Communication anonyme by design	OUI	OUI	OUI	NON
Internet Caché	CHK : / SSK :	Extension des sites b32.i2p	Extension des sites .onion	Deep web
Accès Au web Anonyme	NON	NON	OUI	NON
Stockage Anonyme	OUI	NON	NON	NON
Friend to Friend	OUI	NON	NON	NON
Topology / Design	Distribué	Décentralisé	Décentralisé	Centralisé

Centralisé



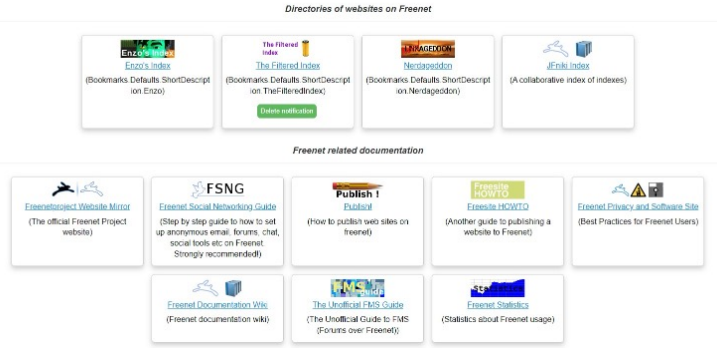
Décentralisé



Distribué

Freenet :

Très résilient, et procurant certainement l'anonymat le plus fort des trois, il permet de stocker de l'information de manière anonyme en utilisant un réseau distribué mais aussi un stockage des données distribuées. Il a ainsi permis de créer un dark web dans lequel les sites sont exclusivement des fichiers. Il permet aussi de communiquer via des forums ou un réseau social. Le fait qu'il soit totalement distribué lui permet une forte résilience, mais aussi une lenteur certaine.



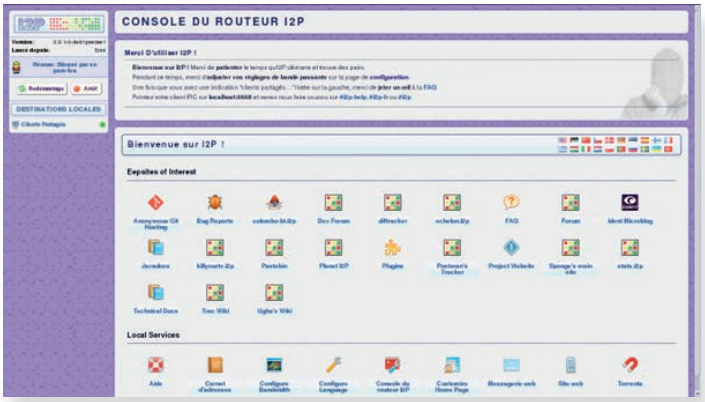
Comment accéder au dark web de Freenet ?

Quelques point d'entrée sont disponibles dès la page d'accueil de Freenet.

I2P :

Il a la force de la souplesse et permet d'anonymiser d'autres technologies comme, par exemple, le protocole de téléchargement torrent. Ainsi, il permet de rendre discrets les outils de téléchargement à base de fichiers torrent.

Comme Tor et Freenet, I2P dispose de son propre dark web ; celui-ci est constitué de micro sites web hébergés sur votre ordinateur (finissant par l'extension b32.i2p). On ne peut y accéder qu'en entrant dans le réseau anonyme I2P.



Comment accéder au dark web de I2P ?

Quelques sites du dark web I2P sont disponibles en utilisant l'interface.

Tor :

De la même façon que I2P, Tor est composé de plusieurs sites web dont le nom des sites finit par l'extension .onion. C'est certainement le réseau le plus volumineux en termes de contenu ; la mise en forme des sites du réseau Tor est d'une qualité identique à celle du clear web. C'est néanmoins son utilisation permettant d'anonymiser l'accès au web qui a fait son succès.

Si Tor a pris la quasi-totalité de l'espace en termes d'usage, il n'en reste pas moins que chacune de ces technologies garde des propriétés intrinsèques dignes d'intérêts :

- **Tor : accès au web standard de manière anonyme**
- **Freenet : stockage résilient et anonyme**
- **I2p : anonymisation multi-protocoles**

C'est grâce au fait que l'accès au web standard était possible en utilisant Tor (et plus spécifiquement le navigateur Tor Browser) que le dark web a pu se développer comme un ensemble de sites cachés finissant par l'extension .onion, accessibles avec le même navigateur.

Comment accéder au dark web de TOR ?

L'installation de Tor Browser est nécessaire, mais vous n'accéderez qu'à la page d'accueil du navigateur ; celle-ci vous propose d'effectuer des recherches via le moteur Duck Duck Go, mais les résultats que ce moteur vous proposera vous renverront sur des sites du clear web. Vous aurez donc besoin de trouver un point d'entrée (répertoires de sites onion ou moteurs de recherche dédiés au réseau Tor)

Et le web ?

.. et les webs ! La démocratisation du web et son essor fulgurant ont mis les moteurs de recherche au centre de l'accessibilité du web. Cependant, certains sites sont très mal référencés par lesdits moteurs, voire non référencés ; ils sont soit " perdus " au milieu du web (ils apparaîtront donc dans les dernières pages de résultats, que personne ne consulte jamais), soit paramétrés par l'administrateur de manière à ne pas être référencés par les moteurs de recherche, pour des raisons de discrétion. Ainsi, cette zone du web très faiblement accessible allait devenir le deep web, par opposition au clear web (le web utilisé par le plus grand nombre). Par opposition au dark web, les sites du clear et du deep web partagent la même technologie centralisée non anonyme by design.

A RETENIR :

1 - Il existe trois grands réseaux dans le dark web : **Freenet, Tor et I2P, avec des schémas de réseau différents**. À l'instar de I2P et Tor qui ont les mêmes caractéristiques décentralisées, Freenet est un réseau créé de façon distribuée, permettant un fort anonymat.

2 - Avec près de 100 000 sites actifs, Tor est le réseau du dark web le plus utilisé (contre moins de 10 000 pour I2P).

3 - Il est très difficile de naviguer dans ces webs. En effet, les moteurs de recherche publics sont rares et de piètre qualité (**cf. Tome 1 : chapitre sur les moteurs de recherche**), les utilisateurs du dark web utilisent de manière générale des sites proposant des listes de sites identifiés sur le dark web (comme au début du web classique).

Aleph Search Dark est un outil essentiel qui permet de naviguer sur l'ensemble de ces réseaux en toute sécurité et discrétion. Il permet la recherche et l'analyse, la visualisation de contenus et la cartographie des sites concernés. C'est un moteur de recherche et d'analyse indépendant, avec lequel il est possible d'avoir une vue d'ensemble du dark web et d'une partie du deep web en quelques clics.

Les communautés sur le dark Web : Les hackers

Initialement conçu pour garantir l'anonymat et contourner la censure, le dark web permet une liberté quasi-totale d'expression et d'action. C'est dans cet environnement anonyme que des hackers évoluent. Il n'est plus nécessaire d'avoir de solides connaissances techniques pour effectuer une **cyberattaque**. Désormais, il est possible d'engager un hacker ou de suivre un guide sur un forum. Les hackers à forte compétence opèrent désormais en groupe pour renforcer leurs connaissances, leur anonymat et **factoriser** leurs ressources.

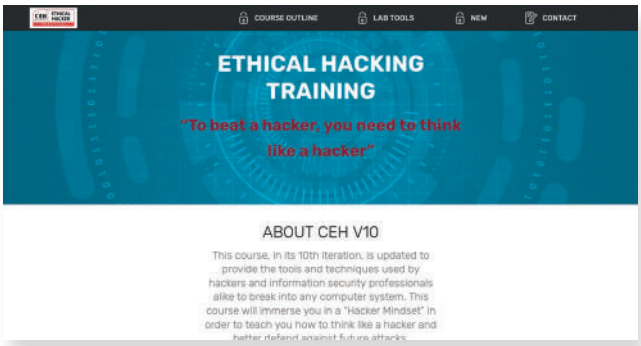
La présence de deux types de hackers

Lorsque nous parcourons le dark web nous pouvons observer l'activité de **black hats** mais aussi de **white hats.**

Un white hat est un hacker doté d'une éthique, il s'oppose au **black hat**, qui lui est un hacker malintentionné.

Mais tout n'est pas toujours blanc ou noir, certains hackers peuvent être gris. Ils agissent alors différemment, parfois avec éthique, parfois non, en fonction des sujets qui les intéressent ou qu'ils défendent.

Peu importe la couleur du chapeau, leur présence se traduit essentiellement par des blogs qui ont trait à la technologie de l'anonymat, ou des sites officiels de conférences de hackers.

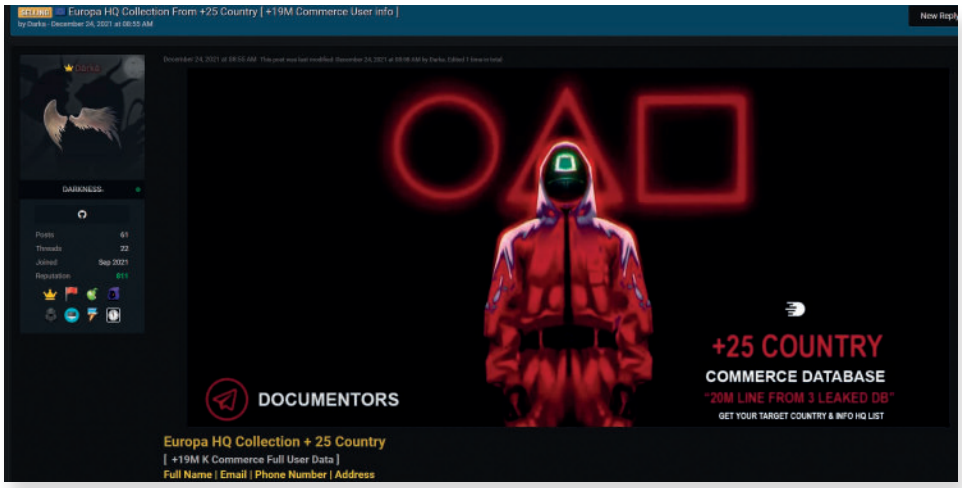


Miroir en .onion du site ' hack this site.org '– Exemple de White hat

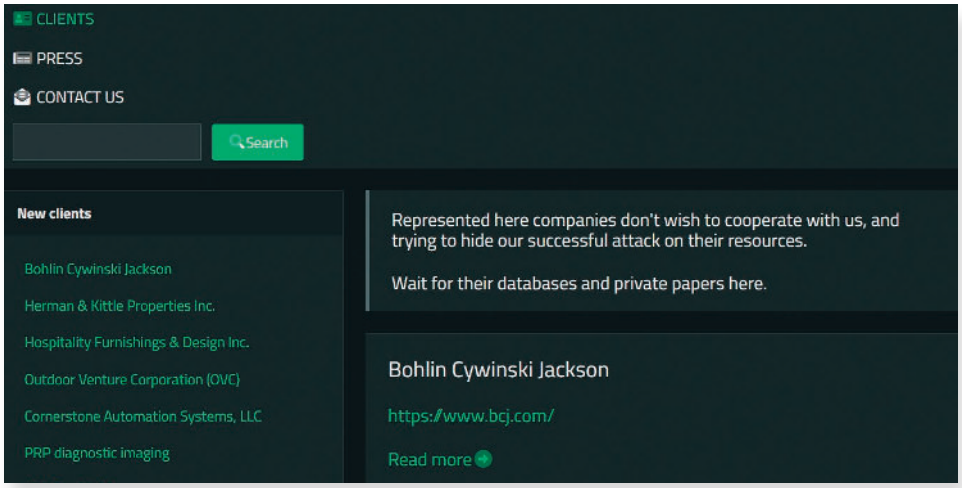
Une véritable économie de la donnée

Depuis ces 3 dernières années, une véritable économie de la donnée s'est développée. L'explosion du nombre de fuites de données est une des conséquences principales avec l'utilisation de **l'hameçonnage** (ou phishing en anglais) comme vecteur de compromission.

En effet, le nombre d'adresses électroniques est tellement important, que l'hameçonnage est désormais la technique la plus rentable pour compromettre un système d'information. Des hackers isolés récupèrent ou achètent des bases de données entières d'adresses électroniques, pour ensuite lancer des campagnes d'hameçonnage ou mettre en place des scénarii de fraudes au président avec de l'hameçonnage ciblé.



Exemple d'une vente de données issues de plusieurs pays

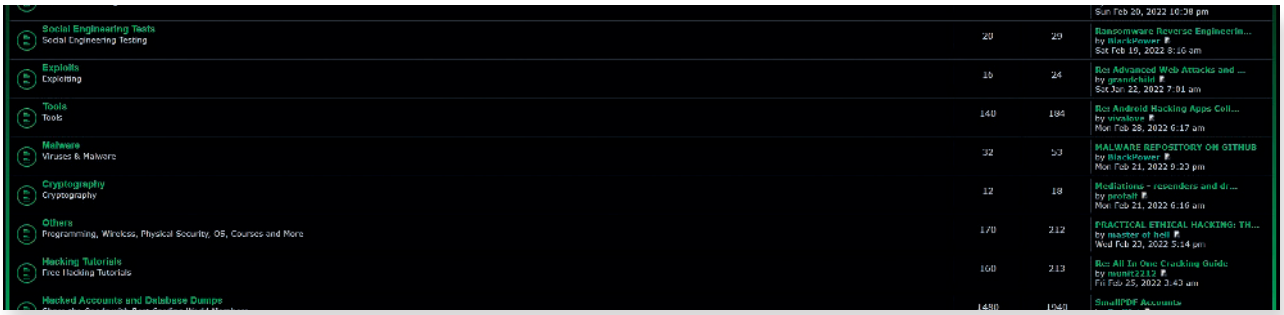


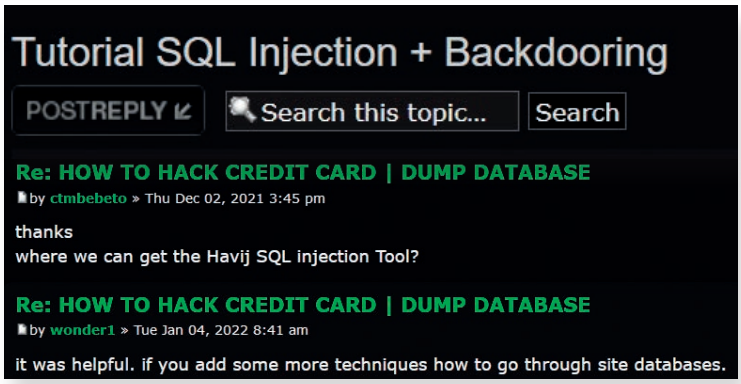
Site du groupe de hackers Suncrypt

Les groupes de hackers semblent **se renforcer avec le temps au sein du dark web** et nous remarquons une véritable consolidation des groupes.

Ces derniers touchent des cibles, possèdent des sites dédiés à leur activité et présentent leurs actions comme arme de communication. Cela a pour but d'inciter les entités touchées à s'acquitter d'une rançon ou entrer en contact avec ces derniers afin d'endiguer toute fuite.

Néanmoins, même malveillants, tous les hackers ne sont pas mercantiles. De nombreux forums d'entraide référençant des techniques et des tutoriels de hack existent. **Ces derniers dispensent diverses techniques de compromission à travers la mise à disposition de guides, ou de virus prêts à l'emploi.**





Guides et tutoriels proposant diverses techniques de hack

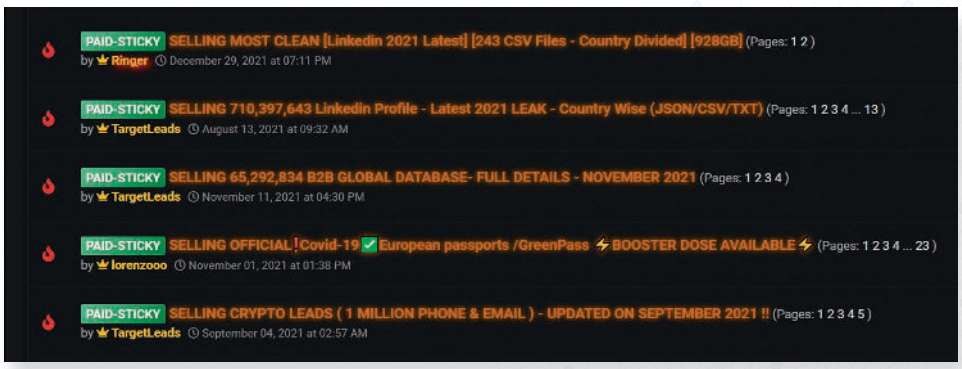
La donnée est une ressource précieuse pour toutes les entreprises et facilement exploitable par les hackers. C'est pourquoi la revente de celles-ci ou de services à haute valeur ajoutée devient une de leur principale activité sur le dark web.

Certains hackers perpétuent eux-mêmes la cyberattaque dans le but de revendre les données, d'autres ont pour seul but de nuire à une entité. La finalité est toujours la même, mettre au profit ses connaissances ou ses informations dans un double but : mercantile et malveillant.

Des revendeurs individuels écument les forums en proposant des fuites de données à la vente. Ces fuites sont issues de leurs propres cyberattaques ou sont simplement des données volées à d'autres dans le but de gagner de l'argent facilement. En parallèle, ils diffusent un échantillon ou des images pour en prouver la véracité.

Ces données sont majoritairement des adresses électroniques, qui peuvent être utilisées pour lancer des campagnes de phishing.

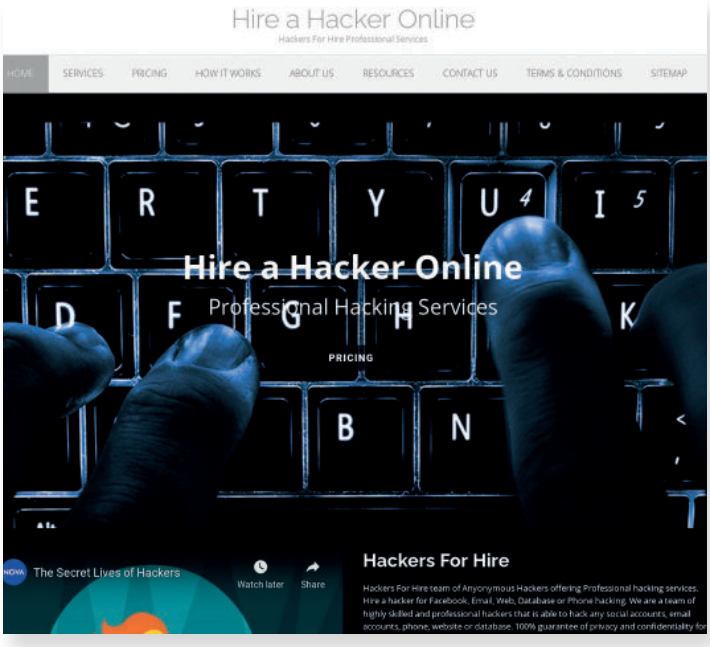
Le commerce de la donnée volée est le résultat d'actions de black hat.

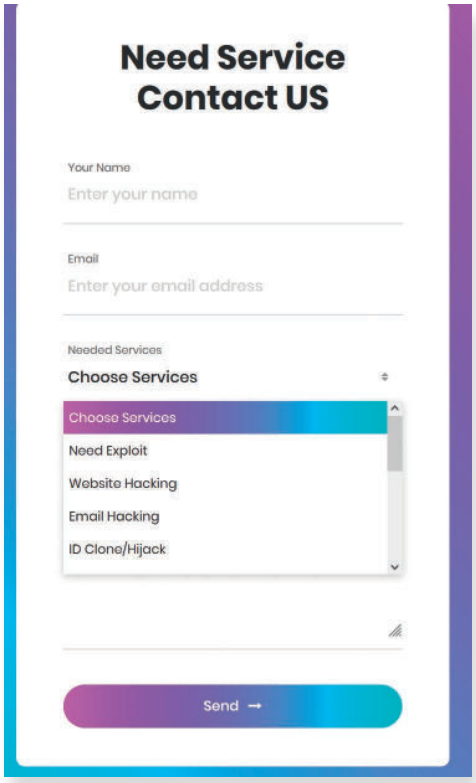


Extrait d'un forum revendant des fuites de données

Il existe également des hackers à louer. Ces derniers proposent des cyberattaques à la demande. La finalité est de compromettre une entité désignée selon un mode opératoire choisi.

Nous remarquons une véritable croissance de services proposés comme nous allons le développer dans le chapitre dédié aux Ransomwares as a service. Il devient possible à n'importe qui de solliciter les services d'un hacker. Il est toutefois difficile de déterminer si ces plateformes sont des arnaques ou si elles proposent des services réels.





Guides et tutoriels proposant diverses techniques de hack

A RETENIR :

1 - Il existe deux grandes catégories de hackers, les white hats, hackers respectant une éthique positive et les black hats, hackers malintentionnés ayant une orientation " destructive ".

2 - Le recel de données d'entreprise et de données personnelles est une activité commerciale à part entière. Les données qui n'ont pas trouvé d'acheteur sont " libérées " et mises à disposition publiquement.

3 - Des services de hack sont proposés, permettant ainsi d'obtenir des données " à la demande " ou de provoquer un arrêt de service du système d'information d'une cible.

Aleph Search Dark permet de collecter et visualiser les données des sites, blogs et forums ouverts, mais également d'analyser les métadonnées associées. Cette navigation se fait en toute discrétion à l'intérieur de la solution, en évitant à l'utilisateur de prendre le risque d'aller sur le dark web. Nous travaillons aussi en étroite collaboration avec des partenaires habilités, qui permettent d'accéder aux données de forums et blogs avec accès en mode authentifié.

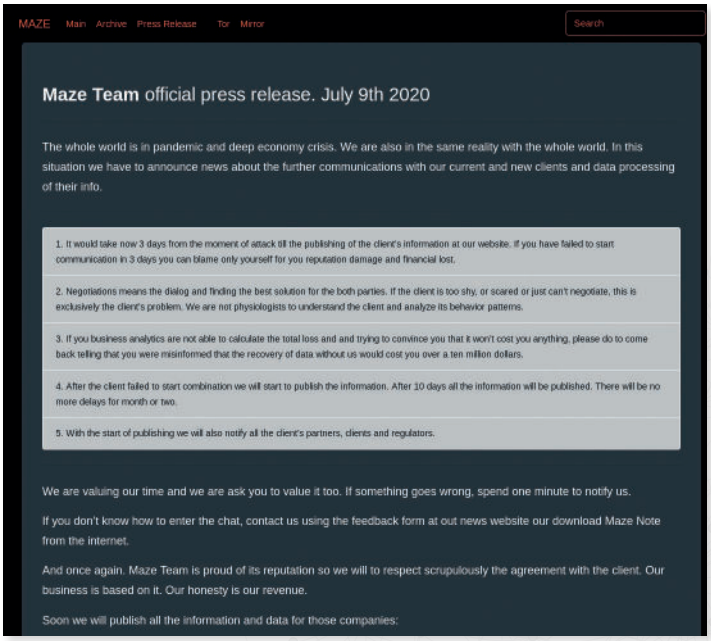
Ransomwares, divulgation de données et malware as a service dans le dark web

Après la crise sanitaire liée à la COVID-19, la cybersécurité constitue une véritable pierre angulaire de notre environnement. D'une part, elle doit assurer la résilience du système d'information étatique et de santé, d'autre part, elle doit assurer des conditions pérennes de télétravail aux personnes pouvant exercer leurs activités à distance.

Cette résilience est mise à rude épreuve avec les attaques successives d'entités de différents secteurs. Les cyberattaques, bénéficiant d'un contexte de crise inédit, se traduisent par une croissance exponentielle des attaques de type ingénierie sociale, hameçonnage, compromission d'atouts commerciaux et enfin une recrudescence de malware et de ransomware. En effet, les hackers capitalisaient sur la confusion et sur la peur liée à la pandémie, afin d'en tirer parti et d'optimiser leurs chances d'atteindre leur cible.

Cela se traduit par la déstabilisation et la paralysie d'encore plus d'entités, qu'elles soient publiques ou privées. Ainsi, nous pouvons prendre comme exemples le secteur hospitalier avec la cyberattaque du Centre hospitalier Sud Francilien (CHSF) de Corbeil-Essonnes en août 2022[1], le secteur privé avec La Poste Mobile en juillet 2022[2] , ou encore les collectivités territoriales avec le département d'Indre et Loire en juillet 2022[3]

> Les attaques de type hameçonnage ont augmenté d'environ 665% depuis le début de la crise



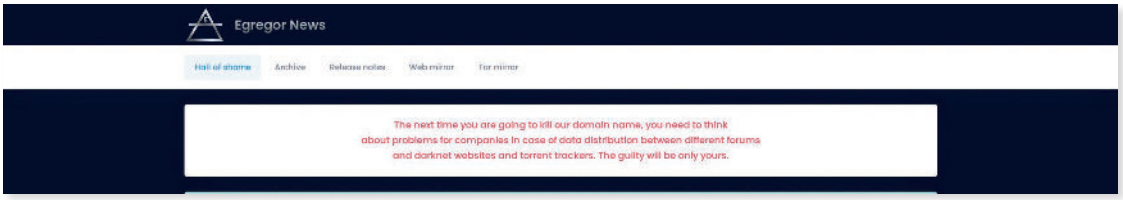
Communiqué des hackers responsables du malware Maze sur le dark web à propos du Covid-19

1 / https://www.leparisien.fr/high-tech/cyberattaque-contre-un-hopital-de-lessonne-les-hackers-ont-diffuse-des-donnees-piratees-25-09-2022-NKKMW4XNJFCRNPTAADYT327UVQ.php
2 / https://www.generation-nt.com/poste-mobile-piratage-rancongiciel-actualite-2003070.html
3 / https://www.francebleu.fr/infos/faits-divers-justice/le-departement-d-indre-et-loire-victime-d-une-cyberattaque-1657554147

Depuis 2020, les ransomwares figurent à la première place des risques les plus fréquents et dangereux.

Les attaques par ransomware qui visent des entreprises ou des institutions ont pour but initial d'obtenir le paiement d'une somme d'argent en échange de la libération des données chiffrées. Il n'est donc pas prévu d'emblée que l'attaque soit rendue publique ; tout peut se passer dans la plus grande discrétion entre l'attaquant et sa victime. Il est néanmoins fréquent que les attaques fassent l'objet d'une communication sur certains canaux.

La principale raison qui peut conduire l'attaquant à communiquer sur son action est le refus de la victime de payer la rançon. Les opérateurs du ransomware passent alors à une pratique beaucoup plus classique qui consiste à menacer de diffuser les données de la victime. C'est donc une nouvelle étape dans la tentative d'extorsion. La menace est matérialisée par le biais d'un site web dédié et géré directement par l'équipe de hackers. Il s'agit très souvent d'un site du deep web, doublé d'un **miroir** dans le dark web destiné à contrer les tentatives de blocage de nom de domaine.

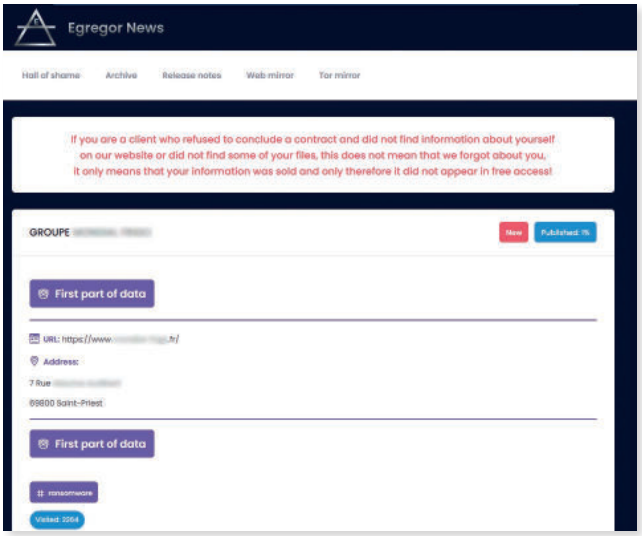


Sur leur site, les hackers recensent toutes les victimes qui ne leur cèdent pas. Dans un premier temps, ils mettent en libre accès un fichier texte qui donne la liste des fichiers détenus ainsi qu'un extrait des données subtilisées (teaser).

```
2017-05-22 14:17:57 ....A        32954            _other_2\CONTRATS\2.DDS\    -    \EXIBIT IV.docx.jaff
2013-11-28 14:24:33 ....A        95100            _other_2\CONTRATS\2.DDS\    -    \NDA      v DJ     SA(2).docx
2017-05-22 14:17:57 ....A        95370            _other_2\CONTRATS\2.DDS\    -    \NDA      v DJ     SA(2).docx.jaff
2013-12-02 11:17:40 ....A       179569            _other_2\CONTRATS\2.DDS\    -    \Pouvoir GL - BD.pdf
2017-05-22 14:17:57 ....A       179850            _other_2\CONTRATS\2.DDS\    -    \Pouvoir GL - BD.pdf.jaff
2013-11-28 10:33:23 ....A       271360            _other_2\CONTRATS\2.DDS\    -    \Power G        to B        .doc
2017-05-22 14:17:58 ....A       271642            _other_2\CONTRATS\2.DDS\    -    \Power G        to B        .doc.jaff
2013-11-28 10:35:58 ....A        95707            _other_2\CONTRATS\2.DDS\    -    \Projets\NDA      v DJ     SA.docx
2013-11-27 11:28:20 ....A        91855            _other_2\CONTRATS\2.DDS\    -    \Projets\NDA      .DOCX
2017-05-22 14:18:00 ....A      8295478            _other_2\CONTRATS\2.DDS\    -    \ReadMe.bmp
2017-05-22 14:18:00 ....A         1431            _other_2\CONTRATS\2.DDS\    -    \ReadMe.html
2017-05-22 14:18:00 ....A          482            _other_2\CONTRATS\2.DDS\    -    \ReadMe.txt
2017-10-10 07:49:59 ..HSA        22016            _other_2\CONTRATS\2.DDS\    -    \Thumbs.db
2015-12-03 14:01:48 ....A       993711            _other_2\CONTRATS\4.KEY ACCOUNTS\    \          INDUSTRIAL MAINTENANCE PRESENTATION.pptx
2017-05-22 14:18:49 ....A       993993            _other_2\CONTRATS\4.KEY ACCOUNTS\    \          INDUSTRIAL MAINTENANCE PRESENTATION.pptx.jaff
2015-12-03 15:24:45 ....A       247294            _other_2\CONTRATS\4.KEY ACCOUNTS\    \ANNEXES    \ANNEX A -    .pdf
2015-12-03 15:29:18 ....A       125952            _other_2\CONTRATS\4.KEY ACCOUNTS\    \ANNEXES    \ANNEX A-    Summary.doc
2015-12-03 13:45:25 ....A       536194            _other_2\CONTRATS\4.KEY ACCOUNTS\    \ANNEXES    \ANNEX E - INFORMATION SECURITY - SECURITY REQUIREMENTS
A1015 Issue D.pdf
2015-12-03 13:45:26 ....A       666434            _other_2\CONTRATS\4.KEY ACCOUNTS\    \ANNEXES    \ANNEX E - INFORMATION SECURITY - SECURITY REQUIREMENTS
```

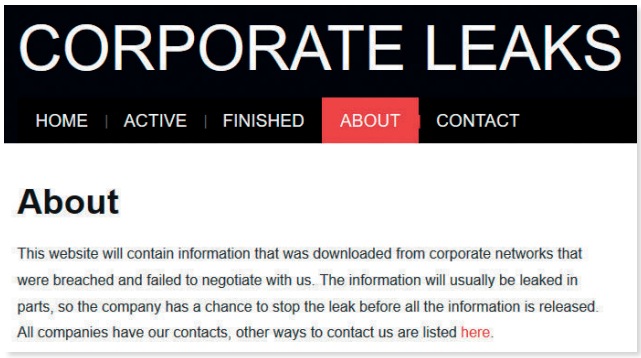
Extrait d'une liste de fichiers chiffrés diffusée par une équipe de hackers

En cas de refus persistant de la victime, les hackers déclenchent alors la première phase de rétorsion : la diffusion partielle des données elles-mêmes. Nous n'avons pas pu identifier de pratique commune en ce qui concerne le choix des premières données divulguées ; suivant les cas, il s'agit de données plus ou moins stratégiques et sensibles.



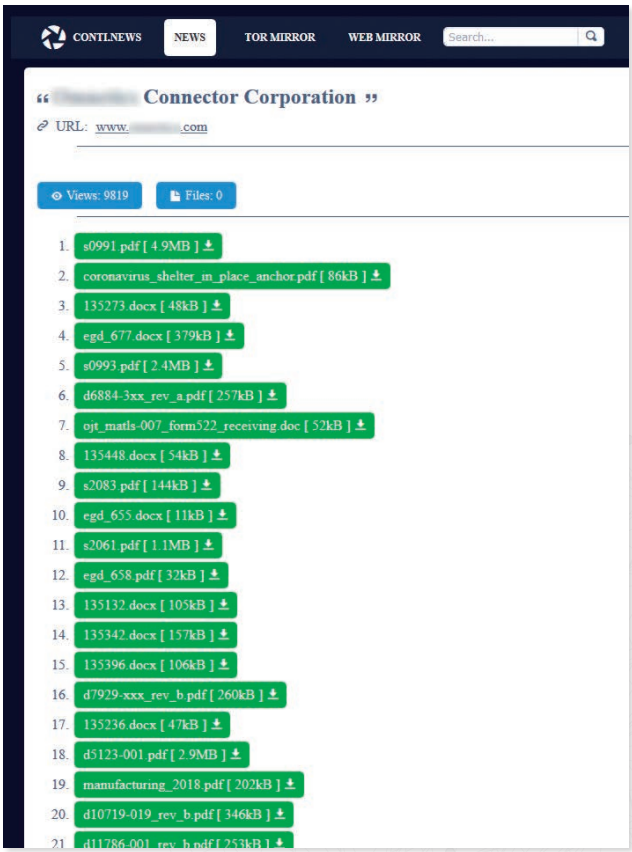
Diffusion d'un premier lot de données d'une victime du groupe Egregor

Si cette diffusion partielle ne suffit pas à faire plier la victime, d'autres fichiers sont alors mis à disposition, jusqu'à la fuite complète des données. En cela, le processus est rigoureusement identique à celui du très usuel chantage à la divulgation de données. **Finalement, la seule nouveauté introduite par l'attaque par ransomware est la phase de chiffrement des données de la cible, qui est déjà en soi un handicap majeur pour la victime.**



Activité classique de chantage à la divulgation de données, sans utilisation de ransomware

Les données sont le plus souvent divulguées sous forme d'archives d'un volume variable, en fonction de la masse de données collectées par les hackers. **Certaines fuites pèsent ainsi au total plusieurs centaines de giga-octets.** Il arrive également que les hackers proposent de télécharger chaque fichier séparément dans une liste non triée. Certains proposent aussi de naviguer dans les données en reproduisant l'arborescence des répertoires de la victime.



Fuite de données non triées

Reproduction de l'arborescence des répertoires de la victime

Le profil des victimes des attaques de groupes tel qu'Egregor (dont une partie a été arrêtée en Ukraine au mois de février 2021) confirme que la menace d'une attaque par ransomware ne concerne pas uniquement des entreprises ou des institutions d'envergure et de notoriété internationales. Certes, **parmi les cibles de ces pratiques, nous retrouvons de grands groupes, mais également des entreprises de taille intermédiaire**, comme une entreprise rhodanienne de 340 salariés ou même une entreprise canadienne de logistique de moins de 60 salariés.

Les opérateurs de ransomwares fonctionnent en effet selon le principe d'opportunité. Le profil économique de la cible leur importe peu ; **c'est la vulnérabilité du système informatique qui conditionne la probabilité de l'attaque.**

Ainsi, il sera plus rentable pour une équipe de cibler plusieurs petites structures mal protégées que de consacrer des efforts à pénétrer les systèmes bien verrouillés d'une entreprise consciente des risques.

La sécurité des systèmes d'information n'est malheureusement ni une préoccupation de tous, ni une garantie que toutes les structures peuvent s'offrir.

Aussi, la facilité d'exécution associée à des canaux d'intrusion démultipliés, fait que **les ransomwares sont devenus rapidement l'une des attaques les plus rentables.** Cette méthode d'attaque est très répandue au sein du dark web, avec une surface d'attaque en augmentation perpétuelle et une structuration du marché du malware as a service

Exemples de " malware as a service " proposés par des hackers sur le dark web

Cette menace, peu coûteuse en moyens et pouvant rapporter gros pour les attaquants, est désormais ancrée au sein du paysage des menaces cyber.

En effet, l'ANSSI[4] , a édité un bulletin d'alerte en septembre 2020 concernant Emotet, un ransomware particulièrement répandu. Celle-ci a noté une recrudescence du ciblage d'entités françaises par ce code malveillant. Toutefois, la France n'a pas semblé être le seul pays touché par Emotet, la Nouvelle-Zélande et notamment le Japon en ont été également victimes.

Discussions sur un forum du dark web à propos de nouvelles cibles (capturées par notre logiciel)

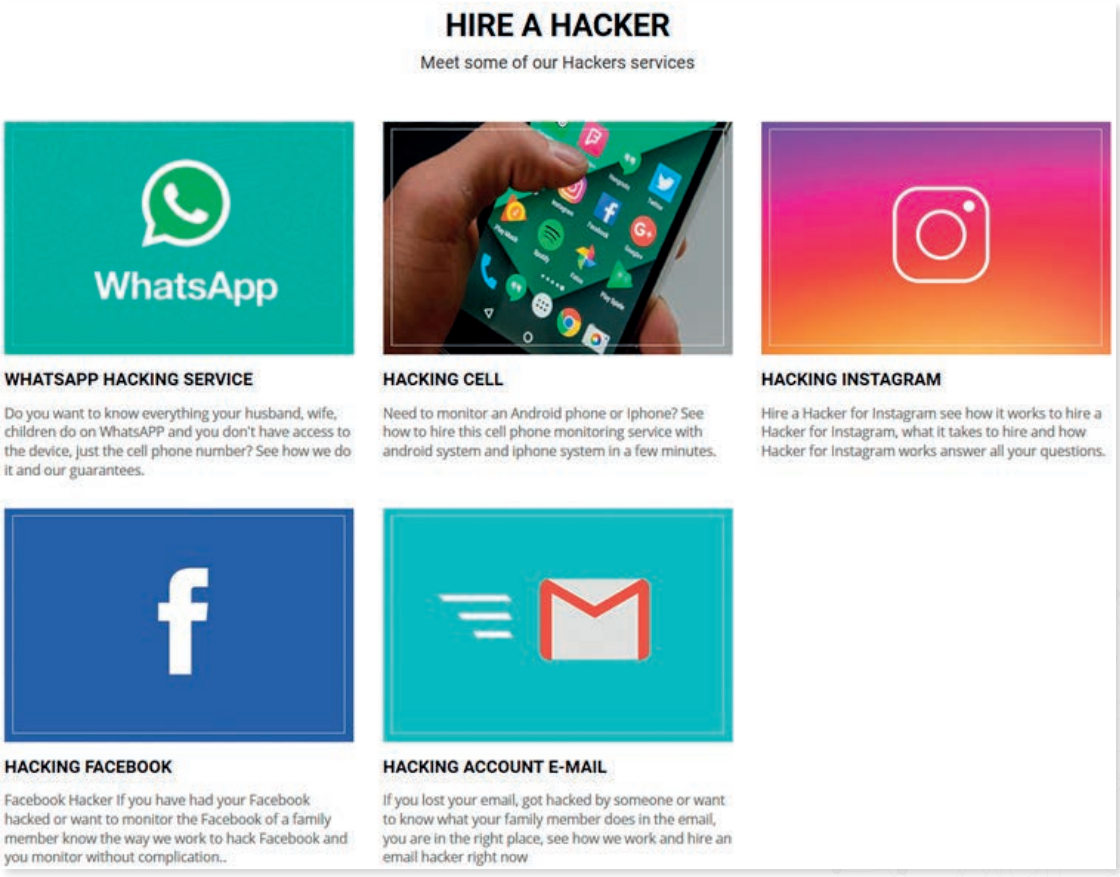
4/ https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-019/

Proposition rémunérée d'un utilisateur cherchant à utiliser le coronavirus comme vecteur de propagation du ransomware Emotet (capturée par notre logiciel)

En plus du bulletin d'alerte de septembre dernier, l'Agence a également publié le 29 octobre 2020 une étude sur le malware as a service en prenant comme exemple l'activité **d'Emotet**[5] . Cette nouvelle tendance permet d'externaliser une cyberattaque auprès d'un hacker contre rétribution, sans aucune connaissance requise.

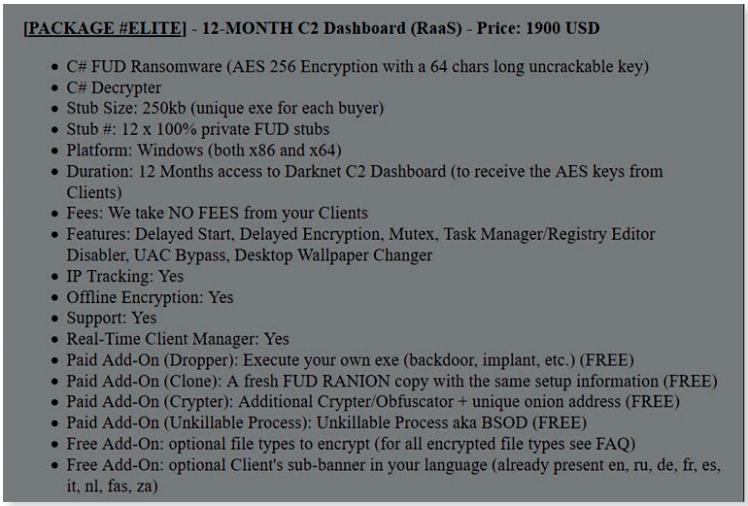
Cette "**ubérisation** " de la **cyberattaque** ne fait qu'amplifier les menaces existantes. Désormais, quiconque ayant les moyens, peut s'offrir les services d'un hacker. Cela pouvant aller de la compromission de simples comptes de réseaux sociaux ou de messagerie à la déstabilisation complète de systèmes d'information.

> "Cette "ubérisation " de la cyberattaque ne fait qu'amplifier les menaces existantes"



Services de hacking " classiques " sur le dark web

5/ https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-010/



[PACKAGE #ELITE] - 12-MONTH C2 Dashboard (RaaS) - Price: 1900 USD

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- Stub #: 12 x 100% private FUD stubs
- Platform: Windows (both x86 and x64)
- Duration: 12 Months access to Darknet C2 Dashboard (to receive the AES keys from Clients)
- Fees: We take NO FEES from your Clients
- Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer
- IP Tracking: Yes
- Offline Encryption: Yes
- Support: Yes
- Real-Time Client Manager: Yes
- Paid Add-On (Dropper): Execute your own exe (backdoor, implant, etc.) (FREE)
- Paid Add-On (Clone): A fresh FUD RANION copy with the same setup information (FREE)
- Paid Add-On (Crypter): Additional Crypter/Obfuscator + unique onion address (FREE)
- Paid Add-On (Unkillable Process): Unkillable Process aka BSOD (FREE)
- Free Add-On: optional file types to encrypt (for all encrypted file types see FAQ)
- Free Add-On: optional Client's sub-banner in your language (already present en, ru, de, fr, es, it, nl, fas, za)

Exemple de mise à disposition de ressources pour exécuter des attaques de type ransomware au sein du dark web

Bien que le réseau de hackers affilié à ce ransomware ait été démantelé fin janvier 2021[6], nous pouvons constater que la France reste une cible privilégiée des hackers concernant ce type de cyberattaque. En effet, alors que les vecteurs d'attaque se multiplient, les hackers en profitent pour structurer leurs activités en créant un véritable commerce de la cyberattaque. Non seulement ce type d'attaque informatique est la plus répandue, mais aussi les conséquences sont lourdes pour les entités touchées.

La prudence semble être la meilleure recommandation de première intention car l'imagination des hackers semble être sans limite. L'ANSSI publie un certain nombre de recommandations dans son guide. Toutes les entreprises sont concernées, quelle que soit leur taille et chaque membre de l'entreprise l'est aussi, car la réussite de ce type d'attaques dépend de l'erreur humaine.

6/ https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
https://www.ssi.gouv.fr/administration/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/

A RETENIR :

1 - Les attaques par Ransomware visent les entreprises ou les institutions dans le but d'obtenir une somme d'argent. Elles permettent de voler une masse très importante de données et de chiffrer l'ensemble du système d'information de la cible.

2 - Le refus de paiement peut conduire le hacker à communiquer sur l'action malveillante et diffuser les données volées en plusieurs phases, tout en laissant les données chiffrées sur le système d'information de la cible.

3 - Le Malware As A Service (MaaS) permet d'externaliser et d'industrialiser de manière massive des cyberattaques pour un coût très faible. Un simple accès à un service en mode SaaS permet ainsi de mener des actions de cyberattaque de manière anonyme et industrielle.

Surveiller ses données sur les deep et dark webs permet, en cas d'incident, de réagir immédiatement tout en ayant anticipé les actions post-incident à lancer au plus vite et de gérer la crise avec une vision d'ensemble : identification des communautés impliquées, volume de données divulguées, origines éventuelles de la fuite, points de faiblesse, risque d'être victime d'une campagne de phishing, suivi de la politique de gestion des mots de passe...

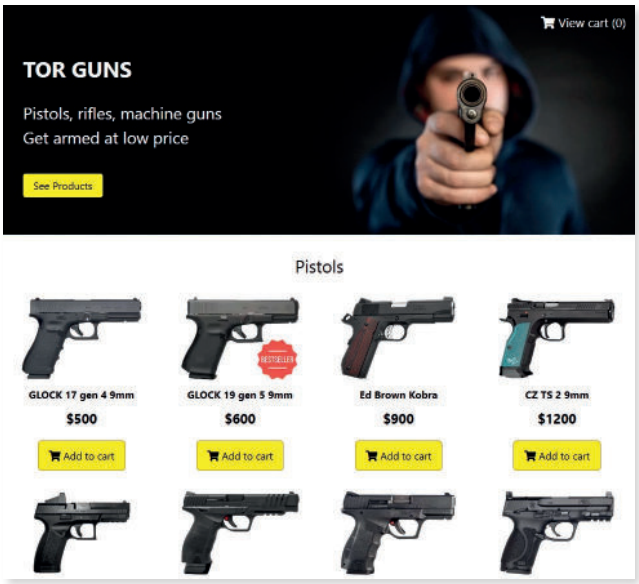
Les places de vente dans le dark web

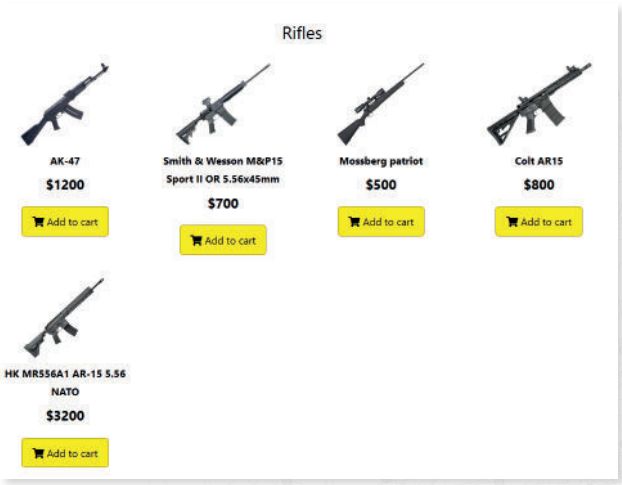
#5.1 - Vente d'armes et de stupéfiants

Le dark web est un lieu où il est possible d'acheter divers biens et services. Nous avons choisi d'aborder dans ce chapitre les types les plus courants, à savoir **les armes, les produits stupéfiants, les contrefaçons et les services financiers.** Une dernière partie évoquera les marchandises plus rares et les légendes urbaines (tueurs à gages et Red Rooms). Les sites pédopornographiques payants seront évoqués dans le prochain Tome .

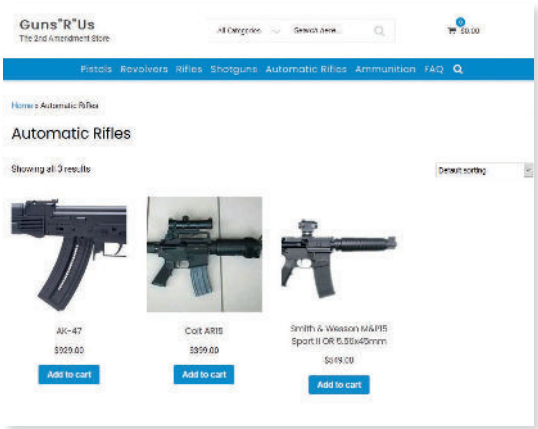
Si nous pouvons soupçonner une part non négligeable des sites que nous indexons d'être des arnaques, il n'en demeure pas moins que des offres réelles existent sur le dark web. Ainsi, en septembre dernier, un individu fiché S a été interpellé en région parisienne pour avoir commandé un fusil d'assaut sur un site américain du dark web. Les armureries clandestines proposent en effet non seulement des armes de poing, mais également des armes longues.

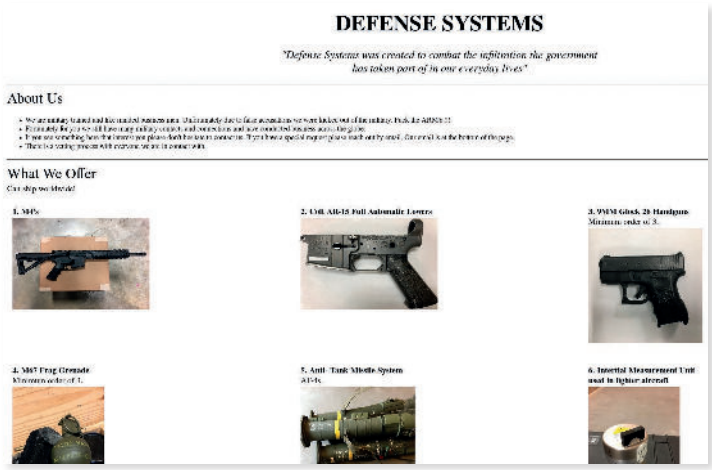
> "Un individu fiché S a été interpellé en région parisienne pour avoir commandé un fusil d'assaut sur un site américain du dark web"





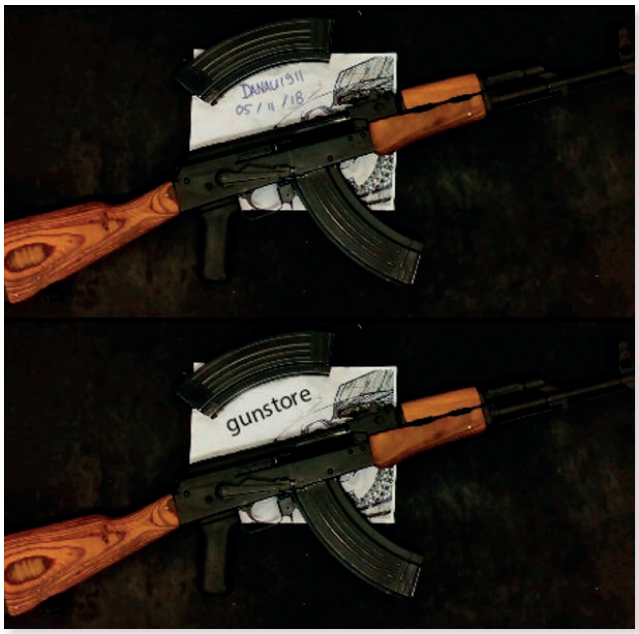
Certains vendeurs proposent d'autres types d'armement : **grenades, lance-roquettes voire missiles anti-char.** Cette dernière offre parait peu crédible, mais les deux premières pourraient être réelles et provenir d'une filière ukrainienne.



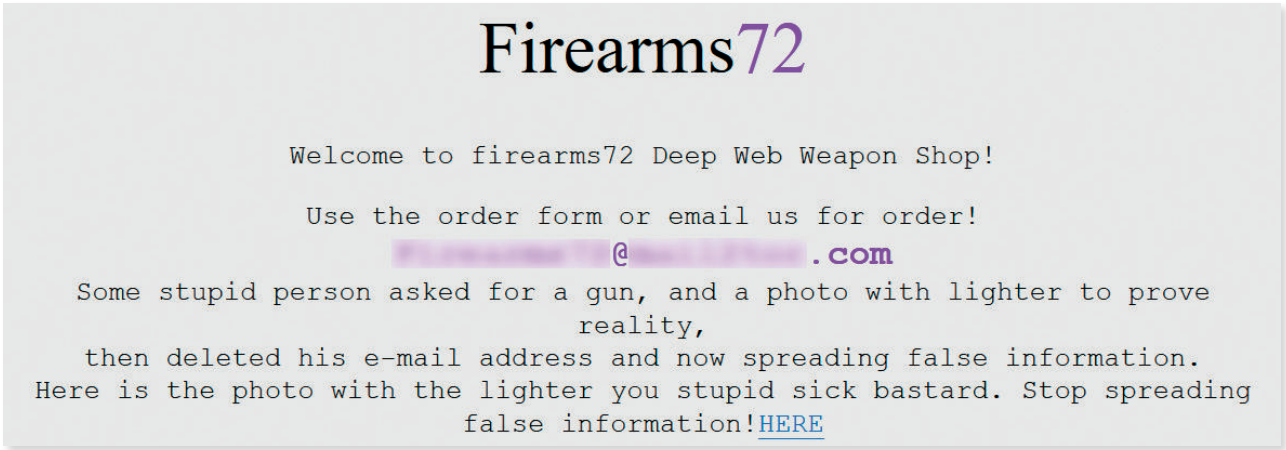


Le plus ancien vendeur d'armes du dark web encore en activité est le site **Black Market Guns.** Nous pouvons observer que les photos d'armes contiennent un filigrane (watermark), destiné à empêcher la copie et la réutilisation de ces photos sur des sites trompeurs.

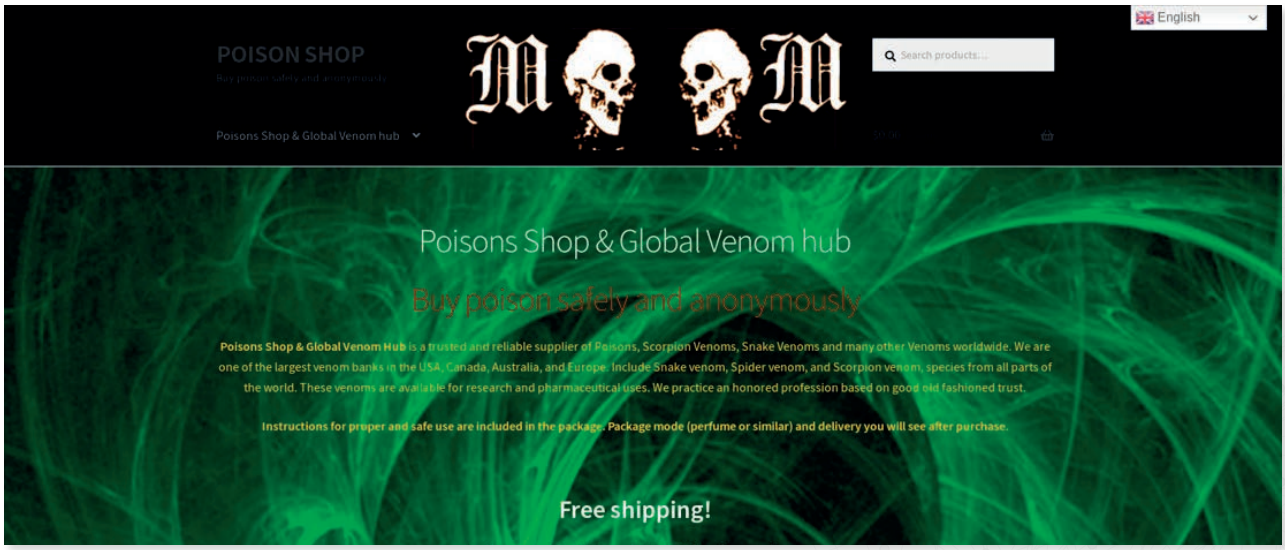
Nous pouvons également remarquer la présence sur certaines photos d'une feuille de papier estampillée **BMG**, censée prouver que le vendeur a bien le produit à sa disposition. Cette forme de preuve ne suffit toutefois pas à déterminer si une offre est réelle. En effet, des utilisateurs plus ou moins talentueux de logiciels d'édition d'images peuvent apposer leur propre marque sur une photo d'arme récupérée dans une banque d'images du web standard.



Deux exemples d'une même image retouchée, provenant de deux vendeurs (Danau et GunStore)

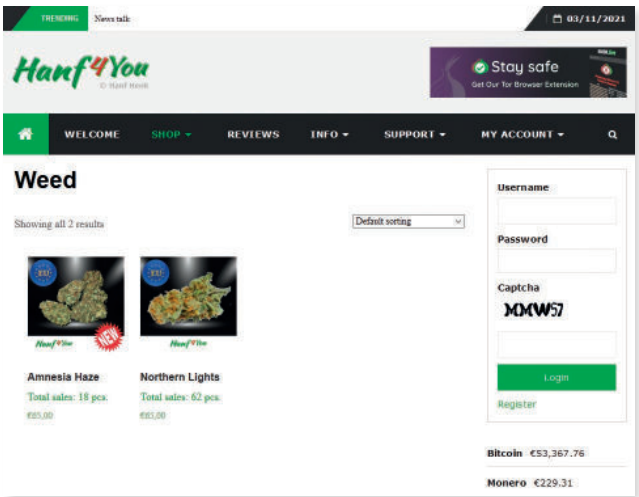


Certains acheteurs méfiants peuvent alors exiger des preuves plus spécifiques, comme le vendeur Firearms72 a pu en faire l'expérience. Un acheteur a demandé en guise de preuve une photo de l'arme en vente avec un briquet en lieu et place de la traditionnelle feuille de papier. La photo de l'arme avec le briquet est disponible sur le site en question, mais rien ne permet de déterminer s'il s'agit d'une photo retouchée ou non.

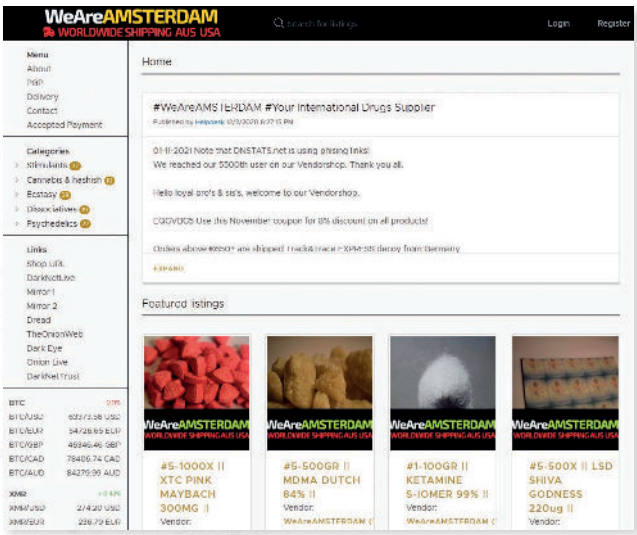


A la croisée des chemins entre les armes et les drogues, un autre vendeur propose toute une gamme de poisons et de venins. Certains produits proposés, comme le Polonium ou le VX, nous font très sérieusement **douter de la réalité de l'offre**.

A l'inverse, les nombreux sites de vente de **produits stupéfiants** nous paraissent beaucoup plus crédibles. Les vendeurs peuvent proposer un seul ou plusieurs types de produit.

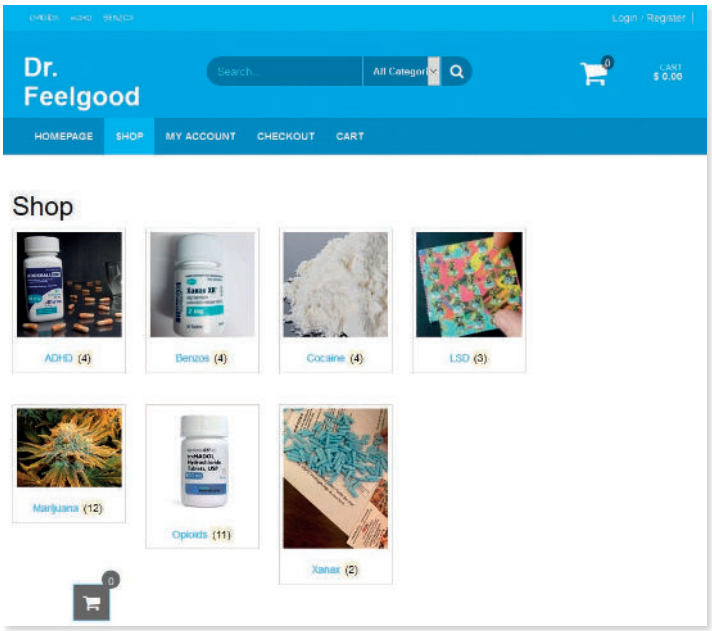


Site spécialisé dans le cannabis

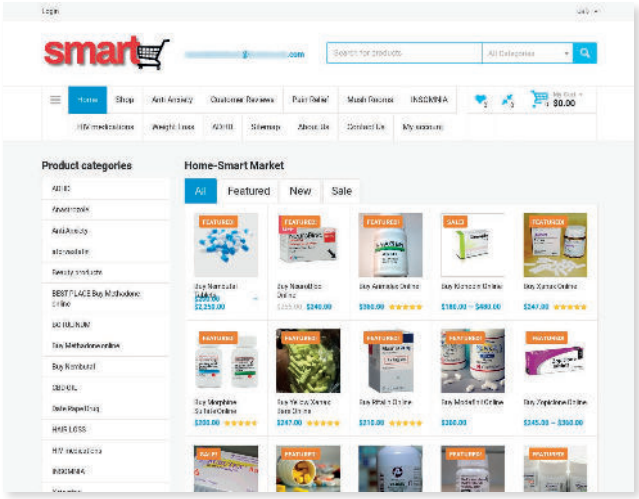


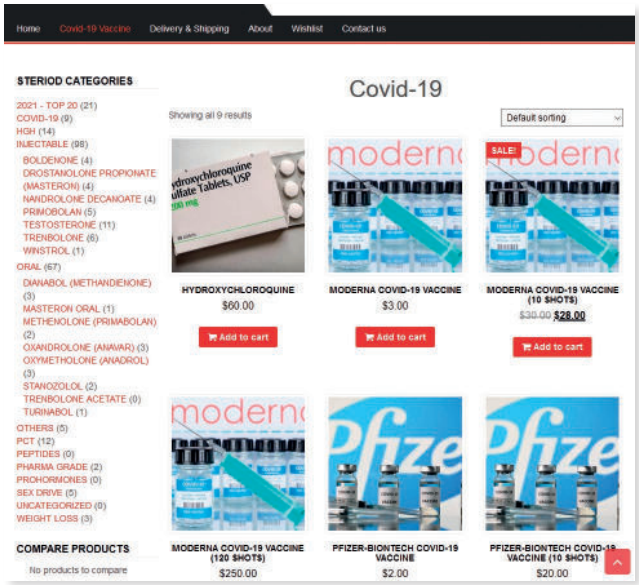
Site proposant une large gamme de stupéfiants

D'autres vendeurs proposent des stupéfiants et des médicaments accessibles sur ordonnance, comme le **Xanax** et autres médicaments psychoactifs.

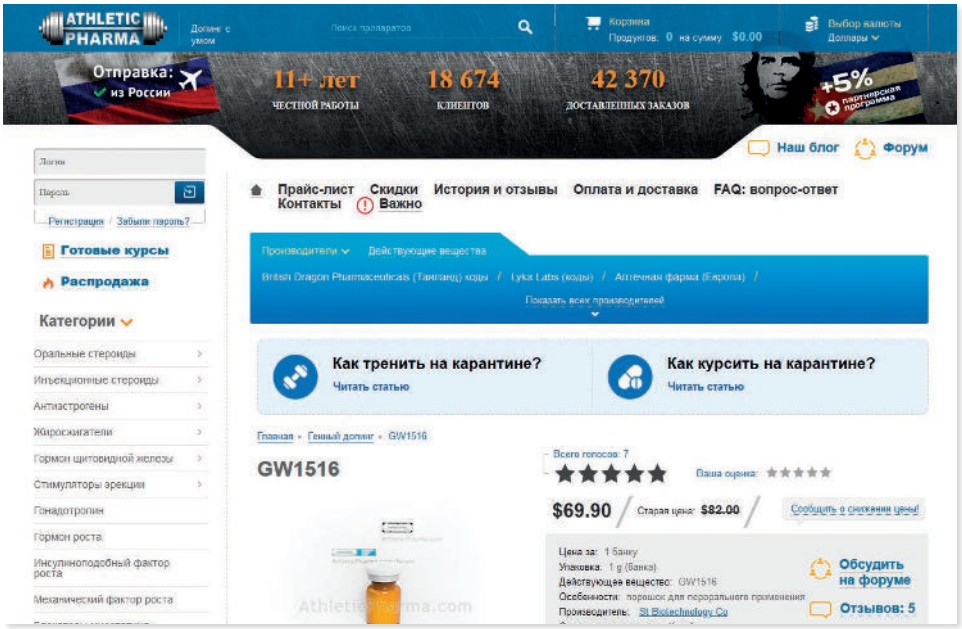


Certains sites sont même de véritables pharmacies clandestines, proposant entre autres des médicaments **anti-VIH**, des médicaments pour la perte de poids ou pour le traitement de l'insomnie. Il n'est pas rare de voir chez ce type de vendeur des propositions de lots de doses de vaccin anti-covid.





Enfin, nous pouvons évoquer le site Athletic Pharma qui, comme son nom le suggère, s'est spécialisé dans les **produits dopants**.



Nous n'avons détaillé ici qu'une très petite partie de l'offre du dark web en termes d'armes et de produits stupéfiants ou pharmaceutiques. Si une partie assez significative de ces sites est sujette à caution, il faut admettre que les prestations bien réelles de certains vendeurs constituent une sérieuse menace d'ordre sécuritaire et sanitaire.

#5.2 - Les contrefaçons

Parmi les produits proposés à la vente sur le dark web, les **contrefaçons** occupent une place privilégiée. En effet, rares sont les places de marché qui ne disposent pas d'un ou plusieurs faussaires. Les contrefaçons les plus couramment rencontrées sont les faux billets, les faux papiers d'identité, les faux documents administratifs les plus divers et les contrefaçons de produits de luxe.

#5.2.1 - Les faux billets

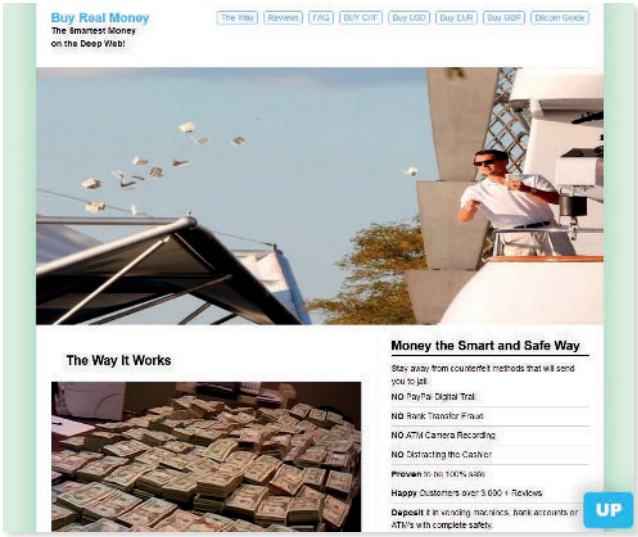
On trouve des contrefaçons des devises les plus courantes sur le dark web : **euro, dollar, yuan, livre sterling**... Les faux billets sont proposés par des vendeurs sur des places de marché ou directement sur des boutiques individuelles, comme chez le marchand suivant.

Page d'accueil du site Bazaar Plastic

Comme de coutume, chaque faux monnayeur pourra vanter la qualité de ses contrefaçons. Ici, les faux billets sont proposés comme tels et le client en fait l'acquisition en toute connaissance de cause. Nous pouvons en revanche supposer qu'il existe pour certains faussaires une autre façon d'écouler leur marchandise.

En effet, un site prétend vendre des billets authentiques usagés et retirés de la circulation, qu'une équipe infiltrée dans les institutions réussirait à subtiliser avant leur destruction.

Si nous faisons l'hypothèse très improbable que ce site n'est pas une arnaque pure et simple, et si ce site (par ailleurs répliqué à plus de 1 800 exemplaires douteux ou scam mirrors) fait parvenir des espèces aux acheteurs, il est tout à fait possible que les billets en question soient des faux.

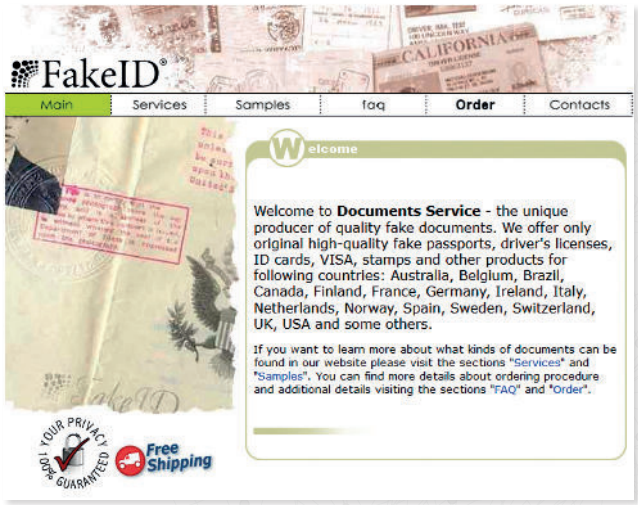


Page d'accueil du site Buy Real Money

#5.2.2 - Les faux papiers et documents

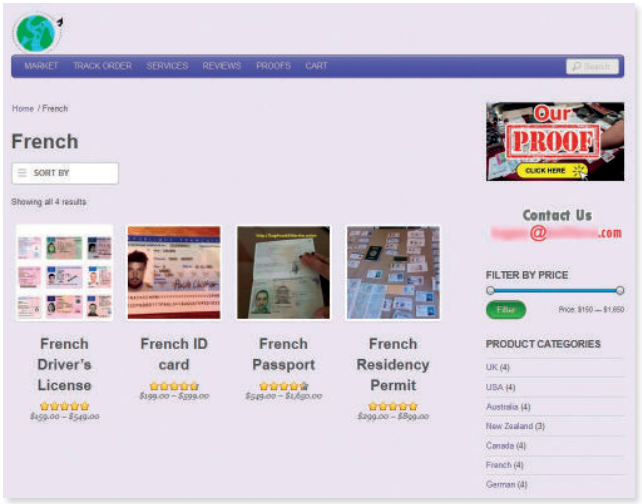
Les faux papiers sont une marchandise très prisée sur le dark web. Les plus fréquemment proposés sont les passeports, mais on trouve une certaine variété de pièces d'identité, comme par exemple des cartes d'identité ou des permis de conduire.

Exemples de passeports en vente sur le site FakeID

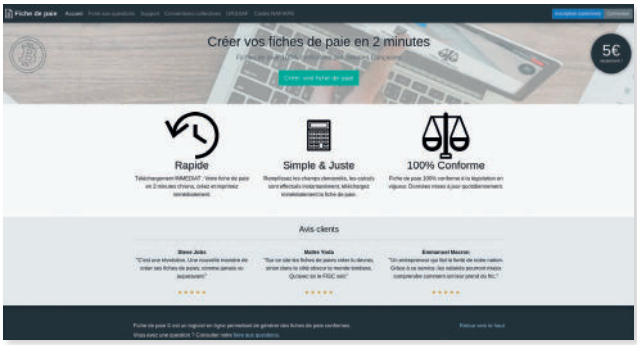


Page d'accueil du site FakeID

Les documents administratifs sont eux aussi l'objet de contrefaçons, comme nous pouvons le voir sur les deux captures d'écran suivantes.



Faux papiers français en vente sur le site Endless Destinations, dont une carte de résident

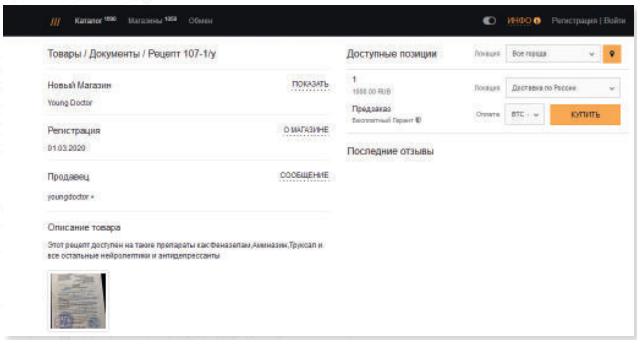


Site spécialisé dans la création de faux bulletins de salaire

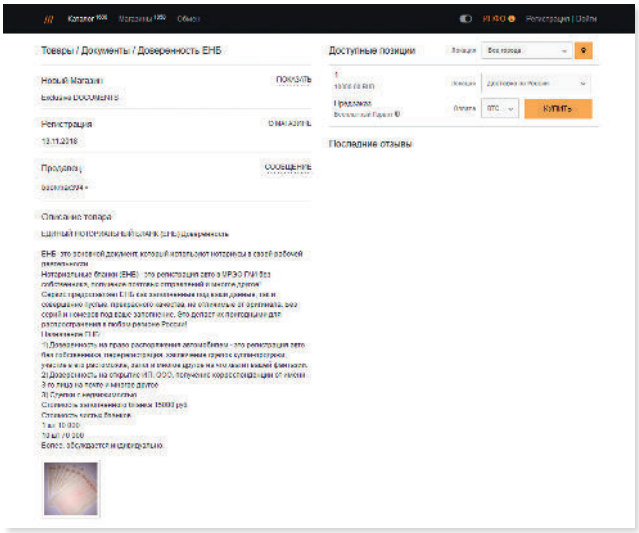
Les **fausses fiches de paie** servent le plus souvent à monter des dossiers de crédit à la consommation. Certains faussaires mettent même en vente des packs spéciaux pour cette utilisation, qui comprennent des scans de toutes les pièces nécessaires. Dans ce cas, les packs peuvent comprendre un mélange de faux documents et de vraies pièces, comme par exemple des fiches de paie authentiques issues de données volées.

Annonce d'un faussaire sur le Trollodrome

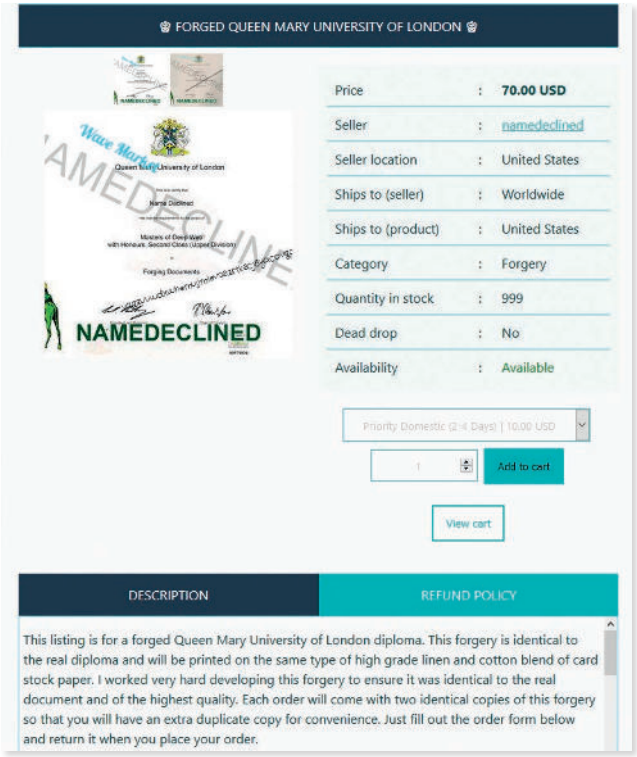
On peut encore trouver une variété impressionnante de documents, **comme des faux diplômes, des ordonnances, des cartes grises**...



Fausse ordonnance russe pour du Phenazepam



Fausse carte grise russe

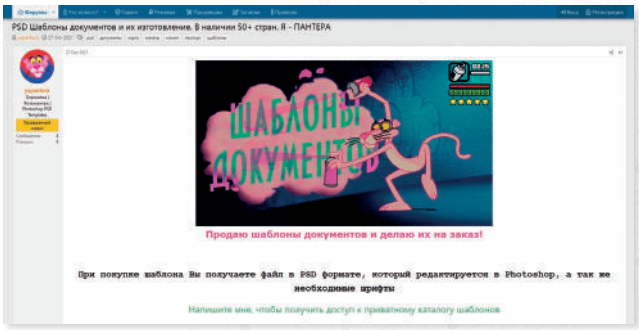


Faux diplôme

Pendant la période de contraintes sanitaires , il était évidemment prévisible que les faussaires produisent des **faux pass.**

Vente de fausse attestation de vaccination

Les faux documents sont le plus souvent vendus sous leur forme physique, mais certains faussaires vendent également des fichiers de projets Photoshop (PSD), qui permettent à leurs acquéreurs de produire une ou plusieurs images de type scan de pièce d'identité, en modifiant à volonté les renseignements qui y figurent.

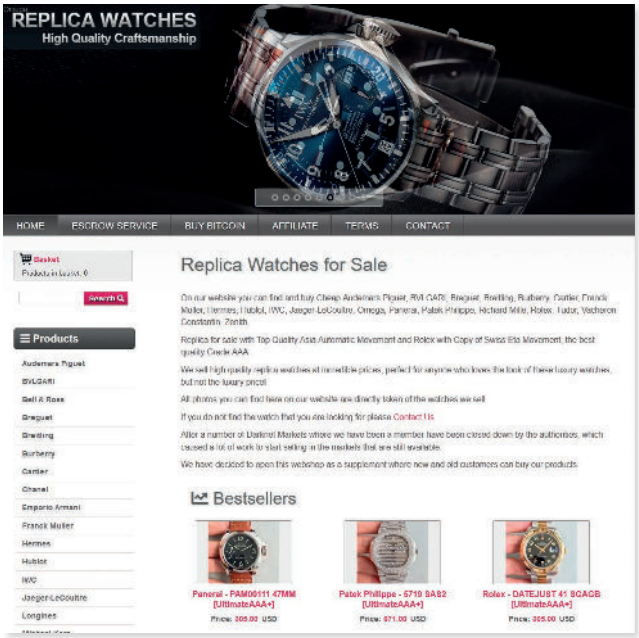


Vendeur de fichiers de projets Photoshop pour faux scans de pièces d'identité

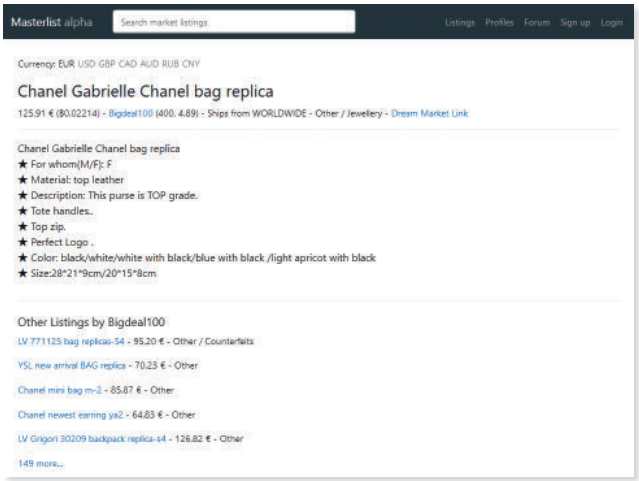
#5.2.3 - Les produits de luxe

La contrefaçon de produits de luxe est une activité plus restreinte sur le dark web, probablement en raison de la facilité avec laquelle il est possible d'acquérir ces articles contrefaits par des moyens plus classiques (vente à la sauvette, vendeurs sur le clear web…).

Par le passé, on trouvait certains vendeurs individuels sur le dark web, comme le site Replica Watches aujourd'hui disparu, spécialisé dans les montres de luxe.

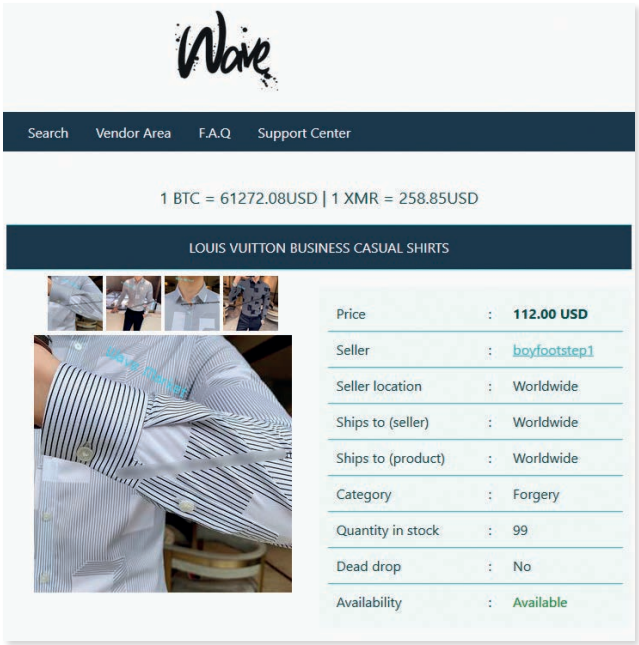


Page d'accueil du site Replica Watches



Articles de maroquinerie contrefaits

Contrefaçon de vêtements de luxe



Désormais, les vendeurs de produits de luxe contrefaits semblent plutôt officier sur des places de marché, sur lesquelles on peut trouver des répliques d'articles de grandes marques.

La vente de faux est donc une activité très répandue sur le dark web. Les sites onion ne représentent certainement pas la plus grande menace pour les produits de luxe, au regard de l'offre assez faible, mais le commerce de faux papiers semble très courant et peut donc faire peser une menace pour les états ou les organismes de crédit.

#5.3 - Les opérations financières

En termes de présence sur le dark web, les sites qui proposent des **opérations financières** (recel de comptes volés, vente de cartes-cadeau, mixeurs de cryptomonnaies…) représentent une part très importante des activités à but lucratif. Le dark web fourmille en effet de propositions faisant miroiter de l'argent facile et rapide. Ce type de service est d'ailleurs si " populaire" que les dix sites les plus répliqués en nombre de miroirs sont actuellement tous des sites de cette nature.

Nom du site	Freenet
[OFFICIAL & ORIGINAL] BITCOIN x200 SERVICE - ©2021	6923
Stolen Cards - Plastic Sharks	1858
AUTOMATED PAYPAL AND CREDIT CARD MARKET	1838
Amazon Gift Cards	1816
Fast Money - Accounts & Transfers	1790
Buy Real Money - The Way	1775
BITCARDS - Prepaid cards	1753
Dumps PayPal & Dumps Credit Card - Shop hacked PayPal accounts and credit card details	1702
easyCARDS	1700
Best Financial Service	1670

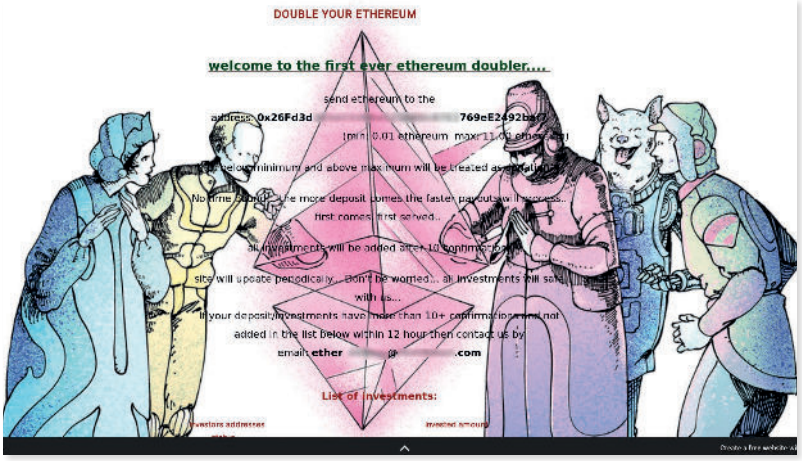
Nous observons au passage que le nombre de miroirs du site Bitcoin x200 est passé de 4000 à pratiquement 7000 depuis notre publication du mois de janvier 2021. Nous ne reviendrons pas ici sur le caractère suspect de cette prolifération de miroirs, puisque le sujet a déjà été traité dans le premier tome.

A tout seigneur, tout honneur. Le site Bitcoin x200 Service propose d'exploiter une faille dans le système de transactions bitcoin. Si l'on accorde (très difficilement) du crédit à ce qui est décrit sur leur page, il est possible d'effectuer des transactions dans lesquelles le vendeur reçoit plus d'argent que l'acheteur n'en a envoyé.

Cela permet ainsi de créer des fonds artificiels et de générer des revenus significatifs. La suite de l'argumentaire est évidemment prévisible : il est proposé d'investir un minimum de 0,005 bitcoin dans ces transactions. Le montant du gain promis est d'un bitcoin

Le site Bitcoin x200 Service

Un autre site propose plus modestement de doubler vos actifs en Ethereum. Aucune explication n'est donnée quant à la méthode employée et le design du site rend celui-ci assez difficilement lisible.



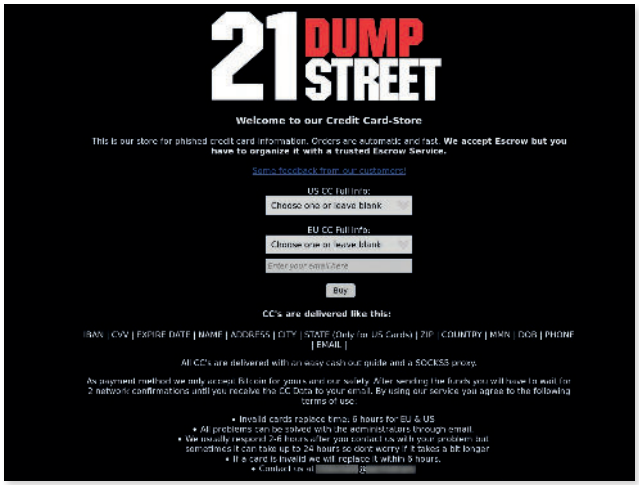
Le site Ethereum Doubler

On trouve également sur le dark web des services de mélange de bitcoins. Ce type de service, appelé **bitcoin mixer**, **bitcoin blender** ou encore **bitcoin tumbler** permet d'ajouter une couche d'anonymat aux transactions effectuées en bitcoin. Il sert donc aux personnes soucieuses de préserver leur vie privée. C'est du moins ce qu'en disent leurs promoteurs, la finalité principale de ces systèmes étant bien plus prosaïquement de blanchir des fonds aux origines douteuses. Le fonctionnement de ces mixeurs ne semble pas différer de celui des mixeurs accessibles sur le clear web.

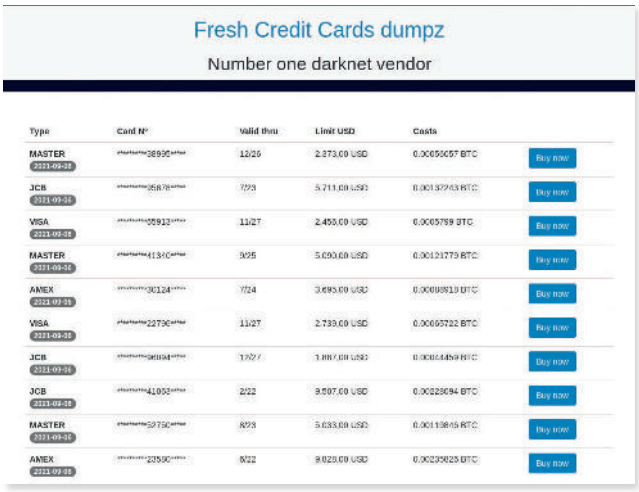
Le site Mixabit

Le site Bitcoin Mixer 2.0

Une autre activité très répandue sur le dark web est le **recel de comptes bancaires piratés**. De très nombreux sites aux noms évocateurs et parfois assez bien trouvés vendent ainsi pour un certain pourcentage de la somme disponible sur le compte toutes les informations qui permettront à l'acquéreur d'utiliser celui-ci.

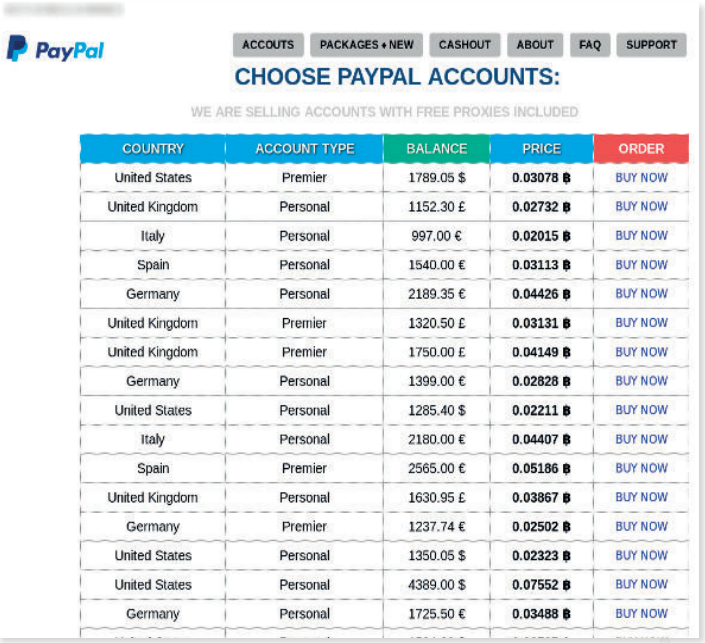


Le site 21 Dump Street

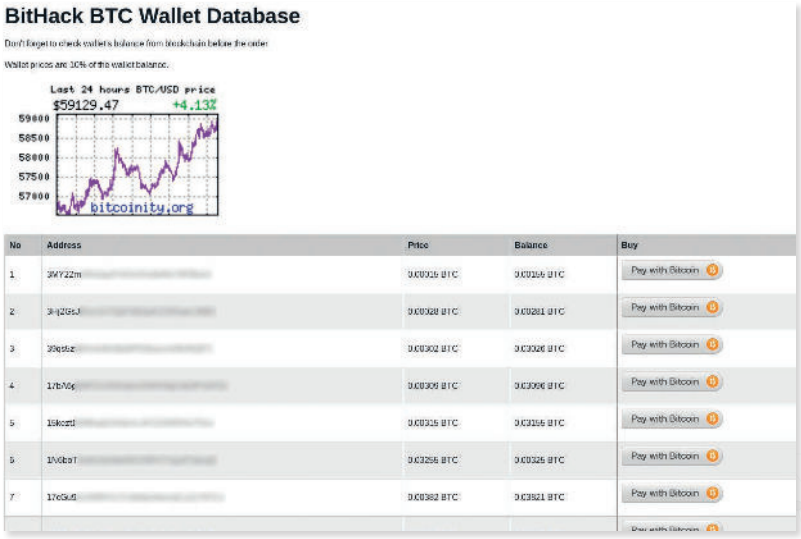


Le site Fresh Credit Cards Dumpz

Les comptes bancaires ne sont pas les seuls moyens de paiement piratés vendus sur le dark web. Certains sites se spécialisent dans la vente de **comptes Paypal ou de portefeuilles Bitcoin.**



Vente de comptes Paypal piratés



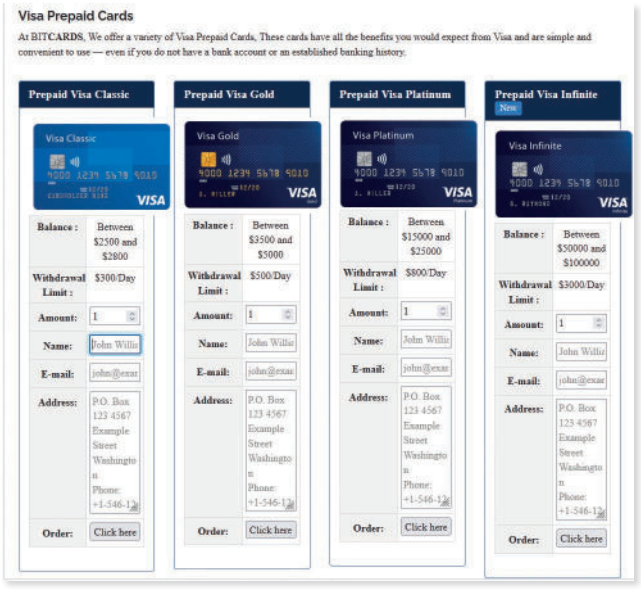
Vente de portefeuilles bitcoin piratés

Là où les services précédemment évoqués ne procurent que des informations dématérialisées, d'autres sites proposent des **packs complets qui comprennent des moyens physiques de paiement** (carte bancaire, chéquier…).

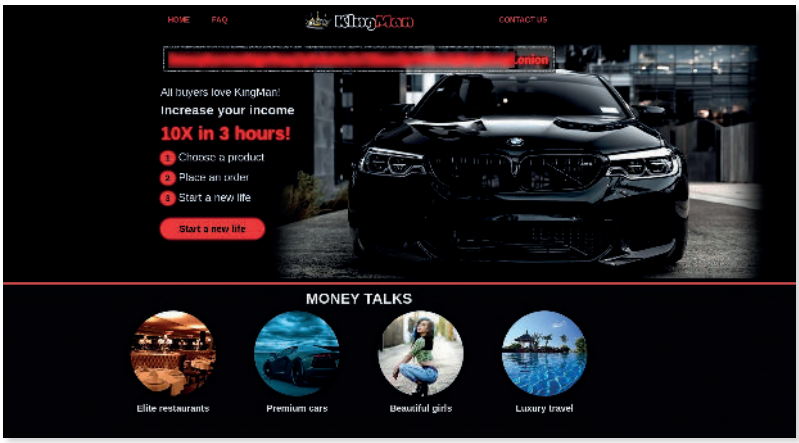
Ces moyens de paiements peuvent servir à l'achat de biens ou à retirer de l'argent aux distributeurs. Il ne s'agit en général pas de comptes piratés mais de cartes pré-payées créées artificiellement et dont l'acquéreur peut modifier les informations.

Vente de packs bancaires complets

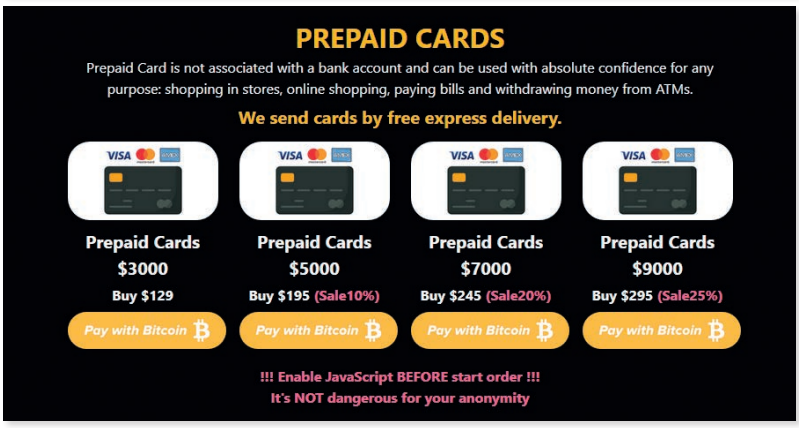
Le site de vente de cartes BitCards



Exemple de cartes vendues sur le site Bitcards



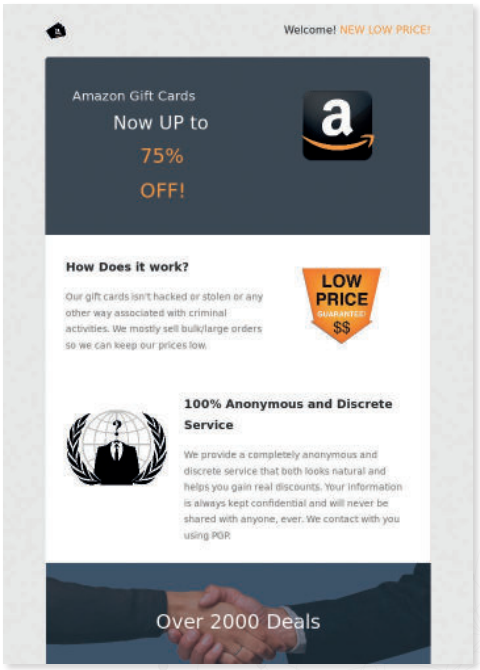
Le site de vente de cartes KingMan



Exemple de cartes vendues sur le site KingMan

Un autre moyen de paiement est proposé à la vente sur le dark web : **les cartes-cadeau de grandes enseignes**. Les cartes sont souvent vendues pour le quart de leur valeur réelle. Selon les vendeurs, il ne s'agit pas de vente de produits d'origine frauduleuse.

L'explication avancée pour justifier les prix anormalement bas est qu'ils achètent des cartes-cadeau en grandes quantités et qu'ils obtiennent ainsi des rabais significatifs. On appréciera la crédibilité toute relative de cette explication, de la même manière qu'on notera avec un sourire la présence d'un encart sur la page d'accueil du site GC King Market, nous avertissant de la présence d'arnaques sur le dark web.



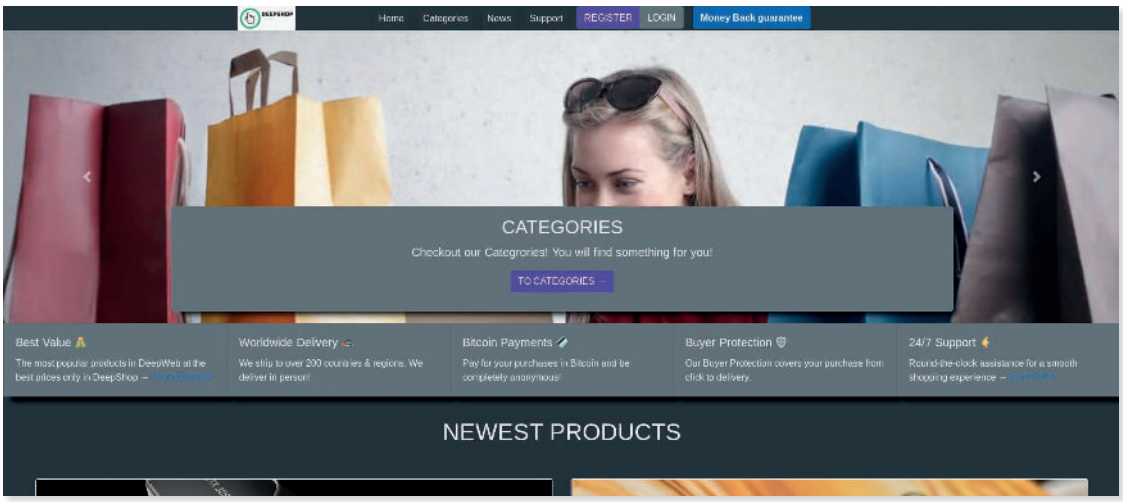
Site spécialisé dans la vente de cartes-cadeau Amazon

GC King Market et son alerte au scam

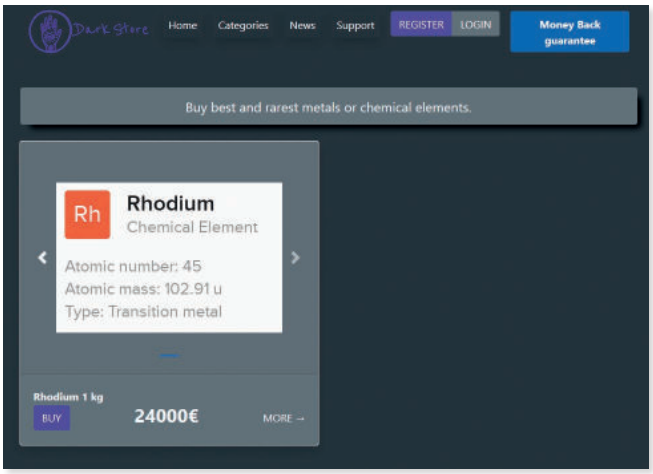
#5.4 - Raretés et légendes urbaines

Après avoir fait un tour d'horizons des biens et services les plus fréquemment vendus sur le dark web, nous aborderons ici quelques propositions commerciales moins courantes.

En plus des marchandises classiques (drogues, armes,...), certaines places de marché du dark web offrent la possibilité d'acheter des produits plus rares ou surprenants. Ainsi, sur le site Dark Store, lui aussi disparu, on pouvait trouver **1 kg de rhodium** pour 24 000 euros. La présence sur une plateforme marchande du dark web de ce métal, utilisé dans l'industrie ou la joaillerie, nous semblait incongrue. Le prix affiché était également suspect, puisqu'un kilogramme de rhodium se négocie aux alentours de 800 000 euros sur les marchés officiels.



Page d'accueil du site Dark Store

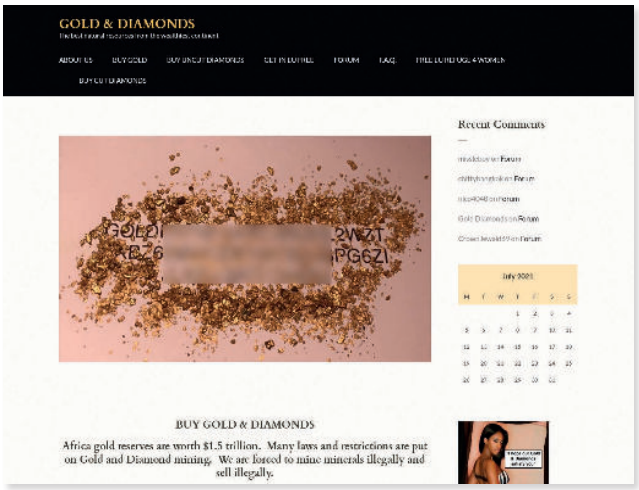


Rhodium en vente sur le site Dark Store

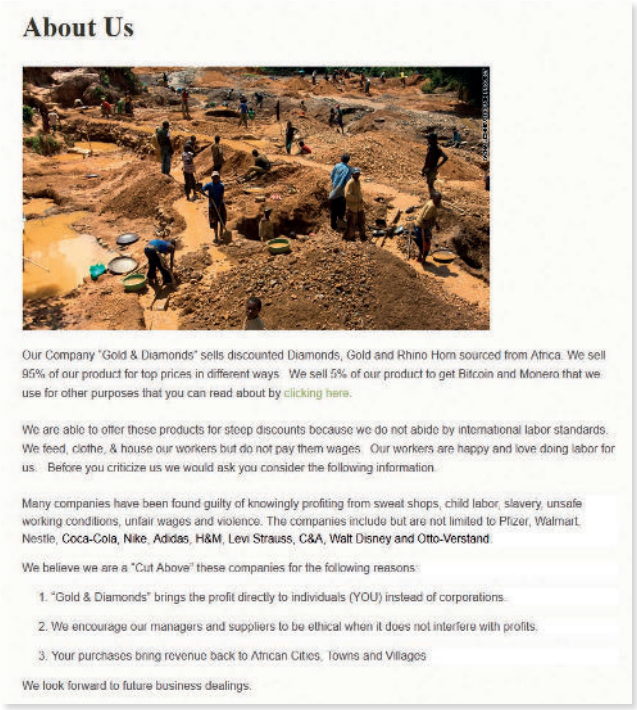
Le site Dark Store ne se limitait pas au **rhodium, aux armes, aux drogues et aux faux billets**. Il proposait également des cartes graphiques, des sous-vêtements soi-disant portés par une femme mais aussi des pochettes surprises (" Random Secret Box"), qui pouvaient contenir des objets en vente sur le site. Il était même possible de participer à un système de loterie avec des lots variés. Ce site marchand très atypique, voire fantaisiste et pour le moins sujet à caution a disparu au cours du mois de novembre 2021 et ne dispose pas de miroir connu à ce jour.

Toujours dans la thématique des métaux précieux, nous trouvons sur le site Gold & Diamonds... de l'or et des diamants.

Ce site au ton très cynique prétend tirer ses ressources de mines africaines clandestines. Il indique que les employés de ces mines sont nourris et logés, mais non payés.



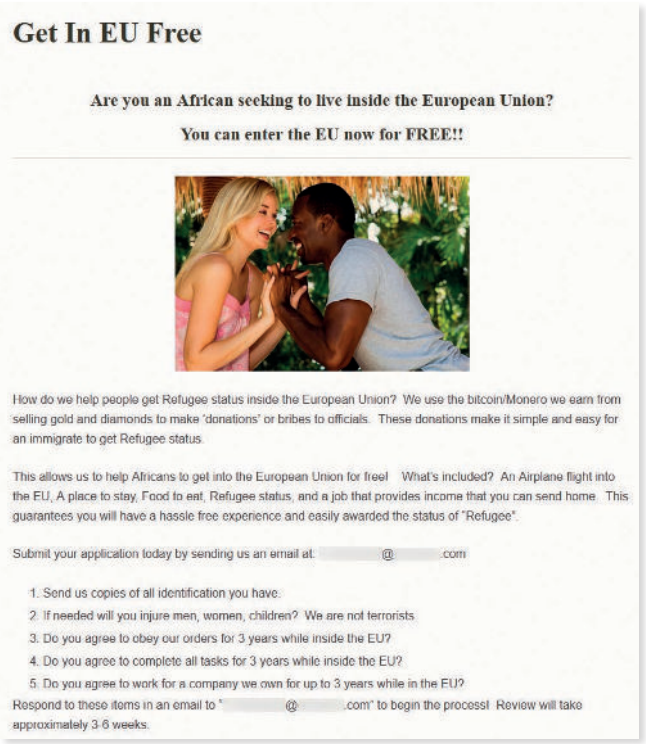
Page d'accueil du site Gold & Diamonds

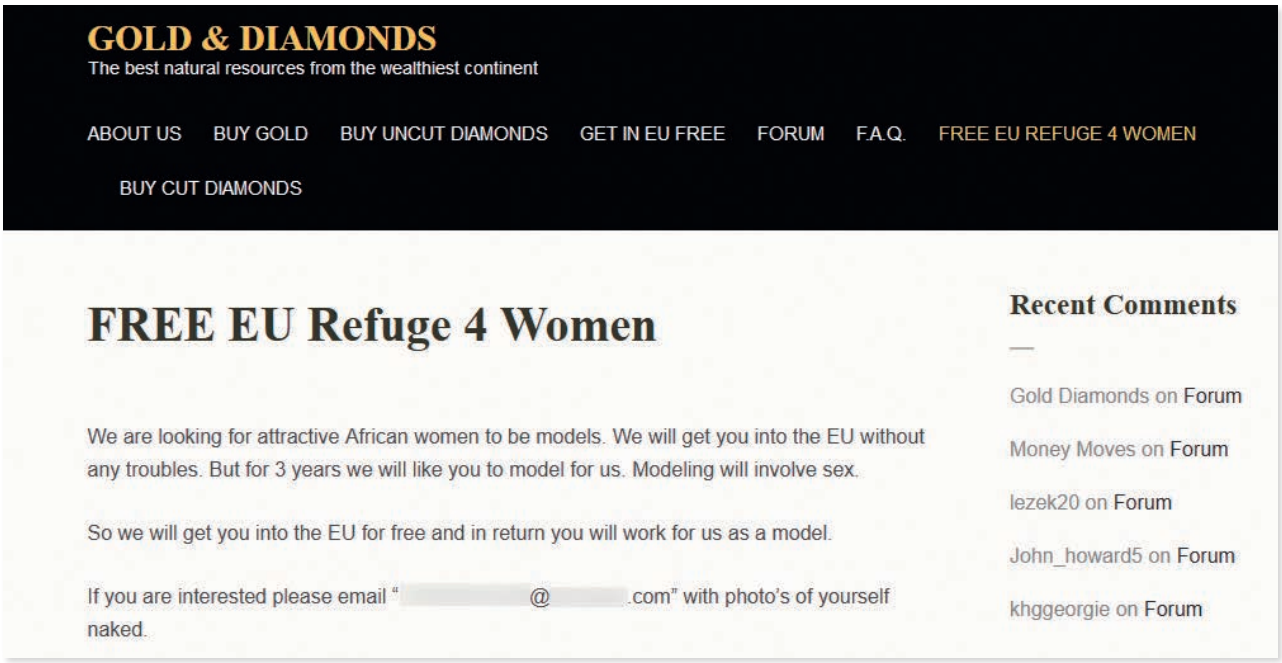


L'éthique selon Gold & Diamonds

Sur la page d'accueil de Gold & Diamonds, nous remarquons deux onglets, intitulés **" Get in EU Free " et " Free EU Refuge For Women"**. Il est proposé à des hommes africains d'obtenir le statut de réfugié dans un pays de l'Union Européenne, moyennant trois ans de travail en UE pour Gold & Diamonds.

Comme souvent dans ce type de commerce, des menaces sur la famille des candidats font office de moyen de pression pour s'assurer l'obéissance de ceux-ci.



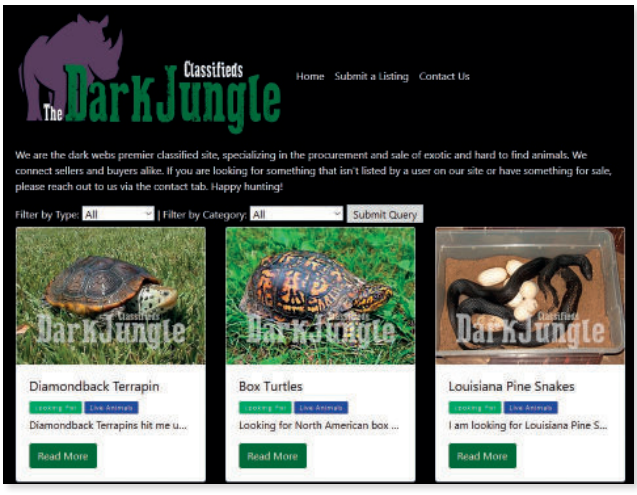


L'offre réservée aux femmes est quasiment identique. Il leur est proposé un accueil en Union Européenne contre 3 ans de " mannequinat " au service de Gold & Diamonds. L'équipe prend tout de même le soin de préciser que ce" mannequinat " **implique des relations sexuelles**.

Le site Gold & Diamonds indique encore qu'il vend des **cornes de rhinocéros**, mais cela ne semble pas être leur cœur de " métier". Certains sites, en revanche, se sont spécialisés dans la vente d'ivoire ou d'espèces protégées.

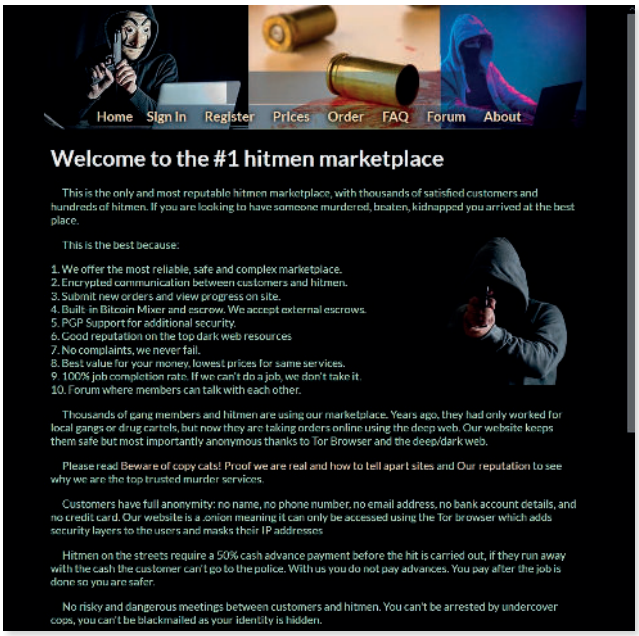
The Dark Jungle, par exemple, mettait en relation des vendeurs et des acheteurs d'animaux exotiques ; on y trouvait aussi des produits à base **d'ivoire et des vêtements en peau d'animaux en voie d'extinction**.

The Dark Jungle a semblé connaître lui aussi une extinction rapide, puisque nous avons détecté son existence en janvier 2021 avant qu'il ne disparaisse au mois de mars.

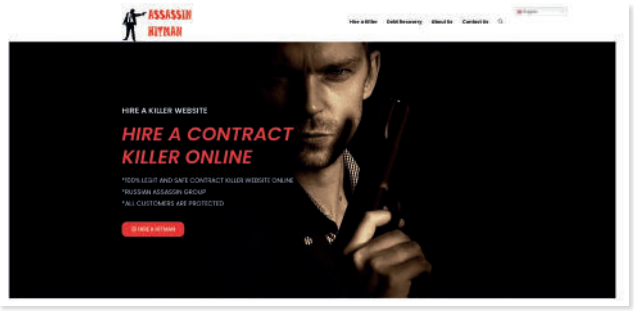


Nous terminons cette recension des propositions commerciales du dark web par deux types d'offre qui ont davantage retenu l'attention des médias ces dernières années : les **services de tueurs à gages et les Red Rooms.**

Un certain nombre de sites du dark web proposent en effet de louer les services de tueurs à gages. Pour quelques milliers d'euros, le client peut désigner une cible pour un assassinat. Pour une somme plus modique, il est aussi quelque fois proposé de procéder à une agression. Les tarifs varient en fonction des dommages que le client souhaite infliger à la cible.



Hire a Hitman



Le site Hire Russian Killer

Il est fort probable que la quasi-totalité des sites qui offrent ce type de services soient des arnaques plus ou moins grossières. Néanmoins, certains faits divers de ces dernières années semblent indiquer qu'il existe bien une offre réelle sur le dark web.

Dans le même ordre d'idée, nous abordons enfin les légendaires **Red Rooms**. Selon les rumeurs complaisamment relayées sur des supports en mal de sensationnalisme, il s'agirait de séances de torture et de mise à mort diffusées en direct sur le dark web.

Moyennant paiement, il serait possible non seulement d'assister à ces séances en streaming, mais certains clients pourraient payer une plus forte somme pour être en mesure de donner des ordres au tortionnaire et ainsi diriger la séance.

Le site Red Room, répliqué sur plus de 1250 miroirs

Un autre site de Red Room

Deux éléments nous font douter de la réalité des Red Rooms.

Le premier est lié au réseau Tor lui-même, dont la relative lenteur ne nous semble pas adaptée à une diffusion vidéo en temps réel. On peut cependant émettre l'hypothèse que les pages sur le dark web ne pourraient servir que d'interface pour l'achat et qu'un lien sur un réseau plus rapide pourrait être communiqué aux clients.

Le deuxième élément est lié au compte à rebours qui est affiché sur la page d'accueil des Red Rooms. On remarque qu'il s'agit dans la quasi-totalité des plus de 1250 miroirs du même compte à rebours : il reste 10 jours, 6 heures et 21 minutes avant la prochaine séance et ce, quel que soit le jour ou l'heure à laquelle on se rend sur ces sites.

Là encore, nous ne disons pas que tous les sites que nous avons évoqués ne sont que des pièges à touriste. Certaines propositions sont en effet très réelles et représentent donc une menace à différents égards.

> Il reste cependant nécessaire de rester prudent et de ne pas suralimenter les fantasmes qui ont cours au sujet du dark web.

Il reste cependant nécessaire de rester prudent et de ne pas suralimenter les fantasmes qui ont cours au sujet du dark web.

A RETENIR :

1 - Les places de vente sur le dark web proposent d'acheter divers biens et services, illégaux ou incongrus. Une part non négligeable des sites indexés sont susceptibles d'être des escroqueries, mais il existe des offres bien réelles.

2 - Les places de vente dans le dark web réservent une offre riche et variée de contrefaçons : faux billets, faux papiers, faux documents ou encore contrefaçons de produits médicamenteux et de produits de luxe.

3 - Les prestations bien réelles de certains vendeurs constituent une sérieuse menace d'ordre sécuritaire, sanitaire et économique pour les personnes, les états et les entreprises.

L'analyse des nombreuses images et métadonnées des domaines et places de vente, ce qui peut permettre de distinguer les escroqueries. C'est également en connaissant les réseaux, en analysant précisément les liens entre les sites, les transactions des portefeuilles de cryptomonnaies qu'il est possible de repérer les vendeurs et les réseaux illicites.

Ce qui est sûr, c'est que les données personnelles volées que nous retrouvons avec notre moteur servent systématiquement à des escroqueries (téléphone, SMS, emails), parfois à de la compromission, de l'arnaque au président... et très rarement, ne servent à rien !

Conclusion

Comme nous l'avons vu, le dark web est un lieu très riche dans sa diversité. Toutefois depuis 2019, une activité se distingue : la place prise par la vente et le dépôt de données exfiltrées (Ransomware, escroqueries, cheval de Troie…).

Nous identifions aisément que le vecteur de ces exfiltrations est aujourd'hui principalement **humain.**

Pourquoi cela ? Parce que tous les jours, nous transportons et partageons nos données, nous les faisons sortir de chez nous et de nos entreprises sur de nombreux supports et par de nombreux vecteurs plus ou moins bien protégés et mis à jour, ou eux-mêmes attaqués, parce que nous ne pouvons pas être toujours totalement vigilants sur tous nos usages informatiques, ni ceux de nos enfants, ni ceux de tous les employés d'une entreprise…

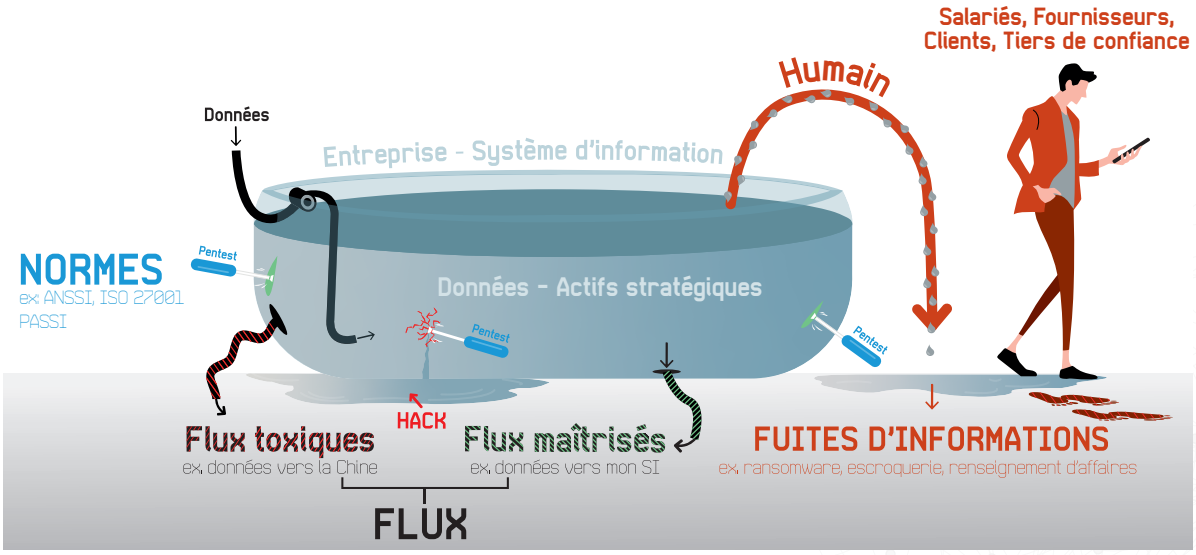
Pour toutes ces raisons, miser sur une cybersécurité centrée sur le système d'information n'est plus du tout suffisant pour garantir l'intégrité des services, des entreprises et la sérénité des foyers.

L'image de la baignoire ci-dessous l'illustre assez simplement.

Aux **normes** de protection cyber actuelles (ISO-207001, PASSI…) nous proposons d'ajouter les périmètres de surveillance suivants :

- **Détection des flux toxiques :** identification de l'ensemble des flux sortant de l'entreprise, afin d'identifier les flux de données non souhaités, vers des serveurs inconnus ou toxiques.
- **Détection des fuites d'informations :** surveiller les dark et deep webs afin d'être alerté au plus vite d'une fuite ou d'un vol de données et pouvoir mettre en œuvre sans attendre les procédures post-incident (pour les court, moyen et long termes) adéquates.

Afin de couvrir l'ensemble des risques cyber, Aleph propose des solutions répondant aux problématiques de flux toxiques et de fuite d'informations. En prenant en compte le facteur humain au même titre que le système d'information, nous pouvons garantir opérationnellement le continuum de sécurité.



Nous espérons que ce second tome vous sera utile.

Il reste encore quelques aspects du dark web à découvrir en notre compagnie, et pour cela nous vous donnons rendez-vous avec plaisir au printemps 2023, pour la sortie du troisième tome...

D'ici là, restez informés !

Suivez-nous sur Linkedin

Abonnez-vous à notre newsletter

Retrouvez nos articles sur notre blog

ALEPH

Analyser, protéger et influencer
votre environnement professionnel

contact@aleph-networks.com
www.aleph-networks.com

413 rue Philippe Héron
69400 Villefranche-sur-Saône
France

Design : frelonbleu.com - Photos Aleph - 03-2023.