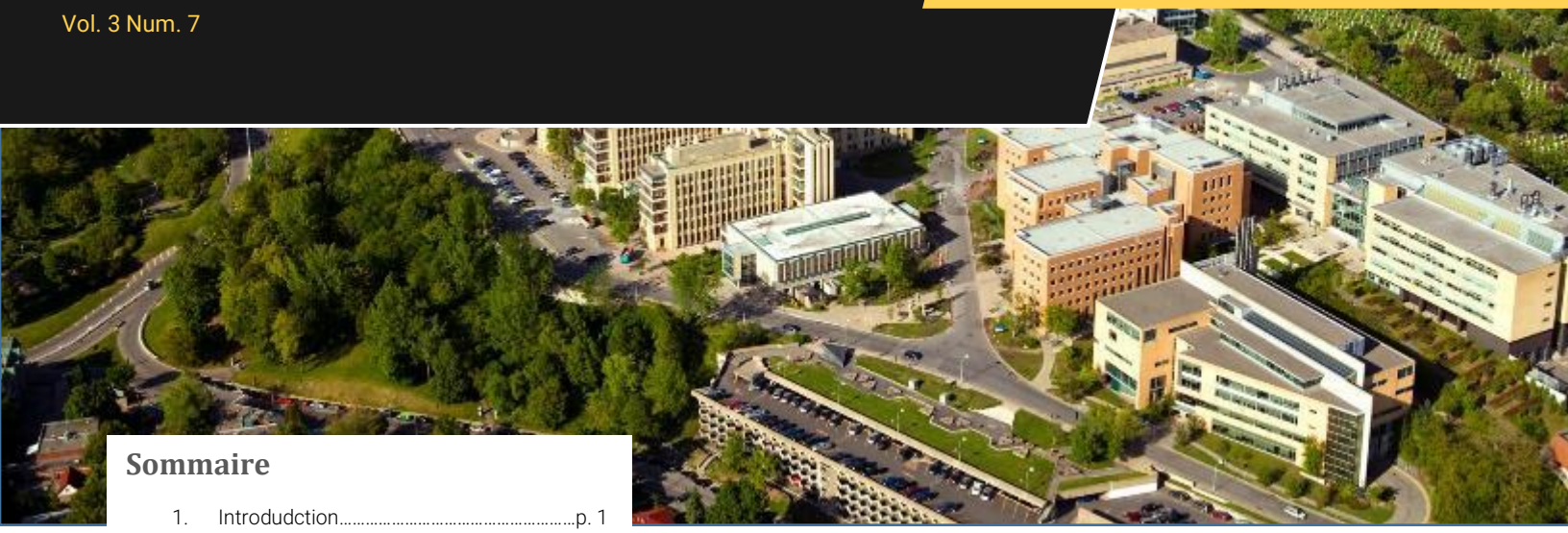
Le Dark Web et les cryptomarchés

Mélanie Théorêt, finissante au baccalauréat en criminologie

Note de synthèse
Vol. 3 Num. 7

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

Theorêt, M. (2023). We The North Market : Fonctionnement et spécificités des échanges entre fraudeurs sur un marché illicite en ligne canadien. (Rapport de stage, UdeM). Disponible à https://www.prevention-cybercrime.ca/projets-de-recherche

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Introduction

La partie cryptée d'Internet, mieux connue sous le nom du *Dark Web*, permet aux utilisateurs de naviguer en tout anonymat sur le Web[1]. Bien qu'il ne soit pas illégal d'y accéder et qu'il peut être utilisé à des fins légitimes, le *Dark Web* est un espace numérique propice à la conduite d'activités illicites. On y retrouve notamment des cryptomarchés qui permettent aux cybercriminels de vendre et d'acheter des biens et services facilitant leurs activités criminelles, ainsi que d'échanger entre eux tout en restant anonymes[1,2,3]. La popularité de ces marchés clandestins a drastiquement augmenté depuis les dernières années, et ce, en dépit des nombreuses opérations policières de démantèlement[4]. Les sites hébergés sur le *Dark Web* facilitent donc la tâche des cybercriminels dans la commission de leurs activités[3].

Cette note de synthèse a pour but d'illustrer le fonctionnement du *Dark Web* et de ses cryptomarchés, ainsi que de mettre en lumière leur rôle dans les diverses activités reliées à la délinquance en ligne, et notamment dans la cyber-fraude. Quelques recommandations pratiques permettant de prévenir le crime sur le *Dark Web*, seront également présentées.

Comprendre le *Dark Web*

L'Internet peut être divisé en trois couches, soit le *Surface Web*, le *Deep Web* et le *Dark Web*[5]. Le *Surface Web*, constitue la couche d'Internet habituellement utilisée par la population générale et qui est indexée et accessible via les moteurs de recherche traditionnels tels que Google, Bing et Yahoo[1,5,6]. Seulement 4% du contenu de tout l'Internet serait disponible sur le *Surface Web*[7]. Le *Deep Web* serait quant à lui, 400 à 500 fois plus grand que le Surface Web[6]. La majorité de son contenu est légitime et comprend, par exemple, les articles académiques qui sont accessibles seulement avec un proxy, ou bien encore les intranets des entreprises qui ne sont accessibles uniquement qu'avec un identifiant et un mot de passe[7,8]. Le *Deep Web* n'est généralement pas accessible avec les moteurs de recherche traditionnels et contient aussi du contenu potentiellement illégitime, tel que des marchés de contrefaçon ou des sites propageant des logiciels malveillants où les internautes peuvent se faire voler des informations personnelles[7].

Le Dark Web constitue, pour sa part, un sous-ensemble du Deep Web dans lequel tout le trafic du réseau est crypté[1,7], ce qui rend beaucoup plus difficile le traçage numérique des activités qui y sont menées[5]. Il est uniquement possible d'y accéder en utilisant des navigateurs spécifiques d'anonymisation, tels que Freenet, I2P et Tor5. Le navigateur le plus populaire pour accéder au *Dark Web* est *The Onion Router (Tor)* qui permet de protéger l'identité d'un utilisateur lorsqu'il navigue sur les sites «.onion »[1,9]. Les serveurs du navigateur fonctionnent avec un réseau de nœuds qui rendent donc impossible de déterminer d'où provient le trafic réseau et sa destination[5]. Ce réseau décentralisé de pair-à-pair permet alors aux cybercriminels d'échapper à la détection et aux réglementations gouvernementales en place[1]. L'anonymat fourni par le *Dark Web* est rapidement devenu attractif pour les cybercriminels, qui peuvent échanger et se livrer à leurs activités en presque totale impunité[1].

Les marchés et les forums du *Dark Web*

À ses débuts, le *Dark Web* était surtout connu pour ses forums permettant le partage de techniques et d'expériences par les pirates informatiques, afin de perfectionner leurs connaissances[10]. Certains de ces forums sont devenus des plateformes et des marchés sophistiqués permettant aux utilisateurs de se procurer facilement des marchandises illicites ou facilitant les activités criminelles[10]. Les marchés du *Dark Web* ressemblent aux sites de vente en ligne conventionnels, tels qu'Amazon et eBay, mais l'offre de produits et les modalités de fonctionnement y sont toutefois différentes et les acheteurs demeurent anonymes[1]. La majorité des biens et services en vente sont des stupéfiants et on peut également y retrouver du matériel l'exploitation sexuelle d'enfants, mais aussi des identités et informations volées, des identifiants de comptes en ligne et des logiciels malveillants[11]. Plus spécifiquement, parmi les produits frauduleux mis en vente, il est possible d'acheter des comptes bancaires, de fausses cartes de crédit, des services de cryptographie et de la contrefaçon[1]. Des tutoriels d'apprentissage sont également offerts sur les marchés, permettant aux cybercriminels d'apprendre les meilleures méthodes pour mener leurs activités en toute sécurité, ainsi que pour maximiser leurs profits[12].

De plus, l'utilisation systématique des cryptomonnaies, telles que Bitcoin, Monero et Ethereum, comme moyen de paiement est une autre garantie permettant d'assurer l'anonymat des transactions sur les marchés illicites pour l'achat de produits ou de services[1]. Les cryptomonnaies rendent les paiements anonymes, réduisent les intermédiaires financiers et les risques de détection[13]. Ce type de monnaie permet d'anonymiser et de sécuriser chaque transaction sur les marchés du *Dark Web*.

Bien que le *Dark Web* apporte plusieurs avantages aux cybercriminels et permette de faciliter leurs activités, il comporte aussi certains inconvénients. En effet, tout comme sur le *Surface Web*, des fraudes contre les utilisateurs peuvent avoir lieu sur le *Dark Web*, notamment auprès des acheteurs de produits sur les marchés clandestins[1]. Par exemple, l'hameçonnage est très répandu sur le

Dark Web, mais, contrairement au *Surface Web*, il est difficile de porter plainte et d'intenter une action en justice contre le fraudeur, car ce dernier est souvent anonyme et intraçable[1]. De plus, l'utilisateur victime de fraude risque de devoir révéler ses activités criminelles, ou du moins expliquer sa présence sur le *Dark Web* en portant plainte aux autorités. Afin de réduire les risques d'escroqueries envers les acheteurs de marchandise sur les marchés du *Dark Web*, une tierce partie nommée *Escrow* y a été ajoutée. Ce système, demandé par les clients pour leur protection, sert à retenir le paiement de l'acheteur jusqu'à ce qu'il confirme avoir reçu le bon produit. Dans le cas où il ne recevrait pas la marchandise demandée, un service de dépôt fiduciaire (*Escrow*) est disponible et rembourse le client en cas de défaut de prestation[14]. Cependant, ce système n'est pas infaillible, car il existe des fraudes de faux *Escrow*[15].

La fraude et le *Dark Web*

Ces dernières années, le nombre de marchés permettant les échanges de produits financiers et de services illégaux a drastiquement augmenté[4]. Les marchés du *Dark Web* sont de plus en plus utilisés pour la vente de produits frauduleux[1]. Ce type de crime touche particulièrement le Canada où les infractions de fraude sont bien présentes[16]. Les produits frauduleux présents sur les cryptomarchés sont nombreux. On y retrouve une grande quantité d'informations confidentielles, facilitant la commission des fraudes, telles que des informations bancaires, des numéros de carte de crédit et des identifiants de connexion[7]. Les forums présents sur le *Surface Web* contiendraient une plus grande quantité d'activités liées aux vols de données telles que la vente d'identifiants de courriels, de réseaux sociaux ou bien encore de sites de magasinage, alors que les forums du *Dark Web* contiendraient une plus grande quantité de ressources facilitant la fraude financière ainsi que des logiciels malveillants[17]. Les marchés et les forums clandestins permettent aux fraudeurs d'apprendre facilement de nouvelles techniques d'escroquerie, de partager leurs propres stratégies et de rechercher de nouvelles données frauduleuses à exploiter[3]. Toutes ces ressources disponibles permettent aux délinquants les moins qualifiés de commettre des fraudes. En effet, il n'est plus nécessaire pour les cybercriminels de maîtriser tous les domaines et les aspects techniques en lien avec leurs activités criminelles, car ils ont la possibilité d'échanger sur le *Dark Web* avec de multiples cyberdélinquants, spécialisés dans chaque partie de la chaîne de production de la cybercriminalité, soit du pirate, au vendeur, en passant par le fraudeur[3]. Les cryptomarchés ont donc permis de faciliter la tâche des cybercriminels, dans la commission des fraudes informatiques et ainsi, d'accroître le nombre de victimes de ce crime[3].

Les opérations policières sur le Dark Web

En raison des activités illicites qui s'y produisent et impactent le monde hors-ligne, certaines opérations des forces de l'ordre ont permis de fermer ces marchés clandestins[10]. Il y a le cas bien connu de *Silk Road*, le premier marché du *Dark Web* mis en place en 2011 et dont la première version du site a été fermée en 2013, après que l'adresse courriel du fondateur ait été répertoriée, révélant ainsi son identité[8]. Le *Dark Web* et l'anonymat qu'il procure n'est donc pas infaillible face à l'erreur humaine et l'ingéniosité policière. Depuis cette opération, les marchés clandestins n'ont cessé de croître, aussi bien par le nombre d'utilisateurs que le volume des échanges et des services proposés[8]. En 2017, ce sont *Alphabay*, *Hansa* et *RAM*, trois marchés internationaux du *Dark Web*, qui ont été fermés par les autorités, ce qui a entraîné un déplacement des utilisateurs vers d'autres marchés secondaires existants[10]. D'autres opérations policières se sont poursuivies, entraînant la fermeture d'*Hydra* 2022 et de *Monopoly Market* en 2023[18]. Comme dans le cas de *Silk Road*, ces différentes opérations de répression, bien qu'elles soient efficaces pour entraîner la fermeture d'un marché, ont conduit à l'émergence et à la sophistication des marchés noirs[10].

Au Canada, c'est le marché *The Canadian Headquarters* qui a été fermé en 2021 à la suite d'une enquête du Conseil de la radiodiffusion et des télécommunications du Canada (CRTC)[16]. Ce marché était devenu l'un des dix plus importants du *Dark Web* depuis son ouverture en 2018[16]. La fermeture a entraîné un déplacement des

utilisateurs vers un nouveau marché créé en 2021 nommé *We The North*[19]. Ce dernier, toujours actif en 2023, offre une variété de produits illicites, tels que des stupéfiants, des produits frauduleux et de la marchandise contrefaite.

On constate donc que, bien que la fermeture des premiers cryptomarchés ait entraîné une augmentation du nombre de vendeurs et de la compétitivité des fournisseurs, les différentes opérations policières, ainsi que d'autres facteurs notamment l'attraction de vendeurs et de la clientèle, font que les nouveaux marchés ne semblent jamais se développer suffisamment[20]. Toutefois, malgré la croissance limitée et la courte durée de vie des marchés du *Dark Web*, leur niveau général d'activité demeure tout de même élevé[21,22,23].

Conclusion et recommandations

En conclusion, le *Dark Web* regorge de possibilité pour les fraudeurs et autres cyberdélinquants d'acheter et vendre des produits illicites, ainsi que discuter en tout anonymat à propos de leurs activités criminelles. **Bien que l'achat et la vente de produits sur les marchés illicites comportent certains risques et inconvénients pour les cybercriminels, leur activité demeure tout de même élevée et ne semble pas près de s'arrêter**[21,22,23]. Il est donc nécessaire de mettre en place des mesures pouvant prévenir les activités criminelles menées sur le *Dark Web*. Il n'est pas question d'interdire complètement l'accès au *Dark Web*, mais plutôt de proposer aux gouvernements et aux décideurs des orientations rationnelles permettant d'en réduire les opportunités criminelles.

De plus, **il est important d'avoir une meilleure connaissance des cryptomarchés et plus précisément de leur rôle dans la commission des différents types de crime**. Plusieurs études se sont particulièrement intéressées à la vente de stupéfiants, d'armes à feu ou bien encore de faux documents. De plus, sur les marchés et les forums du *Dark Web*, les cybercriminels partagent des stratégies pour réaliser leurs crimes, ainsi que des renseignements sur la nature des produits vendus et sur les vendeurs des marchés[3]. Ces informations sont publiquement accessibles et peuvent être utiles pour les forces de l'ordre dans le cadre de leurs enquêtes[24]. Enfin, considérant que les différentes opérations policières visant les marchés clandestins ont entraîné une augmentation de leur activité, ainsi que des déplacements vers d'autres marchés, **il est nécessaire que les forces policières revoient leurs méthodes d'intervention**[10,20,25]. Par exemple, il pourrait être intéressant de se concentrer sur la réduction de la demande des consommateurs de ces marchés et de mettre en place des interventions plus ciblées (p. ex. au niveau des vendeurs) afin de créer un réel impact négatif sur l'écosystème[20].

Références

[1] Jung, B. R., Choi, K. et Lee, C. S. (2022). Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(2), 4-24.

[2] Nardo, M. (2011), Economic crime and illegal markets integration: a platform for analysis. *Journal of Financial Crime*, *18*(1), 47-62.

[3] Wilson, E. (2019). Disrupting dark web supply chains to protect precious data. *Computer Fraud & Security*, *4*, 6-9.

[4] Soldner, F., Kleinberg, B. et Johnson, S. (2022). *A Fresh Look at Fraud*. (1ère edition). Routledge.

[5] Mirea, M., Wang, V. et Jung, J. (2019). The not so dark side of the darknet: A qualitative study. *Security Journal*, *32*(2), 102-118.

[6] Rudesill, D. S., Caverlee, J. et Sui, D. (2015). The deep web and the darknet: A look inside the internet's massive black box. *Woodrow Wilson International Center for Scholars*, STIP, 3.

[7] Chikada, A. et Gupta, A. (2017). *Online brand protection. In Handbook of Research on Counterfeiting and Illicit Trade*. Edward Elgar Publishing.

[8] Lacey, D. et Salmon, P.M. (2015). It's Dark in There: Using Systems Analysis to Investigate Trust and Engagement in Dark Web Forums. Dans Harris, D. (dir.), *Engineering Psychology and Cognitive Ergonomics. EPCE 2015. Lecture Notes in Computer Science (p. 117-128)*, vol 9174. Springer, Cham.

[9] Yetter, R. B. (2015). *Darknets, cybercrime & the onion router: Anonymity & security in cyberspace*. ProQuest Dissertations and Theses. 102.

[10] Gañán, C. H., Akyazi, U. et Tsvetkova, E. (2020). Beneath the radar: Exploring the economics of business fraud via underground markets. *2020 APWG Symposium on Electronic Crime Research (eCrime)*, 1-14.

[11] Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Hernandez Ganan, C., Klievink, B., Christin, N. et Van Eeten, M. (2018). Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets. *In Proceedings of the 27th USENIX Security Symposium*, 1009-1026

[12] Van Hardeveld, G. J., Webber, C. et O'Hara, K. (2016). Discovering credit card fraud methods in online tutorials. *In Proceedings of the 1st International Workshop on Online Safety, Trust and Fraud Prevention* (OnSt '16). Association for Computing Machinery, New York, NY, USA, Article 1, 1–5.

[13] Buxton, J. and Bingham, T. (2015). The Rise and Challenge of Dark Net Drug Markets. *Global Drug Policy Observatory*. Policy Brief No. 7.

[14] Goldfeder, S., Bonneau, J., Gennaro, R., & Narayanan, A. (2017). Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin. *Financial Cryptography*.

[15] Anderson, R.J., Barton, C.J., Böhme, R., Clayton, R., Eeten, M.V., Levi, M., Moore, T.W. et Savage, S. (2012). Measuring the Cost of Cybercrime. *Workshop on the Economics of Information Security*.

[16] Coutu, S. (2022, novembre). Canadian HQ, le darknet bien de chez vous : Comment le CRTC a fermé le plus gros marché canadien du web clandestin. *Radio-Canada*.

[17] Bermudez-Villalva, A. et Stringhini, G. (2021). The shady economy: Understanding the difference in trading activity from underground forums in different layers of the Web. *APWG Symposium on Electronic Crime Research (eCrime)*, 2021, pp. 1-10.

[18] Europol. (2023, mai). 288 dark web vendors arrested in major marketplace seizure. *Europol*.

[19] The Recorded Future. (2021, octobre). WeTheNorth: A New Canadian Dark Web Marketplace. *The Recorded Future*.

[20] Soska, K et Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. *Proceedings of 24th USENIX Security Symposium (USENIX Security '15)*, 33-48.

[21] Broseus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F. et D. Décary-Hétu. (2016). Studying illicit drug trafficking on darknet markets: Structure and organisation from a Canadian perspective. *Forensic Science International*, *264*, 7-14.

[22] Holt T. J., Smirnova O., Chua Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior*, 37, 353-367.

[23] Yip, M., Webber, C. et Shadbolt, N. (2013). Trust among cybercriminals? Carding forums uncertainty and implications for policing. *Policing and Society*, *23*(4), 516-539.

[24] Martin, J. (2014). *Drugs on the Dark Net : How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*. Palgrave Pivot.

[25] DiPiero, C., (2017). Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web. *U. Ill. L. Rev*.