We The North Market

Fonctionnement et spécificités des échanges entre fraudeurs sur un marché illicite en ligne canadien

CRPC | Chaire de recherche en prévention de la cybercriminalité

Auteure

Mélanie Théorêt, finissante au baccalauréat en criminologie

Pour citer: Théorêt, M.(2023). *We The North Market : Fonctionnement et spécificités des échanges entre fraudeurs sur un marché illicite en ligne canadien*. Rapport de stage. Chaire de recherche en prévention de la cybercriminalité.

Ce document est disponible intégralement en format électronique (PDF) sur le site Web de la Chaire de recherche en prévention de la cybercriminalité à : https://www.prevention-cybercrime.ca.

Cette étude a fait l'objet d'une approbation du Comité d'éthique de la recherche - Société et culture (CERSC) de l'Université de Montréal (2023-4102: DARKWEB-CAN)

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.

Sommaire exécutif

La partie cryptée d'Internet, mieux connue sous le nom du DarkWeb, permet aux utilisateurs de naviguer en tout anonymat sur le Web. 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. La popularité de ces marchés clandestins a drastiquement augmenté depuis les dernières années, et ce, en dépit des nombreuses opérations policières de démantèlement. Les sites hébergés sur le Dark Web facilitent donc la tâche des cybercriminels dans la commission de leurs activités, notamment les fraudes.

Le Dark Web regorge d'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. Les marchés et les forums du Dark Web 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 .

Ce rapport de stage porte sur les échanges sur le forum et le marché de fraude de We The North afin de mettre en lumière les techniques utilisées par les fraudeurs canadiens pour commettre leurs crimes. Les questions de recherche sont les suivantes: (1) quels sont les principaux services et produits de la fraude offerts sur le marché et (2) quelle est la nature des échanges entre les fraudeurs sur le forum.

Les principaux résultats montrent que les types de produits frauduleux les plus fréquents sur la plateforme sont les cartes de crédit (CVV), les dossiers de crédit et les identités volées. On constate également que les prix des produits en vente varient selon le type de produit et les caractéristiques de l'article. De plus, par les rétroactions, les acheteurs du marché se disent en grande partie satisfaits des produits frauduleux achetés et les vendeurs arrivent à obtenir des gains pouvant dépasser les 50 000$ grâce à diverses stratégies de vente. L'analyse du forum montre que les fraudeurs utilisent les fils de discussion entre autres pour partager leur avis sur les vendeurs et leurs produits, pour faire de la publicité, pour rechercher des services et articles, ainsi que pour s'entraider en s'échangeant des conseils et des techniques de fraude.

Table des matières

Introduction

Description du milieu de stage et mandat

Le milieu de stage est la Chaire de recherche en prévention de la cybercriminalité (CRPC). Cette Chaire a vu le jour en septembre 2018 à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Sa mission est de contribuer à « l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention, à travers des projets de recherche appliqués développés en collaboration avec ses deux partenaires industriels » (Chaire de recherche en prévention de la cybercriminalité, s. d.). La CRPC est dirigée par le professeur Benoît Dupont et elle encadre les projets de recherche de différents étudiants en stage, à la maîtrise et au doctorat. Les activités de la Chaire visent à répondre aux besoins des industries en matière d'enjeux de cybercriminalité en offrant des outils concrets pour la formation, la prévention et le développement de politiques. La diffusion des résultats de recherche sous forme de publications académiques, de notes de synthèse, de conférences et de produits de vulgarisation fait partie intégrante du mandat de la CRPC. En plus de produire des connaissances scientifiques visant à prévenir la cybercriminalité, la Chaire a également pour but de former les professionnels du milieu sur la prévention et la gestion du risque cybercriminel.

Le présent projet de stage portant sur une analyse d'un marché illicite de fraude s'aligne donc avec les objectifs et le mandat de la Chaire. La recherche vise à maximiser les connaissances sur un enjeu de cybercriminalité peu étudié dans la littérature. Les résultats obtenus sont présentés dans le présent rapport. Une note de synthèse portant sur le fonctionnement du *Dark Web* et sur les marchés illicites de fraude sera également disponible sur le blogue de la CRPC, afin de permettre à tous les partenaires d'y accéder. Les résultats seront aussi partagés lors d'une conférence devant des membres de Desjardins.

Présentation de la recherche

Malgré les nombreux avantages d'Internet, nous observons que certains individus ont profité de cette prolifération et de l'avènement des nouvelles technologies pour s'engager dans des activités criminelles en ligne. La littérature révèle que l'accessibilité aux technologies et son utilisation plus fréquente par la population ont contribué à faire augmenter les cybercrimes à plusieurs endroits dans le monde (Koziarski & Lee, 2020).

Parmi ces cybercrimes, il y a notamment la fraude en ligne dont le nombre de victimes potentielles a drastiquement augmenté avec la démocratisation d'Internet, les sites d'achats en ligne et l'émergence des technologies permettant le transfert d'argent en ligne (Cross, 2019). Selon le centre antifraude du Canada, ce sont 47 803 personnes qui ont été victimes de fraude en 2021. Les pertes financières reliées à ces crimes atteignent 383,6 millions de dollars en 2021 et 420,8 millions de dollars au 31 octobre 2022 (Centre antifraude du Canada, 2022, novembre).

Par ailleurs, la partie cryptée d'Internet, aussi appelée Dark Web, permet de faciliter la tâche des fraudeurs dans la commission de leurs activités criminelles (Wilson, 2019). En effet, les marchés du Dark Web qui ressemblent aux marchés en ligne conventionnels, tels qu'Amazon et eBay, permettent aux cybercriminels de vendre et d'acheter des produits frauduleux, ainsi que d'échanger entre eux tout en restant anonymes grâce aux réseaux décentralisés de pair-à-pair permettant d'échapper à la détection et aux réglementations gouvernementales en place (Jung et al., 2022; Nardo, 2011 ; Wilson, 2019). Le Dark Web est alors un endroit en ligne où les fraudeurs et autres cyberdélinquants peuvent discuter en tout anonymat à propos de leurs activités criminelles. Il existe différents forums pour ce faire, dont certains qui se concentrent principalement sur la fraude financière (Bermudez-Villalva et Stringhini, 2021).

Cette recherche a donc pour objectif d'étudier les échanges entre les fraudeurs sur le marché canadien We The North sur le Dark Web, afin de mieux comprendre comment la vente de produits frauduleux fonctionne sur le marché illicite et de mettre en lumière les stratégies utilisées par les fraudeurs pour escroquer les citoyens canadiens. Cette étude permettra de clarifier la façon dont les fraudeurs gèrent leurs affaires et ainsi de mieux prévenir les cas de fraude. Les paragraphes suivants présenteront d'abord une recension de la littérature en lien avec le sujet d'étude, suivie de la problématique et de la méthodologie. Les résultats obtenus seront ensuite présentés et interprétés. Finalement, une discussion des résultats, les limites de la recherche, ainsi qu'une conclusion seront expliquées.

Recension des écrits

Les cybercrimes et leur typologie

Les cybercrimes sont des infractions criminelles commises à l'aide d'Internet et des technologies en ligne, cependant il y a une distinction à faire entre les cybercrimes qui dépendent des technologies pour avoir lieu et ceux qui sont facilités par les nouvelles technologies (McGuire et Downling, 2013; Levi, Doig, Gundur, Wall et Williams, 2015). En effet, certains crimes en ligne tels que les attaques par déni de service distribué, qui rendent indisponible un service en ligne ou un site Internet, et les rançongiciels qui constituent des attaques à l'aide de logiciels malveillants, n'ont pas vraiment d'équivalent hors-ligne (McGuire et Downling, 2013; Levi et al., 2015). Ces infractions n'existeraient donc pas sans Internet. Les recherches existantes se sont d'ailleurs principalement concentrées sur ce type de cybercrime qui est généralement motivé par les gains monétaires, mais aussi parfois par des idéologies politiques (Levi et al., 2015).

D'un autre côté, certains cybercrimes, bien que leur portée soit accrue par les plateformes informatiques, ne nécessitent pas Internet pour exister (Levi et al., 2015). Ces crimes peuvent alors se dérouler en ligne et hors-ligne. La vente frauduleuse et la fraude sentimentale sont des exemples de ce type de crime (McGuire et Downling, 2013; Levi et al., 2015). Il est donc possible de constater que bien qu'Internet occupe une place prépondérante dans la façon de faire des fraudeurs, ceux-ci peuvent avoir recours à diverses plateformes de communications et autres mécanismes hors-ligne pour commettre leurs crimes (Cross, Richards et Smith, 2016).

Qu'est-ce que la fraude?

L'article 380 (1) du Code criminel (2022) détermine qu'un individu coupable de fraude correspond à « quiconque, par supercherie, mensonge ou autre moyen dolosif, constituant ou non un faux semblant au sens de la présente loi, frustre le public ou toute personne, déterminée ou non, de quelque bien, service, argent ou valeur ». Du côté de l'Agence de la consommation en matière financière du Canada (2022), la fraude, pouvant aussi être qualifiée d'escroquerie, constitue un « acte malhonnête commis pour nuire à une autre personne ou pour s'emparer de son argent ou de ses biens ». Ces deux définitions sont générales et semblent englober tous les types de fraude. Cependant, il faut savoir que certains articles du Code criminel viennent préciser la définition de la fraude. En effet, la définition de l'article 402.2 aborde plus précisément le vol d'identité où on mentionne au

au paragraphe 1 que « commet une infraction quiconque obtient ou a en sa possession des renseignements identificateurs sur une autre personne dans l'intention de les utiliser pour commettre un acte criminel dont l'un des éléments constitutifs est la fraude, la supercherie ou le mensonge ». Le paragraphe 2 du même article ajoute que le trafic de ces renseignements identificateurs, donc une personne qui les « transmet, rend accessible, distribue, vend ou offre en vente, ou a en sa possession à une telle fin », commet également une infraction. Certains articles du Code criminel viennent clarifier l'infraction selon le type de fraude. L'article 342 aborde par exemple le vol, la falsification et le trafic de cartes de crédit et l'article 403 aborde la fraude à l'identité.

Bien que les précédentes définitions de la fraude ne fassent de distinction entre la fraude qui a lieu dans un environnement virtuel et celle qui a lieu hors-ligne, les messages textes, les appels téléphoniques et la communication en face à face demeurent tous des moyens efficaces pour permettre aux fraudeurs d'escroquer leurs victimes (Cross, 2019). La fraude constitue donc une infraction criminelle facilitée par Internet et les nouvelles technologies, ne dépendant pas de ces dernières pour exister (Cross, 2019 ; McGuire et Downling, 2013). La présente recherche portera uniquement sur les fraudes commises en ligne, qui sont aujourd'hui beaucoup plus fréquentes que les fraudes hors-ligne (Jung, Choi et Lee, 2022). En ajout aux définitions précédentes, les fraudes informatiques peuvent alors être considérées comme des crimes qui dépendent de la technologie pour exister.

Ingénierie sociale et manipulation des victimes

L'ingénierie sociale est une pratique qui consiste à manipuler le comportement de la victime pour l'inciter à transmettre ses données personnelles (Conteh et Schmick, 2016). Les fraudeurs qui collectent des renseignements personnels sur un individu, tels que le numéro de carte de crédit, les informations bancaires et les mots de passe, peuvent utiliser ces informations pour se faire passer pour cette personne et ainsi obtenir certains avantages. On parle alors de vol d'identité et de fraude à l'identité (Centre antifraude du Canada, 2021). Plusieurs autres types de fraude existent également et on constate que les fraudeurs vont utiliser diverses stratégies pour tenter de tromper leur victime, mais leur objectif reste le même, soit d'obtenir des renseignements personnels ou des gains financiers (McGuire et Downling, 2013). Pour y arriver, ils doivent avoir de bonnes capacités de communications pour réussir à persuader leurs victimes par le mensonge et pour réussir à gagner leur confiance (Wang, 2021).

Les fraudeurs vont avoir recours à différents stratagèmes pour arriver à leurs fins. Ils vont notamment tenter de tromper leur victime par le mensonge et la manipulation, en se faisant passer pour une autre personne, afin de convaincre la victime de lui fournir ses renseignements personnels ou financiers (Wang, 2021).

Pour ce faire, les fraudeurs utilisent différentes tactiques et méthodes. Certains vont par exemple utiliser la technique d'hameçonnage, qui consiste à se faire passer pour une personne de confiance ou une organisation légitime, afin d'obtenir les renseignements personnels ou financiers de la victime (Bureau de la Concurrence Canada, 2017). Cela peut se faire par le biais d'une copie exacte d'un site légitime ou d'une pièce jointe envoyée par courriel ou par texto par exemple. Une autre méthode pour les fraudeurs est de se faire passer pour un prétendant amoureux dans l'espoir d'obtenir de l'argent auprès d'une victime (Bureau de la Concurrence Canada, 2017). Il s'agit de la fraude sentimentale ou amoureuse. Dans ce cas-ci et dans d'autres types de fraudes comme la fraude à l'investissement ou la fraude à l'héritage par exemple, l'escroc va tenter d'établir un lien de confiance avec la victime pour obtenir des gains financiers (Cross, 2019). Le cybercriminel peut même aller jusqu'à utiliser la violence psychologique pour obtenir un contrôle sur sa victime et ainsi qu'elle accepte de répondre à toutes ses demandes (Cross, Dragiewicz et Richards, 2018).

D'autre part, la motivation principale des fraudeurs à escroquer leurs victimes se résume par l'appât de gains monétaires, soit par la vente de renseignements personnels volés ou directement par l'obtention d'argent de la part de la victime (Jung et al., 2022). Selon McGuire et Downling (2013), certains types de fraude servent exclusivement à obtenir des renseignements confidentiels sur la victime, tandis que d'autres, qui constituent la majorité des fraudes, tentent plutôt d'obtenir directement de l'argent. Généralement, c'est soit un ou l'autre, mais rarement les deux (McGuire et Downling, 2013).

La fraude au Canada et ailleurs

Comme l'observe David Décary-Hétu, chercheur en criminologie, la fraude est un crime très développé au Canada, spécifiquement dans les régions de Montréal et Laval où se concentre ce type d'activités criminelles (Coutu, 2022). Le rapport de VIDOCQ (2022) sur l'écosystème de la fraude à Montréal vient confirmer cette affirmation. En effet, le rapport met en lumière trois plateformes marchandes vendant des informations bancaires volées sur le Dark Web, qui semblent être opérées par des fraudeurs de Montréal. Ces informations bancaires permettent de faire un large éventail d'activités illégales permettant aux fraudeurs d'obtenir de l'argent, en effectuant des retraits de sommes importantes au compte, en utilisant le compte pour faire du blanchiment d'argent, ou encore en vendant les identifiants du compte sur des marchés clandestins (Maimon et Fraser, 2022). L'étude de Holt, Smirnova et Chua (2016) examinant plusieurs forums clandestins mentionne aussi que la fraude de compte bancaire est commune au Canada. D'un autre côté, les résultats de la recherche de Smirnova et Holt (2017) montrent plutôt que parmi les produits frauduleux en vente sur des forums et des marchés clandestins,

89% des produits du Canada étaient des cartes de crédit (CVV ou dumps). L'étude de Holt et Lampke (2010), mentionne également que les cartes de crédit sont des produits populaires au Canada. Ces recherches montrent donc que les Canada est un endroit où les marchés illicites de vente de comptes bancaires compromis, ainsi que de cartes de crédit volées sont opérés.

D'autre part, la fraude est aussi présente ailleurs dans le monde. Les résultats de la recherche de Lusthaus (2018) montrent que les différents types de fraude se spécialisent géographiquement. Pour ce qui est du Brésil, le pays se spécialise dans la fraude par carte de crédit, ainsi que la fraude bancaire. En Roumanie, ce sont la fraude au guichet automatique, aussi appelée fraude ATM, ainsi que la fraude aux enchères en ligne qui sont présentes. Au Nigeria, le pays est reconnu pour la fraude 4-1-9 qui consiste à promettre une somme d'argent importante à une victime en lui exigeant d'abord des informations personnelles ou une petite somme d'argent. Lusthaus (2018) mentionne aussi que d'autres types d'arnaques où le fraudeur tente de gagner la confiance de sa victime sont fréquents au Nigeria. En Chine, le vol de crédits ou d'articles de jeux vidéo en ligne est un problème, ainsi que le vol de propriété intellectuelle. Dans la région des États post-soviétiques, on se spécialise dans la production et dans la distribution de logiciels malveillants. Concernant les pays occidentaux, ils se spécialisent dans l'encaissement d'argent et dans les mules qui sont des personnes recrutées par les fraudeurs, afin de servir d'intermédiaire pour le transfert d'argent volé (Centre antifraude du Canada, 2022, juillet). Du piratage et de l'exploitation de logiciels malveillants sont également fréquents en Occident. Aux États-Unis plus précisément, le pays est une source importante pour les identités et les cartes de crédit volées (Holt et al., 2016).

Lusthaus (2018) constate donc que l'Europe de l'Est s'occupe davantage de fournir et de produire les produits frauduleux, tandis que l'Occident va plutôt acheter ces produits et ensuite s'occuper du côté monétaire, soit d'encaisser et de transférer l'argent. Il y a donc une collaboration vendeur-acheteur entre les deux parties. Bref, la recherche de Lusthaus (2018) permet de montrer que la fraude est une problématique présente dans différents pays à travers le monde. Elle permet aussi de mettre en lumière l'existence d'une certaine régionalisation des produits et services de la fraude.

Comprendre le Dark Web

L'Internet peut être divisé en trois couches, soit le Surface Web, le Deep Web et le Dark Web (Mirea et al., 2019). Le Surface Web ou web de surface en français, constitue la couche d'Internet habituellement utilisée par la population générale et qui est indexé et accessible via les moteurs de recherche traditionnels tels que Google, Bing et Yahoo (Jung et al., 2022; Mirea et al., 2019; Rudesill, Caverlee et Sui, 2015). Seulement 4% du contenu de tout l'Internet serait disponible sur le web de surface (Chikada et Gupta, 2017).

Quant au Deep Web, traduit par web profond en français, il serait de 400 à 500 fois plus grand que le Surface Web (Rudesill et al., 2015). La majorité de son contenu est légitime et comprend les articles académiques qui sont accessibles seulement avec un pare-feu, ainsi que les intranets des entreprises qui sont accessibles uniquement avec un identifiant et un mot de passe (Chikada et Gupta, 2017; Lacey et Salmon, 2015). Cependant, 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 diffusant des logiciels malveillants où les internautes peuvent s'y retrouver involontairement et se faire voler des informations personnelles (Chikada et Gupta, 2017).

Le Dark Web constitue, pour sa part, un sous-ensemble du Deep Web dans lequel tout le trafic du réseau est crypté, ce qui fait qu'aucune trace numérique ne peut être retracée (Mirea et al., 2019). Il est uniquement possible d'y accéder en passant par des navigateurs spécifiques d'anonymisation, tels que Freenet, I2P et Tor (Mirea et al., 2019), car le Dark Web est constitué de réseaux superposés dont les adresses IP sont complètement cachées (Jung et al., 2022 ; Chikada et Gupta, 2017). 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 » (Jung et al., 2022 ; Yetter, 2015). Les serveurs fonctionnent avec un réseau de nœuds qui rendent donc impossible de déterminer d'où vient le trafic réseau et où il va (Mirea et al., 2019). L'anonymat qu'apporte Tor, fait que le Dark Web est rapidement devenu un espace numérique où les cybercriminels peuvent se livrer à leurs activités (Jung et al., 2022).

Le rôle du Dark Web dans la fraude

La mise en place du Dark Web a permis de faciliter la tâche des cybercriminels, dans la commission des fraudes informatiques et ainsi, d'accroître le nombre de victimes de ce crime (Wilson, 2019). En effet, il est possible de retrouver sur le Dark Web 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 (Chikada et Gupta, 2017). Les marchés et les forums du Dark Web 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 (Wilson, 2019). Ils sont donc de plus en plus utilisés pour la vente de produits frauduleux (Soldner, Kleinberg et Johnson, 2022). Cela dit, même les délinquants les moins qualifiés peuvent commettre des fraudes avec l'aide de ces plateformes cachées. En effet, les cybercriminels n'ont aujourd'hui plus le besoin 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 à chaque partie de la chaîne, soit du pirate, au vendeur, en passant par le fraudeur (Wilson, 2019).

D'autre part, les fraudes peuvent avoir lieu sur le web de surface, mais également directement sur le Dark Web. Par exemple, la recherche de Jung et al. (2022) suggère que les clients sur les marchés financiers du Dark Web sont susceptibles d'être ciblés par une escroquerie lors de leurs achats sur les plateformes. Le type de fraude financière le plus courant sur l'Internet clandestin serait l'hameçonnage (Handalage et Prasanga, 2021). Cependant, contrairement à la fraude sur le Surface Web, il est difficile de porter plainte et d'intenter une action en justice contre le fraudeur sur le Dark Web, car ce dernier est anonyme et intraçable (Jung et al., 2022).

Les marchés et les forums du Dark Web

Dans ses débuts, le Dark Web comportait des forums qui avaient pour but de permettre le partage de techniques et d'expériences par les pirates informatiques, afin d'aider d'autres individus à perfectionner leurs connaissances (Gañán, Akyazi et Tsvetkova, 2020). Ces forums sont devenus aujourd'hui des plateformes et des marchés sophistiqués qui permettent aux consommateurs d'accéder facilement à des marchandises découlant d'activités criminelles (Gañán et al., 2020). Les espaces de forums restent tout de même présents sur certains marchés. La majorité des marchandises échangées constituent des stupéfiants, mais l'échange d'informations financières volées, l'usurpation d'identité, les faux comptes et les logiciels malveillants occupent aussi une place importante (Van Wegberg et al., 2018). Parmi les produits vendus, il y a également les comptes bancaires, les fausses cartes de crédit, les services de cryptographie et la contrefaçon (Jung et al., 2022). Selon Bermudez-Villalva et Stringhini (2021), les forums présents sur le web de surface contiennent une plus grande quantité d'activités liées aux vols de données, tandis que les forums du Dark Web contiennent une plus grande quantité de ressources liées à la fraude financière et aux logiciels malveillants. Les données volées par les fraudeurs, qui se retrouvent en vente sur les cryptomarchés du Dark Web, se divisent en trois grandes catégories, soit les données personnelles qui incluent des informations comme le nom, le numéro d'assurance sociale et la date de naissance d'un individu, les données financières qui comprennent les numéros des cartes de crédit et des comptes bancaires, puis les données d'entreprise qui regroupent les informations sur les employés d'une entreprise ou sur les activités de celle-ci et de ses fournisseurs (Wilson, 2019).

Les forums du Dark Web ont été étudiés par divers chercheurs, tels que Broseus et al. (2016) qui ont analysé les marchés canadiens de stupéfiants, Holt et al. (2016) qui ont exploré les forums russes et anglais d'identités volées et Yip, Webber et Shadbolt (2013) ayant étudié les marchés chinois de vente de cartes de crédit volées. Ces forums facilitent la commission des fraudes et permettent aux cybercriminels de discuter entre eux au sujet des transactions illicites et des tactiques utilisées (Yip et al., 2013).

Par exemple, les forums de vente de cartes de crédit volées analysés par Yip et al. (2013), se divisent en différentes sections pour les discussions générales et les tutoriels. Les fraudeurs ont aussi l'option de discuter dans un chat privé. Ces différentes sections facilitent le réseautage entre les cybercriminels. L'accès à certains de ces réseaux criminels cachés semble cependant difficile, car il faut y être invité pour pouvoir interagir avec le groupe et avoir accès aux discussions (Chikada et Gupta, 2017).

Par ailleurs, pour permettre aux cybercriminels d'apprendre les meilleures méthodes afin d'effectuer des transactions illicites en toute sécurité, certains marchés du Dark Web offrent à ses membres des tutoriels d'apprentissage, qui sont en majorité payants (Van Hardeveld, Webber et O'Hara, 2016). Plus ces tutoriels sont dispendieux, plus ils permettent à l'acheteur de faire des revenus importants. Dans une communauté de fraudeurs par carte de crédit, les tutoriels pour débutants se vendent généralement pour moins de 100$ et se concentrent sur les étapes de base pour pouvoir encaisser les cartes de crédit volées (Van Hardeveld et al., 2016). Des tutoriels sur les techniques de cryptage, empêchant la détection par les forces de l'ordre, sont parfois également offerts à ces communautés.

Les prix et le processus de paiement

Concernant les prix de la marchandise frauduleuse en vente sur les marchés, quelques recherches s'y sont attardées (Steel, 2019; Vargas, 2019). La littérature montre que les prix varient énormément selon le type de produits en vente, le marché, ainsi que le pays. Par exemple, le prix pour une carte de crédit volée de type Visa ou Mastercard dans l'étude de Vargas (2019) est de 6 dollars américains ($USD) aux États-Unis, 25$USD en Europe et 15$USD au Canada. Le prix pour un passeport canadien contrefait s'élève à 3 500$USD et celui pour un vrai passeport volé, bien que ce soit rare, dépasse les 10 000$USD. De plus, le fait pour un individu d'être le premier à exploiter un certain type de fraude lui permet de vendre ses produits à des prix plus élevés sur le Dark Web (Steel, 2019). En effet, dans les cas de vol d'identité, le prix minimum pour une identité volée est à la baisse, car de nombreuses personnes ont vu leur identité se faire voler et être vendue plusieurs fois avec l'accroissement de la fraude (Steel, 2019). Le prix le plus bas pour une identité volée au moment de l'étude de Steel (2019) était de 0,004$USD, tandis qu'il était de 10$USD en 2007. Cela dit, il est avantageux pour les fraudeurs d'exploiter rapidement les nouvelles opportunités de fraude pour maximiser leurs gains financiers (Steel, 2019)
Par ailleurs, ces marchés virtuels restent anonymes grâce à l'utilisation des cryptomonnaies comme Bitcoin, Monero et Ethereum (Jung et al., 2022).

Les cryptomonnaies correspondent à des fonds d'argent virtuel qui peuvent être échangés, de façon anonyme, directement à un autre utilisateur et avec un faible risque de détection (Buxton et Bingham, 2015). Ce type de monnaie permet de sécuriser chaque transaction sur les marchés du Dark Web.

Afin de réduire les risques d'escroqueries envers les acheteurs de marchandise sur le Dark Web, une tierce partie nommée Escrow a été ajoutée sur les marchés du Dark Web (Jung et al., 2022). 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, le service Escrow intervient et rembourse le client (Goldfeder et al., 2017). Cependant, ce système n'est pas infaillible, comme il est possible de le voir dans la recherche de Anderson et al. (2017) avec les fraudes de faux Escrow.

La confiance des vendeurs sur les marchés

La confiance des clients envers les vendeurs est un élément essentiel dans la vente de produit sur les marchés du Dark Web (Laferrière et Décary-Hétu, 2022; Tzanetakis et al., 2016). Les clients des marchés clandestins veulent obtenir des produits de qualité en évitant de se faire arnaquer, alors ils vont porter une attention particulière aux signaux pouvant indiquer la crédibilité des vendeurs (Laferrière et Décary-Hétu, 2022). Cependant, considérant que les marchés clandestins sont entièrement en ligne et que les utilisateurs ne se rencontrent pas en face à face, il peut être difficile pour les vendeurs d'obtenir la confiance de leurs clients (Lorenzo-Dus et Di Cristofaro Citation2018). Il est donc important pour les vendeurs de montrer une bonne image d'eux-mêmes sur les plateformes illicites en ligne, afin d'obtenir cette confiance de la part de la communauté (Laferrière et Décary-Hétu, 2022; Tzanetakis et al., 2016).

Les systèmes de rétroactions sont l'un des éléments les plus importants dans le développement de la réputation des vendeurs (Barratt et Aldridge 2016; Laferrière et Décary-Hétu, 2022; Tzanetakis et al. 2016). Être actif dans la communauté, notamment sur les forums de discussion ou en message privé, est une autre façon efficace pour les vendeurs d'augmenter leur crédibilité (Décary-Hétu et Leppänen, 2016; Holt et al., 2016; Tzanetakis et al., 2016; Yip et al., 2013). Les vendeurs qui ont une plus longue période d'activité sur les marchés sont également plus susceptibles d'être dignes de confiance (Holt et al., 2016; Jung et al. 2022). Les clients vont donc utiliser les renseignements qu'ils trouvent en ligne sur les vendeurs, afin de déterminer s'ils veulent acheter leurs produits ou avoir recours à leurs services (Laferrière et Décary-Hétu, 2022).

Les opérations policières sur les marchés du Dark Web

D'autre part, certaines opérations des forces de l'ordre ont eu lieu dans le but de fermer ces marchés clandestins (Gañán et al., 2020). 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 a été répertoriée, révélant ainsi son identité (Lacey et al., 2015). Le Dark Web et l'anonymat qu'il procure n'est donc pas infaillible face à l'erreur humaine. Depuis cette opération policière, les marchés clandestins n'ont pas arrêté de croître, quant aux nombres d'utilisateurs, au volume des échanges et aux services proposés (Lacey et al., 2015). 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 (Gañán et al., 2020). 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 (Gañán et al., 2020).

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, font que les nouveaux marchés ne semblent jamais se développer suffisamment (Soska et Christin, 2015). Toutefois, malgré la croissance limitée et la courte durée de vie des marchés du Dark Web, leur activité demeure tout de même élevée, comme il a été montré dans les différentes recherches sur les marchés du Dark Web (Broseus et al., 2016; Holt et al., 2016; Yip et al., 2013).

We The North Market

Le marché qui sera étudié lors de cette recherche se nomme We The North et a été mis en place en juillet 2021 (The Recorded Future, 2021). Il s'agit d'un marché canadien qui offre une variété de produits illicites, tels que des stupéfiants, des produits frauduleux et de la marchandise contrefaite. Ce marché a été créé à la suite de la fermeture du marché clandestin The Canadien Headquarters en juillet 2021 (The Recorded Future, 2021). The Canadien Headquarters, actif depuis octobre 2018, était un marché canadien similaire à celui de We The North et il était devenu l'un des dix plus gros marchés illicites du Dark Web (Coutu, 2022). C'est une enquête du Conseil de la radiodiffusion et des télécommunications du Canada (CRTC) qui a permis de fermer ce marché et de punir l'administrateur du site, ainsi que trois vendeurs importants (Coutu, 2022). Plusieurs utilisateurs de The Canadien Headquarters, se sont donc déplacés vers le nouveau marché We The North pour continuer leurs activités (The Recorded Future, 2021).

La mission de We The North est d'offrir un environnement sécuritaire pour permettre aux acheteurs et aux vendeurs du marché d'effectuer leurs transactions sans risque (The Recorded Future, 2021). Pour ce faire, des règles strictes ont été mises en place par les administrateurs et sont affichées sur le site du marché, afin de maintenir un contrôle sur les types de produits et services vendus. Il est par exemple interdit de vendre des armes et des explosifs, des services de prostitution, du contenu d'exploitation sexuelle d'enfants, des services de tueur à gages et tout ce qui est lié au terrorisme. De plus, tous les échanges de produits doivent obligatoirement se faire au Canada. Des mesures additionnelles de sécurité telles que l'authentification à deux facteurs, obligatoire pour tous les vendeurs du marché, le non-remboursement des frais de 300$ pour la création d'un compte vendeur, l'obligation pour les vendeurs d'avoir une clé PGP sur le profil pour assurer le chiffrement des échanges et l'interdiction de laisser de faux avis après l'achat d'un article ont aussi été mises en place pour assurer davantage la sécurité des utilisateurs. Les règles du site ont pour but de rendre le marché plus légitime et de ne pas attirer un certain type de clientèle non désirée (The Recorded Future, 2021).

Concernant, les transactions sur We The North, elles se font exclusivement en cryptomonnaie, soit en Bitcoin et Monero pour assurer l'anonymat des vendeurs et des clients. Le système Escrow est également présent sur le site pour sécuriser les échanges. Les produits digitaux doivent être envoyés à l'acheteur avant 48h et les produits physiques doivent être livrés en 14 jours. Dans le cas contraire, l'acheteur peut contester la commande ou demander un remboursement à Escrow. Dans le cas où un acheteur se ferait arnaquer, ce dernier peut signaler l'arnaque dans le forum prévu à cet effet et demander de l'assistance aux administrateurs en créant un ticket. We The North offre, comme la plupart des marchés du Dark Web, un support client 24/7 en anglais et en français à tous les utilisateurs du marché qui pourraient avoir besoin d'aide (The Recorded Future, 2021).

Problématique

La fraude est un enjeu qui a pris énormément d'ampleur depuis la démocratisation d'Internet et qui fait des millions de victimes chaque année, tout en entraînant des pertes financières non négligeables (Cross, 2019). Le Canada constitue un pays où ce type de crime est bien développé (Coutu, 2022). De plus, le nombre de marchés du Dark Web permettant les échanges de produits financiers et de services illégaux a drastiquement augmenté depuis les dernières années (Jung et al., 2022). Ainsi, l'étude des échanges entre les fraudeurs sur le Dark Web et les techniques de fraude utilisées par ceux-ci est pertinente, afin de mieux comprendre ce phénomène, peu documenté dans la littérature.

La revue de littérature a montré que les marchés et les forums du Dark Web facilitent la tâche des fraudeurs en leur permettant d'acheter et de vendre des produits frauduleux, ainsi que d'apprendre de nouvelles techniques d'escroquerie (Wilson, 2019). L'existence de marchés clandestins canadiens, tels que Canadian Headquarters, qui faisait partie des marchés les plus importants dans le domaine de la fraude, montre l'ampleur de ce crime au Canada (Coutu, 2022). Le marché We The North, contribue donc à cette problématique canadienne en permettant la vente de produits frauduleux qui peuvent par exemple permettre d'usurper l'identité d'une personne ou d'obtenir illégalement des gains financiers.

Bien que la littérature recense plusieurs études sur la fraude et sur les marchés noirs, peu d'entre elles se concentrent sur les produits frauduleux qui se vendent sur le Dark Web. Par l'étude des échanges sur le forum et le marché de fraude de We The North, il sera donc possible de combler ce manque dans la littérature en clarifiant quelles sont les techniques utilisées par les fraudeurs canadiens pour commettre leurs crimes, c'est-à-dire de comprendre (1) quels sont les principaux services et produits de la fraude offerts sur le marché et (2) quelle est la nature des échanges entre les fraudeurs sur le forum. Cette étude est donc pertinente, car elle permettra possiblement l'avancement des connaissances cybercriminelles en clarifiant la façon dont les fraudeurs gèrent leurs affaires.

Méthodologie

Le sujet de la recherche est d'étudier les échanges entre les fraudeurs sur le Dark Web, afin de contribuer à l'avancement des connaissances en lien avec la vente de produits frauduleux et les stratégies utilisées sur le marché noir pour escroquer les citoyens canadiens. Cette recherche est donc de type exploratoire, car à la suite de la recension des écrits, il est possible de constater qu'il existe peu de littérature en lien avec le sujet. L'étude permettra alors de mettre en lumière un sujet encore peu documenté en criminologie.

Provenance de l'échantillon

Concernant l'échantillon, le marché illicite du Dark Web nommé We The North sera examiné. Ce marché contient une plateforme marchande où les produits frauduleux sont vendus, ainsi qu'un forum où les fraudeurs peuvent discuter entre eux. Les échanges sur la plateforme ont lieu principalement en anglais et parfois en français. Ce marché a été choisi, car il est canadien, donc les produits offerts se vendent uniquement au Canada. Il est aussi pertinent pour la recherche, parce qu'il contient une plateforme marchande et un espace de discussion, alors il permet de répondre aux deux questions de recherche. C'est-à-dire de déterminer les principaux types de services de la fraude offerts sur le marché et d'en apprendre plus sur la nature des discussions entre les fraudeurs.

De plus, le marché illicite contient différentes catégories de produits en vente. Sur un total de onze catégories, il y a par exemple « Drugs & Chemicals » et « Guides & Tutorials » qui sont celles offrant le plus de produits sur le marché, soit plus de 2000 produits pour chacune des sections. Il y a également une section « Fraud » où près de 1000 produits et services frauduleux sont offerts. Dans le cadre de cette présente recherche qui se concentre sur la fraude, uniquement la section « Fraud » du marché sera analysée. Parmi tous les produits et services de fraude mis en vente dans cette catégorie, on en compte 963 au moment de la collecte de données. Tous les articles présents sur le marché depuis juillet 2021, soit la date de création du marché, jusqu'en janvier 2023, soit le moment de la collecte, et ayant au moins une vente seront examinés. Seulement les produits frauduleux, tels que des cartes de crédits, des comptes bancaires, des dossiers de crédit et des identités volées seront retenus jusqu'à saturation. La section « Fraud » contient aussi des doublons, des produits contrefaits, des commandes personnalisées et des guides qui seront alors exclus de la collecte de données, car ils ne correspondent pas aux produits que nous voulons étudier. En effet, comme l'équipe de The Recorded Future (2021) le mentionne, de nombreux articles sont publiés en double ou sont publiés dans la mauvaise

La plateforme contient également une section nommée « Autoshop » où les fraudeurs peuvent acheter des identités volées et des cartes de crédit en filtrant selon les caractéristiques désirées de la victime. Cette section se distingue principalement par le fait que la vente se fait à l'instant même sans la possibilité d'avoir recours à Escrow. Cette section ne sera cependant pas étudiée lors de la recherche, car les informations présentes sur le marché régulier telles que le nombre de vente et le nombre de rétroactions ne sont pas disponibles sur « Autoshop ».

Concernant le forum présent sur We The North, il se divise en trois sections. La première est « Information board » où les administrateurs publient des messages destinés à la communauté et où les utilisateurs du marché peuvent se présenter. La deuxième section se nomme « Listing Reviews ». Il s'agit d'une section où les vendeurs peuvent faire de la publicité et où il est possible de discuter à propos des produits en vente. Cette partie est elle-même divisée en quatre sous-sections, soit « Fraud », « Guides », « Drugs » et « Others ». La troisième section constitue celle de « Discussions », permettant aux cyberdélinquants d'échanger sur différents sujets, parmi les sous-sections « Fraud », « Guides » « Drugs », « OPESEC » et « Others ». Dans chacune des sous-sections, les acheteurs et les vendeurs du marché peuvent créer des fils de discussions sur les sujets de leur choix. Les fils de discussion sont tous classés par ordre chronologique, du plus récent ou plus ancien. Dans le cadre de notre recherche, ce sont les deux sous-sections sur la fraude qui seront examinées. Celle dans « Listing Reviews » contient 501 fils et 1030 messages et celle dans « Discussions » contient 312 fils et 813 messages au moment de la collecte de données.

Tous les individus ayant un compte sur le marché, que ce soit un compte vendeur ou un compte client, ont la possibilité de participer aux discussions sur le forum. Les administrateurs peuvent aussi y laisser des messages. Les usagers ont également l'option de laisser une mention j'aime sur les messages ou de répondre directement à un message précis avec le bouton « Reply ». Lorsqu'une personne écrit sur le forum, son rôle est identifié sous son pseudonyme et une couleur lui est attribuée. Les individus ayant un compte client ont la mention « Customer » et leur pseudonyme est noir, les vendeurs se distinguent par la mention « Seller » et un pseudonyme de couleur bleu, puis les administrateurs sont reconnaissables par la mention « Admin » et un pseudonyme rouge. Afin de pouvoir vendre des produits, il est nécessaire de posséder un compte vendeur qu'il est possible d'obtenir en payant la somme de 300$. Afin de réduire les risques d'arnaque, les administrateurs mentionnent qu'il est impossible de faire des achats avec un compte vendeur. Les vendeurs voulant acheter des produits doivent donc également se créer un compte client. De plus, les individus ne respectant pas les règles du marché peuvent être bannis de ce dernier. Les messages de ces utilisateurs bannis demeurent tout de même disponible sur le forum, mais une mention « Blocked » est inscrite et le pseudonyme de l'utilisateur est rayé d'une ligne.

Approche méthodologique et stratégie d'analyse

Concernant la partie quantitative, une analyse de contenu a été faite sur les produits en vente sur le marché We The North. L'objectif est de catégoriser les différents produits de la fraude qui y sont vendus, afin de faire un portrait global des produits et des services frauduleux disponibles sur le marché illicite ciblé. À partir des éléments trouvés, il a été possible de bâtir une grille de codification qui a permis de quantifier les produits et d'avoir une vue d'ensemble sur le marché. Des analyses quantitatives descriptives ont ensuite été faites à partir des données codifiées dans la grille. Des tableaux de résultats ont ensuite pu être créés pour présenter les données.

L'approche méthodologique privilégiée pour cette recherche constitue une méthodologie mixte, soit une combinaison des approches quantitative et qualitative. Du côté qualitatif, il est question d'analyser les interactions et les discussions entre les fraudeurs sur le Dark Web. Nous avons réalisé une analyse de contenu, qui consiste à observer et à examiner le contenu des interactions et des discussions entre les utilisateurs du forum de We The North. Lors de cette étude, le chercheur joue donc un rôle d'observateur qui est non participant. En effet, il n'a pas été question d'interagir et de discuter avec les fraudeurs, mais plutôt d'observer ce dont ils discutent et de répertorier les éléments qui nous intéressent. Pour cette partie qualitative, l'obtention d'un certificat d'éthique auprès du Comité d'éthique de la recherche - Société et culture (CERSC) de l'Université de Montréal a été nécessaire, car l'analyse des discussions des forums implique des participants humains. À la demande du Comité et par souci d'anonymat, le contenu des discussions du forum a été paraphrasé plutôt que d'être cité directement, afin de ne pas être en mesure de retracer les propos à l'utilisateur.

Collecte des données

Pour accéder au Dark Web, le navigateur d'anonymisation Tor a été utilisé. Il a été téléchargé sur un ordinateur et une fois connecté au navigateur Tor, nous avons accédé au site du marché We The North présent sur le Dark Web en passant par le lien « .onion » du marché. Une fois que le site du marché a été accessible, un compte utilisateur a été créé pour y entrer. Il faut fournir un nom d'utilisateur, un mot de passe et un PIN de 6 chiffres. Il a ensuite été possible de débuter la collecte de données par l'observation non participante.

La cueillette de données pour la partie quantitative a été faite en répertoriant tous les produits frauduleux qui nous intéressent dans le marché sous forme de listage jusqu'à saturation des données. Ces éléments ont ensuite été catégorisés dans une grille de codification lors de l'analyse. Concernant la partie qualitative de la recherche, la collecte de

de données a été faite à partir des forums de discussions du marché. Les discussions pertinentes en lien avec la fraude ont été retranscrites dans un document Word et une grille d'observation a été créée pour classer les discussions par thématiques, afin de faciliter l'analyse. Les données ont été collectées depuis la création du marché, soit juillet 2021, jusqu'au mois de la collecte de données, soit janvier 2023. Il a ainsi été possible d'avoir une vue d'ensemble sur les services frauduleux offerts sur le marché et sur les discussions entre les fraudeurs.

Opérationnalisation des concepts et variables

La présente étude se concentre sur les échanges entre les fraudeurs sur le marché clandestin We The North. Il est alors possible de diviser ce concept d'échange en deux dimensions, soit les interactions sur le forum et les services frauduleux vendus. Le concept d'échange entre fraudeurs correspond donc à tous les échanges, peu importe leur nature, entre les fraudeurs sur le marché du Dark Web ciblé. Un échange pouvant être un échange écrit, donc une discussion, ou bien un échange marchand, soit l'échange d'un produit frauduleux contre de l'argent. L'échange de produits a été déterminé selon le nombre d'articles vendus indiqué pour chaque produit en vente et les discussions ont été observées dans le forum du marché.

Pour la dimension de l'échange de produits frauduleux, elle a été divisée en trois indicateurs. Le premier est le type de produits frauduleux offerts, le deuxième est les informations sur le vendeur et le troisième indicateur constitue les caractéristiques de la marchandise. Concernant les types de produits offerts, l'indicateur a été divisé en sept variables selon les produits trouvés lors de la collecte. Tout d'abord, les cartes de crédit (CVV) correspondent aux informations d'une carte de crédit, notamment le numéro de la carte et le code de sécurité à trois chiffres qui permettent aux fraudeurs de faire des transactions en ligne (Bulakh et Gupta, 2015). Les cartes de crédit (dumps) sont des copies digitales de cartes de crédit qui permettent aux fraudeurs de cloner la piste magnétique et de créer une carte physique (Bulakh et Gupta, 2015). Ensuite, les identités, connues aussi sous le nom de fullz, correspondent aux informations personnelles complètes sur une personne, telles que le nom, l'adresse, la date de naissance et le numéro d'assurance sociale. Ce type de produit permet de voler l'identité d'une personne et de se faire passer pour elle (Smirnova et Holt, 2017). Les identités synthétiques sont des identités fictives qui ont été créées par les fraudeurs à partir de différentes informations provenant d'identités réelles (Equifax, 2022). Concernant les comptes bancaires, ce type comprend les informations bancaires volées d'une personne qui permettent alors aux fraudeurs d'accéder au compte de la victime grâce aux identifiants et aux questions de sécurité obtenues.

Le type des comptes de compagnie correspond aux identifiants permettant de se connecter à un compte sur le site d'une entreprise et sur lequel une carte de crédit y est généralement affiliée. La dernière variable est les dossiers de crédit qui sont les informations sur une victime, telles que le nom, la date de naissance, le numéro d'assurance sociale et l'adresse, ainsi que les identifiants permettant aux fraudeurs d'accéder au dossier de crédit de la victime.

Du côté de la dimension des informations sur les vendeurs, les variables qui ont été retenues lors de la collecte sont d'abord le nom du vendeur qui correspondant à un pseudonyme sur le marché et qui a été anonymisé pour la recherche. Une autre variable est le niveau du vendeur. Les administrateurs de We The North expliquent qu'à chaque 5000$ de ventes qu'un vendeur fait, son niveau monte de 1 jusqu'à un maximum de 10. Puis, la date de création du compte vendeur sur le marché a été identifiée en examinant les profils des différents vendeurs.

Concernant les caractéristiques de la marchandise, le prix du produit a été déterminé selon le prix affiché pour chaque produit sur le marché en dollars canadiens. D'autres variables additionnelles, soit le nombre de ventes d'un produit, le nombre de rétroactions, ainsi que la date depuis laquelle le produit frauduleux est sur le marché ont été identifiées en examinant l'affichage du produit et sa description.

Par ailleurs, la dimension des interactions et discussions entre fraudeurs sur les forums du Dark Web a été divisée en sept indicateurs qui comprennent chacun diverses variables. Ces indicateurs correspondent aux thématiques identifiées lors de l'observation du forum de discussion sur la fraude, soit la publicité par les utilisateurs, la recherche de produits, les avis sur les vendeurs, le partage de conseils et méthodes, la recherche de partenaires et services, la qualité des produits, ainsi que le fonctionnement du marché. Pour chaque thématique, des sous-thèmes ont été identifiés. Les sous-thèmes correspondent aux variables et regroupent les différents types de produits frauduleux, ainsi que d'autres sujets abordés dans les discussions. Les thèmes, ainsi que leurs sous-thèmes sont définis et présentés en annexe dans le tableau 3.

Résultats et analyse

La présente recherche porte sur les échanges entre fraudeurs sur le marché et le forum de We The North de juillet 2021 à janvier 2023. Les objectifs de l'étude sont d'examiner (1) quels sont les principaux services et produits frauduleux offerts sur le marché et (2) quelle est la nature des échanges entre les fraudeurs sur le forum. Les résultats obtenus permettront de mieux comprendre comment les fraudeurs gèrent leurs activités et permettront également l'avancement des connaissances sur la fraude en ligne.

La vente de produits frauduleux

Le tableau 1 présente un portrait global des produits frauduleux en vente sur le marché à l'étude de juillet 2021 à janvier 2023. Les différents articles offerts sont séparés en sept types de produit de la fraude et des mesures descriptives ont été calculées pour chacun des types.

Type de produit	*n*	Fréquence	Prix min	Prix max	Moyenne prix	Nombre ventes	% ventes	Nombre rétroactions	Acheteurs satisfaits
Carte de crédit (CVV)	23	19,0%	$2,10	$84,00	$39,35	2130	36,7%	1020	94,4%
Dossier de crédit	25	20,7%	$11,55	$78,75	$49,81	1623	28,0%	737	97,6%
Identité	31	25,6%	$3,15	$31,50	$14,98	1538	26,5%	638	98,3%
Carte de crédit (dump)	4	3,3%	$31,50	$168,00	$115,50	187	3,2%	60	96,7%
Identité synthétique	4	3,3%	$157,50	$525,00	$249,38	101	1,7%	44	97,7%
Compte compagnie	19	15,7%	$8,40	$81,90	$27,47	125	2,2%	60	88,3%
Compte bancaire	15	12,4%	$26,25	$525,00	$210,35	99	1,7%	51	98,0%
Total	**121**	**100,0%**	**$240,45**	**$1 494,15**	**$706,84**	**5803**	**100,0%**	**2610**	**96,3%**

Tableau 1- Portrait des produits frauduleux en vente sur le marché We The North selon leur type

Un total de 121 produits frauduleux a été retenu pour cette étude. Le type de produit frauduleux qui se retrouve le plus en vente sur le marché est les identités volées (25,6%). Cependant, les clients achètent en plus grande proportion des cartes de crédit (CVV) (36,7%), suivi des dossiers de crédit (28,0%) et des identités volées (26,5%). Bien que les comptes de compagnie et les comptes bancaires ont des fréquences respectives de 15,7% et 12,4%, ces produits représentent plus ou moins 2% des ventes sur le marché. Concernant les prix de vente, les identités synthétiques se vendent le plus cher avec une moyenne de prix de 249,38$. L'article le moins cher en moyenne est les identités régulières. Pour tous les types de produits, la grande majorité des acheteurs ayant laissé une rétroaction se disent satisfaits de leur achat. Le score de satisfaction global pour les produits frauduleux sur le marché est de 96,3%.

Le tableau 2 présente les sept vendeurs les plus importants du marché selon leur nombre de ventes depuis leur entrée sur le marché jusqu'en janvier 2023.

Nom du vendeur	Nombre de produits en vente	Nombre de ventes	Nombre de ventes par unité	Niveau du vendeur	Revenu estimé	Vendeur sur le marché depuis
Vendeur 3	20	1662	83,1	10	±50 000$	2021-07-03
Vendeur 2	10	1536	153,6	10	±50 000$	2021-08-23
Vendeur 1	9	1472	163,6	10	±50 000$	2021-09-24
Vendeur 9	8	147	18,4	9	±45 000$	2021-07-08
Vendeur 4	2	309	154,5	3	±15 000$	2021-12-29
Vendeur 6	1	56	56,0	4	±20 000$	2021-07-12
Vendeur 7	1	49	49,0	5	±25 000$	2021-07-05

Tableau 2- Top 7 des vendeurs du marché We The North selon leur nombre de ventes

Sur un total de 33 vendeurs identifiés lors de la collecte de données et ayant effectué au moins une vente de produit de la fraude, ceux ayant vendu le plus de produits frauduleux depuis leur arrivée sur le marché sont Vendeur 3, Vendeur 2 et Vendeur 1. Ces trois vendeurs ont également atteint le niveau de vendeur maximal sur le marché. Les administrateurs du marché mentionnent que le niveau du vendeur monte de 1 échelon à chaque tranche de 5000$ de ventes, jusqu'à atteindre un maximum de 10. Les trois vendeurs les plus importants ont atteint le niveau maximal, donc cela signifierait qu'ils ont obtenu des gains d'au moins 50 000$ en vendant des produits sur We The North. Les vendeurs qui ont effectué le plus de ventes par unité, soit le nombre de ventes moyen par produit, sont Vendeur 1 (163,6), Vendeur 4 (154,5) et Vendeur 2 (153,6). Tous les vendeurs sont sur le marché depuis soit le milieu de l'été 2021 ou vers la fin de l'été 2021, à l'exception de Vendeur 4 qui a débuté ses activités en décembre 2021.

Les discussions entre fraudeurs

Tel qu'expliqué dans la méthodologie, l'ensemble du forum comprend plusieurs sections portant entre autres sur différents types de produits illicites en vente sur le marché. Afin de répondre à la question de recherche, seulement les messages des deux sections portant sur la fraude ont été examinés. Les caractéristiques des participants du forum, ainsi que les différents thèmes soulevés lors de la collecte de données seront abordés dans les paragraphes suivants.

Les participants du forum

La plupart des messages dans les fils de discussions sur la fraude proviennent d'individus ayant un compte client et la majorité des discussions se déroulent en anglais. Quelques messages en français sont présents. Les fraudeurs semblent assez actifs sur le forum, car de nouveaux messages sont publiés régulièrement dans les fils de discussions.

De plus, par l'observation des échanges, il semble que la majorité des utilisateurs soient des hommes. En effet, les pronoms utilisés sont presque en totalité masculins et les usagers s'adressent entre eux avec des termes qui sont généralement attribuables au genre masculin tels que « bro », « guy » et « man ». Les pseudonymes des participants peuvent également laisser des indices sur le genre de l'individu ou encore sur la province où il habite.

Les thèmes des échanges

L'observation des échanges sur le forum a permis de recenser les principaux thèmes, provenant des discussions entre fraudeurs sur We The North, soit la publicité, la recherche de produits, les avis sur les vendeurs, le partage de conseils, la recherche de services, la qualité des produits et le fonctionnement du marché. Ces thèmes ont été identifiés lors de collecte de données à partir des discussions examinées dans les deux sections de discussion nommées « Fraud ». Ils ont été définis dans le tableau 3 présent en annexe et ils seront présentés ici.

La publicité faite par les utilisateurs

Un thème fréquent sur le forum est celui des publicités faites par les utilisateurs. On observe donc des fils de discussions où des individus publient des messages pour annoncer qu'ils ont un produit spécifique en vente et invitent les clients à les contacter s'ils sont intéressés. Les publicités couvrent une variété de produits frauduleux correspondant aux six sous-thèmes présentés dans le tableau 3. Deux discussions parmi les messages examinés ont été classées dans le sous-thème nommé « produit gratuit ». On observe donc qu'un utilisateur du marché a donné les informations d'une carte de crédit volée sur le forum, mais un autre usager lui a répondu en mentionnant que la carte était déjà brûlée. La deuxième discussion sur ce thème constitue un vendeur du marché disant offrir cinq identités volées gratuitement à la première personne qui laisse un commentaire sous son message et qui possède une clé PGP sur son profil.

Bien que certaines de ces publicités proviennent de personnes ayant un compte vendeur sur la plateforme, la majorité des annonces sont faites par des utilisateurs qui ont un compte client. Plusieurs d'entre eux vont d'ailleurs inviter les clients à les rejoindre sur des plateformes de messagerie tierces telles que Telegram, Jabber, ICQ et Wickr. C'est le cas par exemple d'un utilisateur qui faisait une publicité pour des cartes de crédit (CVV) à un coût de 35$ et demandant aux intéressés de le contacter sur Telegram. Les individus demandant aux clients de les rejoindre sur une plateforme tierce n'ont généralement pas de compte vendeur et la majorité d'entre eux ont été bannis du marché par les administrateurs pour non-respect des règles.

La recherche de produits

Plusieurs clients vont avoir recours au forum lorsqu'ils recherchent un produit en particulier. Un total de six types de produits frauduleux étaient recherchés par les clients du marché lors des discussions. Ces types ont été identifiés et classés en sous-thèmes, soit les identités, les comptes bancaires, les comptes de paiement en ligne, les comptes de compagnie et les cartes de crédit (CVV et dumps). Dans la catégorie des comptes de paiement en ligne, un client va par exemple demander si une personne vend les identifiants pour un compte Authorize.net, qui est une compagnie fournissant des passerelles de paiement, tandis qu'un autre cherche à acheter un compte Coinbase, permettant le transfert de cryptomonnaies. Concernant les dumps, une seule personne dit en chercher parmi les messages du forum examinés. Quant aux autres types de produits frauduleux, des dizaines de clients ont créé des fils de discussions à la recherche de ces types de produit. En général, des individus n'ayant pas de compte vendeur sur le marché vont répondre aux messages des clients disant avoir les articles recherchés. Les vendeurs les plus importants du marché, qui ont été identifiés dans le tableau 2, vont rarement commenter dans les forums de discussion. Vendeur 2 a par exemple répondu dans un fil de discussion une seule fois à un client qui recherchait l'accès à un compte Bell pour l'informer qu'il vend des comptes Fido et Rogers incluant la date de naissance et le numéro d'assurance sociale du propriétaire du compte.

Les avis sur les vendeurs et leurs services

Ce thème est le plus fréquent sur le forum. De nombreux clients vont donner leur avis, qu'il soit positif ou négatif, sur les vendeurs du marché et sur leur satisfaction quant aux produits achetés et au déroulement de la transaction. Plusieurs avis laissés par les utilisateurs sont négatifs. Un utilisateur a par exemple partagé sa mauvaise expérience avec Vendeur 1 en expliquant que parmi les cinq cartes de crédit qu'il a achetées, seulement deux d'entre elles étaient encore actives. Un autre client de Vendeur 1 a répondu au fil de discussion disant que les cartes qu'il a reçues étaient bien actives, mais que leur montant était très faible et qu'elles ne lui serviront donc pas. Un seul client a laissé un message plutôt positif disant que sur cinq cartes de crédit achetées, trois d'entre elles lui ont permis d'en tirer profit. Des messages positifs sont donc présents dans les discussions, mais les fraudeurs semblent davantage utiliser le forum pour se plaindre des vendeurs.

Certains utilisateurs vont également avoir recours au forum pour demander l'avis des autres acheteurs avant de faire un achat avec le vendeur en question. Un utilisateur a par exemple créé un fil de discussion demandant à quoi il doit s'attendre de Vendeur 9, Vendeur 2et Vendeur 1.

Plusieurs individus ont répondu au message initial pour partager leur expérience avec ces vendeurs. Les vendeurs visés par les avis ne répondent généralement pas aux critiques positives ou négatives à leur égard sur le forum. Ceux qui le font sont généralement des plus petits vendeurs, ne faisant pas partie des vendeurs du tableau 2. Par exemple, Vendeur 26 répond très souvent sur le forum lorsque son nom est mentionné par des clients, ce qui peut mener à des discussions agitées. En effet, Vendeur 26 a d'ailleurs à plusieurs reprises eu des conflits avec le même client qui était insatisfait de ses services. On observe que ces derniers vont s'insulter sur le forum et tenter de se discréditer l'un et l'autre. Le client en question a cependant été banni du forum après un certain temps et aurait créé, selon ce que Vendeur 26 affirme, un nouveau compte sous un autre nom. Les échanges ne se font donc pas toujours dans le respect et dans la politesse. On observe que les administrateurs semblent bannir les utilisateurs lorsqu'ils ne respectent pas les règles de la plateforme, afin de tenter de maintenir l'ordre. En effet, lors d'un échange entre un administrateur et un client du forum se plaignant d'avoir été arnaqué par un vendeur, l'administrateur répond en indiquant avoir banni l'arnaqueur en question pour ne pas avoir suivi les règles du marché.

Le sous-thème de la confiance envers les vendeurs regroupe les conversations quant à la fiabilité d'un vendeur. Par exemple, un client affirme qu'un vendeur, n'ayant pas de compte vendeur sur la plateforme, serait en fait un policier infiltré, car le vendeur aurait insisté plusieurs fois pour rencontrer le client en personne. Deux autres vendeurs sont également suspectés d'être des policiers et seulement l'un d'entre eux a un compte vendeur sur le marché. Le sous-thème nommé « Recherche de vendeurs » couvre les discussions où un individu cherche un vendeur qui était connu pour la vente de produits frauduleux sur d'autres marchés illicites. Plusieurs clients font d'ailleurs référence au marché Canadian Headquarters qui est maintenant fermé. Un client dit par exemple rechercher deux vendeurs, introuvables sur We The North, qui étaient supposément des références en matière d'identités volées.

Le partage de conseils et de méthodes

Ce thème comprend quelques discussions où des utilisateurs vont prodiguer des conseils généraux pour réussir à faire de la fraude ou des méthodes précises sur un type de produits frauduleux. Parfois, les utilisateurs vont créer des fils de discussions pour prodiguer des conseils sans qu'une autre personne l'ait demandé, mais la plupart du temps les méthodes seront partagées lorsqu'un utilisateur ayant moins d'expérience le demande. Par exemple, un individu disant être nouvellement père demande de l'aide pour faire de l'argent ou obtenir des produits tels que de la nourriture grâce à la fraude. Un utilisateur lui répond et lui explique une méthode pour se faire livrer de la nourriture avec l'application SkipTheDishes en utilisant une carte de crédit volée. Certaines personnes vont prodiguer des conseils généraux tels que de toujours utiliser le système Escrow, comme recommandé par les

administrateurs du marché et de ne jamais rencontrer un individu dans un lieu physique. Plusieurs discussions proviennent d'individus demandant de l'aide pour obtenir de l'argent à partir de cartes de crédit volées. Un autre exemple est une personne qui dit avoir acheté différents produits frauduleux, notamment des identités et des cartes de crédit, mais qui n'arrive pas à faire de profits. Un fraudeur lui répond en expliquant que pour obtenir des identités, il est possible de le faire en ayant recours à des techniques d'ingénierie sociale et en parcourant des profils sur les réseaux sociaux tels que Facebook.

La recherche de partenaires et de services

Comme il a été vu, certains utilisateurs ont recours au forum lorsqu'ils recherchent des produits frauduleux, mais certaines personnes vont plutôt rechercher des partenaires ou des individus offrant leurs services pour réaliser certaines tâches. Quelques individus disent rechercher une personne travaillant dans une grosse compagnie ou une institution financière qui pourrait servir d'intermédiaire pour réaliser des activités frauduleuses. Un des messages promet une rémunération jusqu'à cinq fois le salaire de l'employé. De plus, certains fraudeurs disent rechercher des pirates informatiques ou des individus ayant des compétences avec l'exploitation de logiciels. On observe donc que les fraudeurs qui n'ont pas nécessairement les compétences et les connaissances nécessaires pour réaliser une tâche vont avoir recours aux services de leurs pairs ayant davantage d'expérience dans le domaine.

Pour d'autres fraudeurs, ce n'est pas par manque de connaissances techniques, mais par manque de temps qu'ils vont vouloir faire équipe avec une autre personne. En effet, un fraudeur qui dit être familier avec les méthodes pour encaisser des cartes de crédit demande à faire affaire avec un partenaire, car il possède un grand nombre de cartes volées et il manque de temps pour les encaisser. Les partenaires les plus en demande semblent être les individus pouvant transférer des fonds dans des comptes bancaires volés, ainsi que ceux pouvant encaisser des cartes de crédit. Dans les messages, certaines personnes précisent la rémunération pour le partenaire, mais celle-ci varie d'une tâche à l'autre et d'une personne à l'autre. Par exemple, un fraudeur dit avoir besoin d'un partenaire pouvant charger un compte PayPal et que les gains seront séparés également (50/50). Une autre personne recherchant également quelqu'un pouvant charger des comptes PayPal dit donner 35% des gains au partenaire. Généralement, les fils de discussions sous ce thème contiennent plusieurs réponses d'individus prêts à collaborer et offrant leurs services.

La qualité des produits au Canada

Ce thème comprend une petite partie des discussions du forum en lien avec la qualité des produits frauduleux spécifiquement au Canada. Quelques utilisateurs abordent le sujet de la vente de cartes de crédit volées (CVV et dumps) au Canada. Concernant les dumps, un fraudeur dit qu'il est très difficile de trouver des cartes de crédit de type dumps en vente. Deux autres utilisateurs ajoutent que ce type de produit frauduleux ne fonctionne pas au Canada. Certains affirment que les cartes de crédit dumps en vente sont généralement brûlées, car elles sont faciles à encaisser, alors lorsqu'une personne va en avoir une, il est plus avantageux pour elle d'encaisser l'argent que de la vendre à un tiers. Cependant, certaines personnes sont d'avis contraire concernant ce type de produit. Un vendeur répond disant que les dumps de bonne qualité existent encore au pays, mais qu'il faut seulement avoir une bonne source. L'individu mentionne en vendre sur le marché. Les utilisateurs semblent d'avis qu'il est difficile de fabriquer ce type de carte de crédit et que ça prend énormément de temps et de pratique pour être capable de les faire. Cela expliquerait pourquoi il est difficile d'en trouver au Canada et que seulement 3,3% de dumps sont en vente sur le marché tel que vu dans le tableau 1.

Concernant les cartes de crédit de type CVV, plusieurs usagers avisent les autres de ne pas les acheter, car elles risquent d'être brûlées ou d'avoir très peu d'argent dessus. Comme pour les dumps, les utilisateurs expliquent qu'une personne en possession d'une carte de crédit de qualité va encaisser l'argent elle-même plutôt que de vendre le produit. Certains rétorquent que les vendeurs de ces cartes préfèrent les vendre plutôt que de les encaisser, afin d'éviter les risques de se faire arrêter par les forces de l'ordre. Cependant, un utilisateur explique qu'il est plus risqué de vendre à des inconnus sur un marché et que la façon la plus sécuritaire est d'encaisser l'argent par le biais de mules de confiance.

Du côté des identités volées, des utilisateurs mentionnent que plusieurs d'entre elles ont déjà fait l'objet d'une fuite et qu'elles sont brûlées. Certains acheteurs et vendeurs précisent ne pas vouloir acheter ou vendre les identités provenant des données de Desjardins pour cette raison. Certains utilisateurs se plaignent également du prix trop élevé de ce type de produit en vente sur We The North. Un fraudeur explique que les identités vendues sur le marché sont de bonne qualité, mais qu'il faut être prêt à payer le prix.

Le fonctionnement du marché

Ce dernier thème porte sur la méconnaissance des utilisateurs quant au fonctionnement du marché. On observe que certains usagers de We The North ont des questionnements par rapport au système Escrow et comment le remboursement fonctionne.

Un client dit par exemple avoir fait une commande pour une carte de crédit, mais qu'il n'a rien reçu. Il demande alors comment fonctionne la procédure avec Escrow pour annuler la commande et obtenir un remboursement. On observe que les administrateurs laissent des messages de temps en temps rappelant aux utilisateurs de toujours effectuer les transactions sur la plateforme par le système Escrow pour éviter les problèmes. Dans le cas où Escrow ne pourrait pas régler le problème, les clients ont la possibilité de lancer une réclamation contre le vendeur. Les administrateurs analyseront par la suite la problématique et décideront si la réclamation est acceptée ou non. Dans le cas où elle serait acceptée, le vendeur devra rembourser le client sous peine d'être banni du marché et de voir sa réputation être entachée. Le nombre de contestations contre un vendeur est accessible à tous sur son profil. Les utilisateurs de la plateforme ont également la possibilité d'ouvrir un « ticket », afin de parler avec les administrateurs en cas de besoin.

Le deuxième sous-thème concerne toutes les discussions qui touchent au faux site de We The North. En effet, il semble qu'un lien « .onion », très similaire à celui pour accéder au vrai site, mènerait vers un site d'hameçonnage tentant de répliquer celui de We The North. Quelques utilisateurs disent avoir tenté de déposer de la cryptomonnaie sur leur compte afin de pouvoir acheter des produits, mais que le dépôt n'est jamais apparu sur leur compte. Des utilisateurs ont répondu expliquant qu'ils se sont fait avoir par le site d'hameçonnage. Les administrateurs rappellent encore une fois aux usagers d'être prudents.

Discussion

À la suite de l'analyse des échanges entre fraudeurs sur le marché et le forum de We The North, les résultats obtenus nous permettent de faire certains liens avec la littérature. D'abord, concernant les principaux services et produits frauduleux offerts sur le marché, nous constatons que les produits les plus populaires auprès des clients sont les cartes de crédit (CVV), suivi des dossiers de crédit et des identités volées. Ces résultats concordent avec ceux de l'étude de Holt et Lampke (2010), ainsi que celle de Smirnova et Holt (2017) montrant que la vente de cartes de crédit volées est commune au Canada. Bien que les recherches de Maimon et Fraser (2022) et Smirnova et Holt (2017) abordent la vente de comptes bancaires compromis au Canada, les ventes pour ce produit atteignent seulement le 1,7% sur le marché à l'étude (tableau 1). Le sujet des comptes bancaires est pourtant assez fréquent dans les discussions sur le forum. Plusieurs utilisateurs disent rechercher ce type de produit et des individus n'ayant pas de compte vendeur sur le marché disent en avoir en vente. Il est donc possible que la vente de comptes bancaires se fasse principalement à l'extérieur du marché. De plus, il semble être plus complexe pour les fraudeurs d'encaisser l'argent provenant d'un compte bancaire que d'une carte de crédit, car les cartes de crédit sont facilement et rapidement utilisables par les fraudeurs contrairement aux comptes bancaires. Cela pourrait donc également expliquer les ventes faibles pour les comptes bancaires.

Concernant les prix, chaque vendeur décide de ceux-ci et des stratégies de vente qu'il utilise. Certains vendeurs offrent des échantillons gratuits, afin d'attirer les clients, tandis que d'autres offrent des rabais tels que des 2 pour 1. Les prix varient d'un type de produit à l'autre et selon divers facteurs. On observe que les dossiers de crédit ayant des cotes de crédit plus hautes se vendent à un prix plus élevé. Par exemple, Vendeur 3 offre un dossier de crédit ayant un score de plus de 800 à un prix de 52,50$, tandis que pour un dossier ayant un score minimal de 700, le prix est de 26,25$. Les cartes de crédit ayant des balances plus hautes se vendent également plus cher. L'étude de Vargas (2019) mentionne que la balance de la carte constitue le facteur le plus important dans la détermination du prix de vente. De plus, les produits frauduleux d'un même type n'ont pas nécessairement toutes les mêmes caractéristiques. C'est-à-dire que pour la vente d'une identité volée par exemple, certains vendeurs vont inclure, en plus des informations de base telles que le nom, la date de naissance, le numéro d'assurance sociale, et l'adresse, des informations supplémentaires telles que le permis de conduire de la victime. Généralement, les vendeurs précisent dans l'annonce que le permis de conduire est fourni sur demande. Certains disent plutôt charger un montant supplémentaire, généralement de 5$, au client qui veut l'obtenir. Les identités ou les dossiers de crédit de femmes se vendent moins chers que ceux des

des hommes. Cela pourrait s'expliquer par le fait que la majorité des fraudeurs sont des hommes (Gekoski, Adler et McSweeney, 2022), alors ils auraient besoin d'usurper l'identité d'un homme.

Par ailleurs, les études montrent que les rétroactions constituent l'un des facteurs les plus importants pour déterminer la confiance envers un vendeur (Barratt et Aldridge 2016; Laferrière et Décary-Hétu, 2022; Tzanetakis et al. 2016). We The North a mis en place, sur son marché, un système permettant de donner des avis aux vendeurs après avoir acheté un produit. Il est possible de laisser un avis positif ou négatif et de l'accompagner d'un commentaire. Le nombre d'avis et les commentaires sont accessibles à tous sur le marché, ce qui est un indicateur de la qualité des produits du vendeur et de la confiance que les clients peuvent avoir envers ce dernier. Les systèmes de rétroaction sur les marchés clandestins permettent de faciliter le développement de la confiance des vendeurs (Laferrière et Décary-Hétu, 2022). Certains vendeurs utilisent des tactiques pour maximiser leurs rétroactions positives et ainsi gagner en confiance. Certains mentionnent offrir un cadeau, souvent un produit gratuit, aux clients laissant des avis positifs sur leurs produits. Le nombre de réclamations semble également être un indicateur de la confiance envers un vendeur et peut venir entacher sa réputation. Certains vendeurs demandent aux clients dans leur description de ne pas entamer une réclamation et de plutôt régler le problème par message privé, sous peine de ne plus pouvoir acheter les produits du vendeur.

De plus, le forum permet aux fraudeurs de discuter à propos de différents sujets en lien avec la fraude. Il a été observé que les utilisateurs vont écrire dans les fils de discussion entre autres pour donner leurs avis sur les vendeurs et sur les produits frauduleux qu'ils offrent. Ces avis partagés dans les discussions sont généralement négatifs. Cependant, comme indiqué dans le tableau 1, 96,3% des acheteurs de produits frauduleux sur le marché se disent satisfaits selon les rétroactions laissées. Cette différence entre les avis laissés sur le forum et sur la plateforme marchande pourrait s'expliquer par divers facteurs. Certains vendeurs peuvent par exemple publier de fausses rétroactions ayant pour but d'améliorer leur réputation sur le marché ou encore de nuire à un vendeur de compétition (Markopoulos, Xefteris et Dellarocas 2020). Les règles de We The North précisent d'ailleurs que cette pratique est interdite sur la plateforme. L'offre de cadeaux aux utilisateurs laissant une rétroaction positive pourrait également exercer une influence sur le nombre de rétroactions positives sur le marché. Il est aussi possible que les acheteurs satisfaits soient moins enclins à partager leur avis dans les forums que ceux ayant vécu une mauvaise expérience avec un vendeur.

Bien que la littérature mentionne que les vendeurs participant le plus aux discussions sur les forums et étant les plus actifs ont plus de chances d'être vus comme des vendeurs de

confiance (Décary-Hétu et Leppänen, 2016; Holt et al., 2016; Yip et al., 2013), les vendeurs les plus populaires de We The North, ne semblent pas être très actifs sur le forum, et ce, même quand leur nom est mentionné. Ce sont plutôt des individus n'ayant pas de compte vendeur qui vont participer aux discussions et faire des publicités pour leurs produits. Il est cependant possible que les vendeurs du marché communiquent plutôt par message privé ou dans des groupes de fraudeurs sur des plateformes tierces, afin de construire leur réseau (Décary-Hétu et Leppänen, 2016). Considérant les frais de 300$ à payer pour obtenir un compte vendeur, cela peut expliquer pourquoi la majorité des utilisateurs préfèrent vendre hors plateforme. Cependant, comme plusieurs clients le disent dans les discussions du forum, les individus n'ayant pas de compte vendeur sont moins crédibles et il y a davantage de risques de se faire arnaquer par eux, car il y a moins de protection pour les acheteurs. En effet, puisque les ventes se feraient hors marché, il n'y a pas de moyens pour les clients de faire une réclamation en cas d'arnaque, comme il est possible de le faire sur We The North. Les vendeurs se faisant suspecter d'être des policiers peuvent également voir leur réputation être entachée. De plus, une manière efficace d'obtenir la confiance des clients est de mentionner avoir des années d'expérience dans le domaine (Jung et al. 2022). On observe que certains vendeurs mentionnent dans les forums de discussions avoir plusieurs années d'expérience en fraude et avoir vendu de nombreux produits sur Canadian Headquarters ou encore Alphabay. Cependant, Jung et al. (2022) mentionnent aussi que c'est une façon de faire croire aux clients que le vendeur est de confiance, mais qu'il s'agit en réalité d'un arnaqueur.

D'autre part, tel que mentionné par The Recorded Future (2021), on constate que plusieurs utilisateurs du forum semblent provenir du marché The Canadien Headquarters qui a été fermé en 2021. En effet, à quelques reprises, sur le forum, on observe des discussions où des individus évoquent The Canadien Headquarters disant avoir fait affaire sur ce marché dans le passé ou recherchant d'anciens vendeurs. Certains se questionnent même sur la fermeture du marché. Vendeur 2 a notamment partagé le communiqué du CRTC annonçant les peines de quatre vendeurs de The Canadien Headquarters qui ont été arrêtés lors de l'opération (Conseil de la radiodiffusion et des télécommunications canadiennes, 2022). Quelques fraudeurs ont répondu au fil de discussion mentionnant leur tristesse concernant la fermeture du marché et l'arrestation de leurs collègues. On constate donc que malgré l'enquête du CRTC et l'arrestation de leurs pairs, les fraudeurs continuent tout de même leurs activités criminelles sur We The North. Cela concorde avec la littérature mentionnant que les opérations visant la fermeture des marchés clandestins entraînent des déplacements vers des marchés secondaires (Gañán et al., 2020; Soska et Christin, 2015).

Les échanges sur le forum de fraude permettent donc aux utilisateurs de partager leurs opinions envers les vendeurs et leurs produits, d'échanger des conseils sur la fraude, de

faire de la publicité pour des produits frauduleux ou encore de rechercher un produit en particulier. Chikada et Gupta (2017) mentionnent que l'accès aux discussions des forums sur le Dark Web peut être difficile et nécessiter d'avoir une invitation, mais sur We The North cela ne semble pas être le cas, car il a été possible d'accéder au forum sans invitation, seulement en se créant un compte sur la plateforme.

Le forum permet aux cybercriminels de s'entraider et semble fonctionner de la même façon que les autres forums étudiés dans la littérature (Broseus et al., 2016; Holt et al., 2016; Yip et al., 2013). Cet aspect d'entraide est surtout mis en lumière dans les discussions où des individus demandent de l'aide sur des méthodes pour frauder et dans les discussions où des fraudeurs recherchent des partenaires ou des personnes offrant certains services. Ces fils de discussions reçoivent généralement plusieurs réponses de fraudeurs prêts à offrir leur aide. On observe donc que malgré certains conflits lors des discussions entre fraudeurs, ceux-ci semblent tout de même vouloir collaborer et s'entraider. Tel que Wilson (2019) le mentionne, les forums de discussions permettent aux cybercriminels de partager leurs connaissances et d'avoir recours aux services d'individus plus expérimentés, ce qui permet aux fraudeurs d'être plus efficaces dans leurs activités criminelles. Le terme « Crime as a service » (CaaS) est une expression du lexique de la cybercriminalité qui fait référence à cet échange de services entre les cybercriminels (Manky, 2013). Cette pratique est observée dans les fils de discussion du forum, alors que des fraudeurs disent rechercher notamment les services de pirates informatiques et d'ingénieurs ou de développeurs logiciels.

Bref, nous constatons que la plateforme marchande de We The North permet aux fraudeurs de vendre des produits frauduleux de tous types. Certains produits demeurent cependant plus populaires auprès de la clientèle. De plus, les prix varient selon les caractéristiques de l'article et on constate que les vendeurs peuvent utiliser diverses stratégies pour augmenter leurs ventes. L'espace de discussion qui aborde différentes thématiques liées à la fraude permet aux fraudeurs d'interagir entre eux, de partager leurs expériences et de s'entraider. Le forum et le système de rétroaction permettent aux acheteurs de donner leurs avis sur les vendeurs et les produits du marché. Ce partage de rétroactions peut avoir une influence sur la réputation des vendeurs, et ainsi sur leur nombre de ventes et leur revenu. Il a également été observé que plusieurs utilisateurs du forum semblent provenir d'anciens marchés illicites, notamment The Canadien Headquarters et Alphabay.

Limites de l'étude

Certaines limites relatives à cette étude portant sur un marché clandestin du Dark Web doivent toutefois être considérées. D'abord, la portée des résultats est limitée, car cette recherche se concentre seulement sur le marché canadien We The North. Ce marché n'est donc pas nécessairement représentatif de tous les marchés illicites canadiens et de l'étendue réelle de l'offre de services frauduleux sur le Dark Web. En effet, sachant que les prix de la marchandise frauduleuse varient d'un marché à l'autre et d'un pays à l'autre (Steel, 2019; Vargas, 2019), les données recueillies sur les produits n'auront pas nécessairement la même prévalence dans un autre marché. De plus, les marchés et les vendeurs individuels sur les plateformes clandestines sont relativement temporaires et transitoires, car lorsqu'un marché prend de l'ampleur et gagne en popularité, il devient une cible pour les forces de l'ordre et il risque de fermer (Soska et Christin, 2015; Steel, 2019). Cela dit, des éléments comme la réputation du vendeur sont limités dans le temps (Steel, 2019). Enfin, les échanges observés quant aux discussions sur les forums et aux produits vendus correspondent seulement à ceux qui sont accessibles à la communauté, en ayant un compte sur la plateforme du marché. Cependant, il a été observé que certains échanges se font sur des plateformes tierces ou par messagerie privée sur We The North, ce qui signifie que ces données ne sont pas accessibles pour la recherche. Les résultats obtenus pourraient être légèrement différents en tenant compte de ces données non accessibles.

Conclusion

Pour conclure, la recherche portait sur les échanges entre fraudeurs sur le marché We The North. L'objectif était de faire un portrait des principaux services et produits frauduleux en vente sur le marché, ainsi que d'observer la nature des échanges entre les fraudeurs sur le forum. Les principaux résultats montrent que les types de produits frauduleux les plus fréquents sur la plateforme sont les cartes de crédit (CVV), les dossiers de crédit et les identités volées. On constate également que les prix des produits en vente varient selon le type de produit et les caractéristiques de l'article. De plus, par les rétroactions, les acheteurs du marché se disent en grande partie satisfaits des produits frauduleux achetés et les vendeurs arrivent à obtenir des gains pouvant dépasser les 50 000$ grâce à diverses stratégies de vente. L'analyse du forum montre que les fraudeurs utilisent les fils de discussion entre autres pour partager leur avis sur les vendeurs et leurs produits, pour faire de la publicité, pour rechercher des services et articles, ainsi que pour s'entraider en s'échangeant des conseils et des techniques de fraude.

La recherche a donc permis d'en apprendre davantage sur l'offre de produits frauduleux au Canada, et plus précisément sur le fonctionnement du marché illicite We The North. Elle a également permis de mettre en lumière l'utilisation des marchés clandestins par les fraudeurs, ainsi que les tactiques qu'ils utilisent pour réaliser leurs activités criminelles. Il a donc été possible d'apporter davantage de connaissances sur un sujet peu documenté dans la littérature. D'autres études sont cependant nécessaires afin d'avoir une meilleure compréhension du phénomène de la fraude et des marchés clandestins de produits frauduleux au Canada. Il serait par exemple intéressant de réaliser des entrevues ou des sondages auprès des utilisateurs du marché pour avoir leur perception sur les échanges de produits frauduleux et sur le fonctionnement du marché.

Annexe

Tableau 3 : Grille thématique des forums de discussion en lien avec la fraude sur We The North

Thèmes	Description
Publicité faite par un utilisateur	Individu faisant la promotion de ses services et produits disponibles pour les acheteurs
Identité (fullz)	Informations personnelles complètes sur une personne, permettant de voler son identité (Smirnova et Holt, 2017)
Carte de crédit (CVV)	Informations d'une carte de crédit permettant de faire des transactions en ligne (Bulakh et Gupta, 2015)
Carte de crédit (dump)	Copie digitale d'une carte de crédit permettant de cloner la piste magnétique et de créer une carte physique (Bulakh et Gupta, 2015)
Compte de compagnie	Identifiants permettant de se connecter à un compte sur le site d'une entreprise et sur lequel une carte de crédit y est généralement affiliée
Compte bancaire	Informations bancaires volées permettant d'accéder au compte déjà existant
Produit gratuit	Utilisateur du marché offrant un produit frauduleux gratuit sur le forum

Recherche de produits	Acheteur recherchant un certain type de produit frauduleux sur le marché
Identité (fullz)	Informations personnelles complètes sur une personne, permettant de voler son identité (Smirnova et Holt, 2017)
Compte bancaire	Informations bancaires volées permettant d'accéder au compte déjà existant
Compte de paiement en ligne	Informations permettant de se connecter à un compte servant au transfert d'argent en ligne
Compte de compagnie	Identifiants permettant de se connecter à un compte sur le site d'une entreprise et sur lequel une carte de crédit y est généralement affiliée
Carte de crédit (CVV)	Informations d'une carte de crédit permettant de faire des transactions en ligne (Bulakh et Gupta, 2015)
Carte de crédit (dump)	Copie digitale d'une carte de crédit permettant de cloner la piste magnétique et de créer une carte physique (Bulakh et Gupta, 2015)
Avis sur les vendeurs et leurs services	Opinions sur le déroulement des transactions et sur les services et produits offerts par les vendeurs du marché
Avis positif sur une transaction	Avis montrant une satisfaction quant à une transaction marchande avec un vendeur
Avis négatif sur une transaction	Avis montrant une insatisfaction quant à une transaction marchande avec un vendeur

Confiance envers les vendeurs	Confiance que les utilisateurs du marché ont envers les vendeurs quant à leur fiabilité
Recherche de vendeurs	Questionnement sur la présence d'un vendeur, sur le marché We The North, qui était connu sur d'autres marchés
Partage de conseils et de méthodes	Partage de conseils et d'astuces sur les techniques de fraude entre les utilisateurs du forum
Carte de crédit (CVV)	Informations d'une carte de crédit permettant de faire des transactions en ligne (Bulakh et Gupta, 2015)
Compte de paiement en ligne	Informations permettant de se connecter à un compte servant au transfert d'argent en ligne
Compte bancaire	Informations bancaires volées permettant d'accéder au compte déjà existant
Carte de crédit (dump)	Copie digitale d'une carte de crédit permettant de cloner la piste magnétique et de créer une carte physique (Bulakh et Gupta, 2015)
Identité (fullz)	Informations personnelles complètes sur une personne, permettant de voler son identité (Smirnova et Holt, 2017)
Général	Conseils généraux pour sur l'utilisation du marché pour réussir à faire de la fraude sans préciser un type de produit frauduleux en particulier

Recherche de partenaire et de services	Utilisateur du marché voulant faire équipe avec un autre utilisateur pour faire de la fraude
Carding	Utilisation illégale des informations d'une carte de crédit (Peretti, 2018)
Compte bancaire	Informations bancaires volées permettant d'accéder au compte déjà existant
Identité	Informations personnelles complètes sur une personne, permettant de voler son identité (Smirnova et Holt, 2017)
Compte de paiement en ligne	Informations permettant de se connecter à un compte servant au transfert d'argent en ligne
Compte de compagnie	Identifiants permettant de se connecter à un compte sur le site d'une entreprise et sur lequel une carte de crédit y est généralement affiliée
Piratage informatique	Individu ayant les capacités techniques pour accéder aux informations ou aux communications sur un appareil informatique en exploitant les failles dans les systèmes (Serene-Risc, 2019)
Autre	Recherche d'un partenaire pour faire de la fraude n'appartenant pas à un type de produit frauduleux en particulier
Qualité des produits au Canada	Discussions sur l'offre et la qualité des produits frauduleux offerts au Canada
Carte de crédit (dump)	Copie digitale d'une carte de crédit permettant de cloner la piste magnétique et de créer une carte physique (Bulakh et Gupta, 2015)

Carte de crédit (CVV)	Informations d'une carte de crédit permettant de faire des transactions en ligne (Bulakh et Gupta, 2015)
Identité (fullz)	Informations personnelles complètes sur une personne, permettant de voler son identité (Smirnova et Holt, 2017)
Fonctionnement du marché	Méconnaissance sur le fonctionnement du marché
Escrow	Questionnement sur le fonctionnement du système Escrow
Faux site	Acheteur s'étant retrouvé sur un site d'hameçonnage du marché

Références

Agence de la consommation en matière financière du Canada. (2022, mai). 12.1.2 Types de fraudes. Gouvernement du Canada.
https://www.canada.ca/fr/agence-consommation-matiere-financiere/services/vos-outils-financiers/fraude/fraude-1/3.html

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. DOI:10.1007/978-3-642-39498-0_12

Barratt, M. J. et Aldridge, J. 2016. "Everything You Always Wanted to Know about Drug Cryptomarkets* (*but Were Afraid to Ask)." International Journal of Drug Policy 35:1–6. doi: 10.1016/j.drugpo.2016.07.005

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. doi: 10.1109/eCrime54498.2021.9738751

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. https://doi.org/10.1016/j.forsciint.2016.02.045

Bulakh, V. et Gupta, M. (2015). Characterizing Credit Card Black Markets on the Web. In Proceedings of the 24th International Conference on World Wide Web (WWW '15 Companion). Association for Computing Machinery, New York, NY, USA, 1435–1440. https://doi.org/10.1145/2740908.2778846

Bureau de la Concurrence Canada. (2017). L'édition canadienne : Le petit livre noir de la fraude – Votre guide de protection contre la fraude. https://ised-isde.canada.ca/site/bureau-concurrence-canada/sites/default/files/attachments/2022/lbbs-web-2017-fra.pdf

Buxton, J. and Bingham, T. (2015). The Rise and Challenge of Dark Net Drug Markets. Global Drug Policy Observatory. Policy Brief No. 7.
https://www.researchgate.net/publication/270818585_The_Rise_and_Challenge_of_Dark_Net_Drug_Markets_Policy_Brief_7_January_2015

Byrne, J.M., and K.A. Kimball. (2017). Inside the Darknet: Techno-Crime and Criminal Opportunity. In Criminal Justice Technology in the 21st Century, 3rd ed, ed. L.J. Moriarty, 206–232. Illinois: Charles C. Thomas Publisher.

Centre antifraude du Canada. (2021, mai). Vol d'identité et fraude à l'identité. Gouvernement du Canada. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/identity-identite-fra.htm

Centre antifraude du Canada. (2022, juillet). Sensibilisation aux mules. Gouvernement du Canada. https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/awareness-sensibilisation-fra.htm

Centre antifraude du Canada. (2022, novembre). Fraudes récentes - Répercussions de la fraude depuis le début de l'année. Gouvernement du Canada. https://www.antifraudcentre-centreantifraude.ca/index-fra.html

Chikada, A. et Gupta, A. (2017). Online brand protection. In Handbook of Research on Counterfeiting and Illicit Trade. Edward Elgar Publishing.
https://www.elgaronline.com/view/edcoll/9781785366444/9781785366444.00024.xml

Code criminel (2022). Code criminel / Codification bilingue 2021, Carswell, Éditions Yvon Blais.

Conseil de la radiodiffusion et des télécommunications canadiennes. (2022, janvier). Une enquête du CRTC cible des fournisseurs et l'administrateur d'un marché du Web invisible. Gouvernement du Canada. https://www.canada.ca/fr/radiodiffusion-telecommunications/nouvelles/2022/01/une-enquete-du-crtc-cible-des-fournisseurs-et-ladministrateur-dun-marche-du-web-invisible.html

Conteh, N. Y., et Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31. http://dx.doi.org/ 10.19101/IJACR.2016.623006

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. https://ici.radio-canada.ca/recit-numerique/4211/darknet-canadian-headquarters-fraudeurs-crtc-montreal

Cross, C. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. Journal of Criminological Research, Policy and Practice. 5. 10.1108/JCRPP-01-2019-0008.

Cross, C., Dragiewicz, M. et Richards, K. (2018). Understanding romance fraud: insights from domestic violence research. British Journal of Criminology, 58(6), 1303-22.
https://academic.oup.com/bjc/article/58/6/1303/4935144

Cross, C., Richards, K. et Smith, R.G. (2016). The Reporting Experiences and Support Needs of Victims of Online Fraud. Trends and issues in crime and criminal justice, 1.
https://www.semanticscholar.org/paper/The-Reporting-Experiences-and-Support-Needs-of-of-Cross-Richards/b2fc34f7825c7c1153bbedc72ef91b8cfc71933f

Chaire de recherche en prévention de la cybercriminalité. (s. d.). Mission de la Chaire. https://www.prevention-cybercrime.ca/mission-et-objectifs

Décary-Hétu, D. Et Leppänen. A. (2016). "Criminals and Signals: An Assessment of Criminal Performance in the Carding Underworld." Security Journal 29 (3):442–60. doi: 10.1057/sj.2013.39

Equifax (2022). Communiqués de presse Blogues : Qu'est-ce qu'une fraude d'identité synthétique? https://www.consumer.equifax.ca/fr/au-sujet-d-equifax/communiques-de-presse/-/blogs/qu-est-ce-qu-une-fraude-d-identite-synthetique-/

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. doi: 10.1109/eCrime51433.2020.9493263.

Gekoski, A., Adler, R. J et McSweeney, T. (2022). Profiling the Fraudster: Findings from a Rapid Evidence Assessment, Global Crime, 23:4, 422-442, DOI: 10.1080/17440572.2022.2137670

Goldfeder, S., Bonneau, J., Gennaro, R., & Narayanan, A. (2017). Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin. Financial Cryptography. https://www.semanticscholar.org/paper/Escrow-Protocols-for-Cryptocurrencies%3A-How-to-Buy-Goldfeder-Bonneau/d492e70db0d350826e48b67ad5e97c80ad2e05b9

Handalage, U. et Prasanga, T. (2021). Dark Web, Its Impact on the Internet and the Society: A Review. 10.13140/RG.2.2.11964.36484.

Holt T. J. et Lampke E. (2010). Exploring stolen data markets online: products and market forces, Criminal Justice Studies, 23, 33-50. https://doi.org/10.1080/14786011003634415

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. https://www.ojp.gov/library/publications/exploring-and-estimating-revenues-and-profits-participants-stolen-data-markets

Holt, T. J., Smirnova, O. et Hutchings, A. (2016). Examining signals of trust in criminal markets online, Journal of Cybersecurity, 2(2), 137–145. https://doi.org/10.1093/cybsec/tyw007

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. https://vc.bridgew.edu/ijcic/vol5/iss2/2

Koziarski, J. et Lee, J.R. (2020). Connecting evidence-based policing and cybercrime. Policing: An International Journal, 43(1), 198-211. https://doi.org/10.1108/PIJPSM-07-2019-0107

Laferrière, D., et Décary-Hêtu, D. (2022). Examining the Uncharted Dark Web: Trust Signalling on Single Vendor Shops. Deviant Behavior, 44, 37 - 56. DOI:10.1080/01639625.2021.2011479

Lacey, D. et Salmon, P.M. (2015). It's Dark in There: Using Systems Analysis to Investigate Trust and Engagement in Dark Web Forums. In: Harris, D. (eds) Engineering Psychology and Cognitive Ergonomics. EPCE 2015. Lecture Notes in Computer Science(), vol 9174. Springer, Cham. https://doi.org/10.1007/978-3-319-20373-7_12

Levi, M., Doig, A., Gundur, R., Wall, D. et Williams, D. (2015), The Implications of Economic Cybercrime for Policing, City of London Corporation", London, available at: www.cityoflondon.gov.uk/business/economicresearch-and-information/research-publications/Documents/Research-2015/Economic-CybercrimeFullReport.pdf (accessed 31 January 2019)

Lorenzo-Dus, N., et Di Cristofaro, M. (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. Discourse & Communication, 12(6), 608-626.

Lusthaus, J. (2018). Industry of Anonymity: Inside the Business of Cybercrime. Cambridge, MA and London, England: Harvard University Press. https://doi.org/10.4159/9780674989047

Maimon, D. et Fraser, I. (2022). Underground bazaars of stolen bank account credentials : A Case Study Focused on the Montreal Fraud Ecosystem. VIDOCQ Group.

Manky, D. (2013). Cybercrime as a service: A very modern business. Computer Fraud & Security, 2013(6), 9–13. https://doi.org/10.1016/S1361-3723(13)70053-8

Markopoulos, P., Xefteris, D. et Dellarocas, C. N. (2020). Vandalizing Review Mechanisms: Theory, Practice, and Applications. http://dx.doi.org/10.2139/ssrn.3630582

McGuire, M et Dowling, S (2013). Cyber Crime: A Review of the Evidence. Summary of Key Findings and Implications. Home Office Research Report 75. London: Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

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. https://doi.org/10.1057/s41284-018-0150-5

Nardo, M. (2011), Economic crime and illegal markets integration: a platform for analysis, Journal of Financial Crime, 18(1), 47-62. https://doi.org/10.1108/13590791111098799

Peretti, K.K. (2008) Data breaches: What the underground world of 'carding' reveals. Santa Clara Computer & High Tech Law Journal 25 (2): 375-413. https://ipmall.law.unh.edu/sites/default/files/hosted_resources/CyberCrime/v025.i2.Peretti023.pdf

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. https://ssrn.com/abstract=2676615

Serene-Risc (2019). Piratage informatique («hacking»). https://www.serene-risc.ca/fr/menaces/piratage-informatique-hacking

Smirnova, O., et Holt, T. J. (2017). Examining the Geographic Distribution of Victim Nations in Stolen Data Markets. American Behavioral Scientist, 61(11), 1403–1426. https://doi.org/10.1177/0002764217734270

Soldner, F., Kleinberg, B. et Johnson, S. (2022). A Fresh Look at Fraud. (1ère edition). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003017189-9/trends-online-consumer-fraud-felix-soldner-bennett-kleinberg-shane-johnson

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. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf

Steel, C. (2019). Stolen Identity Valuation and Market Evolution on the Dark Web. International Journal of Cyber Criminology. 70-83. 10.5281/zenodo.3539500.

The Recorded Future. (2021, octobre). WeTheNorth: A New Canadian Dark Web Marketplace. https://www.recordedfuture.com/wethenorth-canadian-dark-web

Tzanetakis, M., Gerrit K., Bernd W., et von Laufenberg R. (2016). The Transparency Paradox. Building Trust, Resolving Disputes and Optimising Logistics on Conventional and Online Drugs Markets. Internationl Journal of Drug Policy 35:58–68. DOI: 10.1016/j.drugpo.2015.12.010

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. https://doi.org/10.1145/2915368.2915369

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 https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-van_wegberg.pdf

Vargas,V. (2019). The new economic good: Your own personal data. An integrative analysis of the Dark Web. Proceedings of the International Conference on Business Excellence,13(1) 1216-1226. https://doi.org/10.2478/picbe-2019-0107

Wang, Q., Liu, Z., Bernat, E. M., Vivino, A. A., Liang, Z., Bai, S., Liu, C., Yang, B. et Zhang, Z. (2021). Pretending to Be Better Than They Are? Emotional Manipulation in Imprisoned Fraudsters. Frontiers in Psychology, 12. https://www.frontiersin.org/articles/10.3389/fpsyg.2021.562269

Wilson, E. (2019). Disrupting dark web supply chains to protect precious data. Computer Fraud & Security, 4, 6-9. https://doi.org/10.1016/S1361-3723(19)30039-9.

Yetter, R. B. (2015). Darknets, cybercrime & the onion router: Anonymity & security in cyberspace. ProQuest Dissertations and Theses. 102. https://www.proquest.com/dissertations-theses/darknets-cybercrime-amp-onion-router-anonymity/docview/1677185939/se-2

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. https://doi.org/10.1080/10439463.2013.780227