Criminologie

Cryptomarchés et *carding* : impact sur l'offre et la demande
Cryptomarkets and carding: Influence on supply and demand
Mercados criptográficos y *carding*: Impacto sobre la oferta y la demanda

Mathieu Guillot and David Décary-Hétu

Volume 52, Number 2, Fall 2019

La criminologie de l'information : état des lieux et perspectives

URI: https://id.erudit.org/iderudit/1065856ar
DOI: https://doi.org/10.7202/1065856ar

See table of contents

Publisher(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (print)
1492-1367 (digital)

Explore this journal

Cite this article

Guillot, M. & Décary-Hétu, D. (2019). Cryptomarchés et *carding* : impact sur l'offre et la demande. *Criminologie*, *52*(2), 63–82. https://doi.org/10.7202/1065856ar

Article abstract

The present study describes the market activities of carding in cryptomarkets in a sample of 17,619 products or services related to carding as well as a second sample of the activities of 4,294 sellers. We were interested particularly in whether convergence settings such as cryptomarkets have an effect on the supply and demand of carding products and services. We began by creating a typology of products and services which was then used in a descriptive analyses of market share and price distribution to shed the light on how anonymization affected offers. Descriptive analyses of sellers' activities was then used to look at the impact of sales on the demand for carding products and services. The results suggest that cryptomarkets offer all that carders need to carry out the three steps of the criminal script in carding. We also found that, as with online drug dealers, the formal feedback system made it possible to improve processes that generate confidence in the system.

Cryptomarchés et *carding* : impact sur l'offre et la demande

Mathieu Guillot[1]
Candidat à la maîtrise en criminologie
École de criminologie, Université de Montréal
mathieu.guillot@umontreal.ca

David Décary-Hétu
Professeur agrégé
École de criminologie, Université de Montréal
david.decary-hetu@umontreal.ca

RÉSUMÉ • *Dans le présent article, il est question de décrire les activités marchandes des cardeurs sur les cryptomarchés au moyen d'un échantillon de 17 619 annonces de produits ou de services relatifs au* carding *ainsi que d'un second échantillon recensant les activités de 4 294 vendeurs. Notre démarche s'attache plus précisément à constater si l'avènement des cryptomarchés, comme lieu de convergence pour les cybercriminels, a eu un impact sur l'offre et la demande de tels produits et services. Pour mener à bien cet objectif, une typologie des différents produits et services est réalisée. Dans un premier temps, des analyses descriptives, mettant en lumière les proportions des différents types ainsi que la distribution des prix affichés par les annonces, permettent d'offrir un regard sur l'impact des technologies d'anonymat sur l'offre de produits et services. Dans un second temps, des analyses descriptives des transactions effectuées par les vendeurs sont réalisées pour examiner leur impact sur la demande de produits et services. Les principaux résultats indiquent que les cryptomarchés offrent tout le nécessaire pour commettre les trois étapes du script criminel du* carding. *De plus, il est aussi montré que, comme dans le cas des vendeurs de drogue en ligne, le système d'évaluation formel a permis de transcender et d'améliorer les processus générateurs de confiance.*

MOTS CLÉS • *Carding, cryptomarchés, offre, demande, cybercriminalité.*

1. École de criminologie, Université de Montréal, Pavillon Lionel-Groulx, C.P. 6128, succ. Centre-ville, Montréal (Québec), Canada, H3C 3J7.

Introduction

Depuis le lancement en 2011 de *Silk Road 1* (SR1), une multitude de cryptomarchés ont vu le jour pour profiter de l'aubaine financière que représente le fait de faciliter des transactions illicites entre criminels au travers de sites web marchands conviviaux (Broséus *et al.*, 2016 ; Décary-Hétu et Giommoni, 2017). Mais au-delà de leur architecture facile à appréhender, les cryptomarchés sont surtout plus anonymes que la première génération de lieux virtuels où convergent les délinquants (Dolliver, 2015). En utilisant conjointement le réseau TOR et les cryptomonnaies pour permettre aux criminels d'échanger en ligne, les cryptomarchés assurent un anonymat en ce qui a trait à leurs activités et à leurs transactions (Barratt et Aldridge, 2016). Dans cet article, il sera question de décrire les activités marchandes des cardeurs sur les cryptomarchés. Le *carding* consiste à utiliser des données financières ou bancaires compromises pour acheter des biens ou des services de manière frauduleuse (Peretti, 2009) et tombe sous le joug des lois visant à sanctionner le vol ou la fraude d'identité. Bien que le *carding* ait été étudié sous le prisme de lieux de convergence comme les forums ou les *chats* en ligne, sa transposition vers de nouveaux types de lieux de convergence comme les cryptomarchés reste peu explorée.

Revue de littérature

Le script criminel du carding

Le *carding* est un cybercrime consistant, pour des individus nommés cardeurs, à utiliser, de manière non autorisée, des informations financières pour acheter des biens ou des services (Peretti, 2009). Les informations financières sont des numéros de cartes de crédit, des identifiants de comptes bancaires en ligne ou de services de paiements (ex. : PayPal). Van Hardeveld, Webber et O'Hara (2016) ont développé un script criminel (Cornish, 1994) qui explique les trois étapes qui mènent à une fraude de *carding.*

Dans un premier temps, le cardeur subtilise des informations financières. Pour cela, il pourra utiliser différentes solutions technologiques ou appareils. Les *skimmers* sont des dispositifs électroniques que le cardeur implémente sur un lecteur de cartes (distributeur ou système de paiement) pour y enregistrer les informations de la carte qui y a été insérée (Peretti, 2009). Une autre technique consiste à utiliser un

enregistreur de frappes (ou *keylogger*). Un enregistreur de frappes est un logiciel malveillant qui infecte l'ordinateur d'une victime et enregistre les différentes frappes entrées sur le clavier. Il bénéficie d'un degré de configuration élevé qui permet de sélectionner les sites qui l'activent, de choisir d'effectuer des captures d'écran sur certains sites pour outrepasser des systèmes d'identification plus sécuritaires en utilisant uniquement la souris ou un clavier virtuel, ou encore de conduire l'enregistrement des informations dérobées vers un serveur sécurisé (Holz, Engelberth et Freilling, 2009). Les pages d'hameçonnage (ou *phishing*) sont une solution de rechange aux enregistreurs de frappes. Ces pages sont des copies de sites web d'institutions bancaires qui cherchent à berner les victimes afin qu'elles y entrent leurs identifiants (James, 2005 ; Wall, 2007). Finalement, la dernière technique est l'infection de points de vente. Cette technique conduit, de manière anecdotique, à la compromission du plus grand nombre d'informations financières. Il s'agit de logiciels malveillants qui infectent un terminal de paiement présentant des failles sécuritaires (Bulakh et Gupta, 2015). Ce logiciel extrait les informations financières qui passent par la mémoire vive du terminal (Vasiu et Vasiu, 2015). Étant donné que ces terminaux sont reliés au système central du magasin dont ils dépendent, cette infection peut mener à la compromission d'un nombre très important de données financières (Symantec, 2017). Des cas récents ont montré que des dizaines de millions de données pouvaient être compromises par cette technique (Chakraborty, Lee, Bagchi-Sen, Upadhyaya et Rao, 2016 ; Greene et Stavins, 2016 ; Kashmiri, Nicol et Hsu, 2016). Bien que d'autres types de crimes, comme le vol avec violence ou l'extorsion, puissent mener à la subtilisation de données financières, cette première phase du script du *carding* a la particularité d'être fortement empreinte de composantes technologiques qui nécessitent des compétences particulières et engendrent vraisemblablement de plus grands rendements criminels.

Dans un second temps, les informations financières volées seront mises en vente sur des marchés illicites. Selon la qualité des informations récoltées, ces dernières peuvent prendre trois formes. D'abord, un *dump* contient toutes les données de la bande magnétique d'une carte de crédit et permet de contrefaire la carte pour réaliser des achats hors ligne (Holt et Lampke, 2010 ; Peretti, 2009). Ensuite, les *fullz* contiennent à la fois les informations financières et des informations personnelles de la victime (ex. : son numéro d'assurance sociale, son adresse postale)

(Holt et Lampke, 2010 ; Peretti, 2009). Ils sont utilisés pour faire des achats frauduleux en ligne. Finalement, les *CVV*, qui sont une version plus réduite des *fullz*, ne contiennent que le nom de la victime, son adresse postale, son adresse courriel, le numéro de la carte, la date d'expiration et les chiffres composant le cryptogramme visuel (Holt et Lampke, 2010). Les *CVV* sont utilisés pour faire des achats en ligne (Clarke et Newman, 2003 ; Hutchings et Holt, 2014 ; Peretti, 2009).

Bien que cette seconde étape puisse revêtir un aspect de monétisation, elle n'engage pas l'utilisation des informations financières lors de la troisième et dernière étape du script (van Hardeveld *et al.*, 2016). L'accomplissement de cette étape peut se faire par deux voies selon le type de produit qui est à la disposition du cardeur. Avec un *fullz* ou un *CVV*, le cardeur peut faire du *carding* en ligne (Sullivan, 2010). Il utilisera les informations financières pour acheter des biens ou des services sur des sites ne bénéficiant pas d'un système de paiement assez sécuritaire. Avec une carte contrefaite à l'aide d'un *dump*, le cardeur pourra faire des achats hors ligne en allant directement dans les magasins pour régler ses paiements grâce à la bande magnétique de la carte (Sullivan, 2010).

L'évolution des lieux de convergence

Le *carding* est le résultat de plusieurs étapes qui mettent en scène une chaîne d'acteurs. L'organisation de la collaboration entre ces acteurs passe par des lieux de convergence où les cardeurs échangent sur les stratégies de *carding* et bâtissent des relations d'affaires (Leukfeldt, 2014). Ces lieux de convergence en ligne existent depuis les années 1980 et s'appuient aujourd'hui sur des salles de clavardage qui permettent des discussions en direct et sur des forums dont le système de discussion est asynchrone. Les salles de clavardage s'articulent autour de services de messagerie instantanée qui permettent de converser en temps réel, de manière publique ou privée (Décary-Hétu et Dupont, 2012). À titre d'exemple, l'*Internet Relay Chat* (IRC), existant depuis la fin des années 1990, est divisé en centaines de serveurs qui hébergent chacun un grand nombre de salles de clavardages. Ces salles ont leurs propres sujets de discussion et leurs règles de participation (Franklin, Perrig, Paxson et Savage, 2007). IRC a facilité l'émergence d'un véritable réseau social entre les cardeurs en favorisant leurs rencontres et en proposant un espace de vente pour les produits et services illicites

en lien avec le *carding* (Thomas et Martin, 2006). IRC, de manière anecdotique, est de plus en plus remplacé par Telegram qui offre les mêmes capacités, tout en chiffrant les communications, garantissant plus d'anonymat à leurs utilisateurs.

Les forums de discussion sont divisés en sous-forums sur la base des thèmes de discussion (ex. : apprentissage, vie personnelle, technologie). Les sous-forums sont eux-mêmes divisés en fils de discussion plus spécifiques (Holt, 2007 ; Holt et Lampke, 2010 ; Motoyama, McCoy, Levchenko, Savage et Voelker, 2011). Contrairement aux salles de clavardage, les discussions sur les forums sont asynchrones. Tous les acteurs ne doivent donc pas être en ligne en même temps pour pouvoir participer aux conversations et disposent d'une archive de tous les messages publics ainsi que d'une messagerie privée (Yip, Webber et Shadbolt, 2013). Dans le cadre du carding, les forums servent de lieux de convergence. Grâce à leurs fonctionnalités et leur facilité d'utilisation, ils fournissent aux cardeurs une interface permettant d'articuler leurs activités et forment de véritables lieux de marchandage (Décary-Hétu et Leppänen, 2013 ; Yip *et al.*, 2013), et ce, dans de nombreux langages (Haslebacher, Onaolopo et Stringhini, 2016 ; Motoyama *et al.*, 2011). Les forums ne sont pas uniquement destinés à offrir une infrastructure pour soutenir des échanges, ce sont aussi des communautés organisées autour de normes et de valeurs (Afroz, Garg, McCoy et Greenstadt, 2013 ; Jordan et Taylor, 1998 ; Motoyama *et al.*, 2011) qui jouent un rôle de facilitateur pour les activités des cardeurs (Yip *et al.*, 2013). Les forums utilisent un système de rôles qui ne sont pas mutuellement exclusifs pour assurer leur bon fonctionnement et déléguer les responsabilités (Franklin *et al.*, 2007 ; Holt, 2013 ; Yip *et al.*, 2013). Les *administrateurs* et les *modérateurs,* dont la fonction est d'assurer la gestion globale des forums (Dupont, Côté, Savine et Décary-Hétu, 2016), peuvent mettre à l'écart les participants ne respectant pas les règles. Ils peuvent aussi se positionner comme *courtiers financiers* pour recevoir le paiement de l'acheteur et attester de la qualité du produit du vendeur lors d'une transaction ou encore en tant que *vérificateurs* pour contrôler que le vendeur offre bel et bien ce qu'il annonce sur le forum (Décary-Hétu et Eudes, 2015 ; Holt, Smirnova, Chua et Copes, 2015).

Depuis 2011, un nouveau type de lieu de convergence a fait son apparition. Les cryptomarchés ont connu un essor retentissant en 2011 lors de la médiatisation du premier cryptomarché SR1 (Olson, 2013). Lancé en février 2011, SR1 visait principalement la vente de drogue

illicite, mais facilitait aussi la vente de produits licites comme des vêtements et du matériel informatique (Devine, Egger-Sider et Rojas, 2015). Cette innovation criminelle a su profiter de l'émergence du réseau TOR ainsi que des cryptomonnaies comme le Bitcoin, permettant à la fois aux criminels de bénéficier d'un anonymat de leurs activités et de leurs transactions (Barratt et Aldridge, 2016). Ces technologies n'ont pas été une panacée pour les administrateurs, dont certains ont été arrêtés par les forces policières. Elles ont cependant grandement limité les arrestations des participants aux cryptomarchés. Le fonctionnement et la facture visuelle des cryptomarchés sont très largement inspirés des grands sites marchands comme eBay et Amazon (Broséus *et al.*, 2016 ; Décary-Hétu et Giommoni, 2017). Un système automatisé de réputation permet aux acheteurs d'évaluer l'expérience et la fiabilité des vendeurs. En cas de conflit, les acheteurs peuvent demander réparation aux administrateurs. Ces derniers jouent un rôle important dans les conflits, car la plupart des paiements doivent transiter par eux étant donné qu'ils jouent aussi le rôle de *courtier financier* (Christin, 2013 ; Décary-Hétu et Eudes, 2015). En forçant les acheteurs à utiliser leurs services, les administrateurs se garantissent des commissions importantes et peuvent poser des garanties sur le niveau de service des vendeurs.

Problématique

Certains travaux soutiennent que les salles de clavardage et les forums de discussion sont des lieux de convergence utiles et efficaces pour discuter et vendre des données financières (Fallman, Wondracek et Platzer, 2010 ; Franklin *et al.*, 2007). Le système d'enregistrement de compte présent sur les deux plateformes permet aux délinquants de masquer leurs identités réelles et de créer ainsi, autour d'un pseudonyme, un réseau de relations marchandes qu'ils peuvent entretenir sur différents lieux de convergence (Franklin *et al.*, 2007). De plus, l'inscription peut se faire exclusivement grâce à une invitation ou au parrainage d'un membre déjà établi pour éviter les indésirables (Holt, 2007 ; Markham, 2011). Les utilisateurs inscrits ont ainsi accès à un vaste bassin de contacts potentiels et peuvent aisément transiger avec des acteurs dont l'historique de transactions est conservé dans les archives. Bien qu'il n'existe aucun doute sur la popularité des salles de clavardage et des forums de discussion chez les cardeurs, certains chercheurs ont remis en question l'efficacité de ces lieux de convergence

en raison de la fraude interne (Herley et Florêncio, 2010). Les cardeurs n'ont en effet aucune idée de la validité des données qu'ils achètent et ont peu de recours lorsqu'un vendeur agit de manière opportuniste. Néanmoins, il a été vu que certains lieux de convergence, comme les salles de clavardage, bénéficient d'un flux constant de nouvelles informations à vendre, ce qui peut être le témoin de leur efficacité (Fallman *et al.*, 2010 ; Franklin *et al.*, 2007). Ces constats laissent donc en suspens tout consensus au sujet de l'efficacité des lieux de convergence de première génération à soutenir des marchés de *carding*.

Le fait que les participants au *carding* utilisent aussi les cryptomarchés nous pousse à nous questionner sur les avantages qu'offre ce nouveau type de lieu de convergence aux cardeurs. Ainsi, l'objectif général de cet article exploratoire est de décrire les activités marchandes des cardeurs sur un échantillon de cryptomarchés. En créant un environnement plus anonyme et plus convivial, les cryptomarchés pourraient permettre une offre différente de services ou encore une organisation différente de celle des lieux de convergence de première génération. Le premier objectif spécifique sera de décrire la distribution des offres des produits et services relatifs au *carding* sur les cryptomarchés. Le script criminel du *carding* a mis en évidence divers outils, services et types de produits dont la présence et les proportions devront être examinées. Le second objectif spécifique sera de décrire la demande des produits et services relatifs au *carding* sur les cryptomarchés. Deux étapes du script criminel du *carding* impliquent la génération de revenus : la vente d'informations financières volées sous forme de produits et la monétisation de ces dernières. En examinant la demande, il sera possible d'estimer les gains qui peuvent être engendrés par les cardeurs lors de la vente d'informations financières et de caractériser les produits les plus populaires.

Cet article sera pertinent de deux points de vue. Tout d'abord, le *carding* est aujourd'hui facilité par les cryptomarchés et leurs impacts sont encore mal compris. Peu de travaux ont étudié les cardeurs opérant sur ce type de lieu de convergence et, au vu des importantes pertes financières que ce phénomène engendre (Anderson *et al.*, 2019), il est important d'accroître les connaissances à ce sujet. Cet article viendra donc combler un besoin d'étendre les études sur le *carding* sur un lieu de convergence distinct de ceux étudiés dans le passé. Par ailleurs, les études sur les cryptomarchés (pour un sommaire récent, voir Kruithof *et al.*, 2016) se sont surtout intéressées à la vente de drogue. Or, les ventes de produits et services de *carding* sont de plus en plus populaires

sur les cryptomarchés. Elles occupent une place de choix sur les pages d'accueil des cryptomarchés. Cet article permettra de mettre en lien les résultats des études sur la vente de drogue et le *carding* pour mieux comprendre comment se façonne la vente de produits et services en lien avec ces activités illicites.

Les données à l'étude

Les données utilisées lors de ce travail proviennent du logiciel DATACRYPTO (Décary-Hétu et Aldridge, 2013). Ce logiciel est un *web scraper* conçu pour extraire le contenu des cryptomarchés. Le processus d'extraction s'opère en deux phases. Dans un premier temps, ce logiciel va parcourir l'ensemble des pages web du cryptomarché. En démarrant de la page d'accueil, il indexera les différents hyperliens présents sur cette dernière. En répétant cette opération pour tous les hyperliens collectés, DATACRYPTO disposera *in fine* de l'arborescence complète des liens publics du cryptomarché. Dans un second temps, un robot d'indexation prendra le relais pour parcourir l'ensemble des pages composant cette arborescence afin d'en extraire les informations. La configuration préalable du robot d'indexation permettra de discriminer les informations que le chercheur souhaite collecter. L'identification de la présence d'informations restant consistantes au travers des différents cryptomarchés (ex. : catégories de produits, pseudonymes des vendeurs) permet de constituer une base de données homogène. Ceci permettra au chercheur d'effectuer des analyses sur un ensemble de cryptomarchés (Kruithof *et al*., 2016). Dans le cas de notre étude, cette opération a été répétée sur 10 cryptomarchés présents sur le réseau TOR sur une période de 20 mois entre le 21 novembre 2014 et le 16 juillet 2016.

À l'issue de cette collecte, deux bases de données ont été utilisées. La première contient des informations sur 147 575 annonces, parmi lesquelles se trouvent 12 % (N = 17 619) de produits ou services de *carding*, qui ont été trouvées et sélectionnées grâce aux systèmes de catégorisation des offres. Ces annonces contiennent un titre, une description, un prix, le pays d'origine du vendeur ainsi que des évaluations faites par d'anciens acheteurs. La seconde base de données regroupe les informations présentes sur le profil des 4294 vendeurs ayant opéré sur les cryptomarchés. Les profils des vendeurs contiennent en général leur pseudonyme, une description, la date de début de leurs activités, le nombre de transactions réalisées et des évaluations laissées par leurs clients.

Méthodologie

Dans la description du script criminel du *carding*, nous avons vu qu'intervient une chaîne d'acteurs qui vendent et achètent divers produits. Le Tableau 1 présente une typologie des différents produits et services liés au *carding*. Cette typologie s'appuie sur le système de catégorisation des cryptomarchés. L'ensemble des annonces ont été vérifiées et, au besoin, recodées à la main pour s'assurer qu'elles correspondaient bien à leur catégorie de référence.

TABLEAU 1

Types de produits et catégories subséquentes

Types de produits	Catégories de produits
Produits physiques	Cartes physiques
	Cartes-cadeaux
	Contrefaçon de cartes de crédit
	Lecteurs/copieurs de cartes
Produits virtuels	Comptes en ligne
	Dumps, fullz et *CVV*
	Listes de numéros BIN
	Logiciels malveillants
Contenus intellectuels	Services de piratage informatique
	Services de *carding*
	Services de transferts financiers
	Guides et vidéos sur le *carding*

Cette typologie distingue trois types de produits : les *produits physiques du* carding incluent toutes les catégories de produits matériels, les *produits virtuels du* carding se composent des produits pouvant être transmis virtuellement et les *contenus intellectuels du* carding regroupent les annonces proposant des services pour sous-traiter certaines tâches du script ou apprendre à en effectuer d'autres.

Pour répondre à notre premier objectif spécifique, nous utiliserons cette typologie pour décrire comment se distribuent les annonces entre les différents types et catégories de produits. Nous utiliserons des analyses descriptives qui feront appel aux prix affichés par ces annonces pour offrir un regard plus en profondeur sur les différences intra-catégories. Des statistiques descriptives seront également utilisées pour

répondre à notre second objectif. Pour observer la demande, nous utiliserons les évaluations laissées aux vendeurs comme variable proxy des ventes. En effet, lorsqu'une vente a été effectuée, l'acheteur peut laisser un commentaire associé à une note s'échelonnant de 0 à 5 pour qualifier sa satisfaction. Pour chaque annonce, le nombre de ventes sera multiplié par le prix affiché pour obtenir une approximation des revenus générés. Cette opération sera répétée pour chaque type et catégorie de produits.

Résultats

Premièrement, le Tableau 2 présente la distribution des annonces de *produits physiques du* carding. Nous avons répertorié 606 annonces de produits physiques. Les catégories de ce type représentent une proportion marginale des annonces relatives aux produits du *carding.* En effet, mis à part la catégorie des *contrefaçons de billets* (n = 332) qui représente environ 2 % du total de ces annonces, les autres catégories représentent chacune moins de 1 %. Les forts écarts-types et les fortes variances témoignent aussi d'une importante dispersion des prix entre les offres d'une même catégorie. À titre d'exemple, il y a un écart-type de 1080 $ pour les annonces de *cartes physiques* alors que la médiane est de 181 $. Cela s'explique par le fait que le prix de vente dépendra du solde du produit acheté ou de la qualité du matériel commandé. Par exemple, dans le cas de la *contrefaçon de carte bancaire*, les annonces peuvent proposer divers types de matériels intervenant dans la manufacture de fausses cartes qui seront plus ou moins coûteux. Les *produits physiques* ne disposent pas d'une grande popularité en termes d'offres au sein des cryptomarchés. Le script criminel du *carding* pouvant être réalisé exclusivement virtuellement, il n'est pas étonnant de constater que ce type de produits représente une très faible proportion des produits offerts. Ce qui est contraignant car impliquant des modalités d'envoi plus complexes et risquées que l'envoi d'un produit virtuel, ces produits sont moins offerts et réservés à un petit contingent de vendeurs.

Deuxièmement, le Tableau 3 présente la même démarche pour les *produits virtuels du* carding qui représentent le quart des offres relatives au *carding* (n = 4463 ; 25 %). La catégorie des *logiciels malveillants* est la plus représentée et regroupe 11 % des annonces relatives au *carding* (n = 2016). Cette catégorie contient des offres proposant, par exemple, des logiciels de piratage informatique permettant de voler des données

TABLEAU 2

Répartition des offres et indices de tendance centrale et de dispersion des prix pour les produits physiques du *carding*

	n	%	Mdn	M	É.-t.	Min	Max
Produits physiques	**606**	**3 %**	**97 $**	**705 $**	**2 260 $**	**< 1 $**	**32 315 $**
Cartes physiques	65	< 1 %	181 $	605 $	1 080 $	5 $	6 753 $
Cartes-cadeaux	120	< 1 %	34 $	217 $	550 $	< 1 $	4 887 $
Contrefaçon de cartes bancaires	48	< 1 %	26 $	95 $	154 $	< 1 $	763 $
Contrefaçon de billets	332	2 %	147 $	1 025 $	2 947 $	1 $	32 315 $
Lecteurs/copieurs de cartes	41	< 1 %	87 $	411 $	698 $	5 $	2 479 $

personnelles ou encore des dispositifs permettant l'envoi massif de pourriels. Bien que rien n'indique que les logiciels malveillants offerts soient tous effectifs, ce constat peut tout de même être inquiétant. En effet, les cryptomarchés à l'étude permettent aux acheteurs de bénéficier d'un large choix d'outils pour parachever la première étape du script au cours de laquelle les informations financières sont dérobées. La catégorie des *dumps, fullz et CVV* est la deuxième en importance avec 1473 annonces (8 % des offres relatives au *carding*). Cette catégorie affiche la plus grande étendue de prix (Min < 1$; Max = 50 285 $). En effet, bien qu'il semble courant d'acquérir des informations financières pour une quinzaine de dollars (Mdn = 15 $), cette catégorie affiche de fortes fluctuations de prix (É.-t. = 2088 $). Ceci illustre bien le fait que certaines annonces de cette catégorie varient en termes de nombre d'informations financières offertes, pouvant être vendues en lots de plusieurs dizaines, voire de centaines d'informations financières. Cette fluctuation s'explique aussi par le fait qu'il y a plus ou moins d'argent sur les comptes associés aux informations vendues. Cette interprétation s'applique aussi à la catégorie des *comptes bancaires en ligne* qui offre des identifiants pour se connecter au site de banques (É.-t. = 1636 $) et représente 5 % des annonces relatives au *carding*.

Finalement, le Tableau 4 présente la même trame analytique pour le type *contenus intellectuels du* carding. Ce type est le plus largement représenté (N = 12 550 ; 71 %). Ceci s'explique principalement par la présence de la catégorie *guides et vidéos sur le* carding qui canalise 68 %

TABLEAU 3

Répartition des offres et indices de tendance centrale et de dispersion des prix pour les produits virtuels du *carding*

	n	%	Mdn	M	É.-t.	Min	Max
Produits virtuels	**4 463**	**25 %**	**10 $**	**180 $**	**1 412 $**	**< 1 $**	**50 285 $**
Comptes bancaires en ligne	845	5 %	95 $	523 $	1 636 $	< 1 $	28 930 $
Dumps, *fullz* et *CVV*	1 473	8 %	15 $	192 $	2 088 $	< 1 $	50 285 $
Listes de numéros BIN	129	< 1 %	3 $	10 $	29 $	< 1 $	201 $
Logiciels malveillants	2 016	11 %	6 $	38 $	193 $	< 1 $	5 014 $

des annonces relatives au *carding*. Cette prévalence fait écho au fait que le script criminel du *carding* implique une série d'actions qui nécessitent des compétences différentes et qui peuvent être menées de diverses manières. Au-delà de retranscrire la malléabilité du script du *carding*, cette observation témoigne aussi du fait que les cardeurs doivent sans cesse renouveler et mettre à jour leurs techniques pour mettre à mal les stratégies de défense mises en place par les institutions financières. Ainsi, il n'est pas étonnant de constater l'abondance de telles offres. De plus, la nature non consommable de tels guides pourrait aussi permettre à un acquéreur de revendre un guide bonifié qu'il aurait préalablement acheté. Les trois autres catégories d'annonces de ce type sont des services proposés par les vendeurs. Les *services de piratage informatique* proposent par exemple d'envoyer des spams ou de collecter des informations personnelles et les *services de* carding offrent d'acheter des biens acquis à l'aide d'informations financières ou encore de blanchir de l'argent provenant des activités des cardeurs. Ces différents services ont eux aussi de fortes variations de prix et représentent une petite proportion des annonces relatives au *carding*. Ce constat s'illustre particulièrement bien par les prix des *services de piratage informatique* qui affichent l'écart-type le plus élevé, toutes catégories et tous types confondus (É.-t. = 11 198 $).

Notre second objectif porte sur la demande de produits du *carding* sur les cryptomarchés et mobilise notre second jeu de données qui se concentre sur le nombre de ventes des vendeurs. Pour rappel, ces mesures s'étalonnent sur une période de 20 mois entre le 21 novembre 2014, date de la première vente d'un produit relié au *carding*, et le

TABLEAU 4

Répartition des offres et indices de tendance centrale et de dispersion des prix pour les contenus intellectuels du *carding*

	n	%	Mdn	M	É.-t.	Min	Max
Contenus intellectuels	**12 550**	**71 %**	**4 $**	**84 $**	**950 $**	**< 1 $**	**42 205 $**
Services de piratage informatique	73	< 1 %	5 $	3 042 $	11 198 $	< 1 $	42 205 $
Services de *carding*	117	< 1 %	38 $	716 $	2 043 $	< 1 $	12 799 $
Services de transferts financiers	362	2 %	601 $	1 031 $	1 225 $	< 1 $	8 356 $
Guides et vidéos sur le *carding*	11 998	68 %	3 $	31 $	138 $	< 1 $	3 323 $

16 juillet 2016, date de la dernière vente avant la clôture de la collecte. Sur cette période, un ensemble de 79 345 ventes ont été effectuées par 4294 vendeurs sur les 10 cryptomarchés à l'étude pour un chiffre d'affaires de plus de 2,6 millions de dollars. De prime abord, il est intéressant de constater que la demande n'est pas équitablement répartie entre les trois types de produits. En effet, les *produits virtuels* concentrent une large majorité des ventes (n = 51 572 ; 66 %) suivis des *contenus intellectuels* qui accaparent le tiers restant (n = 25 375 ; 33 %). La demande de *produits physiques* est très marginale. En effet, les ventes qui leur sont associées ne représentent même pas un centième des achats effectués (n = 739 ; < 1 %). Cette observation prolonge le constat effectué plus tôt quant à l'offre des *produits physiques du* carding : leur faible étendue sur les cryptomarchés s'applique aussi à la demande qu'ils suscitent et conforte l'idée que ces produits ne sont pas populaires. D'autant plus que cette idée se retrouve dans la moyenne des évaluations, qui est la plus faible parmi les autres types de produits (M = 4,62).

La catégorie la plus prégnante est celle des *dumps, fullz* et *CVV* qui concentre à elle seule plus de la moitié de la demande (n = 41 036 ; 53 %) et des revenus estimés (Somme = 1 511 460 $). Ceci nous amène à penser que ces produits phares du *carding* demeurent les plus populaires et les plus prisés parmi les cardeurs. Le fait qu'ils puissent être transférés électroniquement facilite grandement les échanges en réduisant le temps de livraison et les risques inhérents à l'envoi de matériel

TABLEAU 5

État de la demande, évaluations et revenus estimés

Types et catégories de produits	Nombre de ventes	% de parts de marché	Somme des revenus estimés	Moyenne des évaluations (sur 5)
Produits physiques	**739**	**< 1 %**	**92 569 $**	**4,62**
Cartes physiques	93	< 1 %	14 687 $	4,55
Cartes-cadeaux	663	< 1 %	69 610 $	4,95
Contrefaçon de cartes bancaires	83	< 1 %	5 165 $	4,95
Lecteurs/copieurs de cartes	35	< 1 %	3 107 $	4,33
Produits virtuels	**51 572**	**66 %**	**1 870 713 $**	**4,69**
Comptes bancaires	5 764	7 %	311 889 $	4,55
Dumps, *fullz* et *CVV*	41 036	53 %	1 511 460 $	4,63
Listes de numéros BIN	619	< 1 %	5 321 $	4,80
Logiciels malveillants	4 153	5 %	42 043 $	4,77
Contenus intellectuels	**25 375**	**33 %**	**715 545 $**	**4,82**
Services de piratage informatique	985	1 %	20 108 $	4,70
Services de *carding*	206	< 1 %	57 397 $	4,94
Services de transferts financiers	435	< 1 %	86 810 $	4,82
Guides et vidéos sur le *carding*	23 749	31 %	551 239 $	4,81
Total	**77 821**	**100 %**	**2 678 836 $**	**4,71**

illégal. La seconde catégorie à avoir généré le plus de ventes est celle des *guides et vidéos sur le* carding avec 23 749 ventes (31 %). Cette catégorie a engendré plus d'un demi-million de dollars de revenus estimés (Somme = 551 239 $). Ce genre de produit est donc relativement populaire au sein des cardeurs. Ce constat correspond bien au fait que cette catégorie de produits était la plus représentée en termes d'offres et souligne l'importance pour les cardeurs de bénéficier de supports d'apprentissage pour mener à bien leurs activités. Bien qu'ayant généré beaucoup moins de ventes que les catégories précédentes, il est intéressant de souligner que les *comptes bancaires en ligne* et les *logiciels malveillants* ont tout de même suscité un certain intérêt (respectivement n = 5 764 ; 7 % et n = 4 153 ; 5 %).

Nous avons émis plus tôt une explication quant aux raisons de l'impopularité des *produits physiques*. Cependant, nous constatons aussi que des catégories des *produits virtuels* et des *contenus intellectuels*, auxquelles notre rationnel ne peut s'appliquer, ne semblent pas susciter

l'engouement des acheteurs. Les *services de piratage informatique*, de *fraude*, de *transferts financiers* ainsi que les *listes de numéros BIN* constituent chacun de 1 % à moins de 1 % de la demande. Cette observation s'explique par le fait que les catégories populaires font de l'ombre à ces dernières. En effet, les acheteurs sont très réticents à engager de tels services dans la mesure où d'autres offres leur permettent de réaliser ou d'apprendre à réaliser eux-mêmes la tâche qu'ils souhaitent initialement sous-traiter. Par exemple, un cardeur souhaitant dérober des informations financières pourra plutôt développer cette compétence en achetant un *logiciel malveillant* plutôt que d'engager un *service de piratage informatique* qui le réalisera pour lui.

Discussion et conclusion

Cette recherche exploratoire avait pour objectif de décrire les activités marchandes des cardeurs sur les cryptomarchés. Les résultats de nos analyses nous ont permis de mettre en lumière certaines tendances. En effet, la typologie développée et par laquelle nous avons analysé les offres nous a permis de constater qu'un grand nombre de types et de catégories de produits sont présents sur les cryptomarchés. Bien que la littérature scientifique ait mis en évidence la présence et la popularité des *dumps*, *fullz* et *CVV* (Holt et Lampke, 2010), nos résultats ont montré que les cryptomarchés offrent tout le nécessaire maîtriser le script criminel décrit par van Hardeveld et ses collaborateurs (2016). Nous trouvons donc que les cryptomarchés offrent les mêmes produits que les lieux de convergence comme les salles de clavardage et les forums de discussion. Tout comme pour les vendeurs de drogue, les cryptomarchés semblent avoir permis aux cardeurs d'offrir un large éventail de produits et de services dans un lieu de convergence à la facture visuelle et à l'utilisation agréable (Broséus *et al.*, 2016 ; Décary-Hétu et Giommoni, 2017). Cependant, les cryptomarchés ne proposent pas, comme les lieux de convergence de première génération, de systèmes de communications permettant les discussions plus informelles qui consolident les communautés (Afroz *et al.*, 2013 ; Jordan et Taylor, 1998 ; Motoyama *et al.*, 2011 ; Yip *et al.*, 2013). Ainsi, il n'est pas étonnant de constater la forte popularité des guides et vidéos sur le *carding* qui peut être considérée comme une démonstration de cette difficulté à tisser des liens dans un marché peu structuré.

À la différence des produits trouvés sur les forums et salles de clavardage, les cryptomarchés offrent une nouvelle catégorie de produits utilisée par les cardeurs : les identifiants de comptes en ligne. Une autre différence vient du fait que les acheteurs peuvent facilement parcourir toutes les offres pour un type de produit et pourront choisir parmi une multitude d'offres de qualités diverses, comme en témoignent les indices de dispersion des prix. Il devient dès lors plus facile de comparer les offres. Dans une autre mesure, le système d'évaluation formel mis en place permet aussi de transcender et de simplifier les mécanismes générateurs de confiance qui prenaient place sur les lieux de convergence de première génération. Ce système d'évaluation associé à la multiplicité des offres permet aux cryptomarchés de générer une concurrence entre les vendeurs permettant de réduire le phénomène de victimisation endogène entre les cardeurs (Herley et Florêncio, 2010).

Ces impacts sont à nuancer lorsque l'on se penche sur la demande. En effet, nous avons constaté que malgré cette effervescence en termes de produits, la demande reste relativement canalisée sur certaines catégories. Nous avons remarqué que les *produits physiques* attirent un petit contingent d'acheteurs. Ceci s'explique par le fait que les technologies d'anonymat utilisées par les cryptomarchés ont amorcé une forme de constance quant à la manière dont les cardeurs mènent leurs activités. En utilisant des *produits physiques*, par exemple des *skimmers* (Peretti, 2009), les cardeurs s'exposent plus à une détection qu'en menant leurs activités exclusivement en ligne. Ce constat est doublement renforcé par la forte demande de *produits virtuels*, par exemple les *dumps, fullz et CVV*, que nous avons observée lors de nos analyses. Ainsi, les cardeurs sont plus enclins à utiliser la voie du *carding* en ligne pour monétiser les informations financières ou bancaires. De plus, cette concentration de la demande sur certains produits pourrait venir en quelque sorte polluer ou saturer le marché. Étant donné les fortes variations de prix relevées et le fait qu'une partie non négligeable des produits se vend à des prix relativement dérisoires, il est important tout de même de se questionner sur la qualité de certains produits offerts.

Références

Afroz, S., Garg, V., McCoy, D. et Greenstadt, R. (2013). Honor among thieves : A common's analysis of cybercrime economies. Dans *2013 APWG eCrime Researchers Summit.* https://doi.org/10.1109/eCRS.2013.6805778

Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganán, C., Grasso, R.,… Vasek, M. (2019). Measuring the changing cost of cybercrime. Dans *Proceedings of the 17th Workshop of the Economics of Information Security (WEIS)*. Boston, MA.

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.

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

Bulakh, V. et Gupta, M. (2015). Characterizing credit card black markets on the web. Dans *Proceedings of the 24th International Conference on World Wide Web.* Florence, Italie.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S. et Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores : An examination of older and younger adults. *Decision Support Systems*, *83*, 47-56.

Christin, N. (2013). Traveling the silk road : A measurement analysis of a large anonymous online marketplace. Dans *Proceedings of the 22nd international conference on World Wide Web* (p. 213-224).

Clarke, R. V. et Newman, G. R. (2003). *Superhighway robbery : Preventing e-commerce crime.* Cullumpton, Royaume-Uni : Willan Publishing.

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies*, *3*, 151-196.

Décary-Hétu, D. et Aldridge, J. (2013). DATACRYPTO : The Dark Net Crawler and Scraper.

Décary-Hétu, D. et Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160-175.

Décary-Hétu, D. et Eudes, M. (2015). Partenariats criminels au sein d'un forum de carding : alliés, rivaux ou escrocs ? Étude de l'utilisation d'identités virtuelles multiples. *Revue internationale de criminologie et de police technique scientifique*, *68*(3), 299-314.

Décary-Hétu, D. et Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets ? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, *67*(1), 55-75.

Décary-Hétu, D. et Leppänen, A. (2016). Criminals and signals : An assessment of criminal performance in the carding underworld. *Security Journal*, *29*(3), 442-460.

Devine, J., Egger-Sider, F. et Rojas, A. (2015). The evolving impact of the invisible web : Exploring economic and political ramifications. *Journal of Web Librarianship*, *9*(4), 145-161

Dolliver, D. S. (2015). Evaluating drug trafficking on the Tor network : Silk Road 2, the sequel. *International Journal of Drug Policy*, *26*(11), 1113-1123.

Dupont, B., Côté, A. M., Savine, C. et Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime*, *17*(2), 129-151.

Fallmann, H., Wondracek, G. et Platzer, C. (2010). Covertly probing underground economy marketplaces. Dans *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (p. 101-110). Bonn, Allemagne.

Franklin, J., Perrig, A., Paxson, V. et Savage, S. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. Dans *ACM Conference on Computer and Communications Security* (p. 375-388).

Greene, C. et Stavins, J. (2017). Did the Target data breach change consumer assessments of payment card security ?. *Journal of Payments Strategy & Systems*, *11*(2), 121-133.

Haslebacher, A., Onaolapo, J. et Stringhini, G. (2017). All your cards are belong to us : Understanding online carding forums. Dans *Electronic Crime Research (eCrime), 2017 APWG Symposium on* (p. 41-51). IEEE.

Herley, C. et Florêncio, D. (2010). Nobody sells gold for the price of silver : Dishonesty, uncertainty and the underground economy. Dans *Economics of information security and privacy* (p. 33-53). Boston, MA : Springer.

Holt, T. J. (2007). Subcultural evolution ? Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171-198.

Holt, T. J. (2013). Exploring the social organization and structure of stolen data markets. *Global Crime*, *14*(2-3), 155-174.

Holt, T. J. et Lampke, E. (2010). Exploring stolen data markets online : Products and market forces. *Criminal Justice Studies*, *23*(1), 33-50.

Holt, T. J., Smirnova, O., Chua, Y. T. et Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81-103.

Holz, T., Engelberth, M. et Freiling, F. (2009). Learning more about the underground economy : A case-study of keyloggers and dropzones. Dans *Computer Security – European Symposium on Research in Computer Security 2009* (p. 1-18).

Hutchings, A. et Holt, T. J. (2014). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596-614.

James, L. (2005). *Phishing exposed : Uncover secrets from the dark side*. Rockland, MA : Syngress.

Jordan, T. et Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757-780.

Kashmiri, S., Nicol, C. D. et Hsu, L. (2016). Birds of a feather : Intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science*, *45*(2), 208-228.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E. et Hoorens, S. (2016). Internet-facilitated Drugs Trade : An Analysis of the Size, Scope and the Role of the Netherlands. *WODC, Ministerie van Veiligheid en Justitie*. Repéré au https://www.rand.org/pubs/research_reports/RR1607.html.

Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in Organized Crime*, *17*(4), 231-249.

Markham, A. N. (2011). Internet research. Dans D. Silverman (dir.), *Qualitative Research : Issues of Theory, Method, and Practice* (3e éd., p. 111-127). SAGE.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S. et Voelker, G. M. (2011). An analysis of underground forums. Dans *Proceedings of the 2011 Internet Measurement Conference.* Berlin, Allemagne.

Olson, P. (2013). The man behind Silk Road – the internet's biggest market for illegal drugs. *The Guardian.* Repéré à https://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht

Peretti, K. K. (2009). Data breaches : What the underground world of carding reveals. *Santa Clara Computer & High Tech. LJ*, *25*, 375.

Sullivan, R. J. (2010). The changing nature of US card payment fraud : Industry and public policy options. *Economic Review-Federal Reserve Bank of Kansas City, 95*(2), 101.

Symantec. (2017). *Internet security threat report.* Repéré à https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Thomas, R. et Martin, J. (2006). The underground economy : Priceless. *; login : : the magazine of USENIX & SAGE*, *31*(6), 7-16.

van Hardeveld, G. J., Webber, C. et O'Hara, K. (2016). Discovering credit card fraud methods in online tutorials. Dans *Proceedings of the 1st International Workshop on Online Safety, Trust and Fraud Prevention.* Hanovre, Allemagne.

Vasiu, I. et Vasiu, L. (2015). Riders on the storm : An analysis of credit card fraud cases. *Suffolk Journal of Trial & Appellate Advocacy*, *20*, 184-217.

Wall, D. (2007). *Cybercrime : The transformation of crime in the information age.* Cambridge, Royaume-Uni : Polity.

Yip, M., Shadbolt, N. et Webber, C. (2013). Why forums ? An empirical analysis into the facilitating factors of carding forums. Dans *Proceedings of the 5th Annual ACM Web Science Conference*. Paris, France.

Cryptomarkets and carding : Influence on supply and demand

ABSTRACT • *The present study describes the market activities of carding in cryptomarkets in a sample of 17,619 products or services related to carding as well as a second sample of the activities of 4,294 sellers. We were interested particularly in whether convergence settings such as cryptomarkets have an effect on the supply and demand of carding products and services. We began by creating a typology of products and services which was then used in a descriptive analyses of market share and price distribution to shed the light on how anonymization affected offers. Descriptive analyses of sellers' activities was then used to look at the impact of sales on the demand for carding products and services. The results suggest that cryptomarkets offer all that carders need to carry out the three steps of the criminal script in carding. We also found that, as with online drug dealers, the formal feedback system made it possible to improve processes that generate confidence in the system.*

KEYWORDS • *Carding, cryptomarkets, supply, offer, cybercriminality.*

Mercados criptográficos y *carding*: Impacto sobre la oferta y la demanda

RESUMEN • *Este artículo describe las actividades comerciales del* carding *por los mercados criptográficos, examinando una muestra de 17 619 anuncios de productos o de servicios relativos al* carding*, y una segunda muestra de las actividades de 4294 vendedores. Nuestro proceso se interesa más específicamente en constatar si el advenimiento de los mercados criptográficos, como lugar de convergencia para los cibercriminales, tuvo un impacto sobre la oferta y la demanda de tales productos y servicios. Para llevar a cabo este objetivo, una tipología de los diferentes productos y servicios fue realizada. En primer lugar, un análisis descriptivo fue realizado, poniendo a la luz las proporciones de los diferentes tipos, así como la distribución de los precios publicados en los anuncios, permite observar el impacto de las tecnologías de anonimato sobre la oferta. En segundo lugar, otros análisis descriptivos fueron efectuados sobre las transacciones realizadas por los vendedores para examinar este impacto sobre la demanda. Los resultados principales indican que los mercados criptográficos ofrecen todo lo necesario para cometer las tres etapas del guion criminal del* carding*. Además, también es demostrado que, de la misma forma que los vendedores de droga en línea, el sistema de evaluación formal permitió trascender y mejorar los procesos generadores de confianza.*

PALABRAS CLAVE • *Carding, mercados criptográficos, oferta, demanda, criminalidad cibernética.*