BitCluster: un outil d'analyse des bitcoins

David Décary-Hétu[1] et Mathieu Lavoie[2]

Les monnaies facilitent depuis très longtemps les échanges commerciaux. D'abord valorisées par leur valeur intrinsèque en métal, elles sont graduellement passées à un mode fiduciaire où leur valeur repose sur la confiance dans leur émetteur, en général un État. Plus récemment, un nouveau type de monnaie a fait son apparition : la cryptomonnaie. Cette forme bien particulière d'argent numérique mise avant tout sur la cryptographie pour garantir son intégrité et n'a plus besoin du recours d'une autorité centrale, comme une banque centrale, pour en gérer le cours.

La cryptomonnaie la plus utilisée est le bitcoin, dont la valeur marchande dépasse aujourd'hui les 69 milliards de dollars américains. Des milliers de transactions de bitcoins s'effectuent tous les jours et, comme pour n'importe quelle technologie, le bitcoin peut être utilisé à des fins autant légitimes qu'illégitimes. Pour aider les chercheurs à mieux comprendre les comportements illicites des utilisateurs de bitcoins, ainsi que pour augmenter la capacité de renseignement sur ses flux, il existe un outil gratuit et à code source ouvert, le BitCluster, dont nous analyserons l'efficacité à la lumière d'une étude de cas sur les logiciels de rançon, dont certains sont très sophistiqués.

Des monnaies fiduciaires aux monnaies virtuelles

Les monnaies de type *fiduciaire* comprennent toutes celles qui sont émises par les États : les pièces métalliques et les billets de banque (ou leur représentation virtuelle) utilisés pour la quasi-totalité des transactions faites dans nos sociétés modernes. La valeur de cette monnaie vient avant tout de

[1] Professeur adjoint, École de criminologie, Université de Montréal.
[2] Chef d'équipe, Sécurité applicative, Institution financière canadienne.

la confiance des utilisateurs dans le système politique et financier qui leur garantit qu'on pourra acheter des biens ou des services d'une valeur équivalente. Des institutions centrales, nommément les banques centrales, gèrent habituellement les monnaies fiduciaires et en contrôlent la quantité en circulation, ce qui, entre autres choses, stabilise l'économie et promeut les activités économiques en général.

Bien qu'elles jouent un rôle crucial dans les économies modernes, les monnaies fiduciaires n'ont jamais eu le monopole des transactions monétaires. Cela est encore plus vrai depuis l'apparition, au cours des vingt dernières années, des monnaies numériques, qu'on peut définir comme « des monnaies non régulées et numériques créées et contrôlées par leurs créateurs et utilisées dans une communauté en ligne spécifique » (European Central Bank, 2012, p. 13). Elles peuvent être obtenues en échange de monnaies fiduciaires sur des sites d'échanges ou encore en accomplissant certaines actions (p. ex : passer un certain nombre d'heures dans une communauté en ligne chaque mois).

Selon Tanaka (1996), les monnaies numériques offrent plusieurs avantages par rapport aux monnaies fiduciaires. Elles permettent notamment de réduire les coûts associés aux transferts monétaires. En effet, au fil des siècles, les banques sont devenues de lourdes bureaucraties nécessitant de coûteux systèmes informatiques, un grand nombre d'employés, de succursales et d'immeubles. Ce sont les clients qui payent les coûts de cette bureaucratie, au moment des transferts. Les transferts numériques pour leur part se font au moyen d'une connexion internet et des appareils informatiques des parties qui négocient les fonds. Les coûts en infrastructure sont donc inexistants, ce qui permet de réduire considérablement les coûts de transferts. Un deuxième avantage de ces monnaies numériques est qu'elles ne connaissent ni frontières ni heures d'ouverture. On peut ainsi effectuer un transfert à tout moment de l'année, instantanément et

partout sur la planète. Il n'est donc plus nécessaire d'attendre que la succursale de la banque soit ouverte pour entreprendre un transfert qui pourra prendre plusieurs jours. Le dernier, et probablement le plus grand, avantage des monnaies numériques réside dans le fait qu'elles peuvent être utilisées par quiconque ayant un accès internet. Même si l'accès au système financier est tenu pour acquis dans les pays industrialisés, plusieurs segments plus vulnérables de la population, dans les pays industrialisés comme dans les pays en voie de développement, n'ont tout simplement pas accès à des comptes d'épargne et au crédit bancaire. Les monnaies numériques permettent ainsi à de nombreuses personnes de s'émanciper financièrement.

Ce sont des entités privées qui créent et gèrent la plupart des monnaies numériques et elles réglementent comme elles l'entendent leur accès et l'utilisation qui en est faite. Les compagnies légitimes ont donc tout intérêt à limiter leur utilisation illicite afin de préserver la confiance de leurs clients. Cependant, la probité ne caractérise pas tous les émetteurs de monnaies virtuelles. Par exemple, jusqu'en 2013, la compagnie Liberty Reserve a géré une monnaie très prisée par les délinquants en raison de l'anonymat qu'elle leur fournissait. On pouvait en effet y créer un compte en ligne sans avoir à fournir de pièces d'identité. Au cours de ses quelques années d'existence, la firme a facilité le blanchiment de 6 milliards de dollars US auprès de plus d'un million de clients, avant d'être fermée par les services de police américains (U.S. Department of Justice, 2013).

LE BITCOIN ET LES AUTRES CRYPTOMONNAIES

Les échanges de monnaies numériques, tout comme celles des monnaies fiduciaires, reposent sur la confiance dans les institutions qui les gèrent. En 2008, un individu ou un groupe d'individus anonymes utilisant le pseudonyme Satoshi Nakamoto ont voulu s'attaquer à cette nécessité de faire confiance aux institutions en proposant un nouveau type de monnaie numérique fondée uniquement sur la cryptographie. Cette cryptomonnaie, le *bitcoin*, une monnaie numérique

anonyme, se voulait libre de toute ingérence et contrôle et en prime, impossible à copier. Elle devait donc être autogérée par l'offre et la demande.

LE FONCTIONNEMENT DU BITCOIN

Celui qui souhaite se procurer des bitcoins doit d'abord se créer un portefeuille (*wallet*) qui deviendra son identité publique. Ce portefeuille est représenté par un identifiant unique qui ne donne aucune information sur l'identité réelle de son propriétaire. Pour mieux garantir leur anonymat, chacun des propriétaires peut contrôler un nombre illimité de portefeuilles et, si nécessaire, l'automatisation du processus permet de générer des milliers de nouveaux portefeuilles à heure. Ainsi, il est pratiquement impossible de dénombrer le nombre de personnes possédant des bitcoins.

Pour se procurer des bitcoins, on peut passer par des sites d'échange qui mettent en contact ceux qui en détiennent avec les gens qui ont des monnaies fiduciaires. Les transferts de monnaies fiduciaires peuvent se faire en personne, à l'aide d'argent comptant, ou en ligne par virement bancaire selon le degré d'anonymat désiré. Le marché des bitcoins est extrêmement fluide avec des milliers de transactions par jour.

Un réseau poste-à-poste (P2P) d'ordinateurs gère de manière autonome le bitcoin à l'aide d'un logiciel créé par une équipe qui en assure le maintien. Le réseau a pour tâche principale de conserver des traces des transactions et d'en approuver les transferts. Une caractéristique centrale des bitcoins est que toutes ses transactions sont publiques et enregistrées dans un grand livre (*blockchain*). L'identité réelle des acteurs n'y est pas indiquée, le registre ne conservant que les informations nécessaires aux transferts. Un portefeuille ne peut par définition posséder des bitcoins, mais il possède le droit d'échanger des bitcoins reçus lors d'une transaction passée. Ainsi,

pour commencer un transfert, un acteur A publiera un message sur le réseau P2P en indiquant que les bitcoins qu'il a reçus du portefeuille 1 peuvent maintenant être dépensés par l'acteur contrôlant le portefeuille 2. Le réseau P2P vérifiera que l'acteur A contrôle bien le portefeuille 1 et qu'il n'a pas déjà dépensé ses bitcoins. Si la vérification est positive, l'acteur du portefeuille 2 pourra dès lors dépenser les bitcoins reçus dans la transaction. Pour faire valider le fait qu'il détient bien un portefeuille, l'acteur A devra produire une preuve cryptographique avec un secret connu par lui seul. Celui-ci prouve qu'il contrôle bien le portefeuille 1 sans qu'il ait à dévoiler le secret. Cette manière de procéder évite d'avoir à conserver une liste de tous les portefeuilles en circulation avec leur solde courant. L'information nécessaire pour autoriser les transferts se trouve plutôt dans le *blockchain*, ce qui diminue la quantité d'information à enregistrer sur chaque poste du réseau bitcoin et assure que le montant de bitcoins à dépenser n'a pas été manipulé.

La RÉGULATION DU BITCOIN

Le bitcoin se démarque également des autres monnaies numériques par son infrastructure décentralisée. Il n'y a pas d'institution responsable de la génération de nouveaux bitcoins qui pourrait être garante de l'utilisation problématique ou illicite des bitcoins. Cette situation est problématique d'un point de vue légal puisque les premières lois sur les monnaies numériques, notamment en Europe, visaient avant tout les émetteurs : elles ne peuvent donc pas réguler le bitcoin.

Il existe actuellement quatre approches pour encadrer l'utilisation ce cette monnaie, selon Borroni (2016). La première, en fait, est celle de ne pas faire d'encadrement. Étant donné le petit nombre de personnes impliquées dans les échanges de bitcoins par rapport à celles du système financier traditionnel, il n'est guère surprenant de constater l'inertie des États : les bitcoins ne représentent tout simplement pas un problème sérieux pour eux. La deuxième est de les considérer comme une

source de revenus et d'imposer des taxes, des redevances et des impôts sur les transactions et les profits qu'elles génèrent. Une troisième est de reconnaître le bitcoin comme une monnaie pleine et entière et de soumettre les intermédiaires qui facilitent les transactions aux normes du système financier traditionnel. À la différence cependant des banques et des autres facilitateurs d'échanges, les intermédiaires permettant de convertir des bitcoins ne connaissent pas la valeur totale des bitcoins détenus par leurs clients qui peuvent à tout moment faire des échanges avec d'autres intermédiaires. Ceux-ci ne peuvent donc être tenus responsables des actions de leurs clients et ne peuvent surveiller leurs actions, comme le font les banques. La dernière approche consiste à interdire l'utilisation des bitcoins, comme c'est le cas actuellement en Chine. Cette interdiction est difficile à appliquer, surtout pour les citoyens qui sont à l'extérieur des frontières nationales et donc des outils de surveillance étatique.

LA SÉCURITÉ DES BITCOINS

Avec une valeur marchande totale de près de 69 milliards de dollars US, le bitcoin est une cible attrayante pour d'éventuels fraudeurs. L'attaque la plus courante consiste en la double dépense, où un acteur demande au réseau P2P bitcoin d'autoriser le transfert des mêmes bitcoins au même moment, mais avec deux récipiendaires différents. À cause de la taille du réseau P2P bitcoin, il était encore possible, il y a quelques années, que deux transactions soient approuvées temporairement avant que l'une d'elles ne soit rejetée. Des mesures ont cependant été prises pour bloquer ce type d'attaque. Un autre type d'attaque, par déni de service distribué (DDOS), empêche un acteur ou une plateforme d'échange de communiquer avec le reste du réseau P2P bitcoin. Cela permet de retarder une transaction, mais non sa réalisation. Une telle attaque perturbe les activités des acteurs plutôt que remettre en question l'existence même du bitcoin. Finalement, un dernier type d'attaque vise à acquérir le secret qui établit le contrôle d'un acteur sur un portefeuille donné.

Cela peut se faire en installant un logiciel espion sur l'ordinateur d'un acteur pour en exfiltrer des fichiers ou surveiller les touches tapées. Toutes ces menaces, bien que réelles et importantes, ont pu être détectées et atténuées au cours des dernières années et n'ont, jusqu'à maintenant, pas remis en cause la pérennité du bitcoin comme monnaie d'échange.

LES AUTRES CRYPTOMONNAIES

La création du bitcoin,a inspiré plusieurs développeurs à lancer des cryptomonnaies alternatives. Les trois monnaies les plus citées sont le litecoin, le dogecoin et l'ether. Ces cryptomonnaies cherchent toutes à remédier à une ou plusieurs limites du bitcoin. Le litecoin, par exemple, veut démocratiser la production de cryptomonnaie pour s'assurer qu'un petit groupe d'acteurs ne puisse en prendre le contrôle. Cet objectif a été atteint jusqu'à un certain point mais n'a, en réalité, que relancé la recherche de systèmes informatiques encore plus puissants donnant un avantage à l'un ou l'autre des acteurs. Les autres monnaies visaient à proposer une alternative moins dispendieuse que le bitcoin. Malgré cette compétition, le bitcoin reste le plus utilisé, avec une valeur marchande totale deux fois et demie plus élevée que celle de l'ether et vingt fois plus que celle du litecoin (Coin Market Cap, 2017).

LE BITCOIN, UNE bonne ou une mauvaise innovation ?

Ses défenseurs affirment que, à cause de sa flexibilité et de sa nature innovante, le bitcoin a été une invention des plus positive, qui pourrait permettre le développement de plusieurs secteurs d'activité économique comme la finance ou le sport professionnel. D'autres chercheurs mettent cependant en doute son caractère positif en montrant les nombreuses innovations illicites que le bitcoin a instaurées. En effet, la littérature mentionne de nombreuses formes de criminalité que le

bitcoin faciliterait, notamment la vente d'arme, le trafic de drogues illicites, la fraude fiscale, la vente de pornographie juvénile, le contournement de sanctions économiques et l'extorsion.

La fraude fiscale est la première forme de criminalité à avoir été associée au bitcoin. Les inquiétudes venaient du fait qu'il permet de transférer de grandes sommes d'argent instantanément, internationalement et anonymement. Il est donc très aisé de placer à l'abri de l'impôt des sommes importantes en les convertissant en bitcoin. L'anonymat qu'offre le bitcoin est aussi très utile pour éviter d'avoir à déclarer des revenus basés sur la spéculation sur le prix du bitcoin ou encore sur les revenus tirés de sa vente. Le bitcoin a aussi été associé au blanchiment d'argent à travers l'utilisation de *tumblers,* ces services en ligne permettant de camoufler l'origine et la destination de transferts. Des casinos en ligne permettent d'ailleurs de faire sensiblement la même chose en acceptant que des joueurs y déposent des sommes importantes, jouent quelques mains, puis retirent la quasi-totalité de leur argent qu'ils aient à montrer de pièces d'identité.

Plus récemment, on a aussi dénoncé l'utilisation du bitcoin dans le contexte de la vente de drogues illicites sur Internet à travers des sites web marchands, qui ne sont pas sans rappeler les eBay et Amazon de ce monde. D'abord popularisée par le site Silk Road (SR1), la vente de drogues illicites sur Internet génère aujourd'hui des ventes de plusieurs centaines de millions de dollars par année (Kruithof *et al*., 2016). Plusieurs technologies sont mises à contribution, dont le réseau Tor qui permet de camoufler l'identité des visiteurs et des serveurs qui hébergent les sites facilitant la vente de drogues illicites. Le chiffrement est aussi utilisé pour sécuriser les communications entre les vendeurs et les acheteurs et les paiements sont généralement effectués en bitcoins.

La toute dernière forme de criminalité qui a attiré l'attention des chercheurs est le logiciel de rançon, un type qui date de la fin des années 1980. Il chiffre les données d'un ordinateur et affiche ensuite un message exigeant le paiement d'une rançon en échange de la clé de chiffrement. Avant

la création du bitcoin, ce genre de paiement restait complexe, en raison de la traçabilité des paiements dans le système financier traditionnel. Le bitcoin offre maintenant une méthode de paiement anonyme et internationale qui permet aux délinquants de recevoir les paiements, peu importe le pays dans lequel la victime se trouve.

LA DÉANONYMISATION DES UTILISATEURS DU BITCOIN

Ces nombreux scénarios d'utilisation illicite du bitcoin ont attiré plusieurs acteurs de la sphère publique et privée qui ont cherché à percer l'anonymat qu'elle procure à ses utilisateurs. On a tout d'abord testé des méthodes d'enquêtes traditionnelles pour identifier les utilisateurs, une approche jusqu'à maintenant fructueuse, surtout dans les cas où ceux-ci utilisent des intermédiaires reconnus et accrédités pour acheter et vendre leurs bitcoins. Ces intermédiaires exigent en général que leurs clients leur soumettent des copies de pièces d'identité; un mandat peut même leur permettre d'obtenir une copie de ces documents. À la recherche de solutions plus techniques, des chercheurs ont recensé les différentes méthodes pour lier un portefeuille bitcoin à une adresse IP, ce qui représente une première étape vers la déanonymisation des utilisateurs de bitcoins. Toutefois, comme l'infrastructure du réseau P2P bitcoin a été conçue pour empêcher ce genre de surveillance, les résultats des recherches laissent planer des doutes sur l'efficacité réelle de cette approche.

D'autres chercheurs ont tenté d'évaluer la possibilité d'obtenir des renseignements en étudiant les flux de bitcoins et se sont intéressés aux transactions plus complexes, où les portefeuilles sont utilisés comme source de bitcoins (figure 1.1).

Figure 1.1 : Exemple de transaction bitcoin complexe

Dans cette figure, deux portefeuilles sont utilisés comme source de la transaction pour effectuer un paiement de 4 bitcoins (BTC) vers le portefeuille 3. Étant donné qu'un acteur doit prouver à l'aide d'un secret qu'il contrôle bien un portefeuille, il est raisonnable de penser que le portefeuille 1 et le portefeuille 2 appartiennent tous deux au même acteur, car ce dernier aura prouvé qu'il possède le code secret des portefeuilles 1 ET 2 pour initier la transaction. Cette technique simple de renseignement ne permet au départ que de regrouper deux portefeuilles. Appliquée à l'ensemble du grand livre des transactions du bitcoin, elle permet toutefois de faire de très nombreux rapprochements entre des portefeuilles en apparence indépendants mais qui sont en fait connectés par leur propriétaire.

À ce jour, différents chercheurs ont testé cette méthodologie pour recueillir de l'information sur les détenteurs de portefeuilles bitcoin. Fleder et al. (2015) ont proposé un article reprenant cette idée sans pour autant publier un logiciel ou du code source capable de regrouper les portefeuilles les uns avec les autres. Le mémoire de maîtrise de Spagnuolo et al. (2014) a mené à la création de BitIodine, un outil disponible en ligne, mais qui est maintenant incompatible avec les dernières versions du grand livre des transactions. Des compagnies qui ont repris cette même idée ont obtenu d'importants contrats des forces policières.

Notre objectif, à partir de ces recherches, est d'offrir un logiciel à code source ouvert et gratuit qui pourrait aider les chercheurs à mieux comprendre le comportement des utilisateurs de bitcoins. Pour ce faire, il s'agit d'augmenter les capacités de renseignement sur le réseau, et en premier lieu, de bien connaître le BitCluster, un outil que nous avons élaboré, et qui vise à présenter visuellement les informations contenues dans le blockchain en regroupant notamment les portefeuilles en fonction des acteurs qui les contrôlent. Pour bien évaluer la capacité de renseignement de cet outil, nous présenterons une étude de cas sur les logiciels de rançon. En même temps que le bitcoin acquiert de la valeur, nous prenons mieux conscience de son potentiel de criminalité. Il est crucial de bien comprendre la cryptomonnaie dans son ensemble pour savoir comment la réglementer.

Le BITCLUSTER

Nous avons créé BitCluster en 2016[3], un logiciel qui a pour principale fonction d'amasser dans des nœuds des groupes de portefeuilles contrôlés par un même acteur. À l'automne 2016, BitCluster a repéré plus de 146 millions de portefeuilles qui ont par la suite été regroupés dans 58 millions de nœuds, dont le plus gros – et de loin –était Mt. Gox, un intermédiaire qui convertissait le bitcoin en monnaies fiduciaires, avec 12 millions de portefeuilles, mais qui, depuis, a été fermé dans la controverse. Au total, ces portefeuilles ont généré plus de 387 millions de transactions.

Figure 1.2 : Interface graphique de BitCluster

Le logiciel BitCluster décrit chacun des nœuds, en commençant par un identifiant unique (*Node Id*). La figure 1.2 présente les informations descriptives de ce nœud, qui a reçu et dépensé un nombre identique de bitcoins – soit 1.58 – et qui n'a été actif qu'une journée en 2010. Les trois panneaux du bas permettent à l'utilisateur du logiciel de télécharger la liste des transactions qui entrent dans le nœud et qui en sortent. Par ailleurs, la liste des transactions de tous les portefeuilles contrôlés par ce nœud est disponible et on peut l'ordonner par dates, par nœuds impliqués ou par montants. Chaque transaction est interactive et l'utilisateur peut donc cliquer sur l'identifiant de l'acteur ayant envoyé ou reçu des bitcoins de la part du nœud. On peut ainsi suivre pas à pas les flux entrants et sortants.

BitCluster sera toujours en ligne disponible gratuitement sur http://dev.bit-cluster.com. Cette version du logiciel est hébergée sur un serveur nous appartenant. Un développeur peut également télécharger la base de données et le code source, les modifier ou les publier. Cela permettra, nous l'espérons, de poursuivre l'innovation et de trouver de nouvelles applications.

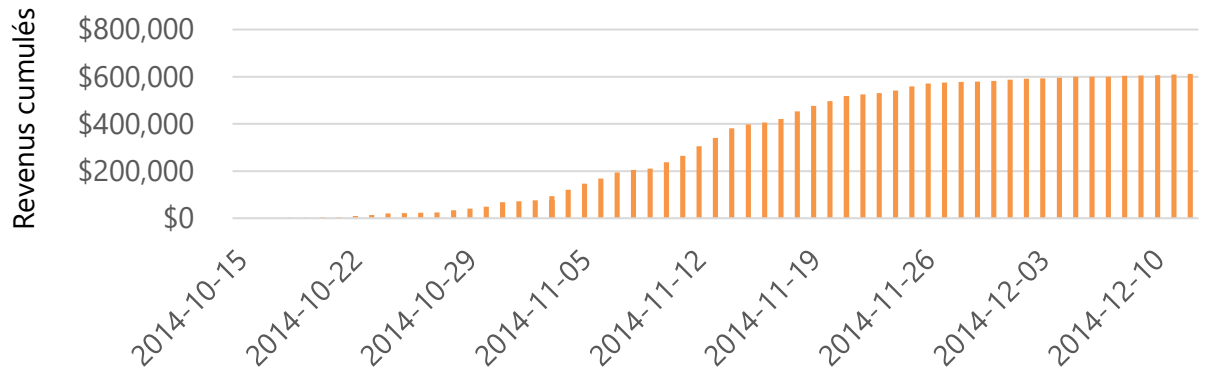
LA DÉANONYMISATION DES ACTIVITÉS ILLICITES AVEC BITCLUSTER

BitCluster aide à comprendre les activités licites et illicites sur le réseau P2P bitcoin; le cas des logiciels de rançon que nous exposons ici en montrera toute son utilité et sa portée. À l'automne

2016, nous avons demandé à nos contacts du monde de la sécurité informatique de nous fournir des identifiants de portefeuilles bitcoin qui ont reçu des rançons, à la suite à d'une infection par un logiciel. Au total, nous avons pu obtenir un échantillon de trente portefeuilles. Nous avons alors lancé des analyses descriptives de l'argent accumulé par les nœuds contrôlant ces portefeuilles pour déterminer l'évolution dans le temps de leurs revenus illicites. Pour ce faire, nous avons téléchargé, pour chaque portefeuille, une liste des paiements reçus dans les portefeuilles à des fins de rançon. Comme les montants varient grandement, nous avons limité les analyses à ceux de 75 $ à 1,200 $ US. Cette limite a peut-être éliminé certains transferts, mais elle assure que ceux non liés aux logiciels de rançon ne seront pas analysés.

À l'aide de cette méthodologie, nous avons trouvé trois types de campagnes de logiciels de rançon différents les uns des autres par leur façon d'évoluer dans le temps, qui ont généré des revenus illicites, fruits du travail de délinquants au degré de sophistication varié.

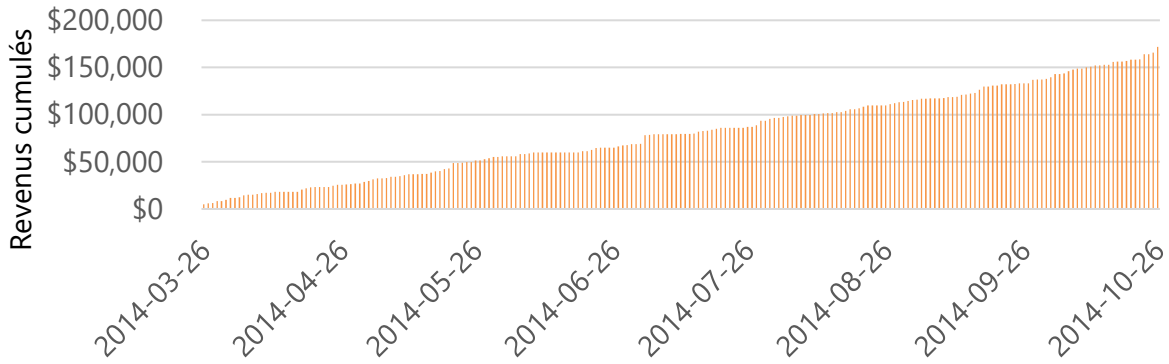
Figure 1.3 : Évolution des revenus cumulés liés à un logiciel de rançon de type I



En 2014, le logiciel de type I a fait, en 58 jours seulement, 1,127 victimes, ce qui représente une moyenne quotidienne de 19 individus générant des revenus de plus de 10,000 $ US. Entre le 2

novembre et le 24 novembre 2014, soit en 22 jours, les escrocs ont pu accumuler 80% des revenus qui, cumulés, ont dépassé 600,000 $ US – revenus qui ont plafonné au bout de quelques semaines.

Figure 1.4 : Évolution des revenus cumulés liés à un logiciel de rançon de type II



Ce logiciel de rançon de type II (figure 1.4) a fait 250 victimes en cumulant plus de 170,000 $ US. La courbe nous indique que les activités se sont arrêtées abruptement en 2014 alors que les revenus croissaient toujours. Ce comportement contraste avec celui du type I et on peut penser que ces criminels, pour une raison ou une autre, ont décidé d'utiliser de nouveaux portefeuilles impossibles à relier aux anciens. Il est donc possible que les revenus aient continué à augmenter après la date de la dernière transaction, ou alors que leur grand succès les a décidé d'arrêter avant que leur chance ne tourne.

Le troisième type de logiciel ne peut être schématisé puisque sa particularité est de ne faire qu'une victime à la fois. Cette victime paye en général une rançon de quelques centaines de dollars; aucune autre activité n'est enregistrée avant ou après la date du paiement. Les possibilités de renseignement sur ce type de logiciel de rançon sont limitées, à moins de suivre pas à pas les flux sortants du portefeuille où la rançon est déposée.

DISCUSSION ET CONCLUSION

Nos analyses, bien que sommaires, nous aide à mieux comprendre ces trois types de logiciels de rançon. Ceux de type I sont administrés par des acteurs qui connaissent apparemment peu le fonctionnement du réseau P2P bitcoin et ne semblent faire aucun effort pour camoufler l'ampleur de leurs activités, ce qui permet de suivre à la trace le paiement des victimes. Il serait intéressant de poursuivre l'analyse pour savoir si ces délinquants ont transféré leurs bitcoins directement à des plateformes d'échanges où les pièces d'identité sont obligatoires. Une enquête classique pourrait faire le lien entre une identité physique et les activités criminelles. Le fait qu'autant de portefeuilles puissent être reliés les uns aux autres suggère que leurs détenteurs ont effectué un seul transfert en inscrivant comme source l'ensemble des portefeuilles contenant les rançons. Il s'agit d'une manière efficace de consolider les gains illicites, mais elle est plus risquée que transférer des bitcoins de comptes un par un. Les acteurs des logiciels de type II semblent légèrement plus sophistiqués en faisant l'arrêt de leurs activités au bout de quelques jours. Il est possible que ces escrocs aient compris le risque qu'il y a à centraliser leurs revenus et qu'ils soient passés au type III, encore plus sophistiqué. Leur stratégie de ne mélanger à aucun moment la source des transferts de bitcoins, met en effet un frein à la collecte de renseignements, mais requiert de la part des acteurs un plus grand effort pour gérer les flux de bitcoins. Cela veut probablement dire que certains délinquants connaissent bien les risques associés à l'utilisation du bitcoin et qu'ils savent comment les gérer efficacement.

Leur ingéniosité pourrait amener dans les prochaines années d'autres fraudeurs à développer, dans un esprit de coopération, des pratiques plus sécuritaires, pour eux. Leurs échanges se feraient dans des lieux de convergence en ligne ouverts aux seuls initiés. Tremblay (2010) donne de nombreux

exemples de délinquants se regroupant et raffinant leurs techniques, notamment pour les vols de voitures. Il sera aussi intéressant, dans l'avenir, d'étudier la réaction des délinquants face à l'arrivée d'outils de surveillance comme BitCluster; on imagine qu'ils pourraient les utiliser pour mieux gérer leurs risques, avant que les services de sécurité ne l'utilisent pour identifier ces mêmes risques.

BitCluster n'est pas une panacée et il est avant tout utile pour suivre à la trace les délinquants moins sophistiqués qui ne maîtrisent pas parfaitement le fonctionnement du réseau P2P bitcoin. Il est facile de contourner le logiciel en utilisant un seul portefeuille comme source pour tous ses transferts, mais cette méthode est plus fastidieuse quand des centaines ou des milliers de portefeuilles doivent être vidés. Il n'existe pas de raccourci aux questions de sécurité dans le cas des bitcoins, mais dans l'avenir, on verra sûrement des délinquants être un peu moins efficaces pour mieux camoufler leurs activités. Il y a fort à parier que bon nombre d'entre eux ne seront pas prêts à faire ce sacrifice. Il sera aussi intéressant de continuer à suivre l'évolution d'autres monnaies numériques et cryptomonnaies qui attireraient moins l'attention que le populaire Bitcoin et qui permettraient aux escrocs de soustraire à une surveillance de plus en plus intense. Nous avons vu que la réglementation du bitcoin et son statut légal sont encore bien flous. Une décision sur le statut d'autres cryptomonnaies de plus petite envergure pourrait prendre encore plus de temps.

À terme, BitCluster devrait être en mesure de surveiller un plus grand nombre de cryptomonnaies et surtout d'offrir des analyses automatisées des flux de transactions. Cela permettrait au logiciel d'identifier un nœud représentant un casino en ligne, un site de vente de drogues illicites ou encore un *tumbler*. Pour ce faire, on devra étudier les patrons de transactions entrantes et sortantes pour chaque type d'acteur et leurs tendances lourdes. Nous aurons alors une bien meilleure

connaissance de la nature des acteurs du réseau P2P bitcoin et de l'évolution de cette monnaie qui, à bien des égards, a transformé le phénomène criminel moderne.

References

BORRONI, A. (2016). « Bitcoins: Regulatory Patterns. » *Banking & Finance Law Review*, vol. 32, nº 1, 47-68.

COIN MARKET CAP. (2017). « Crypto-Currency Market Capitalizations. » [En ligne] https://coinmarketcap.com/ (consulté le 11 février 2017).

EUROPEAN CENTRAL BANK. (2012). « Virtual Currency Schemes. » [En ligne] https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (consulté le 11 février 2017).

FLEDER, M., KESTER, M. S., et PILLAI, S. (2015). « Bitcoin Transaction Graph Analysis. » [En ligne] https://arxiv.org/pdf/1502.01657.pdf (consulté le 11 février 2017).

KRUITHOF, K., ALDRIDGE, J., HÉTU, D. D., SIM, M., DUJSO, E., et HOORENS, S. (2016). « The Role Of The 'Dark Web' In The Trade Of Illicit Drugs. » [En ligne] http://www.rand.org/pubs/research_briefs/RB9925.html (consulté le 11 février 2017).

LAVOIE, M., et DÉCARY-HÉTU, D. (2016). « BitCluster. » [En ligne] http://www.bit-cluster.com (consulté le 11 février 2017).

SPAGNUOLO, M., MAGGI, F., et ZANERO, S. (2014). « Bitiodine: Extracting Intelligence From The Bitcoin Network. » *International Conference On Financial Cryptography And Data Security*, Bridgetown, Barbades.

TANAKA, T. (1996). « Possible Economic Consequences Of Digital Cash. » *First Monday*, vol. 1, nº 2.

TREMBLAY, P. (2010). *Le délinquant idéal. Performance, discipline, solidarité*. Montréal, Canada: Liber.

U.S. DEPARTMENT OF JUSTICE. (2013). « Co-founder of Liberty Reserve Pleads Guilty to Money Laundering in Manhattan Federal Court. » [En ligne] https://www.justice.gov/opa/pr/co-founder-liberty-reserve-pleads-guilty-money-laundering-manhattan-federal-court (consulté le 11 février 2017).

WANG, Y., et MAINWARING, S. D. (2008). « Human-Currency Interaction: Learning From Virtual Currency Use In China. » *Proceedings Of The SIGCHI Conference On Human Factors In Computing Systems*, Florence, Italie.