Revue internationale de **CRIMINOLOGIE** et de **POLICE** technique et scientifique

ISSN 1424-4683
Volume LXIII

Table des matières

Avril - Juin
2010

Revue internationale de **CRIMINOLOGIE** et de **POLICE** technique et scientifique

ISSN 1424-4683
Volume LXIII

Table of contents

April - June
2010

Les multiples facettes du vol d'identité*

par **Benoît DUPONT**** et **Esma AÏMEUR*****

Résumé
Le vol d'identité est communément présenté depuis quelques années comme l'un des crimes connaissant la plus forte croissance en Amérique du Nord, tout en constituant également une préoccupation émergente dans de nombreux autres pays. Pourtant, les connaissances dont on dispose sur le sujet restent extrêmement parcellaires, voire anecdotiques. Cet article se propose donc d'examiner de manière plus systématique les conditions techniques et criminologiques du vol d'identité. Dans une première partie, nous examinons les différentes méthodes utilisées par les délinquants afin d'acquérir des identifiants personnels, des plus rudimentaires aux plus sophistiquées. Dans une seconde partie, nous utilisons les résultats de deux projets de recherche portant sur des victimes et des auteurs pour analyser l'ampleur du problème, notamment dans ses dimensions sociologique et criminologique.

Mots-clés: vol d'identité, cybercriminalité, victimes, auteurs, Canada, États-Unis

Summary
Identity theft is often described as the fastest growing crime in North America, and it is becoming an emerging concern in many other countries. However, our knowledge about this phenomenon remains extremely fragmented, and even anecdotal in many instances. This article seeks to examine more systematically the technological and criminological features of identity theft. In the first section, we examine different strategies used by offenders to acquire personal information, from the most rudimentary to the most sophisticated. In the second section, we analyse the results of two research projects on victims and offenders in order to assess the extent of the problem, particularly in its sociological and criminological dimensions.

Keywords: identity theft, cybercrime, victims, offenders, Canada, United States

Le vol d'identité est communément présenté depuis quelques années comme l'un des crimes connaissant la plus forte croissance en Amérique du Nord (Finklea, 2009). Aux États-Unis, les plus récentes statistiques font état de 9,9 millions d'adultes ayant été victimes d'un vol d'identité au cours de l'année 2008, ce qui représente 4,3% de la population adulte (Monahan et Kim, 2009). Au Canada, 6,7% de la population adulte aurait été victime d'une telle fraude en 2008 (Sproule et Archer, 2008), ce qui représente environ 1,7 millions de personnes. Malgré le

* Les recherches présentées dans cet article ont été rendues possibles grâce au soutien financier du Ministère de la Sécurité Publique du Québec, du Fonds Québécois de Recherche sur la Société et la Culture et du Conseil de Recherches en Sciences Humaines du Canada.

** Professeur agrégé, Titulaire de la Chaire de recherche du Canada en sécurité, identité et technologie, Centre International de Criminologie Comparée, Université de Montréal.

*** Professeure titulaire, Co-directrice de la Maîtrise en commerce électronique, Département d'Informatique et de Recherche Opérationnelle, Université de Montréal.

volume significatif de cette criminalité émergente, les connaissances dont nous disposons sur le sujet restent encore relativement parcellaires. Si les comptes rendus factuels, voire anecdotiques, prolifèrent dans les médias généralistes à la rubrique des faits divers, les quelques études scientifiques menées à ce jour prennent exclusivement la forme de sondages de victimisation (Baum, 2006; ISIQ, 2007; Synovate, 2007; Dupont, 2008; ITRC, 2008; Sproule et Archer, 2008; Monahan et Kim, 2009) qui permettent de mesurer la prévalence de cette forme de crime, les caractéristiques de ses victimes et l'ampleur des préjudices subis. Cependant, ces sondages nous renseignent mal sur les délinquants eux-mêmes ou les stratégies qu'ils mettent en œuvre.

Cette difficulté éprouvée par les chercheurs dans l'appropriation de cet objet trouve son origine dans plusieurs causes. La première concerne les fortes variations pouvant être observées concernant l'ampleur du problème d'un pays à l'autre. Il semble en effet que l'Amérique du Nord et l'Angleterre, où l'accès au crédit semble répondre à des logiques marchandes très agressives et modérément régulées, soient bien plus exposées à ce phénomène que l'Europe continentale ou l'Asie (van der Meulen, 2006). Cela a pour effet de donner lieu à des définitions juridiques et techniques très différentes de ce qui constitue —ou pas— un vol d'identité (1). Ainsi, le vol d'identité est explicitement criminalisé dans certains pays (notamment les États-Unis), alors que des projets de loi sont à l'étude dans d'autres juridictions (France et Canada par exemple), ou qu'un troisième groupe de nations, dont la plupart des pays européens, préfère s'en remettre à des qualifications pénales déjà existantes. Les diverses définitions du vol d'identité caractérisent également ce dernier de manière plus ou moins large, certaines y incluant l'appropriation frauduleuse d'instruments financiers comme le numéro de carte de crédit ou d'outils de communication comme l'adresse de courrier électronique et l'identifiant permettant d'accéder à des sites Internet de réseaux sociaux ou de jeux en ligne. Dans un souci d'harmonisation, on adoptera donc comme définition de travail celle proposée par l'OCDE, selon laquelle «un vol d'identité se produit quand une tierce partie acquiert, transfère, possède ou utilise les informations personnelles d'une personne physique ou morale sans autorisation, avec l'intention de commettre, ou en lien avec une fraude ou d'autres crimes» (Acoca, 2008, 12).

Cette définition relativement générale possède l'immense avantage de refléter la grande diversité des stratagèmes employés par les délinquants. On distingue dans la littérature trois grandes étapes du vol d'identité (Sproule et Archer, 2007). Dans un premier temps, l'acquisition d'identifiants appartenant à des personnes vivantes ou décédées peut aussi bien prendre la forme d'un banal vol de sac à main ou de portefeuille que le piratage informatique d'une base de données protégée par des systèmes de sécurité devant être déjoués par des individus disposant d'une expertise et d'un équipement spécifique, comme ce fut le cas dans l'affaire TJX (magasins Winners et HomeSense). Dans un deuxième temps, les identifiants volés vont être soit revendus sur des marchés clandestins en ligne où la loi de l'offre et de la demande va permettre d'en déterminer la valeur d'usage (pour les fraudeurs), soit être modifiés afin de créer des identités synthétiques, c'est-à-dire des identités qui ne correspondent pas à des personnes réelles mais qui sont

néanmoins crédibles aux yeux des institutions fraudées. La troisième et dernière étape comprend la fraude proprement dite, puisque dans de nombreuses juridictions, la possession d'éléments d'identification personnelle appartenant à des tiers ne représente pas une infraction à la loi. Cette fraude pourra avoir des objectifs pécuniaires, mais elle pourra aussi faciliter des crimes connexes liés à l'immigration clandestine, au terrorisme ou permettre au fraudeur de se soustraire à la justice en assumant l'identité d'une personne sans casier judiciaire. Ces trois étapes font appel à des connaissances techniques qui varient de manière significative selon le mode d'acquisition, de conversion ou de fraude privilégié par les délinquants, qui n'hésitent d'ailleurs pas à opérer selon les principes de division du travail bien connus des économistes.

Cet article sera donc organisé en deux grandes parties. Dans une première section, nous examinerons les différentes méthodes utilisées par les délinquants afin d'acquérir des identifiants personnels, des plus rudimentaires au plus sophistiquées, en mettant l'accent sur les dispositifs technologiques qu'ils mobilisent. Dans une seconde partie, nous utilisons les résultats de deux projets de recherche portant sur les victimes et les auteurs pour analyser l'ampleur du problème, notamment dans ses dimensions sociologique et criminologique.

1. Les moyens technologiques du vol d'identité

Dans cette section, nous examinons tout d'abord l'aspect non automatique des stratégies qu'utilisent les voleurs d'identité pour récolter l'information. Ensuite, nous passons en revue les moyens technologiques (automatiques) les plus répandus. Lorsque des personnes surfent sur le Web, effectuent des achats ou des opérations bancaires en ligne, communiquent à l'aide de la messagerie électronique ou instantanée, ou encore visitent des sites de jeux sur Internet, elles s'exposent parfois à de grands risques dont la violation de leur vie privée (Aïmeur *et al.,* 2008; Ghernaouti-Hélie, 2008). Les logiciels malveillants (*malwares*), parmi lesquels les virus, les *spywares*, les chevaux de Troie, les *botnets*, etc., constituent des armes technologiques de plus en plus prisées par les cybercriminels. De ce fait, le vol d'identité est devenu une véritable pandémie. Tout le monde est concerné, le particulier comme l'entreprise.

Rappelons que les informations recherchées sont de nature très variées. En effet, le voleur d'identité peut vouloir obtenir des *informations d'identification* (nom, prénom, âge, sexe, adresse, numéro de téléphone, nom de jeune fille de la mère, numéro d'assurance sociale [NAS], numéro d'identification personnel [NIP], revenu, emploi, situation familiale, lieux de résidence, code utilisateur, pseudonyme, etc.), des *habitudes de consommation* (magasins fréquentés, relevés de compte, actifs, obligations, etc.), des *habitudes de navigation* (sites web visités, fréquences des visites, nom des forums, amis sur le net, etc.), des *habitudes de vie* (loisirs, relations, moyens de déplacement, périodes de congés, etc.), ou encore des *données sensibles* concernant la carrière, l'employeur, le dossier médical, ou encore le casier judiciaire.

1.1 L'analyse des rebuts

Les poubelles sont de véritables mines de renseignements. Les futures victimes jettent dans leur corbeille les papiers, brouillons, post-it (quelques fois celui sur lequel est inscrit un mot de passe!), factures, dossiers, etc. Pourtant, ces corbeilles sont vidées dans des poubelles beaucoup plus grandes qui se retrouvent sur les trottoirs à la disposition de personnes potentiellement malveillantes.

1.2 Le vol de courrier

Dans la même lignée, le vol de courrier permet à une personne malveillante de détourner des informations personnelles transmises par voie postale. Il est entre autres possible de voler des factures avant même qu'elles ne soient reçues par la victime, et rien n'empêche le voleur de remettre la lettre en circulation une fois les informations récoltées, ce qui retardera la détection de la fraude par la victime. Parfois, malgré les contrôles d'identité, une personne malveillante peut enregistrer au bureau de poste un changement d'adresse (fictif, bien sûr), suite à quoi tout le courrier de sa victime lui parviendra automatiquement!

1.3 L'ingénierie sociale (social engineering)

Il s'agit d'une forme d'escroquerie utilisée en informatique pour soutirer d'une personne, à son insu, un bien ou une information. Cette pratique exploite l'aspect humain et social de la structure à laquelle est lié le système informatique visé. Le délinquant abuse de la confiance, de l'ignorance ou de la crédulité de personnes possédant les informations qu'il tente d'obtenir.

Parmi les personnes particulièrement sujettes à risque, nous citerons les employés d'une entreprise dont les indiscrétions peuvent porter préjudice, les employés temporaires qui ne sont pas au fait des mesures de sécurité de l'organisation, les personnes âgées qui ont peu de connaissances en matière de nouvelles technologies, les administrateurs de systèmes qui abusent de leurs pouvoirs, d'anciens employés qui veulent se venger, etc.

Les lieux les plus exposés sont les salles de réception d'hôtels, les salons d'affaires, les restaurants, les cafés, et les moyens de transport comme les trains ou les avions. Mentionnons aussi les discussions à haute voix au téléphone ainsi que les discussions animées entre professionnels dans un lieu public où une tierce personne pourrait prêter l'oreille (écoute passive).

L'amitié se nourrit de confidences, et celles-ci ne manquent pas au sein des communautés que forment les plates-formes Web 2.0. Les utilisateurs des forums, des messageries instantanées (MSN, Skype, etc.) et réseaux sociaux (Facebook, Myspace, linkedIn, etc.) ont souvent accès à des configurations permettant de décider qui peut avoir accès à leurs informations: cela peut être leurs amis ou les amis de leurs amis ou encore tout le réseau. Or, il arrive souvent que les utilisateurs paramètrent mal leurs options de confidentialité, mettant ainsi en danger à la fois leurs identités et celles de leurs «entourage numérique».

Prenons le cas d'Adam Morrison, étudiant, qui a créé son profil sur le site Facebook. À son insu, sa photographie et son identité ont été détournées par un «faussaire» pour créer un second «faux compte» au nom de… Adam Morrison. Le

vrai Morrison s'est rendu compte de la supercherie quand des policiers se sont présentés chez lui pour lui demander pourquoi il avait écrit sur Facebook qu'il voulait tuer un grand nombre de personnes, rappelant ainsi les événements de la tuerie de l'école Columbine. L'affaire est rentrée dans l'ordre pour l'étudiant, après que la police ait effectué des vérifications sur son ordinateur (CBC News, 2007).

Par ailleurs, en mai 2008, des informaticiens de la chaîne BBC en Grande-Bretagne ont pénétré dans le profil de quatre individus par le biais de leurs applications (API). Ce sont des applications qui tournent sur des serveurs n'appartenant pas à Facebook et les usagers peuvent en installer autant qu'ils veulent et inviter leurs amis à en faire de même. En moins de trois heures, l'application de fouille de données «Miner» créée par les techniciens de la BBC a permis de récolter noms, dates de naissance, lieux de résidence, lieux d'étude, centres d'intérêts, photos ainsi que les noms de leurs employeurs. De quoi faire le bonheur des voleurs d'identité (Kelly, 2008)!

1.4. Les logiciels malveillants (malware)

Les logiciels malveillants se présentent sous plusieurs formes et se propagent par divers moyens, que leurs concepteurs rendent de plus en plus difficiles à détecter. Certains vont s'introduire par les périphériques externes comme une clé USB ou un DVD infecté, d'autres vont s'acharner à exploiter des erreurs dans les logiciels de Microsoft, Adobe ou de toute compagnie disposant d'une certaine renommée et de parts de marché conséquentes.

Ils ont tous en commun une chose: une fois installés, il est difficile de déloger ces applications indésirables. Toutefois, les *malware* n'ont pas tous le même objectif. Certains ont pour seul but de détruire le plus de fichiers possible, d'autres ne servent qu'à créer un point d'entrée pour qu'une personne mal intentionnée prenne le contrôle de l'ordinateur infecté. Les plus insidieux épient et récoltent des informations sur leurs victimes, leurs habitudes et leurs informations d'authentification.

1.4.1. Les virus

Un virus est écrit dans le but de se propager vers d'autres ordinateurs, infectant au passage des programmes légitimes lui servant «d'hôtes». Le virus est la forme la plus simple de logiciel malveillant. Tentant de minimiser son impact sur le système, le virus est un redoutable combattant. Les compagnies se spécialisant dans l'éradication de ce fléau livrent une bataille continuelle contre les concepteurs de ces codes malicieux. La résultante concrète de ce combat est la nécessité pour les utilisateurs de constamment mettre à jour les logiciels antivirus installés sur leurs machines, à défaut de quoi les informations personnelles qui y sont stockées sont exposées à des risques importants.

1.4.2. Les vers

Un ver, contrairement à un virus, n'a pas besoin d'un programme hôte pour se reproduire. Les vers sont souvent conçus pour créer des réseaux permettant de multiplier le potentiel destructif des attaques menées par les pirates. Le but des

vers peut être d'espionner, d'offrir un point d'accès caché, de détruire des données, de faire des dégâts, ou même d'envoyer de multiples requêtes vers un site Internet dans le but de le saturer. On note souvent un ralentissement de la machine infectée, ou même un ralentissement du réseau. Le ver tente également souvent de se protéger en causant des dénis de services lorsqu'on tente de l'éradiquer.

1.4.3 Les chevaux de Troie

Le cheval de Troie dissimulé dans un programme ou un fichier permet de détourner, diffuser ou détruire des informations, ou encore d'ouvrir une porte dérobée qui permettra à un attaquant de tenter de prendre à distance le contrôle d'un ordinateur. Pour éviter la détection, un cheval de Troie ne contient jamais de code malicieux. Il va s'installer et récupérer le code malicieux depuis un serveur externe, en utilisant parfois des ports réseaux différents du port 80 (le port http standard, par lequel transitent les données Web). Les chevaux de Troie ne se propagent pas d'eux-mêmes, et ont besoin d'une intervention de l'utilisateur pour s'exécuter. Les logiciels de partage de fichiers (comme LimeWire) sont traditionnellement la principale source de diffusion des chevaux de Troie, car les utilisateurs malicieux peuvent facilement propager leurs logiciels en les faisant passer par exemple pour le tube du moment. Dans un logiciel, une porte dérobée (*backdoor*) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel. En sécurité informatique, la porte dérobée peut être considérée comme un type de cheval de Troie.

1.4.4. Les logiciels espions ou spyware

Un logiciel espion, mouchard ou espiogiciel, est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, sans que l'utilisateur n'en ait connaissance. L'installation d'un spyware requiert souvent l'approbation de l'utilisateur, que le hacker obtient en utilisant un subterfuge bien ficelé. Souvent, il s'installe de pair avec un outil simple, comme les «applications de fond d'écrans» ou les «applications d'icônes souriants» (emoticons).

Une première catégorie extrêmement dangereuse du spyware concerne les enregistreurs de frappes clavier ou *keyloggers*. Ce sont des logiciels espions qui peuvent enregistrer en arrière-plan les touches frappées sur le clavier et les transmettre aux pirates. Par exemple, certains enregistreurs de frappes analysent les sites visités et enregistrent les codes secrets et mots de passe lors de la saisie. D'autres sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts retraçant ainsi toute l'activité de l'ordinateur.

Les *screenloggers* sont une variante des *keyloggers*: ils permettent en plus des données du clavier et de la souris d'enregistrer des captures d'écran, en associant ainsi un clic clavier ou souris à un écran particulier. Ce type de logiciel permet ainsi de contourner les systèmes de sécurité utilisés par certains sites web, où les utilisateurs sont amenés à s'authentifier sur un clavier numérique à l'écran (IronPort, 2008).

1.5. Le pourriel ou spam

Le pourriel désigne une communication électronique, notamment du courrier électronique, non sollicitée par les destinataires, expédiée en masse à des fins publicitaires ou malhonnêtes. Les spammeurs ont d'abord réalisé des profits sur la vente de divers produits (compléments à base de plante, prêts hypothécaires, placements boursiers douteux, …), avant de se rabattre sur des activités criminelles (fraudes aux cartes de crédits, vente illicite de médicaments etc.). Ces profits sont ensuite réinvestis dans de nouvelles technologies et infrastructures de diffusion de spam et fournissent de généreux dividendes aux opérateurs de ces systèmes.

1.6. L'hameçonnage ou phishing

L'hameçonnage**,** appelé en anglais *phishing*, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels: mot de passe, numéro de carte de crédit, date de naissance, etc. L'hameçonnage peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Le terme *phishing* s'inspire du terme *phreaking*: mot-valise de «phone» et «freak». Originellement, le *phreaking* était un type d'arnaque utilisé afin de profiter de services téléphoniques gratuits surtout présents dans les années 1970, à l'époque des appareils analogiques. Le mot *phishing* aurait été inventé par les *pirates* qui essayaient de voler des comptes AOL, un des principaux fournisseurs d'accès à Internet à la fin des années 1990. Il serait construit sur l'expression anglaise *password harvesting fishing*, soit «pêche aux mots de passe». Un exemple classique est celui de l'attaquant qui se faisait passer pour un membre de l'équipe AOL et envoyait un message instantané à une victime potentielle. Ce message demandait à la victime d'indiquer son mot de passe, afin par exemple, de «vérifier son compte AOL» ou de «confirmer ses informations bancaires». Une fois que la victime avait révélé son mot de passe, l'attaquant pouvait accéder au compte et l'utiliser à des fins malveillantes, pouvant mener au vol d'identité

D'après une étude de l'Anti-Phishing Working Group (APWG) réalisée en 2007 (citée dans Acoca 2008), de nombreux sites de *phishing* hébergent également du malware. Ainsi, l'utilisateur se fait non seulement voler ses données confidentielles, mais il télécharge aussi à son insu des logiciels espions sur son poste de travail qui continueront à lui voler ses données.

Le terme *vishing* est une contraction de «voix sur IP» (VoIP) et de *phishing*. L'escroc met en place des serveurs VoIP qui composent des numéros de téléphone aléatoires. Un message enregistré incite celui qui répond à appeler un serveur local au numéro spécifié. S'il appelle, on lui demande, sous prétexte de l'identifier, de saisir des données personnelles (comme un numéro de carte bancaire) sur le clavier de son téléphone. Il existe de nombreux cas répertoriés de vishing par l'envoi de SMS (Constantin, 2009).

Le *pharming* est une technique de piratage informatique exploitant des vulnérabilités dans la façon dont les ordinateurs communiquent sur Internet pour récupérer les données d'une victime. Pour réaliser cette attaque, les pirates doivent préalablement modifier la correspondance entre le nom de domaine (comme paypal.ca) et l'adresse IP, représentant le code pour rejoindre le serveur en charge de répondre à l'utilisateur s'adressant à paypal.ca. Le hacker peut s'y prendre au moyen d'un virus, ou d'une autre attaque. Ainsi, par exemple http://www.paypal.ca ne pointera plus vers l'adresse IP du serveur de l'entreprise de paiement en ligne, mais vers un autre serveur frauduleux qui va présenter la même page que l'original. L'utilisateur ne sera pas conscient du détournement, puisque c'est son système d'exploitation qui est en charge de la correspondance, et entrera ses informations d'authentification dans la page. La plupart de ces serveurs vont même jusqu'à rediriger ensuite leurs victimes vers le bon service, pour masquer leurs traces et ne pas alerter ces dernières.

Le *phishing* est favorisé par l'existence sur Internet de nombreux «kits de phishing», prêts à l'emploi et faciles à trouver, qui contiennent des outils facilitant considérablement la vie d'apprentis pirates ayant peu de connaissances techniques et souhaitant lancer ces attaques. Ces kits peuvent contenir un logiciel complet de développement de site Internet afin de créer le faux site ressemblant à un site légitime. Le *Universal Man-in-the-Middle Phishing Kit* (Wilson, 2007) est un de ces outils. Il permet de configurer facilement les paramètres de l'attaque, et récolte les données dynamiquement. Les fraudeurs offrent même une période d'essai avant l'achat! Ce *phishing kit* se monnaie en deçà de 800 euros.

Les réseaux d'ordinateurs zombies (ou «Botnets») constituent la forme la plus élaborée de logiciels malveillants. En sécurité informatique, un ordinateur zombie est une machine sur laquelle est installé un code malicieux à l'insu de l'utilisateur, mais qui ne commet pas encore d'action malveillante. A l'issue de l'installation, le pirate peut dès lors demander à distance au poste infecté de réaliser une attaque. Le poste infecté devient un véritable zombie aux ordres du pirate et ce, à l'insu de son propriétaire. Un zombie est souvent infecté à l'origine par un ver ou un cheval de Troie. Un *botnet* est par extension un ensemble de machines zombies reliées entre elles. Il s'agit d'une des menaces les plus sérieuses pour la sécurité des systèmes d'information. Comme les zombies sont très nombreux et disséminés dans divers pays, il devient difficile de localiser l'initiateur de l'attaque. Le parc total de machines zombies sur Internet est aujourd'hui estimé à plusieurs millions d'ordinateurs, même si les méthodologies utilisées pour mesurer le nombre de machines compromises restent sujettes à de nombreuses critiques (Stone-Gross et al., 2009). Les botnets sont souvent utilisés pour contourner les listes noires et envoyer de nouveaux *spams* qui sont utilisés à des fins de *phishing* menant ainsi au vol d'identité. D'autres opérateurs de *botnets* ont implanté dans les ordinateurs zombies qu'ils contrôlent des *keyloggers* afin de s'emparer des informations bancaires de leurs victimes. Par exemple, un *botnet* nommé Clampi (Derest, 2009) associé à plus de 4500 sites et spécialisé dans le vol de données financières a été détecté en 2006. Par ailleurs, le réseau *Storm* a touché 40 millions de PC à travers le monde entre janvier 2007 et février 2008. Les zombies du réseau Storm sont

organisés de façon décentralisée, et se connectent entre eux en mode peer-to-peer, rendant inefficace les mesures de protection des éditeurs de sécurité (par exemple *blacklister* les attaquants, concept permettant de repérer et de bloquer les adresses des serveurs de commande de zombies). Quant au réseau de zombies *Kraken*, il comprend des postes appartenant à au moins 50 des 500 entreprises les plus riches au monde, montrant par là que l'infection en tant que zombie ne concerne pas que les postes du grand public mais aussi ceux des entreprises les plus aguerries en termes de sécurité informatique.

1.7. Les vecteurs de diffusion des menaces

Durant de nombreuses années, les codes malicieux se sont infiltrés via l'e-mail. De nos jours, l'infection se fait via le Web car elle est souvent plus facile. En effet, lorsqu'un utilisateur reçoit un spam ou un virus via sa messagerie électronique, il s'en rend parfaitement compte (même si c'est trop tard dans le cas où il exécute un virus). Dans le cadre du Web, l'utilisateur ne sait pas que son poste a été infecté, ce qui rend d'autant plus dangereux ce type d'infection.

Examinons trois exemples:

Les attaques *piggyback*: un logiciel malveillant embarqué dans une application non malveillante. Par exemple, un utilisateur télécharge une vidéo sur Internet qui, au moment de la lire, lui demande de downloader un codec («compression-décompression»), logiciel permettant de comprendre un des différents formats de fichiers. L'utilisateur télécharge alors et installe le codec. La vidéo fonctionne, mais l'utilisateur a sans le savoir également téléchargé et installé un logiciel espion.

Par ailleurs, une autre forme courante d'infection via le web est le clic d'un utilisateur sur une publicité ou une fenêtre pop-up, qui entraîne le téléchargement du logiciel malveillant. Le pirate va pousser l'utilisateur à cliquer sur ce pop-up, en lui proposant une offre alléchante ou encore de cliquer pour effectuer un scan anti-spyware, alors même que ce clic va déclencher le téléchargement du dit spyware!

Le téléchargement automatique par exploitation d'une vulnérabilité du navigateur Web *drive-by download.* Ce type de téléchargement se fait sans que l'utilisateur ne voie quoi que ce soit, et sans même qu'il ne clique sur une quelconque fenêtre. Le logiciel malveillant hébergé sur une page Internet va tout simplement exploiter une vulnérabilité du navigateur Web pour s'installer tout seul sur le poste de l'utilisateur quand celui-ci consulte cette page.

Finalement, la convergence des technologies de localisation et de traitement des données numériques a donné naissance à la radio-identification, souvent identifiée par l'acronyme RFID (*radio frequency identification*). Depuis quelques années, on l'intègre à toutes les cartes et pièces d'identification pour faciliter le processus d'identification d'une personne. Toutefois, les radio-étiquettes, ces puces chargées de transmettre des informations par ondes radios, ne permettent pas pour l'heure de bloquer les requêtes d'informations de personnes malveillantes. En effet, la puce ne sait pas discriminer entre une requête légitime ou une requête abusive, et les puces peuvent être interrogées à distance par toute personne disposant de l'équipement requis. En août 2008 (Boggan, 2008), un

chercheur britannique a été capable de manipuler, cloner et insérer une puce modifiée à l'intérieur d'un faux passeport. Il n'a utilisé que trois items pour réussir cet exploit: un logiciel gratuit, un lecteur de carte RFID et deux puces RFID, le tout lui ayant coûté moins de 60 euros.

2. Quelques données empiriques sur le vol d'identité

Dans cette section, nous examinerons le vol d'identité dans sa dimension sociale, en mobilisant les résultats de deux projets de recherche portant sur les victimes et les auteurs pour essayer d'appréhender l'ampleur du phénomène, aussi bien en ce qui concerne le nombre des victimes que les préjudices subis. On analysera aussi les facteurs de risques individuels et collectifs, les techniques employées par les délinquants, ainsi que leurs compétences techniques, afin de mieux comprendre si l'on est effectivement confronté à une migration du crime organisé vers cette forme profitable de fraude, ou si on est au contraire confronté à un processus d'adaptation technologique de la part de délinquants tout à fait ordinaires.

Ces deux études ont été menées à l'aide de méthodologies très différentes qui méritent d'être détaillées. La première consiste en un sondage de victimisation réalisé au Québec en 2007 pour le compte du Ministère de la sécurité publique (Dupont, 2008). Ce sondage téléphonique fut administré à un échantillon de 1'100 répondants majeurs choisis au hasard et provenant de tout le Québec (2), ce qui correspond à une marge d'erreur de 2,95% pour un intervalle de confiance de 95%. Les questions du sondage portaient sur les types d'incidents de vol d'identité dont les répondants (et non leur famille ou leurs amis comme on peut le trouver dans d'autres sondages cherchant à enfler les statistiques) avaient été victimes au cours des 12 mois précédents l'enquête, les caractéristiques de ces incidents, le degré de satisfaction et de confiance à l'égard des organisations publiques et privées exerçant un contrôle sur ce phénomène, et le profil sociodémographique ainsi que les habitudes d'utilisation d'Internet des répondants. Par contraste, la seconde recherche (Dupont et Louis 2009), qui portait sur les auteurs de vols d'identité, dut s'appuyer sur une méthodologie plus créative. L'objectif était en effet de constituer une base de données d'affaires de vols d'identité traitées par la police et la justice à l'échelle de toute l'Amérique du Nord. Quelques rares études ont été consacrées aux voleurs d'identité (Allison et al., 2005; Copes et Vieraitis, 2007; Gordon et al., 2007), mais elles portent sur des échantillons réduits ou se limitent à des enquêtes menées par une organisation de référence, ce qui introduit un biais de sélection difficile à surmonter. Nous avons donc mis en œuvre un système de veille médiatique portant sur 4'500 sources d'informations mises à jour en continu qui a permis de recenser 195 affaires impliquant 422 délinquants sur une période de six mois (janvier à juin 2008). Ces affaires rapportées dans les médias ont fait l'objet d'une codification relative au profil sociodémographique des délinquants, à leurs motifs, à leur mode opératoire quant à l'acquisition et l'utilisation des identités dérobées, à leurs liens avec les victimes, ainsi qu'à la réponse judiciaire. Bien que cette recherche ne soit pas exempte de biais de sélection judiciaire

et médiatique (Dupont et Louis, 2009, 10), elle permet néanmoins par la taille de l'échantillon constitué de mener des analyses statistiques relativement pertinentes. Les données des deux projets de recherche ont été analysées à l'aide du logiciel statistique SPSS.

2.1 Les victimes

L'une des principales découvertes du sondage sur le vol d'identité concerne la signification encore incertaine attribuée au terme 'vol d'identité' par les répondants. En effet, deux stratégies destinées à mesurer l'ampleur du phénomène furent testées. Dans un premier temps, les répondants étaient invités à répondre à une question d'ordre général portant sur leur victimisation en matière de vol d'identité, qui était défini comme «une fraude consistant à collecter et à utiliser des renseignements personnels à l'insu et sans l'autorisation de la victime, à des fins généralement criminelles». La proportion de répondants se déclarant victime de vol d'identité à l'issue de cette première question était de 2,5%. Dans un second temps, cinq vignettes correspondant aux cinq formes de vol d'identité que l'on retrouve le plus fréquemment dans la littérature furent présentées aux répondants (3), qui devaient ensuite préciser s'ils avaient été exposés à une telle fraude au cours des 12 derniers mois. Le nombre des victimes de ces cinq catégories plus spécifiées de vol d'identité atteignit 5,7% de l'échantillon, soit une différence de 3,2% avec la question formulée de manière générale. Plus de la moitié des victimes 'objectives' n'associent ainsi pas leur situation au vol d'identité, malgré le consensus des autorités et des institutions financières à ce sujet. Comme on le voit, les problèmes de définition ne se posent pas uniquement aux chercheurs en ce domaine, et les campagnes de prévention mises en œuvre par un nombre croissant d'institutions publiques et privées auraient tout intérêt à s'assurer que les pratiques recouvertes par le terme 'vol d'identité' sont clairement identifiées par les destinataires de ces campagnes, au risque de voir ces dernières manquer leur cible.

La forme la plus répandue de vol d'identité est sans conteste l'utilisation frauduleuse de cartes de paiement (3%), suivie de près des informations personnelles compromises sans utilisation frauduleuse (2,5%), du piratage des comptes bancaires (1%), de l'obtention de services non financiers (0,9%) et de l'obtention de facilités de crédit (0,8%). Le pourcentage de victimisation est calculé en fonction des cinq catégories de vols d'identité, ce qui explique la différence observée avec la victimisation individuelle. En effet, chaque victime fut associée à 1,4 incident au cours de l'année, ce qui laisse penser que certaines personnes sont surexposées aux risques de voir leur identité compromise. Projetés à l'échelle de la population québécoise, ces chiffres permettent ainsi de penser que le vol d'identité a touché environ 240'000 adultes en 2006-2007. À titre de comparaison, on constatera que le nombre de fraudes officiellement constatées la même année par les services de police québécois dépassait tout juste les 15'000 affaires, et que l'ensemble des infractions contre la propriété enregistrées au Québec pendant la période de référence s'élevait à 267'692 (Rioux, 2008, 66). Ce décalage s'explique notamment par le faible taux de déclaration des victimes auprès des forces de l'ordre. Parmi notre

échantillon, seulement 21,9% des victimes avaient jugé nécessaire d'alerter la police. Cette tendance à la sous-déclaration s'explique notamment par la politique de dédommagement des institutions financières, par les faibles montants impliqués, ainsi que par l'intérêt à tout le moins modéré manifesté par les services de police lorsque les fraudes n'atteignent pas une certaine importance. Il n'en demeure pas moins que la réticence des victimes à déclarer aux autorités le vol d'identité contribue à perpétuer le déficit de connaissances qui existe quant à ce dernier, et limite les opportunités de concevoir et de mettre en œuvre des stratégies de prévention et de lutte adaptées à la réalité.

Dans le cadre d'une catégorie de crimes aussi étroitement associée à l'usage de l'identité personnelle, on peut imaginer que certaines caractéristiques sociodémographiques présentent des facteurs de risques accrus en matière de victimisation. Ainsi, Anderson (2005) examine à l'aide de la littérature économique les risques et les mécanismes protecteurs anticipés associés aux niveaux d'éducation, aux revenus, à l'âge, au statut marital, à la taille du foyer, au genre ou encore à la race. Bien que la taille de l'échantillon de victimes soit assez réduite (n=63), nous avons néanmoins pu identifier une corrélation positive entre le niveau de revenus du foyer et les risques d'être exposé au vol d'identité. En effet, les Québécois dont les revenus bruts annuels sont supérieurs à 80'000 dollars sont surreprésentés parmi les victimes pour trois modes opératoires particuliers. Alors qu'ils ne représentent que 12,5% de l'échantillon, ces répondants à revenus élevés comptent pour 33,3% des victimes d'usage frauduleux de cartes de débit ou de crédit, pour 40% des victimes d'obtention frauduleuse de services (hydro, télécoms…), et pour 48,1% des personnes convaincues que leurs données personnelles ont été acquises frauduleusement, sans qu'un préjudice financier ait encore été constaté (Dupont 2008, 15). Ce lien ne semble pas limité au Québec, puisque des corrélations similaires ont été observées aux États-Unis (Anderson, 2005, 20; Baum, 2006, 2) et au Royaume-Uni (Wagner, 2007, 4). Il est difficile de savoir si l'influence du niveau de revenu concerne l'accès plus facile à des cartes de crédit, entraînant un nombre de transactions plus élevées et donc une plus grande exposition statistique aux risques, ou si ce sont les délinquants qui ciblent en priorité les victimes les plus rentables, celles-ci disposant en effet de cartes de prestige (or et platine) dont le marquage est aisément identifiable.

En effet, seulement la moitié des victimes (n= 33) sont en mesure d'indiquer selon quelle méthode (selon elles) les fraudeurs ont eu accès à leurs données personnelles. Bien que ces statistiques ne puissent prétendre être représentatives, la technique d'acquisition employée serait le clonage de carte dans 39,4% des cas, suivie d'employés corrompus au sein d'une organisation publique ou privée (15,2%), du vol ou du piratage d'une base de données (12,1%) et du vol ou de la perte d'un portefeuille ou d'un sac à main (9,1%). L'hameçonnage ne représente que 3% des cas, cette sous-représentation pouvant s'expliquer par la nature relativement peu discriminante, et donc peu efficace, de cette méthode (où les clients de la banque A reçoivent fréquemment des courriers électroniques frauduleux prétendant provenir de la banque B ou C), et par le facteur de protection que représente la langue française. La forte médiatisation de cette fraude pourrait également

avoir produit des effets préventifs. La prépondérance du clonage de carte expliquerait alors le faible montant du préjudice financier déclaré par les victimes, puisque celui-ci était inférieur à 100$ (environ 65 euros) pour plus de la moitié d'entre elles (58,7%). Seulement 6,3% des victimes ont perdu plus de 5'000$, ce qui correspond aux résultats de 5% observés aux États-Unis sur un échantillon beaucoup plus conséquent de 77'000 foyers (Baum, 2006, 5). En effet, les institutions bancaires, qui représentent les principales victimes institutionnelles du vol d'identité par clonage de carte déploient des systèmes informatisés de lutte contre la fraude capables de détecter cette dernière dans des délais relativement courts, parfois même avant que la victime elle-même en ait pris conscience. Ces logiciels exploitent les méthodes de forage des données (datamining) afin d'analyser les transactions financières menées et d'identifier les anomalies ou les opérations suspectes. Ce profilage, souvent mené en temps réel, reste encore rudimentaire en raison des compromis devant être faits entre la vitesse de calcul liée aux opérations d'achat et de retrait d'espèces et la complexité des algorithmes mis en œuvre (Edge et Falcone Sampaio, 2009, 385). Cependant, dans le contexte bancaire canadien où six grandes institutions se partagent le marché des particuliers, la mise en œuvre de telles solutions anti-fraude serait en mesure, sinon de stopper les transactions suspectes, du moins d'en limiter la répétition et donc de restreindre les montants associés aux fraudes.

Enfin, concernant les préjudices financiers, si plus de la moitié des victimes (57,1%) ont obtenu de leur banque un remboursement intégral, un nombre non négligeable (39,7%) a dû assumer de sa poche l'intégralité des pertes encourues. La majeure partie de ces non-remboursements (68%) correspond toutefois à des pertes inférieures à 100$, ce qui pourrait s'expliquer par l'application d'une franchise. Néanmoins, on voit bien ici que la générosité alléguée des banques en la matière a ses limites, et que celles-ci appliquent à leurs clients victimes de fraudes des régimes de protection de plus en plus restrictifs.

Si les chiffres qui précèdent nous permettent de mieux saisir l'ampleur du phénomène dans une société moderne avancée telle que le Québec, leur contribution reste limitée en ce qui concerne les phases antérieures à la découverte de la fraude, à savoir l'acquisition des données personnelles et leur utilisation, ainsi que l'identité des fraudeurs eux-mêmes. Nous abordons ces diverses questions dans la section suivante.

2.2 Les auteurs

Le profil des 422 personnes mises en cause dans des affaires de vols d'identité qui constituent notre échantillon se distingue d'abord par sa forte diversité interne. On retrouve par exemple une forte proportion de femmes, qui représentent 38,9% des délinquants étudiés, ce qui est nettement plus élevé que dans la plupart des crimes. Cette quasi-parité trouve certainement son origine dans le fait que le vol d'identité repose sur des méthodes qui, à quelques rares exceptions près, ne font pas appel à la violence, et qui de surcroît peuvent aisément être mises en œuvre de manière isolée, ce qui élimine le besoin d'appartenir à des réseaux délinquants en grande majorité masculins. Les voleurs d'identité se répartissent également de

manière relativement équilibrée sur la pyramide des âges, avec une moyenne de 33 ans et un 'doyen' de 67 ans. Toutefois, l'absence de mineurs dans l'échantillon (en raison des interdictions de publications qui protègent l'identité des jeunes délinquants) fausse certainement les résultats, et nous empêche d'établir de manière définitive la proportion de ce type de crimes attribuable à cette tranche d'âge. Enfin, nous avons déjà souligné que la forte proportion de femmes pouvait être en partie attribuée à la possibilité d'agir individuellement, ce qui se confirme lorsqu'on constate que le délinquant a agi seul dans 64,6% des affaires, et que des groupes de trois personnes et plus ne sont observés que de 14% des dossiers. Cette prédilection pour l'action en solitaire vient quelque peu contredire le discours dominant sur le rôle actif joué par le crime organisé dans le vol d'identité, qu'il s'agisse de groupes locaux 'traditionnels' ou d'une menace plus diffuse provenant d'Europe de l'Est (Newman et McNally, 2005; Deloitte, 2008; Winterdyk et Thompson, 2008).

L'analyse quantitative des modes opératoires privilégiés par les voleurs d'identité permet également de mettre à mal quelques mythes, notamment ceux qui concernent leur sophistication technologique et leur exploitation intensive des vulnérabilités de l'Internet pour acquérir des données personnelles en quantité industrielle et les exploiter frauduleusement à l'échelle mondiale (voir à titre d'exemple Berinato, 2007; Symantec, 2008; Thibodeau, 2008). Le juriste américain Paul Ohm (2008) a proposé le terme de «mythe du super-utilisateur» pour désigner cette représentation du cyber-délinquant comme un être doté de compétences confinant à la magie et trop habile pour être arrêté par des forces de l'ordre impuissantes. L'examen des données recueillies reflète une réalité bien plus ordinaire.

À l'étape initiale de l'acquisition des données personnelles, la méthode la plus répandue est le vol physique (45,7%), qu'il s'agisse de vol à la tire de portefeuille ou de sac à main, de vol de courrier ou de vol dans les poubelles. L'utilisation frauduleuse d'un fichier informatique vient en seconde position (28,3%), mais il ne s'agit pas ici de piratage sophistiqué. Cette catégorie englobe plutôt des abus commis par des professionnels ayant accès à des informations privilégiées concernant leurs clients ou leurs patients, et qui utilisent ces informations pour commettre des fraudes. On retrouve ainsi dans l'échantillon de nombreux membres de la profession médicale, ainsi que des employés de concessions automobiles ou d'établissements financiers. L'acquisition de données personnelles par le biais d'Internet (hameçonnage, logiciel espion, piratage ou achat sur les marchés clandestins en ligne) ne représente finalement pas plus de 18,3% des affaires. Cela reste extrêmement faible, pour ne pas dire marginal, au regard de la très forte médiatisation des risques liés à la cyberdélinquance réalisée sous la pression de l'industrie de la sécurité informatique.

C'est à l'étape de la fraude que l'Internet joue un rôle prépondérant. En effet, même si le mode de fraude le plus répandu concerne l'achat de biens et de services en magasin à l'aide de cartes de paiement clonées ou de chèques falsifiés (27,3%), l'obtention de facilités de crédit en ligne (25%) et l'achat de biens et de services en ligne (20,3%) reflètent la prédilection des fraudeurs pour les transactions utilisant l'Internet comme intermédiaire. Encore faut-il souligner qu'il ne s'agit

pas pour eux d'exploiter les failles technologiques de sites de commerce ou de banque en ligne, mais plutôt de se prévaloir de systèmes de validation de l'identité moins rigoureux que ceux opérant dans le monde physique. Cette variation découle principalement des contraintes très particulières qui s'imposent aux entreprises menant des transactions en ligne, aussi bien en matière de facilité d'utilisation de leurs interfaces que de l'établissement d'une relation de confiance avec des clients potentiels (Sasse, 2004). En d'autres termes, les fraudeurs profitent des pratiques plus laxistes de sites Internet prêts à faire des compromis afin de vaincre les réticences de clients peu familiers avec le commerce en ligne, ainsi qu'à la fragmentation de l'infrastructure technique et financière caractérisant ce secteur d'activité.

Malgré leur faible sophistication technique, les voleurs d'identité ont été en mesure de dégager des profits non négligeables, puisque le montant médian par affaire est de 26'000 USD avec une fourchette allant de 500 à 50 millions USD. Au vu des efforts relativement modérés requis des fraudeurs et des risques également limités auxquels ils s'exposent, force est de constater que cette forme de délinquance permet d'obtenir des rendements très avantageux, ce qui explique certainement pourquoi on retrouve au sein de l'échantillon de nombreuses personnes salariées qui utilisent le vol d'identité comme complément de revenu afin de financer un mode de vie plus élevé que leur activité principale ne le leur permettrait. Cependant, les voleurs d'identité arrêtés et condamnés par la justice semblent payer le prix de ce contexte favorable, la peine moyenne prononcée s'élevant à 54 mois de prison pour un crime qui implique rarement le recours à la violence (minimum: 4 mois, maximum: 228 mois). Cette relative sévérité se veut selon toute probabilité dissuasive, cherchant notamment à combattre le sentiment d'impunité qui pourrait se développer parmi les délinquants en raison du faible taux de déclaration et du manque de ressources (et peut-être du désintérêt) des organisations policières. Par contre, des éléments anecdotiques laissent entrevoir que les délinquants impliqués dans les affaires plus complexes semblent obtenir plus facilement des peines assorties de sursis, peut-être en raison de leur meilleure capacité à négocier avec les autorités, ces dernières souhaitant connaître les détails de leurs modes opératoires plus innovants (Dupont et Louis, 2009, 15).

Conclusion

Au fur et à mesure que l'informatique et les technologies numériques s'immiscent dans la vie des utilisateurs et souvent à leur insu, les risques d'attaques et plus précisément ceux liés au vol d'identité se multiplient. Au quotidien, la technologie mobile (téléphones portables, iPhones, Blackberry, etc.), les étiquettes communicantes (RFID) et la domotique constituent de nouveaux terrains d'investigation pour les pirates. Pourtant, sans nier l'existence de ces délinquants à forte compétence technologique (ces innovateurs criminels si l'on veut), les analyses empiriques préliminaires des données portant sur le vol d'identité présentées dans cet article nous montrent qu'une forte proportion des délits commis s'appuient sur des

méthodes rudimentaires et relèvent d'une délinquance tout à fait traditionnelle. La disponibilité des informations personnelles dans les sociétés modernes avancées génère en effet de nouvelles structures d'opportunités qui semblent avoir été clairement identifiées par les délinquants, ces derniers n'hésitant pas à les exploiter de manière extrêmement profitable. Nous disposons encore à l'heure actuelle de peu de connaissances sur cette forme de délinquance et sur ceux qui s'y adonnent. La méthodologie de collecte des données que nous avons utilisée ici permet de lever en partie le voile sur les formes les plus désorganisées de vol d'identité. Néanmoins, des réseaux plus sophistiqués de fraudeurs devraient également faire l'objet de recherches plus approfondies, à l'instar du pirate informatique Alex Gonzalez, arrêté aux États-Unis en 2008 et accusé en août 2009 d'avoir volé à de grands détaillants et à des chaînes de restauration rapide plus de 130 millions de numéros de cartes de crédit revendus à des fraudeurs d'Europe de l'Est (Poulsen, 2008; Zetter, 2009).

Cette connaissance de l'ensemble de l'écosystème criminel et technologique dans lequel se déploie le vol d'identité est indispensable à la conception et à l'implantation de stratégies de prévention et de contrôle qui soient adaptées à la nature des risques existants. Comme nous avons enfin tenté de le démontrer ici, une telle connaissance ne pourra être constituée sans les efforts combinés de chercheurs appartenant à diverses traditions disciplinaires, qu'il s'agisse d'informaticiens, de criminologues, de juristes, d'économistes ou encore de psychologues. En effet, seule la complémentarité de leurs approches et de leurs méthodologies permettra d'appréhender de manière intégrée des problèmes aussi complexes, qui impliquent des systèmes techniques, humains et de gouvernance caractérisés par leurs interdépendances.

Références

Acoca, B., 2008, *Scoping paper on online identity theft*, OCDE, Paris.

Aïmeur, E., Brassard, G., Fernandez, J.M., Mani Onana, F.S., 2008, ALAMBIC: A Privacy-Preserving Recommender System for Electronic Commerce, *International Journal of Information Security*, vol. 7, no 5, 307-334.

Allison, S., Schuck, A., Lersch, K.M., 2005, Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice*, vol. 33, no. 1, 19-29.

Anderson, K.B., 2006, Who are the victims of identity theft? The effect of demographics, *Journal of Public Policy & Marketing*, vol. 25, no. 2, 160-171.

Baum, K., 2006, *Identity theft 2004: First estimates from the National crime victimization survey*. US Department of Justice Bureau of Justice Programs, Washington DC.

Berinato, S., 17 septembre 2007, Who's stealing your passwords? Global hackers create a new online crime economy. *CIO.com*, www.cio.com/article/135500, Consulté le 23 septembre 2009.

Boggan, S., 6 août 2008, 'Fakeproof' e-passport is cloned in minutes, *Times Online*, http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece, Consulté le 11 septembre 2009.

CBC News, 27 décembre 2007, UPEI student entangled in fraudulent Facebook threats, http://www.cbc.ca/canada/prince-edward-island/story/2007/12/24/pe-facebook.html,

Consulté le 11 septembre 2009.

Commérot, S., 2007, Les menaces actuelles d'Internet: Comment s'en protéger, *IronPort*, http://www.cisco.com/web/FR/documents/pdfs/events/cisco_expo2007/03_30_10_30_7_ironport_les_menaces_actuelles_d_internet.pdf, Consulté le 23 septembre 2009.

Constantin, L., 14 juillet 2009, Vishing Attacks Target Regional Banks and Credit Unions, *Softpedia*, http://news.softpedia.com/news/Vishing-Attacks-Target-Regional-Banks-and-Credit-Unions-116660.shtml, Consulté le 11 septembre 2009.

Copes, H., Vieraitis, L., 2007, *Identity theft: Assessing offenders' strategies and perceptions of risk*, University of Alabama, Birmingham.

Deloitte, 2008, *A report on cybercrime in Canada*, Canadian Association of Police Board, Ottawa.

Derest, V., 5 août 2009, Clampi, un cheval de Troie qui s'avère être un botnet de vol de données financières, *Reseaux-Telecoms.net,* http://securite.reseaux-telecoms.net/actualites/lire-clampi-un-cheval-de-troie-qui-s-avere-etre-un-botnet-de-vol-de-donnees-financieres-20642.html, Consulté le 11 septembre 2009.

Dupont, B., 2008, *Résultats du premier sondage sur le vol d'identité et la cybercriminalité au Québec*, Ministère de la Sécurité Publique, Québec.

Dupont, B., Louis, G. (2009). *Les voleurs d'identité: Profil d'une délinquance ordinaire*, Chaire de recherche du Canada en sécurité, identité et technologie http://www.mapageweb.umontreal.ca/dupontb/articlesandpapers/DupontLouisprofilvid.pdf, Consulté le 28 septembre 2009.

Edge, M.E., Falcone Sampaio, P.R., 2009, A survey of signature based methods for financial fraud detection, *Computers and Security*, vol. 28, no. 6, 381-394.

Finklea, K.M., 2009, *Identity theft: Trends and Issues*. Congressional Research Service, Washington.

Ghernaouti-Hélie, S., 2008, *Sécurité informatique et réseaux*, Dunod, Paris.

Gordon, G., Rebovitch, D., Choo, K., Gordon, J., 2007, *Identity fraud trends and patterns: building a data-based foundation for proactive enforcement*, Center for Identity Management and Information Protection, Uttica College.

Identity Theft Resource Center (ITRC), 2008, *Identity theft: The aftermath 2007*, ITRC, San Diego.

Institut pour la sécurité de l'information (ISIQ), 2007, *Sondage auprès des citoyens branchés*, CRIM, Montréal.

Kelly, S., 1er mai 2008, Identity 'at risk' on Facebook, *BBC News*

http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm, Consulté le 11 septembre 2009.

Monahan, M., Kim, R., 2009, *2009 Identity fraud survey report*, Javelin Strategy & Research, Pleasanton.

Newman, G., McNally, M., 2005, *Identity theft literature review*, National Criminal Justice Reference Service, Washington.

Ohm, P., 2008, The myth of the superuser: Fear, risk and harm online, *UC Davis Law Review*, vol. 41, no. 4, 1327-1402.

Poulsen, K., 5 août 2008, Feds Charge 11 in Breaches at TJ Maxx, OfficeMax, DSW, Others, *Wired*, http://www.wired.com/threatlevel/2008/08/11-charged-in-m/, Consulté le 11 septembre 2009.

Rioux, V., 2008, *Statistiques 2007 sur la criminalité au Québec*, Ministère de la Sécurité Publique, Québec.

Sasse, A., 2004, *Usability and trust in information systems*, Cyber trust and crime prevention project, Office of Science and Technology, Londres.

Sproule, S., Archer, N., 2007, *Defining identity theft*. Eight World Congress on the Management of eBusiness, 11-13 juillet, Toronto.

Sproule, S., Archer, N., 2008, *Measuring identity theft in Canada: 2008 consumer survey*, MeRC working paper no. 23, McMaster University, Hamilton.

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., et Vigna, G. (2009). *Your botnet is my botnet: Analysis of a botnet takeover*, University of California Santa Barbara Technical report, Santa Barbara.

Symantec, 2008, *Symantec report on the underground economy July 07 – June 08*, Symantec, Cupertino.

Synovate, 2007, *Federal Trade Commission: 2006 identity theft survey report*, Synovate, McLean.

Thibodeau, P., 8 août 2008, Credit card thieves ran a polite, professional help desk, *Computerworld*, http://www.networkworld.com/news/2008/080708-credit-card-thieves-ran-a.html, Consulté le 23 septembre 2009.

Van der Meulen, N., 2006, *The challenge of countering identity theft: Recent developments in the United States, the United Kingdom, and the European Union*, National Infrastructure Cyber Crime Program, La Haye.

Wagner, N., 2007, *Identity fraud profiles: Victims and offenders*, Eight World Congress on the Management of eBusiness, Toronto, 11-13 juillet.

Wilson, T., 12 janvier 2007, For Sale: Phishing Kit, *Dark Reading,* http://www.darkreading.com/security/management/showArticle.jhtml?articleID=208804288, Consulté le 11 septembre 2009.

Winterdyk, J., Thompson, N., 2008, Student and non-student perceptions and awareness of identity theft. *Revue canadienne de criminologie et de justice pénale*, vol. 50, no. 2, 153-186.

Zetter, K., 17 août 2009, TJX Hacker Charged With Heartland, Hannaford Breaches, *Wired*, http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/, Consulté le 11 septembre 2009.

Notes

1 Le terme 'vol' induit lui-même en erreur, dans la mesure où la victime ne perd pas l'usage de son identité, mais se trouve simultanément confrontée à des utilisations frauduleuses de la part de tiers qui vont progressivement lui être opposées par les institutions financières et les entreprises ainsi trompées. Cela explique pourquoi les délais entre la commission de la fraude et sa découverte sont en général plus élevés que pour les autres crimes. Le préjudice ne découle ainsi pas de l'incapacité d'utiliser son identité, mais plutôt de l'attribution abusive d'usages dont la nature frauduleuse va devoir être démontrée, ce qui entraîne souvent de longues démarches administratives.

2 Lors du recensement de 2006, la population québécoise était estimée à 7,5 millions d'habitants par Statistique Canada.

3 Ces vignettes comprennent : L'utilisation d'une carte de débit ou de crédit pour procéder à des achats non autorisés; L'utilisation frauduleuse de renseignements personnels pour obtenir une nouvelle carte de paiement ou une ligne de crédit; L'accès non autorisé d'un tiers à un compte bancaire pour effectuer des paiements ou des virements; L'utilisation non autorisée de renseignements personnels pour obtenir des services téléphoniques, hydroélectriques, de télévision payante ou autres; L'accès frauduleux à des renseignements personnels même si ces derniers n'avaient pas été utilisés au moment de l'enquête.