L'évolution du piratage informatique :
De la curiosité technique au crime par sous-traitance

Benoit Dupont
Chaire de recherche du Canada en sécurité, identité et technologie
Université de Montréal
Benoit.dupont@umontreal.ca

Publié dans :
AAPI (Association sur l'Accès et la Protection de l'Information) (sous la direction de), *Le respons@ble 2.0 : Acteur clé en AIPRP,*
Cowansville : Éditions Yvon Blais, pp. 63-81, 2010.

De prime abord, il existe peu de points communs entre les féroces bandits qui écument les océans depuis l'Antiquité sous le pavillon noir et les petits génies qui s'infiltrent quotidiennement dans les systèmes informatiques des grandes entreprises, si ce n'est un dédain partagé pour toute forme d'autorité formellement établie. On remarquera à cet égard que la terminologie adoptée par la langue anglaise semble beaucoup moins connotée moralement que celle en vigueur dans la sphère francophone, puisque l'analogie avec l'histoire mouvementée du pillage en haute mer y est délaissée au profit de la vision moins menaçante du *hacker*. Dans l'argot anglais dont il est tiré, ce terme fait référence à la pratique en amateur et sans talent particulier d'une activité professionnelle, ludique ou sportive (Spears 2006), son adoption dans le contexte informatique permettant de mettre l'accent sur l'expertise technique plutôt que sur les illégalismes qui l'accompagnent parfois. De manière générale, le piratage informatique peut être défini comme l'ensemble des pratiques qui portent atteinte à l'intégrité des systèmes et des applications informatiques.

Plusieurs niveaux d'analyse peuvent être mobilisés afin de comprendre la nature et la structure du piratage informatique dans les sociétés technologiquement avancées. Le niveau « macro » place ainsi le piratage informatique dans le contexte beaucoup plus large de l'évolution technologique des moyens de communication et des répercussions sociales de transformations aussi radicales. On pourrait ainsi voir dans les actes de piratage le résultat d'une coévolution naturelle entre les nouvelles technologies et la délinquance. Au niveau « meso », l'unité de référence n'est plus la société dans son ensemble mais des groupes de pirates. On cherche alors à comprendre comment les individus attirés par le piratage s'organisent, acquièrent des compétences très spécifiques et se les transmettent. De telles analyses impliquent l'examen de données relatives à l'environnement immédiat des pirates, aux normes de leur sous-culture, ainsi qu'aux moyens particuliers qu'ils mettent en œuvre pour atteindre leurs objectifs. Finalement, le troisième et dernier niveau d'analyse est le niveau « micro », qui prend pour objet d'étude la dimension psychologique du piratage : observe-t-on parmi les pirates des traits psychologiques qui permettraient d'expliquer leur engagement dans ce type d'activité, et la pratique même du piratage provoque-t-elle des processus d'ordre psychologique qui peuvent être assimilés à des comportements addictifs?

Dans ce chapitre, l'approche intermédiaire (meso) sera privilégiée, tout d'abord parce qu'il est encore trop tôt pour tirer des conclusions définitives de changements technologiques toujours en cours et qui connaissent une accélération constante, et ensuite parce que les recherches psychologiques menées à ce jour sur les pirates informatiques sont frappées de nombreux biais méthodologiques (notamment d'auto-sélection) qui rendent toute généralisation fort hasardeuse (Schell et Dodge 2002). Dans la première partie de ce chapitre, je présente donc un certain nombre de caractéristiques organisationnelles des pirates telles qu'elles se dégagent de la littérature scientifique existante et des informations les plus récentes dont on dispose à leur sujet. Afin de donner une idée plus concrète de l'impact que peuvent avoir les activités de piratage sur les organisations, notamment en matière de protection des renseignements personnels, je reviens en détail dans la seconde partie sur les divers « exploits » d'Albert Gonzalez, un pirate américain condamné en 2010 pour avoir perpétré la plus importante fraude de la jeune histoire du piratage informatique. Cette étude de cas nous permettra notamment de comprendre quelles dynamiques opposent les pirates

aux organisations qu'ils prennent pour cibles, et les répercussions juridiques, financières et de réputation auxquelles ces dernières s'exposent.

1. Le profil des pirates informatiques

Il est possible de classer les pirates informatiques selon deux critères principaux qui sont la motivation et la compétence (Rogers 2005). Alors que le premier critère est en mesure de nous renseigner sur les raisons qui poussent certains individus à se lancer dans ce type d'activités, le second nous permet de mieux cerner les capacités de nuisance que ces derniers sont capables de mobiliser. Un examen plus approfondi des moyens et des méthodes privilégiés par les pirates fait cependant ressortir que des compétences techniques limitées ne représentent plus à l'heure actuelle un obstacle infranchissable à ceux qui désirent intégrer leurs rangs. Pour clore cette section, on examinera certaines des caractéristiques les plus marquantes de l'organisation sociale des pirates, et notamment l'apparente contradiction entre la culture collaborative qui nourrit leurs relations, d'une part, et les manifestations constantes et parfois très agressives de rivalité qui rythment les interactions entre individus, d'autre part.

a. Un répertoire de motivations et de compétences très diversifié

Les motivations qui poussent des individus à prendre illégalement le contrôle de systèmes informatiques appartenant à autrui relèvent de plusieurs ordres. Historiquement, les premiers *hackers* furent des étudiants en informatique de prestigieuses universités américaines qui exploraient le potentiel de communication en réseau et de partage des ressources d'ordinateurs jusque là exclusivement utilisés comme des calculateurs géants. Ces *hackers* conçurent des outils de communication permettant à la contre-culture des années 1960 et 1970 de s'exprimer sur un support technologique « libre » (Castell 2001 : 36). Leur héritage s'est transmis aux pirates contemporains qui se livrent à cette activité afin d'assouvir leur curiosité intellectuelle, et qui partagent dans certains cas les fruits de leurs découvertes avec l'ensemble des utilisateurs sur un registre se réclamant de l'altruisme. Tous les pirates motivés par la curiosité et l'envie de relever des défis techniques ne s'insèrent pas nécessairement dans ce type de démarche de partage des connaissances, et certains d'entre eux se contentent de retirer un plaisir égoïste de leurs exploits, à l'instar du jeune Michael Calce. Ce dernier, plus connu sous le pseudonyme de « Mafiaboy » causa un certain émoi médiatique en l'an 2000 pour avoir temporairement bloqué l'accès à plusieurs grands sites de commerce en ligne comme *Amazon*, *Dell* ou *eBay* au moyen d'une simple attaque par déni de service[1] (Calce et Silverman 2008), démontrant par la même occasion la fragilité technique des grands acteurs de l'économie en ligne quelques semaines seulement avant que n'éclate la bulle internet.

1. Il s'agit d'une attaque contre un site ou un réseau qui cherche à le rendre inopérant en le saturant de requêtes d'information qui dépassent sa capacité de traitement, ce qui l'empêche de répondre aux requêtes légitimes et le déconnecte de l'internet. Les attaques peuvent être simples ou distribuées. Dans ce dernier cas, un nombre élevé d'ordinateurs est mobilisé pour envoyer simultanément des requêtes à la cible afin d'augmenter considérablement les capacités de frappe et de nuisance. L'avantage d'une attaque distribuée est son efficacité exponentielle, mais aussi le fait qu'il est plus difficile de bloquer les requêtes (adresse IP) qui proviennent de milliers ou de millions de machines différentes.

La seconde grande source de motivation est d'ordre idéologique, les pirates se mettant alors au service d'une cause politique ou religieuse. On utilise le terme d'« hacktiviste » pour désigner ces pirates engagés qui recourent principalement à l'attaque par déni de service contre des sites jugés hostiles à leur cause. Au cours des dernières années, des sites gouvernementaux estoniens (2007), ukrainiens (2007), palestiniens et israéliens (2009), ou encore iraniens (2009) ont ainsi été rendus temporairement inaccessibles par ce type d'attaques. Les États ne sont pas les seules victimes, puisque certains grands médias (notamment la BBC et CNN), des partis politiques ou encore des ONG de défense des droits de la personne ont également été touchés, leur seul tort étant d'avoir diffusé sur internet des informations jugées déplaisantes par ces hacktivistes. L'augmentation observée ces dernières années des attaques idéologiquement motivées reflète l'importance d'internet comme moyen de communication (et donc de propagande), y compris dans les démocraties émergentes et les États faibles et défaillants exposés à des conflits internes ou frontaliers. La gravité des attaques menées par les hacktivistes se limite cependant à la perturbation des flux d'information, et à notre connaissance, les infrastructures essentielles d'un État ou d'un mouvement politique ou religieux n'ont jamais été encore menacées avec succès par ces pirates.

Une troisième motivation, plus prosaïque, relève de l'incitatif criminel classique qu'est l'appât du gain. Comme nous le verrons dans l'étude de cas, la dématérialisation au cours des cinquante dernières années des flux financiers et des systèmes de paiement a entraîné le recours intensif à des applications informatiques commerciales et bancaires dont les défaillances peuvent être exploitées de manière extrêmement lucrative par des pirates entreprenants. Les risques d'arrestation restent encore limités, du fait des ressources policières insuffisantes consacrées à ce type de délinquance (Huey 2002), et comme je le montrerai plus loin, une véritable économie clandestine globalisée est en train de se constituer autour de ces pratiques.

La quatrième et dernière source de motivation résulte d'un engagement que l'on pourrait qualifier de « palliatif » dans les activités de piratage Il peut s'agir de rompre l'ennui, d'exprimer des frustrations accumulées, d'assouvir un besoin de reconnaissance, de pouvoir et de contrôle, ou tout simplement de reproduire les sensations agréables associées au « flow », cet état d'exaltation et de plénitude provoqué par l'accomplissement d'activités valorisantes (Rennie et Shore 2007). Dans cette quatrième configuration, il devient difficile d'anticiper le niveau de risque moyen auxquels seront exposés les systèmes et les données personnelles visés. En effet, l'acte de piratage constitue une fin en soi et non un moyen, contrairement aux trois premières sources de motivation.

La figure 1 illustre pour celles-ci les niveaux de risques différentiels qui les caractérisent. Dans le cas des pirates motivés par la curiosité ou le défi, les systèmes sont modérément exposés, puisque l'objectif n'est pas de les détruire mais d'en comprendre le fonctionnement et d'en prendre le contrôle de la manière la plus ingénieuse possible. Quant aux données personnelles, elles représentent une faible utilité pour les pirates dans ce contexte. Ces dernières sont également marginales pour les pirates motivés par une idéologie, à moins qu'elles ne concernent des adversaires politiques ou religieux, alors que les systèmes informatiques représentent une cible de choix devant être neutralisée pour limiter les capacités de communication de l'ennemi. Les pirates motivés par le profit accordent enfin une grande importance à la furtivité, qui retarde la détection des intrusions et étire ainsi la

période pendant laquelle ils peuvent continuer à mener leurs fraudes. Pour cette raison, leur intérêt est de ne pas attirer l'attention par des dégâts trop manifestes causés aux systèmes. Cela leur permet de focaliser leurs efforts sur les données personnelles qu'ils cherchent à se procurer de la manière la plus efficiente possible, en privilégiant les cibles capables de leur procurer des centaines de milliers, voire des millions, d'éléments identificateurs exploitables.

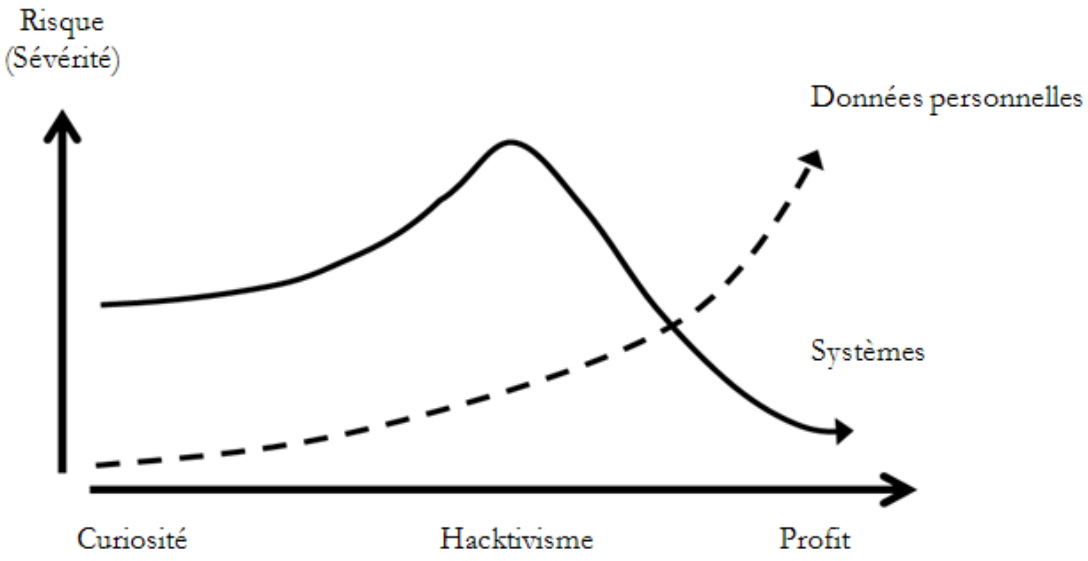

Figure 1. Distribution des risques selon la motivation des pirates

La distribution des risques n'est pas seulement influencée par la motivation principale des pirates. En effet, tous les pirates ne disposent pas de compétences techniques identiques. Dans la culture élitiste des pirates, les « script kiddies » se situent tout en bas de l'échelle hiérarchique informelle basée sur les compétences. Ces débutants ne disposent que de connaissances rudimentaires – voire inexistantes – sur les langages de programmation qui constituent l'architecture d'internet et des applications informatiques, et doivent recourir à des applications malveillantes conçues par des pirates beaucoup plus expérimentés qui automatisent la découverte et l'exploitation des vulnérabilités (Ghernaouti-Hélie 2009 : 42). Si ces logiciels s'avèrent souvent d'une redoutable efficacité, ils se concentrent néanmoins sur des failles de sécurité connues depuis longtemps et ne permettent pas à leurs usagers de revendiquer une expertise unique ou la paternité (le monde du piratage reste majoritairement masculin) d'une nouvelle méthode d'attaque. À l'autre extrémité de cette hiérarchie, que tout « script kiddy » aspire à gravir, on retrouve le « super-utilisateur », terme utilisé par le juriste Paul Ohm pour désigner la figure mythique du pirate omnipotent capable de s'introduire sans peine dans les systèmes les plus sécurisés et de les manipuler à sa guise (Ohm 2008). Cette représentation excessive des compétences des pirates est alimentée par la culture de masse, et notamment des œuvres cinématographiques qui font du pirate le héros (parfois récalcitrant) de l'intrigue (on citera à titre d'exemple « WarGames », « Opération Espadon », « Hackers », ou encore « Les Experts » parmi les plus emblématiques). L'étude de cas nous montrera à quel point cette vision idéalisée du pirate ultra-compétent reste hypothétique. Au centre du continuum de compétences, on retrouve le « pirate entrepreneur », qui s'affranchit

des considérations de prestige et mobilise de manière très instrumentale une expertise technique lui permettant de générer des revenus criminels de la manière la plus efficiente possible, utilisant indifféremment des logiciels prêts à l'emploi ou des scripts « sur mesure ». En effet, le développement d'outils de piratage de plus en plus performants et l'émergence d'une économie clandestine facilitant une division du travail font de la compétence technique une variable qui tend à perdre de son importance.

b. Les outils modernes du piratage

Dans la configuration classique du piratage, l'acquisition et le transfert de compétences techniques se font par l'intermédiaire de technologies de communication plus ou moins sophistiquées qui nécessitent néanmoins un investissement en temps de la part des « script kiddies » qui souhaitent s'élever dans la hiérarchie. Ainsi, des conférences annuelles comme *Defcon* ou *Black Hat* à Las Vegas, et *Hackfest* à Québec, permettent aux pirates de se rencontrer et de partager leurs techniques et leurs plus récents exploits. Pour ceux qui ne peuvent pas se déplacer, un magazine comme *2600* (qui s'autoproclame le « trimestriel des pirates ») est disponible en kiosque (au prix de 7.15$ le numéro) ou sur abonnement et contient des contributions expliquant en détail comment infiltrer, modifier ou neutraliser des applications et des réseaux informatiques à l'aide de procédés technologiques ou d'ingénierie sociale. L'isolement géographique ou social des néophytes est également aboli par l'existence de nombreux forums de discussion et de canaux de clavardage dont le contenu est exclusivement dédié au piratage sous toutes ses formes. Enfin, on assiste depuis quelques années à l'ouverture en Chine de véritables écoles de piratage fournissant à leurs « étudiants » des cours en ligne et des logiciels malveillants à télécharger moyennant des frais d'inscription de quelques centaines de dollars, une somme significative dans un pays émergent. L'une d'entre elles, la *Black Hawk Safety Net*, démantelée en février 2010 par la police chinoise comptait ainsi 12,000 membres payants et plus de 170,000 membres disposant d'un accès gratuit limité (Yiyao 2010).

Pour ceux qui n'ont pas de temps à consacrer à l'acquisition de compétences techniques, des logiciels malveillants automatisant la découverte et l'exploitation de vulnérabilités informatiques sont désormais disponibles sur le marché. Ces logiciels fournissent des solutions de piratage « clés en main » et permettent la prise de contrôle à l'insu de leurs propriétaires de quantités massives d'ordinateurs. On appelle « chevaux de Troie » ces logiciels qui peuvent moissonner les codes d'accès et mots de passe utilisés par leurs victimes lorsque celles-ci réalisent des opérations bancaires en ligne, ou gérer des *botnets* qui vont être utilisés pour expédier des quantités massives de pourriel ou mener des attaques par déni de service distribué (DDoS) (Namestnikov 2009, Stone-Gross et al. 2009). Le plus populaire d'entre eux à l'heure actuelle est sans conteste ZeuS, en raison notamment de sa conception orientée vers le piratage d'informations bancaires et financières. Ce logiciel dont les coûts peuvent varier de 3,000 à 20,000$ selon les options choisies par l'acheteur a été mis à jour une dizaine de fois en 2009, ce qui dénote la volonté de ses concepteurs d'en améliorer constamment la fiabilité et l'efficacité. De manière paradoxale, ce logiciel est doté d'un système de protection qui en limite l'usage à une seule machine autorisée, sur le modèle des mesures anti-piratage de l'industrie informatique (Stevens et Jackson 2010). Cette application est conçue de manière à échapper à la vigilance des anti-virus, puisque 55% des machines infectées disposent d'un mécanisme de sécurité dont la signature est à jour (Trusteer 2009), ce qui explique sa présence sur les équipements informatiques de 88% des 500 plus grandes

entreprises américaines (Bright 2010) et par conséquent, la compromission des renseignements personnels qui transitent par ces machines. Le site spécialisé dans le suivi des activités de ce logiciel (zeustracker.abuse.ch) recensait au 10 juillet 2010 environ 1,500 serveurs de commandement et de contrôle, qui correspondent à autant de pirates ayant installé et activé leur version. Cependant, de nouveaux « produits » font sans cesse leur apparition et cherchent à se tailler une place sur ce marché de plus en plus lucratif. Récemment, la prééminence de ZeuS a été mise à mal par SpyEye, un logiciel qui dispose des mêmes capacités mais qui est vendu à une fraction du prix (environ 500$) et qui offre une nouvelle fonction : la possibilité de désinstaller ZeuS des machines infectées par SpyEye (Khoel et Mieres 2010). La compétition est donc féroce entre concepteurs de logiciels malveillants, et chacun d'entre eux cherche à se distinguer des autres en offrant à ses clients des produits plus profitables ou innovants.

Cette logique commerciale va jusqu'à offrir des services de location d'ordinateurs infectés qui peuvent être contrôlés par des interfaces semblables à celles que l'on retrouve sur les logiciels commerciaux. Le prix de location est alors déterminé par des variables telles que le nombre d'ordinateurs que l'on souhaite contrôler, leur localisation géographique et la durée désirée de l'accès, qui déterminent toutes indirectement la quantité et la qualité des données personnelles qui pourront être exploitées frauduleusement. Le plus connu de ces services fut *76service*, proposé il y a quelques années par le *Russian Business Network* à partir de son botnet Gozi (Berinato 2007).

La nouvelle économie du piratage ne concerne pas uniquement la commercialisation de logiciels malveillants. En effet, la réalisation de fraudes informatiques nécessite la mise en œuvre de compétences variées qui ne se limitent pas à une expertise technique d'intrusion. Des compétences sociales, ainsi que des connaissances du fonctionnement administratif et financier du système attaqué (les compétences systémiques) ou encore des compétences d'intuition sont indispensables aux délinquants afin de réunir les indispensables complices, de maximiser leurs gains et d'anticiper les risques que leurs activités soient détectées ou interrompues (Copes et Vieraitis 2007). Rares sont les pirates qui disposent de l'ensemble de ces compétences, et leur distribution rend indispensable la création de plateformes d'échange qui facilitent la division du travail. Ainsi, les forums de discussion et les canaux de clavardage (IRC en langage technique) regorgent d'offres d'hébergeurs *bulletproof* (blindés) qui garantissent à leurs clients peu recommandables le maintien en ligne de leurs serveurs (y compris face aux demandes policières), de centres d'appels qui se proposent d'aider les fraudeurs à contourner les mesures de sécurité reposant sur une interaction téléphonique, de sites de vérification de la validité des numéros de carte de crédit volés, ou encore de sites de recrutement de « mules », ces intermédiaires parfois trop naïfs qui sont utilisés par les fraudeurs afin de transférer sans risque des sommes d'argent des comptes de leurs victimes vers un destinataire anonyme situé dans un pays étranger. Alors que dans le modèle « historique », les moyens de communication en ligne sont utilisés par les pirates pour échanger des compétences sur un modèle « communautaire », on assiste plutôt ici à l'émergence d'un bazar virtuel où des services spécifiques reliés à la réalisation de fraudes financières sont offerts sur une base marchande, selon une rationalité reposant sur les mêmes arguments commerciaux que ceux sur lesquels s'appuient généralement les entreprises légitimes (rapidité, qualité du service à la clientèle, remboursement ou échange en cas d'insatisfaction de l'acheteur, rabais consentis en fonction des volumes, etc…).

c. L'organisation liquide du piratage

L'existence de telles plateformes d'échange d'outils et de services ne traduit en aucune façon un degré d'organisation formelle très développé de l'univers du piratage. Les pirates informatiques ne suivent pas le modèle hiérarchique contraignant du crime organisé (lui aussi très surévalué d'ailleurs), comme certaines représentations médiatiques ou policières l'affirment (McCusker 2006). Les outils décrits plus haut constituent plutôt des éléments organisants dans un univers caractérisé par la faiblesse de ses liens et l'instabilité des relations de coopération. Nous avons en effet pu observer sur les canaux de clavardage que les discussions sont parsemées d'insultes à connotation misogyne et homophobe, et que les conflits interpersonnels entre pirates sont constants, ce qui se traduit notamment par de nombreuses attaques informatiques menées dans un objectif de vengeance ou de rétorsion, et justifiées par une logique d'autodéfense.

La confiance est également très diffuse, et il n'est pas rare que des pirates engagés dans une transaction n'honorent pas les termes de l'échange. Cela conduit les sites clandestins où se vendent les logiciels malicieux ou les renseignements personnels volés à mettre en place des processus d'évaluation par les pairs destinés à garantir la fiabilité des participants. Ce déficit de confiance n'est pas surprenant dans un contexte où les individus ne se rencontrent en personne qu'à de très rares occasions, et doivent par conséquent mener la majorité de leurs interactions par l'intermédiaire de technologies qui ne permettent pas d'accéder à l'ensemble des signaux visuels ou auditifs utilisés d'habitude par les êtres humains pour prendre une décision. Les équipes de travail qui coordonnent des projets internationaux à l'aide des nouvelles technologies de l'information éprouvent d'ailleurs les mêmes difficultés de gestion de la confiance (Jarvenpaa et Leidner 1999). Ceux-ci sont accentués par la pratique qui consiste pour certains pirates à opérer en ligne sous des pseudonymes différents afin d'éviter de se faire repérer ou parce que leur pseudonyme de prédilection est déjà utilisé par un tiers sur certains forums (Holt 2009).

Il résulte de ces rivalités latentes et de cette confiance ténue que la structure sociale du piratage relève plus de liens faibles et éphémères actionnés de manière ponctuelle en fonction de besoins ou de projets spécifiques que de liens forts basés sur des alliances criminelles persistantes et ancrées dans des normes de comportement communes à l'ensemble des participants. Cela augmente les coûts de transaction pour les pirates qui mettent sur pied des projets ambitieux requérant la participation de plusieurs collaborateurs, dans la mesure où la confiance doit être accordée sur une base individuelle à la suite de nombreux essais et erreurs. D'un point de vue global cependant, cette organisation sociale du piratage induit une dispersion des risques qui complique le travail des organismes d'application de la loi, habitués à focaliser leur attention sur des noyaux durs criminels relativement stables dans l'espace et dans le temps.

2. Albert Gonzalez, le piratage par projet et l'insécurité des données personnelles

Une étude de cas plus concrète illustrera de quelle manière les pirates informatiques motivés par l'appât du gain s'attaquent aux données personnelles détenues par les entreprises afin de

les revendre à des fraudeurs basés dans le monde entier. Cette étude de cas est exemplaire car elle illustre le décalage entre la valeur que représentent les renseignements personnels pour des criminels et les faibles niveaux de protection que leurs opposent les entreprises, mais aussi les conséquences financières et réputationnelles désastreuses qui pèsent sur ces dernières en cas de piratage. Elle montre également qu'il n'est nul besoin de détenir une expertise très développée pour tirer du piratage des revenus conséquents. Enfin, elle met en lumière la complexité des enquêtes criminelles requises dans un tel contexte. Les éléments de cette étude de cas proviennent d'articles de presse, mais aussi de documents de mise en accusation et présentenciels rendus publics par les procureurs et les avocats des parties.

En janvier 2007, l'entreprise *TJX*, un géant américain du commerce de détail propriétaire au Canada des marques *Winners* et *Homesense*, révélait que ses systèmes informatiques avaient été piratés et qu'une quantité limitée de numéros de cartes de crédit, de débit, et de permis de conduire appartenant à ses clients, lui avaient échappés. Le préjudice initial fut évalué à 25 millions de dollars, avant d'être multiplié par dix quelques mois plus tard pour atteindre plus de 250 millions de dollars. L'enquête menée conjointement par le *Secret Service* américain et l'entreprise de sécurité privée engagée par *TJX* fit en effet apparaître un piratage d'une ampleur sans précédent qui avait compromis plus de 90 millions de numéros de cartes de paiement. On se rendit également rapidement compte que *TJX* n'était pas la seule victime des pirates, et que de nombreuses autres entreprises s'étaient faites dérober des quantités considérables de données personnelles.

a. La convergence de pirates déterminés et de gardiens négligents

La condamnation en 2010 du principal instigateur de cet acte de piratage, ainsi que de certains de ses complices, nous permet de reconstituer partiellement la trame des événements. Albert Gonzalez avait 25 ans au moment de son arrestation. Il avait déjà été condamné en 2004 pour avoir cloné des cartes de crédit, et s'était vu offrir le statut d'informateur par le *Secret Service*, qui lui versait un salaire d'environ 75.000$ par an pour infiltrer le monde clandestin des fraudeurs (Zetter 2010). Cela ne l'empêcha pas de poursuivre ses activités de piratage et de monter cette opération de grande envergure qu'il baptisa « Get rich or die trying » (devenir riche ou mourir en essayant). Sa technique était fort simple : après avoir identifié des cibles potentielles à l'aide de la liste des 500 plus grosses compagnies américaines dressée par le magazine Fortune, il parcourut pendant plusieurs mois l'autoroute 1 qui traverse Miami équipé d'un ordinateur portable et d'un logiciel « renifleur » capable de repérer les communications sans-fil non sécurisées entre les points de vente (où sont situés les caisses enregistreuses et les terminaux de paiement des magasins) des magasins et les serveurs installés dans l'arrière-boutique. Dès qu'il identifiait un magasin vulnérable, il lui suffisait de stationner son véhicule à proximité ou de louer un espace de bureau dans un immeuble mitoyen afin de pouvoir intercepter l'ensemble des transmissions contenant les numéros de cartes de crédit des clients. Cette porte d'entrée dans le système informatique de ses victimes lui permettait aussi de remonter jusqu'aux bases de données centrales contenant la totalité des données personnelles détenues par le siège de l'entreprise. Dans un second temps, Albert Gonzalez et ses complices utilisèrent une seconde technique de piratage connue sous le nom d'« injection SQL », qui consiste à exploiter une vulnérabilité présente sur de nombreuses bases de données accessibles par internet.

Ces deux stratégies, dont aucune ne se distingue par sa créativité technique ou sa difficulté de mise en œuvre, ont permis à Gonzalez et à ses complices de piller les bases de données d'une douzaine de grandes entreprises de commerce de détail (dont *7-Eleven*, *JC Penney*, ou *Barnes and Nobles*) et de *Heartland*, une entreprise importante spécialisée dans le traitement des transactions par carte de paiement. Ils se seraient ainsi procuré plus de 130 millions de numéros de cartes de paiement et auraient réalisé des profits de plusieurs millions de dollars, dont une partie fut enterrée dans le jardin d'Albert Gonzalez.

Le plus surprenant dans cette affaire reste cependant le déficit flagrant de mesures de sécurité mises en œuvre par les entreprises ciblées : le magasin *TJX* à l'origine de la faille initiale transmettait les renseignements personnels à l'aide d'un système de communication sans fil non sécurisé, et de nombreuses normes de sécurité recommandées par l'industrie des cartes de paiement étaient ignorées. Ces dernières semblent d'ailleurs largement insuffisantes, dans la mesure où *Heartland* les appliquait à la lettre, sans que cela ne réussisse à la protéger des pirates. Une des principales raisons à cette négligence structurelle réside dans la nature extrêmement compétitive du secteur de commerce de détail, qui est le principal utilisateur du système de paiement par cartes. Les minces marges de profit empêchent que des investissements informatiques conséquents soient réalisés de manière régulière afin de sécuriser les systèmes contre des menaces en constante évolution, et les bas salaires ne permettent pas toujours de retenir les services des employés les plus compétents en matière de sécurité.

Par contraste, les pirates prenaient un soin jaloux des données personnelles dont ils avaient pris le contrôle. Elles étaient en effet stockées sur des serveurs protégés par le logiciel de chiffrement *BestCrypt*, commercialisé par la société *Jetico*, qui se targue de compter parmi ses clients des services de renseignement et des agences d'application de la loi. Quand au disque dur de l'un des complices d'Albert Gonzalez arrêté en Turquie en 2007, il était intégralement crypté à l'aide du logiciel *PGP*, un leader du chiffrement, et le mot de passe requis pour y accéder comptait 17 caractères. Certains complices communiquaient également par l'intermédiaire du service de courrier électronique crypté *SAFe-mail*, basé en Israël.

b. La division du travail

L'organisation de cet acte de piratage de grande ampleur aurait été impossible sans une division du travail poussée entre techniciens, acquéreurs des données, grossistes, détaillants et messagers. Les « techniciens » ont été mobilisés par Albert Gonzalez afin de concevoir des logiciels sur mesure permettant d'infiltrer les réseaux sans fil et de recueillir les mots de passe des usagers pour progresser au cœur des systèmes, ainsi que des applications pour décrypter des fichiers piratés contenant des numéros de carte de crédit. L'un des complices arrêtés correspondant à ce profil est Stephen Watt. Cet ingénieur informatique de la banque d'affaires *Morgan Stanley* dont le salaire avoisinait 130,000$ avait auparavant travaillé pour la société de sécurité *Qualys*. Ce dernier avait durant son adolescence appartenu à plusieurs groupes de pirates et avait également présenté ses techniques d'intrusion lors de l'édition 2002 de la conférence *Def Con* (Zetter 2009). Selon ses propres déclarations, Watt n'aurait obtenu aucune rémunération pour son travail. Un autre complice de Gonzalez, Jeremy Jethro, vendit à ce dernier une technique encore non répertoriée (et donc sans protection adéquate) d'attaque du logiciel Internet Explorer (appelée dans le jargon de la sécurité un

« zero-day exploit ») pour la somme de 60,000$, ce qui permit certainement aux pirates de procéder à leurs « injections SQL » sans être détectés.

Les « acquéreurs de données » ont utilisé ces logiciels fournis à Gonzalez pour effectuer le travail répétitif et laborieux d'identification des cibles, d'introduction dans les systèmes informatiques et de récupération des données convoitées. Une fois volées, les données personnelles n'étaient pas conservées aux États-Unis. Elles étaient plutôt transférées par le biais de connexions cryptées vers des serveurs informatiques hautement sécurisés situés en Ukraine, en Lituanie, et en Estonie. Ces serveurs étaient accessibles à des « grossistes » qui mettaient sur le marché des lots de plusieurs dizaines ou centaines de milliers de numéros de cartes de crédit. Les « revendeurs » qui en faisaient l'acquisition les offraient ensuite au détail sur des sites spécialisés de « carding ». Maksym Yastremskiy, citoyen ukrainien arrêté en Turquie en juillet 2007 pour avoir piraté les systèmes informatiques d'une douzaine de banques locales, était l'un de ces grossistes. Les paiements se faisaient par l'intermédiaire d'un service de transfert d'argent pour les nouveaux clients, et par virement direct dans ses comptes bancaires pour les acheteurs de confiance. Les profits estimés de son activité s'élèvent à une dizaine de millions de dollars. Parmi les « détaillants » figure Sergey Pavlovich, un citoyen Biélorusse, qui administrait le site *dumpsmarket* où vendeurs et acheteurs de numéros de cartes de crédit volées pouvaient conclure leurs transactions. On observe donc ici un système de distribution qui irrigue un marché clandestin planétaire, puisque des détaillants non identifiés chinois furent également mis en accusation par les procureurs américains – sans grand espoir de les voir un jour arrêtés. On notera également que les détaillants connaissaient rarement la provenance initiale de leurs « produits » et qu'ils n'avaient aucun lien direct avec l'équipe de Gonzalez. Il s'agissait simplement d'entrepreneurs engagés sur un marché lucratif, bien qu'illégal.

Enfin, la conversion des numéros de cartes de crédit volés en espèces sonnantes et trébuchantes requiert souvent le recrutement par les fraudeurs de messagers, aussi connus sous le terme de « mules » dans le milieu. Ces derniers procèdent à des retraits d'argent aux distributeurs automatiques à l'aide de cartes clonées grâce aux données volées, et transfèrent les sommes ainsi obtenues après avoir prélevé un pourcentage correspondant à leur commission. Dans le cadre de l'affaire Gonzalez, le *Secret Service* procéda à l'arrestation d'Humza Zaman, un ancien responsable de la sécurité informatique à la banque *Barclays*, qui fut condamné à 46 mois de prison en 2010 pour avoir blanchi de cette manière entre 600,000 et 800,000 dollars.

La division du travail que nous venons de décrire reflète l'écosystème contemporain du piratage informatique motivé par le profit, qui se déploie à travers des réseaux de fraudeurs aux compétences complémentaires situés aux quatre coins de la planète, mais pouvant coordonner leurs efforts de manière relativement aisée grâce à l'internet. La coordination est rarement aussi fluide du côté des forces de l'ordre qui sont chargées de combattre ces pirates.

c. Une enquête sur plusieurs continents

Les investigations relatives à cette affaire ont été menées par le *Secret Service*, l'agence fédérale américaine chargée de lutter contre les crimes économiques et financiers de grande ampleur. Les moyens à la disposition de cette organisation dépassent de très loin les ressources que

peuvent revendiquer des services de police municipaux ou provinciaux confrontés à des cas identiques de piratage. En effet, outre les 28 équipes intégrées de lutte contre les crimes électroniques qu'il chapeaute aux États-Unis, le *Secret Service* peut compter sur 22 bureaux de liaison à l'étranger répartis aussi bien en Europe qu'en Asie, au Moyen-Orient ou même au Canada (United States Secret Service 2009). Dans le cadre de l'affaire Gonzalez, ces capacités conséquentes ont permis aux enquêteurs d'obtenir la saisie et l'analyse d'un serveur en Estonie, l'arrestation d'un suspect en Allemagne, la perquisition clandestine d'un ordinateur portable dans la chambre d'hôtel d'un suspect à Dubaï (ainsi que l'arrestation de ce dernier en Turquie), la saisie d'un disque dur en Biélorussie, ainsi que la perquisition d'un compte de courrier électronique en Israël. À l'heure actuelle, seules des affaires liées au démantèlement de réseaux pédopornographiques sont susceptibles de mobiliser des moyens policiers aussi étendus à l'échelle internationale en matière de crimes informatiques, ce qui conforte les pirates dans la croyance qu'ils peuvent prétendre à une certaine impunité à l'extérieur des frontières américaines. D'ailleurs, la condamnation d'Albert Gonzalez à deux sentences d'emprisonnement concomitantes de 20 ans manifeste plutôt la volonté des tribunaux américains de faire de cette affaire un exemple de sévérité que la capacité du système pénal de dissuader les pirates par la certitude d'une condamnation. Si les risques encourus par les pirates demeurent donc faibles, il n'en va pas de même pour les entreprises victimisées.

d. Les retombées du piratage pour les entreprises visées

Les grandes entreprises victimes d'actes de piratage impliquant le vol de renseignements personnels subissent des préjudices importants qui relèvent du domaine financier, juridique et réputationnel. Sur le plan financier d'abord, la découverte d'un incident de piratage entraîne des coûts significatifs liés à l'enquête qui est la plupart du temps confiée à une entreprise spécialisée. L'objectif est ici de comprendre le mode opératoire des pirates et les failles exploitées, ainsi que l'ampleur des dommages subis, afin d'y remédier dans les meilleurs délais. Les victimes individuelles dont les données personnelles ont été compromises doivent ensuite être averties, et il est courant que l'entreprise s'engage à leur fournir des services de protection contre le vol d'identité et la fraude pendant un certain temps. Une fois la réponse immédiate à l'incident effectuée, des investissements de mise à niveau des équipements et des applications informatiques seront fréquemment requis, accompagnés généralement par le déploiement de nouvelles procédures, programmes de prévention et de formation. Une certification ou un audit destinés à valider la sécurité des nouvelles procédures viendront également gonfler les frais. Il existe aussi des coûts financiers indirects qui pèsent sur les partenaires de l'entreprise victime, et qui lui sont parfois imputables. Ainsi, dans le cas des entreprises qui se font voler des numéros de cartes de crédit ou de débit, les organisations émettrices (*Visa, Mastercard, Amex* ou encore les banques) doivent procéder au remplacement des cartes compromises, et il n'est pas rare qu'elles exigent une compensation pour cela. Dans notre étude de cas, l'une des entreprises victimes, *Heartland Payment Systems*, accepta ainsi de dédommager *Visa* pour un montant de 60 millions de dollars US, et conclut des ententes similaires avec *Mastercard* (41,4 millions) et *American Express* (2,4 millions) (Adams 2010).

En l'absence de telles ententes, des poursuites collectives pour négligence peuvent être lancées par les banques ou les individus affectés. *TJX* fut ainsi attaquée en justice par une alliance de près de 300 institutions financières qui s'ajouta aux douzaines de poursuites intentées par des clients et des actionnaires. Les autorités régulatrices peuvent aussi

sanctionner les organisations sous leur contrôle pour non respect des normes de sécurité. Au Royaume-Uni, qui dispose du régime le plus agressif en ce domaine, l'autorité responsable de la protection de la vie privée peut imposer des amendes maximales de 500,000 livres (environ 800,000 CAD$) aux organisations qui se font voler des données personnelles (Ponemon 2010 : 11). *TJX* finit également par négocier avec 41 états américains une amende globale de 10 millions de dollars US pour éteindre toute procédure des agences régulatrices.

Pour finir, les dommages à la réputation des organisations affectées par un acte de piratage se traduisent par la perte de clients inquiets de la sécurité de leurs propres données, mais aussi par la difficulté accrue à acquérir de nouveaux clients, ce qui engendre des coûts additionnels de marketing et diminue d'autant la profitabilité de l'entreprise. Ces coûts d'opportunité sont d'autant plus élevés dans les secteurs où la confiance des clients est un élément central dans le processus de prise de décision, comme le secteur financier ou celui de la santé (Ponemon Institute 2009 : 16). Cette atteinte à la réputation explique d'ailleurs pourquoi la chaîne de magasins *JC Penney* tenta – sans succès – d'empêcher les procureurs de mentionner son nom dans les poursuites contre Albert Gonzalez, prétextant que les enquêteurs n'étaient pas capables de prouver formellement que des numéros de cartes de crédit avaient été volés sur ses serveurs (même si le piratage n'était pas contesté), et craignant que la publicité négative associée à cette divulgation ne nuise à ses ventes (Poulsen et Zetter 2010).

L'étude menée à l'échelle internationale par le *Ponemon Institute* (2009 : 14) affirme ainsi que le coût moyen global d'une brèche de données s'élève à 142 dollars américains par dossier compromis, avec un minimum de 98 dollars en Australie et un maximum de 204 dollars aux États-Unis. On prend ainsi la pleine mesure de l'ampleur du préjudice subi par les entreprises attaquées par Albert Gonzalez lorsque l'on rappelle que la plupart d'entre elles se sont fait pirater plusieurs centaines de milliers, voire plusieurs millions, de dossiers. L'insouciance avec laquelle ces entreprises géraient les données personnelles de leurs clients semble dans ce contexte un pari bien hasardeux face à des risques dont la sévérité n'a rien de virtuelle.

Conclusion

L'évolution du piratage informatique reflète fidèlement celle de la technologie qui lui donne corps. À mesure que l'internet perdit son statut marginal de technologie en gestation réservée à une certaine élite universitaire pour se transformer en outil de communication et de commerce omniprésent dans la vie quotidienne de milliards d'usagers, la curiosité céda la place à l'idéologie et à l'appât du gain comme motivation dominante. L'organisation sociale du piratage connut un développement similaire, puisque celui qui ne dispose pas des compétences techniques suffisantes peut dorénavant trouver sur internet de nombreux outils lui permettant de mettre sur pied des projets de piratage qui n'auront rien d'anecdotiques. Une économie clandestine d'applications malveillantes, de services de soutien et de données volées s'est ainsi constituée pour structurer le travail des pirates de manière performante, sur un modèle inspiré des entreprises qui renforcent leur compétitivité par un recours intensif à la sous-traitance. Nous avons vu à travers l'étude de cas comment les pirates opéraient, et notamment comment ils exploitaient les nombreuses vulnérabilités des entreprises ciblées.

Le Québec n'est pas épargné par ce type de pratiques. La *Sûreté du Québec* procéda ainsi en février 2008 à l'arrestation à travers toute la province de 17 personnes suspectées

d'appartenir à un réseau de pirates qui contrôlaient des dizaines de milliers d'ordinateurs en Pologne, au Brésil, au Mexique ou encore au Canada (Myles 2008). Ces machines n'étaient pas exploitées pour commettre des fraudes financières (ce qui aurait été possible), mais plutôt pour mener des attaques massives contre d'autres pirates ou des personnes qui leur déplaisaient. Cependant, en septembre 2008, Ehud Tenenbaum (plus connu sous le pseudonyme « the Analyzer » et devenu célèbre en 1998 pour s'être introduit dans les systèmes informatiques du Pentagone et de la NASA) fut arrêté à Montréal, où il prétendait diriger une société de sécurité informatique. On lui reprochait d'avoir accédé aux bases de données de plusieurs institutions financières canadiennes et américaines et d'avoir procédé au même type de fraude que celui présenté dans l'étude de cas, pour un préjudice évalué à 10 millions de dollars (Leyden 2009). Pour finir, la disponibilité sur les forums consacrés au piratage de cartes de crédit canadiennes se négociant à des prix qui fluctuent de 10 à 80$ l'unité implique l'existence de victimes et de fraudeurs locaux.

Pourtant, face à la réalité d'une telle menace et aux connaissances encore limitées dont on dispose pour la comprendre et y répondre, le gouvernement québécois prenait la décision en juin 2010 de fermer l'Institut pour la Sécurité de l'Information du Québec (ISIQ), dont la vocation était justement de fédérer les ressources et les efforts en ce domaine. Alors que les pirates informatiques exploitent pleinement les vertus du partenariat et de la mise en réseau des compétences, le modèle de prévention et de contrôle qui se dessine ici évoque de manière bien anachronique l'anarchie de l'état de nature hobbesien, dans lequel les individus et les organisations ne peuvent compter que sur leurs propres moyens pour repousser les attaques dont ils font l'objet. Si l'adaptation des pirates à leur environnement technologique est indéniable, celle des politiques gouvernementales reste encore, comme on le voit, très hésitante et manque d'inspiration.

Références

John Adams (2010), « Heartland tries to settle breach damages with Mastercard issuers », *Bank Technology News*, disponible à www.americanbanker.com/btn.html (consulté le 16 juillet 2010).

Scott Berinato (2007), « Who's stealing your passwords? Global hackers create a new online crime economy », *CIO.com*, disponible en ligne à www.cio.com/article/135500 (consulté le 11 juillet 2010).

Peter Bright (2010), « Almost all Fortune 500companies show Zeus botnet activity », *Ars Technica*, 15 avril, diponible en ligne à arstechnica.com (consulté le 9 juillet 2010).

Michael Calce et Craig Silverman (2008), *How I cracked the Internet and why it's still broken*, Toronto: Viking Canada.

Manuel Castells (2001), *La galaxie Internet*, Paris : Fayard.

Heith Copes et Lynne Vieraitis (2007), *Identity theft: Assessing offenders' strategies and perceptions of risk*, Birmingham: University of Alabama.

Solange Ghernaouti-Hélie (2009), *La cybercriminalité: Le visible et l'invisible*, Lausanne : Presses Polytechniques et Universitaires Romandes.

Thomas Holt (2009), « Lone hacks or group cracks: Examining the social organization of computer hackers », in Frank Schmalleger et Michael Pittaro (eds.), *Crimes of the Internet*, Upper Saddle River: Pearson, pp. 336-355.

Laura Huey (2002), « Policing the abstract: Some observations on policing cyberspace », *Canadian Journal of Criminology*, vol. 44, no. 3, pp. 243-254.

Sirkka Jarvenpaa et Dorothy Leidner (1999), « Communication and trust in global virtual teams », *Organization Science*, vol. 10, no. 6, pp. 791-815.

Ben Khoel et Jorge Mieres (2010), *SpyEye Bot (part two) : Conversations with the creator of crimeware*, Malware Intelligence. Disponible en ligne à malwareint.com (consulté le 11 juillet 2010).

John Leyden (2009), « Pentagon hacker Analyzer suspected of $10m cyberheist », *The Register*, 25 mars, disponible en ligne à www.theregister.co.uk (consulté le 18 juillet 2010).

Rob McCusker (2006), « Transnational organised cyber crime : distinguishing threat from reality », *Crime, Law and Social Change*, vol. 46, no. 4-5, pp. 257-273.

Brian Myles (2008), « Des pirates québécois du cyberespace mis hors de combat », *Le Devoir*, 21 février, p. A2.

Yury Namestnikov (2009), *The economics of botnets*, Moscou: Kaspersky Lab. Disponible en ligne à www.viruslist.com (consulté le 10 juillet 2010).

Paul Ohm (2008), « The myth of the superuser: Fear, risk and harm online », *UC Davis Law Review*, vol. 41, no. 4, pp. 1327-1402.

Ponemon Institute (2009), *2008 annual study: Cost of a data breach*, Menlo Park: PGP Corporation.

Ponemon Institute (2010), *2009 annual study: Global cost of a data breach*, Menlo Park: PGP Corporation.

Kevin Poulsen et Kim Zetter (2010),

Lara Rennie et Malcolm Shore (2007), « An advanced model of hacking », *Security Journal*, vol 20, no. 4, pp. 236-251.

Marcus Rogers (2005), *The development of a meaningful hacker taxonomy: A two dimensional approach*, CERIAS Tech Report 43, West Lafayette: Centre for Education and Research in Information Assurance and Security.

Bernadette Schell et John Dodge (2002), *The hacking of America: Who's doing it, why and how*, Westport: Quorum Books.

Richard Spears (2006), *Dictionary of American slang and colloquial expressions*, New York: McGraw-Hill.

Kevin Stevens et Don Jackson (2010), *ZeuS banking trojan report*, Atlanta: SecureWorks. Disponible en ligne à www.secureworks.com/research/threats/zeus (consulté le 9 juillet 2010).

Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Chris Kruegel, Giovanni Vigna (2009), *Your botnet is my botnet: Analysis of a botnet takeover*, Santa Barbara: University of California Santa Barbara Technical report.

Trusteer (2009), *Measuring the in-the-wild effectiveness of antivirus against Zeus*, New York: Trusteer. Disponible en ligne à www.trusteer.com (consulté le 9 juillet 2010).

United States Secret Service (2009), *Fiscal year 2009 annual report*, Washington: US Department of Homeland Security.

Wu Yiyao (2010), « Biggest hacker training site shut down », *China Daily*, 8 février, disponible en ligne à www.chinadaily.com.cn (consulté le 18 juillet 2010).

Kim Zetter (2009), « TJX hacker was awash in cash; his penniless coder faces prison », *Wired.com*, disponible en ligne à www.wired.com/threatlevel (consulté le 15 juillet 2010).

Kim Zetter (2010), « Secret service paid TJX hacker $75,000 a year », *Wired.com*, disponible en ligne à www.wired.com/threatlevel (consulté le 14 juillet 2010).