LES PIRATES INFORMATIQUES : NOUVELLES TECHNOLOGIES ET CRIME DÉSORGANISÉ

BENOÎT DUPONT

Les « exploits » de pirates informatiques ayant réussi à s'introduire dans les systèmes d'information font presque quotidiennement la une de journaux et de sites Web, mais nous savons peu sur les individus responsables de ces intrusions. Benoît Dupont présente ici les grandes lignes de son étude qui vise à combler ce déficit de connaissances par une analyse des compétences techniques et sociales d'un groupe de pirates, dont les communications électroniques furent saisies par la police.

The exploits of hackers who successfully penetrate computer systems are mentioned almost daily in newspapers and on Web sites, but we know very little about the individuals responsible for these cyber-intrusions. Benoît Dupont gives us a deeper insight in this article, which is based on an analysis of the technical and social skills of a network of hackers whose electronic communications were seized by the police.

Les pirates informatiques (les fameux *hackers*) sont habituellement dépeints comme des adolescents asociaux mais intelligents qui, depuis leur antre solitaire dans le sous-sol de la maison familiale, déchaînent une apocalypse technique contre leurs victimes impuissantes... Ce stéréotype se trouve renforcé par le fait que la police effectue peu d'arrestations et que le nombre de cas passant en jugement est encore plus insignifiant, car la plupart des accusés plaident coupables afin de négocier une entente favorable avec les procureurs. Notre déficit de connaissances sur les caractéristiques sociales et les modes opératoires des pirates informatiques fait en sorte que les décideurs politiques et les intervenants du système pénal, ainsi que le public, dépendent de représentations romanesques ou d'autobiographies embellies pour comprendre cette nouvelle catégorie de délinquants.

Notre article tente de combler cette lacune. Il est basé sur une étude de cas fondée sur l'analyse des communications électroniques, saisies par la police, d'un groupe de personnes accusées de piratage informatique.

En février 2008, le Module d'enquête sur la cybercriminalité de la Sûreté du Québec a arrêté 17 suspects, dans 12 lieux différents, dans le cadre d'une enquête portant sur un collectif de pirates informatiques. À ses débuts, en 2005, cette enquête était un simple projet de collecte de renseignements visant à obtenir des informations sur le monde clandestin du piratage, mais elle concentra rapidement ses activités sur ce réseau précis de pirates quand il devint évident que ses membres exploitaient de vastes réseaux d'ordinateurs compromis, également connus sous le nom de réseaux de zombies ou *botnets*.

Bien que les membres du réseau n'opéraient pas à une très grande échelle, les enquêteurs qui ont analysé leurs disques durs ont pu répertorier plus d'une centaine de réseaux contrôlés par ce groupe, incluant 630 000 adresses de protocole Internet distinctes (et donc autant de machines), dans 120 pays différents. Parmi les 17 suspects initialement arrêtés, 10 furent accusés par la suite, et tous finirent par plaider coupables aux chefs d'accusation de l'utilisation non autorisée d'ordinateurs, de possession et utilisation de mots de passe, de méfaits en relation avec des données, et de fraude

Benoît Dupont est titulaire de la Chaire de recherche du Canada en sécurité et technologie, et directeur du Centre international de criminologie comparée de l'Université de Montréal. *Cet article est la version abrégée d'une communication présentée lors du troisième atelier de travail international sur les réseaux illicites, organisé à Montréal les 3 et 4 octobre 2011.*

PHOTO: SHUTTERSTOCK

et possession de données reliées à des cartes de crédit. Neuf d'entre eux furent condamnés à des peines de détention à domicile allant de 15 à 18 mois, qui étaient assorties de périodes de travail communautaire. Celui qui était perçu comme le meneur du groupe fut condamné à deux ans de prison ferme et trois ans de probation, certainement la peine la plus sévère infligée en matière de délits liés à l'informatique dans les annales judiciaires canadiennes. Ces 10 pirates informatiques déclarés coupables forment le réseau criminel qu'analyse cet article.

Le profil démographique de ces 10 pirates informatiques correspond largement à celui généralement présenté par la littérature scientifique, puisque tous étaient de sexe masculin, et leur âge moyen était de 20,4 ans au moment de leur arrestation. Bien que l'on ne puisse considérer cet échantillon comme représentatif, ce groupe vient corroborer le cliché d'une sous-culture du piratage essentiellement masculine. Par contre, l'échantillon diffère des représentations classiques des pirates du fait de l'implication antérieure des individus arrêtés dans d'autres types d'infractions, ainsi que de l'orientation professionnelle de ces derniers. La moitié des pirates arrêtés (5) avait déjà un casier judiciaire pour une ou plusieurs infractions liées soit à la drogue (3), soit au vol (2) ou à des voies de fait (2), donc des infractions criminelles mineures non technologiques. La moitié d'entre eux discutait aussi régulièrement de sa consommation de drogues (principalement du cannabis) dans les communications analysées. Parmi les cinq pirates informatiques ayant un emploi stable, un seul d'entre eux travaillait dans l'industrie informatique, les quatre autres occupaient des emplois peu qualifiés. Un sixième recevait de l'aide sociale tout en ayant divers petits emplois non déclarés. Sur les quatre restants, deux étaient étudiants en informatique et deux avaient un statut inconnu.

L'implication précoce dans diverses formes de petite délinquance et un profil d'emploi plutôt orienté vers des métiers manuels contredisent le stéréotype du pirate informatique maniaque de programmation, appelé à joindre les rangs d'entreprises informatiques après une erreur de jeunesse s'étant soldée par une rencontre mémorable avec le système pénal. Dans ce réseau, le piratage se révélait être un passe-temps qui procurait un sentiment de liberté et d'excitation à des individus dont les perspectives professionnelles et personnelles étaient, au mieux, incertaines. Il s'explique au mieux comme le prolongement naturel ou la diversification d'une trajectoire criminelle à l'état embryonnaire plutôt que comme un faux pas dans une biographie apparemment sans histoire.

D'après la typologie des voleurs d'identité élaborée par Heith Copes et Lynne Vieraitis, les pirates informatiques désireux de réussir financièrement ont besoin de trois types de compétences : des capacités techniques, des compétences de monétisation et des compétences sociales. L'examen du degré de réussite des pirates arrêtés, individuellement et collectivement, dans chaque catégorie, démontre que les compétences techniques sont essentielles mais insuffisantes, et que les compétences sociales et de monétisation sont beaucoup plus rares que les capacités techniques.

Dans le cadre de ce réseau de piratage, les compétences techniques correspondent à l'expertise susceptible d'être mobilisée pour la constitution, le déploiement et la maintenance d'un immense bassin d'ordinateurs stables et furtifs. Si les pirates informatiques les plus doués sont capables de créer des réseaux de zombies originaux, la plupart des *botmasters* (les personnes qui dirigent et gèrent les réseaux) préfèrent télécharger des codes malveillants existant dans divers forums Internet et modifier ces appli-

cations génériques pour les adapter à leurs besoins. Parmi les 10 pirates, l'un pourrait être qualifié comme l'expert technique du réseau, capable de modifier considérablement les codes malveillants originels. À l'époque de son arrestation, il contrôlait presque la moitié des machines compromises qui avaient été infectées par ce réseau (291 000 ordinateurs). Les autres membres du groupe avaient des capacités techniques beaucoup plus modestes ; même s'ils se montrèrent d'avides attaquants, l'insuffisance de leurs compétences freinèrent leur capacité à voler des numéros de carte de crédit et des informations bancaires à leurs victimes. Ils éprouvèrent également des difficultés à maintenir leur infrastructure.

Les compétences techniques nécessaires pour monter et opérer un vaste réseau de zombies sont loin d'être négligeables, et seuls ceux qui sont prêts à y investir des sommes d'argent ou des quantités considérables de temps peuvent dépasser la première phase d'expérimentation. Le talent joue également un rôle : au-delà d'un certain niveau de complexité, la motivation elle-même ne suffit pas pour acquérir les habiletés indispensables. Même si des pirates montrant une expertise technique rudimentaire peuvent causer d'importants dommages aux systèmes informatiques, ces apprentis deviennent plus forts principalement grâce aux mentors qui structurent la capacité technique de leur réseau.

Savoir comment contrôler des milliers de machines vulnérables permet au pirate de lancer des attaques contre le système informatique d'un adversaire ou de voler des identifiants bancaires, mais convertir ces habiletés en revenus exige une seconde catégorie de compétences, celles de la monétisation. Elles comprennent un éventail de savoirs, notamment une compréhension de la valeur approximative que divers types d'informations volées peuvent atteindre sur les marchés clandestins ; une connaissance des forums en ligne sur lesquels on peut vendre les données dérobées, louer des réseaux de zombies ou recruter des complices pour vider des cartes de crédit et des comptes bancaires ; une familiarité avec les autres outils financiers régissant les transferts d'argent entre acteurs illicites et avec les règles tacites qui encadrent ces échanges ; ainsi qu'une connaissance des procédures de sécurité qui sont mises en œuvre par les vendeurs en ligne, les magasins de type classique ou les institutions bancaires pour empêcher la fraude et les prises de contrôle non autorisées des comptes de leurs clients.

À ce chapitre, et bien que les membres les plus doués du réseau aient montré des compétences techniques supérieures à celles de simples débutants, leurs compétences en matière de monétisation étaient très limitées. Même l'expert technique du réseau, qui avait grand besoin d'argent, éprouvait des difficultés à convertir des opportunités apparemment simples en argent comptant. Ce qui empêchait ce pirate d'exploiter des numéros de carte de débit volés n'était pas lié à une sorte d'éthique supérieure, mais à un manque de connaissance concernant les types de fraudes les plus élémentaires.

Être un pirate informatique expérimenté et se révéler un fraudeur compétent sont deux réalités bien distinctes. Contrôler un immense réseau de zombies capable de moissonner des milliers de numéros de carte de crédit ne fait pas systématiquement la fortune d'un pirate, sauf si celui-ci dispose d'autres compétences indispensables et de la volonté de prendre quelques risques dans le monde réel. Il semble qu'aucun des autres membres du réseau n'ait développé de solides compétences de monétisation. Le manque de sophistication monétaire démontrée se retrouve également dans le mode de paiement qu'ils privilégiaient, à savoir les virements bancaires sur leurs comptes personnels, ces derniers étant détenus auprès de la même banque que celle qu'ils ciblaient majoritairement dans leurs campagnes d'hameçonnage.

La littérature scientifique sur les pirates informatiques émet généralement l'hypothèse que de vastes réseaux de zombies ne peuvent que générer des revenus proportionnels, mais d'après les données en notre possession, une telle corrélation semble loin d'être systématique. De plus, lorsque les compétences techniques et de monétisation sont détenues par différents membres du réseau, ce sont les compétences sociales qui deviennent indispensables.

Dans le contexte d'Internet, la manipulation des victimes se fait tout d'abord par des moyens techniques, et les compétences sociales jouent un rôle moins central dans les interactions délinquant-victime. Cependant, elles sont essentielles quand il s'agit de trouver des complices possédant l'expertise technique ou de monétisation requise, puisque les occasions de rencontres traditionnelles, telles que le voisinage, les activités partagées de loisirs ou les séjours en prison, ne sont pas accessibles aux cybercriminels. Les compétences sociales requises incluent la capacité à établir et à maintenir des liens interpersonnels productifs, au moyen de communications électroniques, avec des complices fiables n'ayant jamais été rencontrés en personne. La capacité à générer et à cultiver la confiance

Dans ce réseau, le piratage se révélait être un passe-temps qui procurait un sentiment de liberté et d'excitation.

constitue donc un indicateur qualitatif robuste des compétences sociales dont dispose un délinquant.

De 2006 à 2007, le réseau étudié, qui était initialement caractérisé par un degré de confiance élevé, s'est transformé en un collectif miné par la méfiance. Vers la fin de 2007, par exemple, les rivalités internes menèrent à l'expulsion de deux membres, les leaders techniques et sociaux ayant décidé d'utiliser leurs propres réseaux de zombies pour lancer des attaques contre eux. En moins de 24 mois, ce réseau, qui n'avait pas (encore) été l'objet d'une intervention policière et opérait librement, devint spontanément instable et perdit une part de son efficacité. D'importantes ressources durent être diverties des projets de piratage afin de gérer les retombées de nombreux incidents survenus.

Le manque de maturité affiché par les membres du réseau, associé à l'existence d'outils puissants mobilisables à des fins malveillantes, explique dans une certaine mesure pourquoi des relations déjà fragiles se transformèrent rapidement en conflit ouvert. Mais on peut aussi imputer l'instabilité de ces liens sociaux aux caractéristiques structurelles d'Internet, notamment : la capacité à changer d'identité numérique à loisir et à adopter de nouveaux pseudonymes lorsqu'une réputation a été entachée ; le bassin illimité de complices potentiels que l'on peut rencontrer en ligne ; et les faibles risques d'être exposé à la violence physique comme mécanisme de régulation et de contrôle, en raison des distances géographiques et de l'anonymat. Ces facteurs contribuent à réduire les effets d'éventuelles malversations et trahisons ainsi qu'à exacerber la méfiance, une attitude latente parmi les délinquants.

Somme toute, force est de constater que les pirates informatiques ne sont ni des techniciens investis de pouvoirs surnaturels, ni des adolescents asociaux, mais des contrevenants confrontés à des enjeux d'ordre pratique que connaissent bien les délinquants de type plus traditionnel. La taille réduite de ce réseau de pirates et sa nature très localisée interdisent manifestement toute prétention de représentativité, mais des enquêtes journalistiques plus approfondies sur des collectifs de pirates plus sophistiqués et rentables, ont récemment révélé des schémas identiques de méfiance, d'hostilité et de trahison. La carrière criminelle des délinquants qui s'adonnent indifféremment à la criminalité de rue et à la cybercriminalité est donc un thème prometteur, offrant des perspectives de recherche fascinantes. De telles connaissances sont indispensables pour nuancer le discours actuel sur la cybersécurité, trop souvent ponctué de déclarations catastrophistes sur les risques émergents et présentant les pirates informatiques comme un péril numérique imminent nécessitant des pouvoirs de réglementation et des outils de surveillance extraordinaires. Comme le démontre cet article, les pirates ne tirent pas que des avantages des déficiences et des imperfections d'Internet — dans une certaine mesure, ils peuvent eux aussi en être les victimes. ■