Université de Montréal

Les Botmasters et leurs rôles dans le marché des botnets

par Chloé Majdalany

École de Criminologie,
Faculté des Arts et des Sciences

Travail dirigé présenté à la Faculté des études supérieures et postdoctorales en vue de
l'obtention du grade de Maîtrise ès Sciences (M.Sc.)
en Criminologie option Criminalistique et information

Septembre 2017

Résumé

Les botnets continuent à présenter une préoccupation réelle dans la sphère virtuelle. Ces réseaux d'ordinateurs corrompus facilitent la prolifération des crimes en ligne de façon à atteindre une quantité énorme de victimes. De nombreuses études traitent ainsi des mécanismes d'infection de machines ainsi que des comportements de ces botnets. D'ailleurs, les conséquences qui en découlent sont elles aussi bien documentées. On constate cependant un manque dans la littérature en ce qui concerne les botmasters, les pirates informatiques qui créent et contrôlent de tels réseaux. À l'aide d'analyses de contenus du forum Dark0de, 88 botmasters ont été identifiés et catégorisés en fonction des rôles qu'ils occupent dans le marché de botnets. Cette étude exploratoire vise à évaluer le statut, la réputation, le taux d'activité ainsi que les expertises de ces botmasters, soit : les codeurs, les commerçants, les distributeurs, les opérateurs, les curieux, ainsi que les individus qui monétisent les botnets et qui affirment être expérimentés dans ce domaine. Cette étude permet de conclure que les distributeurs et les opérateurs de botnets sont les membres les plus réputés dans leur communauté. C'est auprès des commerçants ainsi que des botmasters d'expériences que l'on retrouve les membres avec les meilleurs statuts du forum. Les catégories de botmasters les plus actifs au sein de Dark0de sont les opérateurs et les commerçants. La plupart des botmasters à l'étude ont été identifiés dans un forum de piratages différent de Dark0de, ou aucun. Pour finir, à part pour les codeurs, dont plus de la moitié se spécialise en programmation, et les botmasters d'expérience, dont le tiers n'ont qu'une seule spécialisation, les autres sujets possèdent diverses expertises non reliées au botnets.

Mots-clés : botnets, botmasters, forum, réputation, statut, activité, publications, compétences, expertises

Abstract

Botnets still represent one of the biggest threats in cyberspace. These corrupted computer networks are used to facilitate the propagation of cybercrime and to reach simultaneously an important number of victims. Previous studies have covered subjects such as the bot infection mechanisms, botnets' behaviour and also the consequences of their usage. While botnets are well documented, there is a gap in literature regarding botmasters, the hackers responsible for creating and controlling these networks. To understand better those individuals, a content analysis of the underground forum Dark0de helped identify a pool of 88 botmasters that were categorised according to their roles in the botnet market. This preliminary study aims to measure the status, reputation, activity and expertise of botmasters according to their groups: coding, business, distribution, operation, monetization, interest and experience. Preliminary results indicate that distributors and operators have a better reputation in their community, while traders and experienced botmasters have higher statuses in the forum. Operators and traders are the most active botmasters in this forum. Also, most of the botmasters in this study have been found in another forum or none. Finally, except for half of the coders and a third of experienced botmasters, most of these individuals possess many expertise in different fields than botnets.

Key words: botnets, botmasters, forum, reputation, status, activity, publications, competence, expertise

Table des matières

Liste des figures

Liste des tableaux

Remerciements

Je tiens à remercier mon directeur de recherche Benoît Dupont, pour son aide précieuse et ses bons conseils. Vos encouragements et votre écoute ont été grandement appréciés. Je vous remercie aussi de m'avoir accordé autant de liberté quant à cette étude, tout en me recadrant lorsque je me perdais. Merci de m'avoir donné la chance de travailler avec vous et de produire ce travail dirigé.

Je voudrais aussi remercier David Décary-Hétu, Massimiliano Mulone et Quentin Rossy pour avoir pris en charge un programme aussi unique et d'avoir rendu possible mon échange à l'Université de Lausanne. Cette expérience a été des plus enrichissantes, tant au niveau académique que personnel. Un merci particulier aussi à Eoghan Casey pour son aide et ses conseils. I can't thank you enough for your time and all your help.

Je veux aussi remercier ma famille, mes amis, mon copain ainsi que mes collègues pour leur énorme support moral! Ce sont vos encouragements, votre écoute et votre foi en moi qui m'ont permis de remettre enfin ce travail. Une mention spéciale à David, Sandra, Audrey, Olivier, Medjine, Mélanie, Romy, sans oublier Christelle et Noémie! Je vous aime! Ces dernières années n'auraient pas été les mêmes sans vous.

À tous ceux et celles qui m'ont permis, de près ou de loin, d'avancer et de déposer mon travail aujourd'hui, merci de tout cœur!

Introduction

L'essor des nouvelles technologies a favorisé le développement rapide de la cybercriminalité. Cette dernière a permis de moderniser et automatiser les crimes dits plus traditionnels, tels la fraude, le blanchiment d'argent, le vandalisme et la pornographie juvénile. La cybercriminalité a aussi favorisé la création de nouvelles formes de crimes, dont l'existence ne peut être possible ailleurs que dans le cyberespace, tel : le piratage informatique, la création et la propagation de logiciels malveillants et les attaques distribuées, entre autres (Leman-Langlois, 2006).

Les intrusions et types d'attaques en ligne deviennent de plus en plus sophistiquées. Le cybercrime est coûteux pour la société, et engendrerait d'énormes pertes. Seulement l'année dernière, le cybercrime aurait coûté 450 milliards de dollars américains à l'économie mondiale (Graham, 2017). Étant donné que le cybercrime n'obéit pas aux frontières, ces crimes peuvent toucher n'importe qui sur le globe, à condition qu'ils aient des ordinateurs connectés. Au cours des dernières années, de nombreuses initiatives se sont développées dans le but d'encourager la coopération internationale comme solution pour lutter contre le cybercrime. Ces collaborations se font de plus en plus présentes tant pour les efforts de démantèlements de réseaux criminels ou encore d'arrestations à l'échelle internationales. Des coopérations entre les secteurs publics et privés aussi sont créées afin de développer des outils et méthodes en cyber sécurité, et des infrastructures sont mises en place afin de faciliter la collecte et les échanges de renseignements.

Une des priorités de ces coopératives internationales est l'enrayement des réseaux de botnets, une des plus grandes menaces dans le cyberespace à l'heure actuelle. Ceux-ci permettent la prolifération et même l'automatisation de crimes en ligne. Ces réseaux d'ordinateurs corrompus et contrôlés à distance sont exploités afin de commettre des crimes à grande échelle dans la sphère virtuelle. Une grande importance est d'ailleurs accordée à cette forme particulière de crime en ligne. En effet, parmi les 30 cybercriminels les plus recherchés par le FBI, au moins 18 étaient impliqués dans des activités criminelles relatives aux botnets (FBI - Cyber's Most Wanted, 2017). Le FBI promet même une

récompense allant jusqu'à 3 millions USD pour des renseignements qui permettront d'arrêter le botmaster responsable du virus GameOver Zeus.

Étant donné que ce type d'outil est néfaste pour les écosystèmes virtuels, de nombreuses études se sont penchées sur les mécanismes d'infection et les modes opératoires de ces réseaux. Les médias couvrent également les nombreuses conséquences qui y sont associées. Qu'il s'agisse des attaques de MafiaBoy en 2000, jusqu'au *hacking* de Yahoo en février 2017, ces cas sont grandement médiatisés au fil des années. Les phénomènes associés aux botnets sont donc bien documentés, cependant on constate que les individus responsables de ce genre d'activités sont peu abordés dans la littérature. C'est pourquoi aujourd'hui il est important de s'attarder à ces individus, surtout dans une perspective criminologique. Voilà pourquoi ce travail portera sur les pirates responsables des botnets : les botmasters.

Récemment, une opération d'envergure internationale menée par le FBI et Europol a permis le démantèlement du forum de discussion Dark0de et de l'arrestation de 28 individus dans 20 pays différents. Ce forum était réputé dans les milieux de piratage, car cette plateforme réunissait des pirates informatiques de hauts calibres. Seule l'élite des *hackers* du monde anglophone pouvait y adhérer, et ce, uniquement par invitation. Nous avons eu la chance de mettre la main sur les conversations qui se trouvaient dans ce forum privé. Puisque les forums sont structurés afin de faciliter les transactions et échanges entre les acteurs intéressés dans la vente ou l'achat de services et produits illicites (Holt et coll. 2016), ils représentent une source riche en information pour la communauté scientifique. Ce projet se penchera alors sur les données recueillies sur Dark0de afin d'étudier les acteurs qui s'adonnaient à des activités commerciales et illicites relatives aux botnets dans cette plateforme.

Ainsi, le présent travail portera sur les botmasters, plus particulièrement sur les différentes fonctions qu'ils peuvent occuper dans le marché des botnets. Dans un premier temps, un survol de la littérature sera produit dans le premier chapitre de ce travail. Un portrait global sur les connaissances actuelles en ce qui a trait aux pirates informatiques en général sera développé. Ensuite les connaissances sur les botnets seront décrites afin de mettre en évidence la nécessité de comprendre qui en sont responsables. L'état des connaissances sur les botmasters sera abordé par la suite. Le second chapitre mettra en évidence les lacunes

au niveau de la littérature ainsi que mettre en valeur le problème concernant la question des botmasters et on y développera la question de recherche et les objectifs de l'étude. Le chapitre suivant détaillera la méthodologie employée pour produire cette recherche. Un chapitre entier sera ensuite dédié à l'analyse des résultats obtenus. Finalement une brève section portera sur l'importance de l'intégration des sciences forensiques pour traiter de questions criminologiques. Ces deux disciplines vont de pairs et permettent le pont entre la recherche sur les questions criminelles et l'enquête. Une conclusion permettra enfin de clore ce travail dirigé, qui est le fruit d'une collaboration entre l'École de Criminologie de l'Université de Montréal et l'École des Sciences Criminelles de l'Université de Lausanne.

Chapitre I - Recension des écrits

Les hackers

Avec le développement des technologies et des niveaux de sophistication des tactiques et outils de cybercrime, on constate depuis les années 70 l'intérêt grandissant que la recherche porte sur les pirates informatiques, mais ces derniers captent encore plus l'imaginaire des médias et de la culture populaire dès les années 80-90. La prolifération des crimes commis dans les espaces virtuels inquiète les décideurs, les agences de mise en application des lois et les utilisateurs, d'où l'importance d'en savoir plus sur les responsables de ces crimes.

Qui sont-ils?

La représentation des pirates comme étant de jeunes garçons adolescents présentant certains traits antisociaux, avec un intérêt marqué pour la science-fiction et ayant des compétences informatiques hors pair a longtemps été véhiculée par les médias (Barber, 2001; Jordan et Taylor, 1998). Nombreuses études démographiques indiquent qu'effectivement la plupart des pirates informatiques sont de jeunes hommes ayant accompli, pour la majeure part, des études de niveau supérieur (Bachmann, 2010; Holt, 2007; Holt et coll., 2008; Jordan & Taylor, 1998 et Schell & Dodge, 2002, cités dans Holt et coll., 2012; Turgeman-Golschmidt, 2005). D'ailleurs, une étude de Turgeman-Goldschmidt (2005), se basant sur 54 entrevues de pirates israéliens, rajoute que ces individus appartiennent en général à la classe moyenne ou supérieure, et qu'ils sont habituellement non violents. Outre les traits démographiques étudiés, nombreux chercheurs se sont attardés sur les types de pirates informatiques. Ainsi, plusieurs typologies ont été développées afin de mieux les comprendre. Certaines d'entre elles s'appuient sur les compétences techniques des pirates (Barber, 2001; Dupont, 2010), d'autres vont plutôt prendre en compte la motivation combinée au niveau de compétences (Rogers 1999, Furnell, 2002, Gordon, 2001 dans Rogers, 2006; Rounds et Pendgraft, 2009; Ghernaouti, 2013), ou encore utiliser les transferts de connaissances (Zhang et coll. 2015).

La typologie de Barber (2001) distingue trois catégories de pirates : les « *script kiddies* », les « *hackers* » et les « *crackers* ». Les *script kiddies* sont des pirates ayant peu de compétences informatiques et qui ne connaissent pas vraiment les mécanismes de fonctionnement d'internet. De façon générale, ils se procurent des outils disponibles en

ligne, dans les forums et les sites de clavardage. Étant donné leurs lacunes techniques, ces nouveaux *hackers* vont souvent commettre de graves erreurs et causer énormément de dommages, et cela, même sans savoir utiliser les outils mis à leur disposition. Cette catégorie de pirates est peu appréciée par leurs pairs dans la communauté. Viennent ensuite les *hackers,* qui sont d'anciens *script kiddies* et qui ont atteint un niveau suffisant d'expérience et de compétences techniques. Ils comprennent les fonctionnements d'internet et de ses protocoles, ainsi que des outils de piratage. Les meilleurs hackers savent écrire et programmer eux-mêmes leurs codes et créent leurs propres outils. Ils ont le potentiel de travailler dans l'industrie des technologies de l'information. Leur motivation principale serait la curiosité, ce qui les distingue de la dernière catégorie identifiée par Barber (2001), les *crackers*. Les *crackers*, quant à eux, ont pour but de causer des dommages en ligne. Plus ils sont compétents, plus leurs attaques virtuelles sont dangereuses. Ils ont pour autres objectifs l'appât du gain ainsi que l'activisme politique. Somme toute, le *cracking* présuppose une intention criminelle. Malgré les différences identifiées pour chacune de ces catégories, celles-ci sont plus ou moins bien délimitées et se chevauchent. Dans une répartition similaire, Dupont (2010) nomme trois catégories générales de pirates informatiques inscrits dans un continuum. Au bas de l'échelle de compétences, on retrouve les *script kiddies*. La catégorie suivante inclurait les « pirates entrepreneurs » dont l'objectif est de générer des revenus criminels. À l'autre extrémité de ce continuum se trouve le «super-utilisateur», ressemblant aux représentations véhiculées par les médias de masse et laissant croire qu'il est omnipotent.

Rogers (2006), quant à lui, propose une typologie basée sur les études de Furnell (2002), Gordon (2001) et Rogers (1999), issue de données empiriques, et suggère neuf catégories de pirates en fonction de leurs expertises informatiques ainsi que de leur motivation, qu'il s'agisse de curiosité, de réputation, de gain financier ou de revanche. Ces catégories sont les suivantes : novice (compétences très limitées), *cyber-punk* (certaines compétences techniques, implication dans des activités illicites), *internal* (employés ou anciens employés qui utilisent leurs accès pour attaquer leurs employeurs; ils sont compétents et motivés par la vengeance), *petty thieves* (utilisation des technologies pour faciliter leurs activités criminelles, motivés par l'appât du gain), auteurs de virus, *Old Guard hackers* (motivés par l'aspect intellectuel du piratage, la curiosité et les défis, ils ne cherchent pas

à commettre des crimes), criminels professionnels (compétents et professionnels, motivés par le gain financier), *information warrior* (très compétents, leurs emplois consistent en la défense, la sécurité ou l'espionnage) et activistes politiques. Ghernaouti (2013) précise plutôt que les types de cybercriminels se définissent en fonction de trois facteurs : la motivation, les compétences et le type de profit obtenu (pas nécessairement financier). Elle rajoute d'ailleurs que les types de cybercriminels se distinguent par deux grandes catégories : les professionnels et les amateurs.

Dans un autre ordre d'idées, certains auteurs se concentrent principalement sur le concept de transfert d'information entre hackers afin de créer leur typologie. Zhang et coll. (2015) identifient quatre catégories de hackers : les gourous, les pirates occasionnels, les apprentis, et finalement les novices. Les *gourous* fournissent les connaissances et sollicitent moins d'informations auprès de la communauté. Leur réputation grandit dans le temps, et ils sont aussi très impliqués et présents dans les discussions, en partageant conseils et avis. Ce sont des acteurs centraux dans le fonctionnement des forums et dans les fils de discussions. Les *pirates occasionnels* semblent moins actifs et centraux dans les forums, cependant ils restent membres. Ils interagissent avec un nombre limité d'individus, posent moins de questions et écrivent des messages plus brefs. Ils ont de très bonnes connaissances, mais ont une moins bonne réputation que les gourous. Ils sont talentueux et toujours à la recherche de nouvelles techniques et des nouveautés sur internet. Les *apprentis* acquièrent des connaissances au fil du temps, et fournissent aussi de plus en plus d'information dans le temps. Leur réputation est généralement faible initialement, mais au fil de leurs interactions, ils gagnent une plus grande réputation que les occasionnels. Ils se trouvent dans les forums pour apprendre, et y restent membres longtemps. Ils sont très actifs dans la communauté. Les *novices*, quant à eux, posent beaucoup de questions et partagent moins d'informations, car ils ont moins de connaissances. Ils n'ont pas une bonne réputation. Ils semblent être plus jeunes et se fient principalement aux ressources qu'ils peuvent trouver en ligne afin de mener des activités en lien avec le hacking (outils et codes d'autrui), de façon similaire aux *script kiddies* (Zhang et coll., 2015).

La plupart de ces études tirent des typologies basées sur des revues de littérature (Barber, 2001; Dupont, 2010; Rogers 2006; Rounds et Pendgraft, 2009) ou d'études de cas (Dupont, 2010; Ghernaouti, 2013). Certaines vont se baser sur des entrevues (Holt, 2007; Jordan &

Taylor, 1998; Turgeman-Golschmidt, 2005), cependant, peu d'entre elles tirent leurs conclusions de données empiriques (Zhang et coll., 2015; Rogers, 1999 et Furnell 2002 cités dans Rogers 2006). Il est alors intéressant de mettre à jour les connaissances sur les typologies de pirates informatiques avec des données plus récentes et plus généralisables.

À noter que dans le cadre de cette étude, les terminologies « pirates » et « *hackers* » seront utilisées pour désigner les individus adoptant des comportements illégaux en ligne, sans faire distinction de leur niveau de compétences ou leurs motivations.

Réputation et mérite

La littérature produite au sujet des pirates informatiques fait aussi état de l'esprit de communauté qui les unit, bien qu'il s'agisse de liens virtuels entre des individus qui, souvent, ne se sont jamais rencontrés en personne (Jordan et Taylor, 1998). Des études révèlent que cette communauté se distingue par sa valorisation de l'apprentissage autonome de techniques de hacking, bien qu'il soit courant que les pirates partagent entre eux les pratiques de piratage les plus efficaces ainsi que les stratégies d'anonymisation (Holt et coll., 2012). Donc, bien que le hacking soit une activité souvent menée seule ou au sein d'un groupe de confiance très restreint, son apprentissage se fait à l'intérieur de la communauté et les individus concernés partagent des informations, des outils, des valeurs et objectifs entre eux (Holt et coll., 2012). Il est possible de retrouver dans les forums de piratage toutes sortes d'informations et de données au sujet des connaissances au niveau du hacking. De nombreux tutoriels en ligne sont accessibles et presque tout individu intéressé pourrait devenir un bon pirate s'il se dévoue à cette activité, bien qu'une part non négligeable de talent et d'esprit analytique soit nécessaire (Dupont, 2014).

Les recherches suggèrent alors que les communautés de hackers fonctionnent de manière méritocratique, ainsi les individus de cette communauté se jugent sur la base du mérite ainsi que des compétences et talents de chacun (Holt et coll., 2012; Abbasi et coll., 2014; Gosh et Turrini 2010 dans Benjamin et Chen, 2012). Les pirates perçus comme experts jouent un rôle central dans cette forme de hiérarchie, que ce soit en aidant des pirates de moins bons calibres, ou en vendant des logiciels malveillants, des outils ou encore des données volées, etc. Les nouveaux hackers vont aussi, de leur côté, acquérir des connaissances auprès de leurs pairs et ainsi se spécialiser dans différents domaines de

hacking (Holt et coll., 2012 et Benjamin et coll., 2012 cités dans Abbasi et coll., 2014). Ainsi, les observations de forums indiquent que les hackers vont partager de l'information, échanger des outils et partager des valeurs et objectifs entre eux, et, par l'intermédiaire de ces mécanismes, ils vont démontrer leurs expertises et se bâtir une réputation (Abbasi et coll., 2014). Cette réputation devient alors primordiale afin d'établir la confiance et le statut, ainsi que d'entretenir des interactions sociales au sein de la communauté (Semmans et coll., 2005, dans Benjamin et Chen, 2012). Une bonne réputation devient ainsi une forme d'indice de dévouement de la part des pirates élites à leur art, et incite au respect. Outre le prestige qu'apporte une bonne réputation, une telle attribution est d'autant plus bénéfique lorsqu'il est question d'établir des relations commerciales ou des partenariats entre pirates, dans un environnement qui nécessite le maintien d'un certain anonymat dû aux activités illicites en ligne commises. Une bonne réputation permet d'attribuer un meilleur degré de confiance entre individus pour ainsi favoriser des collaborations qui permettront de générer plus de revenus criminels (Décary-Hétu et Dupont, 2013; Dupont et coll., 2016). Au contraire, les pirates tels que les *script kiddies* qui démontrent peu d'intérêt au développement de leurs compétences techniques sont bien mal perçus par leurs pairs de la communauté et leurs contributions sont moins sollicitées (Holt, 2007).

Comme les communautés de pirates informatiques se basent sur un système de mérite, mais dans un environnement illégal, on remarque la relation paradoxale entre la recherche de reconnaissance par les pairs et la nécessité de discrétion et du secret afin de ne pas être détecté par les agents de mise en application de la loi (Jordan et Taylor, 1998; Shakarian et coll., 2016). Dans le but d'éviter toute détection policière, les pirates vont adopter diverses stratégies afin de se protéger, tels l'utilisation de pseudonymes, l'usage de connexions Internet publiques, l'utilisation de machines corrompues afin de commettre des délits sur un tiers parti (Van Eeten et Bauer, 2009; Fortin et Gagnon, 2013), utilisation de proxys anonymes[1], de Tor[2], de faux comptes d'utilisateurs ou de comptes piratés, de données bancaires volées ou encore de cartes de crédit ou comptes PayPal volés, parmi tant

[1] « En plus de masquer l'adresse IP, un proxy anonyme peut supprimer les : cookies, pop-ups, bannières, scripts et informations confidentielles en zone de saisie (identifiant et mot de passe) » (Commentçamarche.net, 2015)

[2] Un réseau Tor (The Onion Router) est conçu pour naviguer de façon anonyme sur les réseaux, et empêcher l'analyse de trafic (WhatIs.com, 2015).

d'autres. Ces techniques d'anonymisation favorisent d'ailleurs la commission de crimes entre pirates. Ainsi, pour nombreux membres de la communauté qui se tournent vers la cybercriminalité, s'associer à des pairs pour commettre leurs activités criminelles comporte des risques. C'est pourquoi la notion de réputation devient aussi importante, elle permet d'accorder une certaine confiance entre des individus qui ne se connaissent pas personnellement. Ces collaborations peuvent ensuite résulter en la facilitation d'activités criminelles en ligne et en augmentant l'efficacité de celles-ci, grâce à une tendance de division du travail et de professionnalisation des marchés (Wall, 2015).

Professionnalisation des marchés

On assiste à un changement des motifs d'attaques de piratage. Tandis que les premiers pirates des années 60 agissaient par curiosité et soif de savoirs, les générations de pirates des années 80 devenaient de plus en plus motivées par des raisons criminelles et financières (Taylor, 1999). Les échanges de biens et de services en lien au piratage permettent aux acteurs impliqués de tirer profit de leurs transactions et échanges (Dupont 2010). L'approche sociologique de l'organisation sociale développée par Best et Luckenbill (1994) a permis d'identifier les associations entre individus et groupes, ainsi que les transactions dans lesquelles ils participent. Ce cadre permet de comprendre comment ces relations sociales ont une influence sur la position d'un individu inscrit dans un réseau. Ce cadre théorique prend aussi en compte le rôle ou pattern d'activité que jouent individus dans une organisation ou sous-culture déviante. Dans le cas de transactions virtuelles illicites, les participants sont portés à adopter des comportements qui leur permettent d'obtenir une gratification financière ou autre. Chaque transaction implique une division du travail qui varie d'une action individuelle à une activité de groupe, avec des rôles distincts pour chaque participant. Adler et Adler (2006) identifient trois types de transactions qui s'inscrivent dans ce cadre conceptuel : la déviance individuelle qui requiert un unique participant, les échanges déviants, qui nécessitent deux acteurs ou plus qui collaborent chacun avec un rôle distinct, ainsi que l'exploitation déviante, où un délinquant et une victime sont en situation de conflit (Holt et coll., 2016).

Les forums de piratage sont structurés afin de faciliter les transactions et échanges entre les acteurs intéressés dans la vente ou l'achat de services et produits illicites (Holt et coll. 2016). Ces espaces virtuels réunissent une multitude d'acteurs impliqués dans ce type de

commerce. Les acheteurs et vendeurs s'y retrouvent, mais aussi des services de blanchiment d'argent, d'encaissement, de livraison ou de mule qui opèrent en petits groupes ou en partenariats (Hutchings et Holt, 2014; Holt et coll., 2016). On peut y retrouver aussi des mécanismes d'évaluation de biens et de services gérés par des vérificateurs, ainsi que des systèmes d'évaluation par les pairs. Des administrateurs sont également présents afin d'assurer une forme de contrôle informel des membres pour éviter tout abus. La présence de ces différents acteurs et des nombreux mécanismes de contrôle mis en place permettent à tous les membres d'assurer une certaine gestion de risques (Holt et coll., 2015; Holt et coll., 2016). Outre ces rôles nécessaires aux fonctionnements des marchés illicites, il est tout d'abord primordial de rendre disponible sur ces forums des outils et données convoitées, tels que des données personnelles et financières qui pourront être monétisées (cartes et identifiants bancaires par exemple). C'est pourquoi on y retrouve également des concepteurs de logiciels ainsi que des individus qui vont utiliser ces outils pour récupérer les données souhaitées. Ils peuvent aussi vendre ces produits à un autre parti ou encore monétiser les données récupérées grâce à des mules[3] entre autres (Dupont, 2010).

Ces différents rôles dans les marchés seraient attribuables en partie aux compétences des individus de la communauté de pirates informatiques (Holt et coll., 2012). En effet, nombreuses études relèvent qu'une grande partie des hackers que l'on retrouve dans la communauté auraient des compétences rudimentaires en ce qui a trait aux technologies informatiques. Bien que certains développent leurs connaissances, ils ont de profondes lacunes en ce qui concerne les fonctionnements des réseaux et logiciels. Une part moins grande de la communauté comprend les pirates ayant certaines compétences et qui sont aptes à mener des attaques et en comprendre les mécanismes. Une portion encore plus faible d'individus inclurait les pirates qui, non seulement savent comment mener des attaques, mais sont aussi en mesure de concevoir les outils et logiciels nécessaires pour mener leurs activités (Furnell, 2002; Holt, 2007; Jordan & Taylor, 1998; Schell & Dodge, 2002; et Taylor, 1999, cités dans Holt et coll., 2012). Cette répartition de compétences

[3] Une mule permet d'acheminer de l'argent frauduleusement acquis à des criminels (SafeInternetBanking.be, 2014). Lorsque les devises gagnées illicitement sont transférées dans un compte en banque, un service de mule est requis pour retirer l'argent papier du compte et l'envoyer à son propriétaire dans le monde réel.

indique alors que le transfert de connaissances et d'outils part des pirates ayant le plus de connaissances vers ceux qui en ont le moins. Ainsi, avec l'importance grandissante des marchés virtuels illicites, les études laissent à suggérer que les pirates les plus compétents peuvent profiter plus en offrant leurs services à ceux qui le sont moins (Chu et coll., 2010; Holt & Lampke, 2010; Holt et coll., 2008; Honeynet Research Alliance, 2003; et Thomas et Martin, 2006, cités dans Holt et coll., 2012). Ces marchés réduisent la nécessité de détenir des compétences informatiques exceptionnelles pour pouvoir mener des attaques de grande ampleur, et ainsi engendrent une certaine relation de dépendance envers les pirates les plus compétents (Chu et coll., 2010; et Holt & Lampke, 2010, cités dans Holt et coll., 2012). En somme, ce modèle présuppose qu'un grand nombre d'individus, peu compétents, dépend de l'expertise d'un faible nombre de pirates pour développer divers outils que ces derniers pourront tout de même utiliser, quel qu'il soit. Ces outils et services peuvent même permettre à un hacker de bas niveau de mener des attaques informatiques à grande échelle. Ainsi, un *script kiddie* pourrait aisément se procurer les outils nécessaires auprès d'un autre pirate pour mener une attaque par déni de service (DDoS)[4] ou encore une campagne de pollupostage par exemple, par le moyen d'un botnet.

Ce bref aperçu de la littérature au sujet des pirates informatiques permet de suggérer qu'ils sont bien souvent étudiés de manière générale. En d'autres mots, nombreuses typologies tentent de les classifier selon différents facteurs tels la motivation, les compétences ou le transfert d'information. À l'heure actuelle, il serait pertinent de se centrer sur les différentes activités illicites qu'ils peuvent mener. Celles-ci sont tellement variées qu'il serait intéressant d'évaluer si des typologies basées sur le type de crime seraient aussi adaptées. Ainsi étudier les pirates en fonction de leurs spécialisations, qu'il s'agisse de fraude, d'ingénierie sociale, de carding, d'intrusion de machine ou de contrôle de botnets, pourrait s'avérer une piste intéressante pour de futures recherches. Dans le cadre de la présente recherche, la spécialisation relative aux botnets sera étudiée.

[4] Les attaques distribuées, attaques par déni de service ou *Distributed Denial of Service* DDoS, permettent de « submerger un serveur de demandes d'accès par un ensemble plus ou moins grand d'ordinateurs piratés au préalable, ou botnet (réseau zombies), qui finissent par l'empêcher de fonctionner correctement et de répondre aux demandes légitimes » (Leman-Langlois, 2006, p. 73)

Les botnets

Une propriété unique et problématique du cybercrime est qu'il a la capacité d'affecter simultanément, et même automatiquement, un nombre important de cibles, que ce soit dans l'immédiat ou à un moment ultérieur, en fonction de la volonté du cybercriminel. D'ailleurs, ces activités illicites peuvent être perpétrées à distance, sans être limitées par les frontières géographiques (Ghernaouti-Hélie, 2009). C'est d'ailleurs le cas des botnets qui peuvent être opérés à distance par un individu qui peut en disposer comme il le désire, et qui peut contrôler une quantité énorme de machines.

Définition

Un botnet est un réseau qui peut comprendre jusqu'à des centaines de milliers d'ordinateurs corrompus qui sont liés par un système de commande et contrôle (C&C) par un pirate informatique, le botmaster (Freyssinet, 2016; Van Eeten et Bauer, 2009; Ghernaouti-Hélie, 2009). Le « bot » (ou robot) en soi, est une machine infectée par un logiciel malveillant qui s'installe et s'exécute de façon automatique et autonome, sans que son utilisateur n'en prenne conscience (Li et coll., 2009). Une fois ces logiciels installés, ceux-ci vont rester en mode de veille et attendre les commandes du botmaster (Binsalleeh et coll., 2010). Les vecteurs principaux d'infection qui permettent le développement d'un botnet se font par l'entremise de code d'exécution téléchargé par un cheval de Troie[5], de courriels, ou de sites web malveillants. D'ailleurs, les bots peuvent être programmés pour scanner et détecter des vulnérabilités dans les réseaux pour ensuite infecter d'autres machines mal protégées (Ghernaouti, 2013).

Utilité

Les botnets seraient la plateforme idéale pour commettre des activités illicites à grande échelle, et d'ailleurs, ceux-ci seraient la cause de la majorité des attaques informatiques sur Internet (Ramsbrock et coll., 2008; Binsalleeh et coll., 2010). Nombreuses utilités leur sont attribuées étant donné qu'ils agissent comme facilitateurs dans la commission d'activités illicites en ligne. L'efficacité et la versatilité des botnets en font un outil particulièrement

[5] Un cheval de Troie ou *Trojan Horse* est un logiciel malveillant d'apparence légitime qui téléchargé à l'insu du propriétaire de l'ordinateur et qui en permet, entre autres, le contrôle à distance par un pirate informatique (Kaspersky Lab).

prisé par les cybercriminels (Décary-Hétu et Dupont, 2013). Dans son usage plus courant, le botnet permet au botmaster de commettre des actes criminels virtuels à grande échelle telle que : envoyer du pourriel, exploiter des vulnérabilités informatiques, propager des logiciels malveillants et des virus, voler des informations telles des données bancaires et personnelles ou encore de comptes de messagerie électronique, frauder des victimes et leur extorquer de l'argent, envoyer des campagnes d'hameçonnage, faire de la fraude par clics, gonfler artificiellement le trafic de certaines pages web et mener des attaques distribuées, entre autres (Rajab et coll., 2002; Ghernaouti-Hélie, 2009; Li et coll., 2009; Stone-Gross et coll., 2009; Brenner, 2010; Krebs, 2012; Décary-Hétu et Dupont, 2013). Dans des cas extrêmes, les botnets pourraient potentiellement être employés pour mener des attaques militaires et terroristes, et aussi nuire à la sécurité nationale de plusieurs états, aux systèmes financiers ainsi qu'aux systèmes de télécommunications en général (Ghernaouti-Hélie, 2009; Van Eeten et Bauer, 2009; Farwell et Rohozinski, 2011; Ghernaouti-Hélie, 2013). Le contrôle d'un tel réseau génère nombreux impacts vis-à-vis la déstabilisation de systèmes et d'infrastructures, les gains et pertes financiers et la sécurité de données personnelles et confidentielles, tant auprès des particuliers que des entreprises, des institutions et des États (Ghernaouti-Hélie, 2009).

L'opération d'un botnet peut avoir des retombées lucratives. En effet, cet outil permet d'envoyer des pourriels (*spam*) de nature frauduleuse, c'est-à-dire envoyer massivement des campagnes d'hameçonnage ou de fraudes de types nigérians, ou encore de voler des données bancaires. Une autre manière de rentabiliser un botnet est de mener des attaques distribuées : les botmasters se retrouvent ainsi dans une position avantageuse pour extorquer de l'argent à leurs victimes, soit en leur faisant du chantage, ou encore en les « encourageant » à acheter un logiciel qui prévient ce type d'attaques à un coût exorbitant (Brenner, 2010). On peut donc supposer que le gain financier est une motivation importante de la diffusion et l'opération d'un botnet par un botmaster.

Cependant, opérer un botnet n'est pas l'unique façon de tirer profit d'un tel réseau. Bien qu'il soit possible qu'un individu puisse créer son propre logiciel pour développer son réseau et l'opérer lui-même, il est beaucoup plus aisé d'acheter et télécharger des programmes clés en main. Cela permet alors à des individus ayant peu de compétences

techniques et informatiques de bâtir et contrôler leur propre botnet. Ainsi, les auteurs de ces programmes peuvent tirer énormément de profits par la vente de leurs logiciels, avec des prix variant entre 500$ et 10 000$ (Rouse, 2012; The Associated Press, 2016) pour certains d'entre eux. De plus, il est aussi possible de vendre des bots à l'unité pour la somme modique de 0,10$ et moins par machine (Décary-Hétu et Dupont, 2013; Donohue, 2013), ou même encore louer un réseau d'ordinateurs préalablement infectés. Les prix de location peuvent varier selon le nombre de machines corrompues, de leur géolocalisation et de la durée d'accès désirée (Dupont, 2010).

En somme, les botnets augmentent l'efficacité des marchés virtuels illicites grâce à une infrastructure qui permet la propagation d'activités criminelles à grande échelle. D'ailleurs, la commercialisation de ces botnets réduit les compétences techniques requises pour construire et opérer un tel réseau, grâce à la vente de logiciels simples à utiliser, ou la location de botnets déjà développés (Décary-Hétu et Dupont, 2013). Étant donné qu'il devient de plus en plus aisé pour quiconque de prendre contrôle d'un botnet et d'avoir un potentiel d'utilisation problématique et très dommageable, il devient alors pertinent de comprendre qui sont les acteurs impliqués dans ce marché important.

Les botmasters:

Qui sont-ils?

Les botnets peuvent être très dommageables et couteux pour la société en termes de conséquences. Il s'agit d'ailleurs de la plus grande menace dans le cyber espace à l'heure actuelle. Il devient alors important de comprendre davantage qui sont les botmasters, responsables de ces dommages, et de tenter éventuellement d'établir si ceux-ci auraient des caractéristiques qui les distingueraient des hackers en général, ou alors pas du tout puisqu'il est maintenant facile pour quiconque d'avoir accès à des botnets, ou encore s'ils appartiennent à une sous-catégorie de pirates spécialisés. Il devient donc nécessaire de s'attarder aux caractéristiques de ces individus, à savoir connaître leur profil sociodémographique et psychologique, comprendre leurs motivations, leurs compétences ainsi que le processus de développement de leurs connaissances. Cependant peu de recherches ont été produites sur le sujet et c'est ce que la communauté scientifique constate (Ramsbrock et coll., 2008; Binsalleeh et coll. 2010). Ce que la littérature semble indiquer

est que les botmasters sont des hommes caucasiens, âgés de 19 à 31 ans, qui ont développé un intérêt pour le piratage et les technologies de l'informatique en très bas âge (Krebs 2010 dans Décary-Hétu, 2011; Dupont, 2012). D'ailleurs, ce profil concorde avec la littérature existante sur les pirates informatiques (Bachmann, 2010; Holt, 2007; Holt et coll., 2008; et Schell & Dodge, 2002, cités dans Holt et coll., 2012; Jordan et Taylor, 1998). Bien qu'ils portent un intérêt marqué pour l'informatique, très peu ont étudié dans ce domaine. D'ailleurs, leur niveau scolaire serait plutôt bas, tout comme leurs aspirations professionnelles (Dupont, 2012) contrairement aux études de pirates menées par Turgeman-Golschmidt (2005). Les recherches montrent aussi un certain niveau d'immaturité et une tendance à l'impulsivité chez les botmasters par rapport à leurs décisions et leurs choix d'actions, caractéristiques qui vont de pair avec leurs jeunes âges (Dupont, 2012). Il faut cependant rester prudent face à ces résultats puisqu'un faible échantillon d'individus a été utilisé dans cette étude (N=10) (Dupont, 2012). Au niveau des motivations, la littérature indique d'un côté que l'appât du gain serait suffisant comme motivation criminelle (Décary-Hétu, 2011), tandis que pour d'autres botmasters, il est plutôt question du sentiment de liberté et de plaisir que leur procurent leurs activités (Dupont, 2012).

La firme de sécurité informatique Radware définit le botmaster comme une personne qui opère l'exécution de tâches de commande et contrôle (C&C) des botnets à distance. Le botmaster va trouver des stratégies pour dissimuler son identité par l'intermédiaire de proxys, ou Tor pour camoufler son adresse IP et ainsi éviter la détection policière. Cependant, il n'y a pas que la prise de contrôle d'un botnet qui est problématique. Plusieurs acteurs sont impliqués non seulement dans le contrôle des botnets, mais aussi dans son marché. Ainsi les botmasters peuvent être considérés comme des entrepreneurs de l'industrie des botnets, en occupant diverses fonctions dans l'économie (Décary-Hétu et Dupont, 2013). De ce fait, la littérature révèle qu'il existe différents rôles pouvant être attribués aux botmasters. Ils seraient responsables de la création des logiciels malveillants servant à corrompre les systèmes (Binsalleeh et coll. 2010), de la distribution et de l'élargissement du réseau à plus grande échelle (Thomas et Martin, 2006), de la prise de contrôle du botnet afin de commettre des activités illicites et en tirer profit (Auray et Kaminsky, 2006; Abu Rajab et coll., 2006; Ghernaouti-Hélie, 2009; Li et coll., 2009;

Brenner, 2010), du maintien du réseau afin d'éviter la détection et de continuer les activités clandestines pour une plus longue durée (John et coll., 2009; Stone-Gross et coll., 2011), ainsi que de la monétisation des botnets par la vente d'outils ou de services, ou encore par la conversion de données volées en liquidité (Auray et Kaminsky, 2006; Stone-Gross et coll., 2011; Wall, 2015; Zhuang et coll., 2008). Techniquement, chacun de ces rôles pourrait être accompli soit par différents individus ou un même botmaster. La littérature indique cependant, une tendance de professionnalisation du marché des botnets et de la division du travail.

Professionnalisation

Il devient de plus en plus commun pour un individu, ou un regroupement, ayant peu de compétences informatiques de pouvoir se procurer des codes et programmes clé en main ou encore acheter des services, lui permettant ainsi d'opérer ses propres réseaux zombies (Stone-Gross et coll., 2011; Dupont, 2010; Wall, 2015). Il devient aussi possible de louer un réseau déjà développé à un groupe ou un particulier, afin que ces derniers puissent mener directement des attaques sans avoir à fournir beaucoup d'efforts (Auray et Kaminsky, 2006; Décary-Hétu et Dupont, 2013). On comprend donc que la plupart des acteurs impliqués dans ce type d'attaques n'auraient pas la capacité à coder ou encore à opérer un botnet de façon optimale (Dupont, 2012). De plus, l'aptitude à monétiser les données amassées par l'utilisation d'un botnet n'est pas acquise pour tous les botmasters. Alors que certains seraient plus habiles à contrôler les réseaux, d'autres seraient plus expérimentés dans les stratégies de commercialisation des données volées (Dupont, 2012). Malgré que la plupart des botmasters ne disposent pas de compétences en matière de codage, ils vont tout de même développer des capacités techniques qui leur permettront de dissimuler leur identité en ligne et protéger leur anonymat (Décary-Hétu, 2011).

On constate rapidement qu'il n'est plus simplement question d'avoir des compétences informatiques pour bénéficier efficacement d'attaques virtuelles. Des compétences sociales, administratives et financières ou, du moins, la compréhension de certains de ces domaines deviennent toutes aussi essentielles afin de rentabiliser les activités en lien avec les botnets. Il est rare qu'un seul individu possède toutes ces aptitudes, il est donc important d'assurer une répartition des tâches entre collaborateurs afin de maximiser les gains et

réduire les risques associés à ce type d'activités, telles la détection et l'interruption des réseaux (Dupont, 2010; Dupont, 2012). De tels associations et regroupements seraient signe de maturation des botmasters et de sophistication de leurs pratiques criminelles (Décary-Hétu, 2011). Ainsi, les cybercriminels se retrouveront sur des plateformes d'échanges comme les forums de discussion ou encore les marchés virtuels illicites afin de développer des relations de collaboration.

Malgré cette tendance à la division du travail, les études indiquent que de nombreuses tensions peuvent être détectées dans les communautés de botmasters. Les relations entre ces acteurs seraient pour la plupart conflictuelles et imprégnées de manque de confiance envers autrui. Ceci serait causé par l'esprit de compétition féroce entre ces individus qui doivent d'ailleurs être en mesure de déjouer les tromperies, les attaques et les vols de leurs botnets par leurs pairs (Décary-Hétu, 2011; Dupont, 2012).

Réputation

La réputation et le mérite des botmasters ne seraient pas bâtis uniquement à partir de leurs niveaux de compétences. Dans la communauté des botmasters, le nombre de jours passés sur un forum, la fréquence de publication de messages, le niveau d'expérience et de connaissances, et l'échange et le partage de savoirs sont des facteurs influençant positivement l'attribution de points de réputation. Recevoir des prix et mentions de la part de sa communauté améliore aussi leurs scores, tout comme référer de nouveaux membres, ou encore avoir un large réseau personnel, ce qui permet de faciliter l'accès du botmaster à des ressources et de potentiels partenaires (Décary-Hétu et Dupont, 2013). Il semblerait aussi que les membres plus jeunes se voient décerner plus de points de réputation que leurs pairs plus âgés. Ce résultat pourrait s'expliquer par le fait que les gens plus âgés ne sont pas à jour dans leurs connaissances sur les développements technologiques constants, ou encore par le fait que les jeunes passent plus de temps que leurs comparses en ligne et interagissent plus dans leur communauté. Toutefois, puisque les pirates laissent rarement leurs véritables informations personnelles accessibles, incluant leur vrai âge, il faut rester prudent dans l'interprétation des données (Décary-Hétu et Dupont, 2013). Malgré tous ces éléments, le facteur principal qui influence la réputation des botmasters est celui de l'appartenance à un groupe exclusif et privé (Décary-Hétu et Dupont, 2013). Bâtir une

bonne réputation est central dans ce type de communauté, car c'est ainsi que les différents acteurs pourront développer des liens de confiance nécessaires à la réalisation de leurs projets criminels. Non seulement ils doivent construire cette réputation, mais ils doivent par la suite la maintenir et éviter de la ternir (Décary-Hétu et Dupont, 2013).

Ce que ces études permettent alors de constater est que le phénomène des botnets est mieux compris que les individus qui s'adonnent aux activités relatives à ces réseaux. On comprend aussi qu'opérer un botnet requière nombreuses étapes, de sa création jusqu'à sa monétisation et que chacune de celles-ci nécessite des compétences différentes. Ce que la littérature ne fait pas est d'examiner qui sont les botmasters. D'ailleurs, les recherches existantes ne permettent pas d'établir si ces derniers se différencient des pirates informatiques en général, ou encore s'ils consisteraient en une sous-catégorie de hackers. Pour se faire, il faudrait les étudier et les comparer. La littérature n'adresse pas non plus comment les différents botmasters se distinguent entre eux en fonction de leurs compétences ou encore de leurs rôles dans ce marché illicite, bien que ceux-ci soient diversifiés et complémentaires.

Chapitre II – Problématique

La littérature scientifique a beaucoup documenté les divers impacts des botnets et de leur importance sur le crime dans l'ère moderne. Les conséquences de ces réseaux peuvent avoir des effets néfastes à plusieurs niveaux, les victimes de ces attaques pouvant être des usagers d'Internet, des entreprises ou encore des institutions gouvernementales (Ghernaouti-Hélie, 2009). En plus de causer des dommages à leurs cibles, l'opération de botnets peut tout de même avoir des retombées lucratives pour ses auteurs et opérateurs. Ces réseaux de machines corrompues permettent de mener des activités illicites à distance par un individu qui peut en disposer comme il le désire, et qui peut contrôler une quantité énorme de machines. De par leur nature, les botnets seraient alors la plateforme idéale pour commettre des activités illicites à grande échelle. D'ailleurs, ceux-ci seraient la cause de la majorité des attaques informatiques sur Internet (Ramsbrock et coll., 2008; Binsalleeh et coll., 2010). Nombreuses études traitent ainsi des impacts des botnets et les conséquences néfastes qu'ils peuvent engendrer aux différents usagers d'Internet (Ghernaouti-Hélie, 2009), cependant, les botmasters qui contrôlent ces réseaux restent peu étudiés. Certaines recherches vont toutefois permettre d'inférer que différents rôles leur sont attribués, tels que la création du logiciel, la distribution du réseau, la prise de contrôle du botnet, le maintien du réseau, ainsi que la monétisation des botnets (Binsalleeh et coll. 2010; Thomas et Martin, 2006; Auray et Kaminsky, 2006; Abu Rajab et coll., 2006; Ghernaouti-Hélie, 2009; John et coll., 2009; Li et coll., 2009; Brenner, 2010; Stone-Gross et coll., 2011; Wall, 2015; Zhuang et coll., 2008). De plus, la littérature indique une nouvelle tendance de professionnalisation du marché des botnets et de la division du travail. Il devient de plus en plus commun pour un individu ayant peu de compétences informatiques de pouvoir se procurer des codes et programmes clé en main ou encore acheter des services, lui permettant ainsi d'opérer ses propres réseaux zombies (Stone-Gross et coll., 2011; Wall, 2015). C'est ainsi que les différents acteurs impliqués dans ce marché illicite vont se retrouver sur les forums de piratages en ligne. Ce lieu de communication virtuelle devient alors la plateforme d'échange idéale pour faciliter les transactions entre pirates, puisqu'ils vont permettre aux individus ayant des intérêts similaires de se rassembler dans un lieu

relativement structuré, en plus de permettre de rester anonymes et d'indiquer quels membres sont plus dignes de confiance dans le cadre de transactions efficaces (Holt et al, 2016; Yip et coll., 2013).

Outre ces tendances, l'étude sociale des caractéristiques de ces individus, de leurs profils, et de leurs expertises et compétences n'est pas abordée dans les recherches (Ramsbrock et coll., 2008; Binsalleeh et coll. 2010). Il s'agit d'un manque flagrant dans la recherche scientifique en criminologie. Pour essayer de combler cette lacune, une étude québécoise a tenté de produire un profil des botmasters suite à l'opération Basique menée par la Sûreté du Québec qui permit la mise en accusation de dix individus responsables du contrôle de plus d'une centaine de botnets (Dupont, 2012). Cependant, cette étude est peu représentative.

Il devient alors primordial de s'attarder à la question des botmasters afin de comprendre davantage leurs rôles dans le marché des botnets. L'acquisition des connaissances au sujet de ces individus est essentielle dans le domaine de la criminologie afin de trouver des pistes d'interventions plus appropriées pour lutter contre cette forme particulière du cybercrime. Actuellement, les méthodes de démantèlement de botnets sont peu efficaces puisqu'il s'agit d'un type de réseau assez résilient. En effet, s'attaquer à la structure d'un botnet n'a que de faibles conséquences étant donné qu'il peut être très aisément réactivé (Dupont, 2014). D'ailleurs, même si un botnet est démantelé, les botmasters ne sont pas souvent retrouvés par les agences de mise en application de la loi, ils peuvent donc se bâtir un nouveau botnet en toute impunité (Ramsbrock, 2009).

Dans le cadre de la présente étude, il ne sera pas possible de traiter des caractéristiques sociodémographiques des botmasters, étant donné que ces informations sont difficiles d'accès. Idéalement, pour étudier ces variables il faudrait avoir accès aux données personnelles des botmasters. Toutefois, tant qu'ils ne sont pas identifiés, retracés ou arrêtés, seules des données issues de leurs profils en ligne sont accessibles, cela implique souvent des comptes créés à l'aide de fausses dates de naissance ou encore des informations erronées en ce qui concerne leur localisation géographique. Puisque cet aspect est plus complexe à évaluer, il sera alors question d'aborder les compétences et les rôles de ces pirates dans les marchés de botnets, et plus spécifiquement dans les marchés exclusifs. Pour

se faire, les contenus du forum de discussion Dark0de concernant les botmasters seront analysés.

Étant donné les connaissances scientifiques limitées portant sur les botmasters, l'objectif principal de ce travail sera de comprendre davantage qui sont ces individus, à l'aide d'une démarche exploratoire. Il sera ainsi question d'étudier les compétences et les expertises informatiques de ces sujets, leur réputation et statuts dans le forum, leur activité au sein de la communauté ainsi que les rôles qu'ils occupent dans le marché des botnets. Pour atteindre cet objectif, les botmasters seront, dans un premier temps, classifiés selon leurs rôles dans le marché des botnets. Dans un second temps, pour chacun de ces rôles, un portrait global des compétences, du statut et de l'activité des botmasters sera dressé. Pour finir, les différentes catégories de botmasters définies dans le cadre de cette étude seront comparées entre elles, afin de mettre en évidence leurs différences de profils.

Chapitre III – Méthodologie

Les données

Dans le présent travail, les données sont issues du forum Dark0de. Ce forum privé regroupait l'élite des pirates du monde anglophone (environ 500 membres, mais 250-300 membres actifs au moment du démantèlement); les modes d'adhésion se faisaient par invitation seulement. Dark0de figurait dans le palmarès des cinq forums criminels les plus prolifiques au monde (Europol, 2015), et était considéré comme un des forums présentant la plus grande menace globale pour les infrastructures virtuelles (FBI, 2015). Ce forum a été démantelé en juillet 2015 par le FBI, en collaboration avec le Centre Européen de Cybercrime d'Europol (EC3), ainsi que les services de police de 19 autres pays [6] (Europol, 2015). Cette opération de grande envergure a permis l'arrestation de 28 individus et la saisie d'équipements et d'ordinateurs, ainsi que des serveurs et domaines de Dark0de (Europol, 2015).

Les données exactes qui figurent dans ce travail sont des captures d'écrans de conversations trouvées dans ce forum. Un ancien membre de Dark0de aurait piraté le forum et divulgué sur le net toutes les conversations qui ont eu lieu entre 2009 et 2013. Ce pirate informatique a ainsi rendu publiques plus de 5 000 captures d'écran. Afin de répondre aux objectifs de cette étude et d'en apprendre davantage sur les botmasters, les conversations de la section « Introduction » du forum ont été sélectionnées. Cette section du forum s'est avérée très riche en information, car elle contenait l'équivalent des curriculum vitae des pirates cherchant à être membres de Dark0de. En effet, ceux-ci devaient présenter leurs compétences, expériences, intérêts ainsi qu'identifier le membre qui les a invités au forum. Ainsi, ils doivent mettre en valeur leurs connaissances et savoir-faire afin de prouver qu'ils ont leur place au sein de cette communauté avant de pouvoir être approuvés par les autres membres pour ensuite faire partie du forum. La section d'introduction devient alors une source de données privilégiée pour identifier les botmasters et en apprendre sur leur savoir-faire. Afin de déterminer qui entre dans cette catégorie, chaque individu qui

[6] Royaume-Uni, Lettonie, Australie, Bosnie Herzégovine, Brésil, Canada, Colombie, Costa Rica, Chypre, Croatie, Danemark, Finlande, Allemagne, Israël, Macédoine, Nigéria, Roumanie, Serbie et Suède.

affirmait avoir une expérience quelconque en matière de botnets a été sélectionné et compilé dans une base de données. Au total, 88 individus ont été identifiés en tant que botmasters. Ces 88 pirates constitueront l'objet d'étude.

Une fois ces individus identifiés, des recherches additionnelles sur le Web 2.0 ont été menées à l'aide du moteur de recherche Google (Holt et coll., 2012). Les mots-clés employés sont le nom d'usager du botmaster suivi de termes tels que « hacking » « hacker » « forum » afin de trouver des informations additionnelles. Cette méthode a été utilisée afin de trouver dans quels autres forums ces pirates sont actifs pour ainsi évaluer leur niveau d'activité à travers la communauté de hacking. Suite aux résultats obtenus par ces recherches, les forums les plus fréquemment utilisés ont été identifiés, soient « Hackforums », « Blackhatwolrd » ainsi que « CSU carding forum ». Ensuite, chacun des 88 pirates a été recherché à nouveau dans ces trois forums afin de s'assurer s'ils y sont présents ou pas au cas où des erreurs auraient eu lieu avec les recherches sur Google. Cette méthode s'est avérée problématique puisque les recherches dans les forums n'étaient pas fructueuses : même les individus qui, par l'intermédiaire du moteur de recherche de Google se trouvaient dans le forum en question, ne s'y trouvaient plus. Il semblerait que des changements ont eu lieu dans les archives. Celles de Hackforums par exemple n'allaient pas plus loin que 2016. Un autre problème associé à cette recherche est que les introductions de ces autres forums n'ont pas pu être accessibles afin de comparer avec les données de Dark0de : CSU et Hackforums n'en ont pas, alors que les individus dans BlackHatWorld étaient introuvables.

Ces types de recherches sont problématiques dans un tel milieu, surtout si l'on considère que Dark0de regroupe l'élite des pirates informatiques et que ceux-ci sont généralement plus soucieux de protéger leur identité. Cela emmène son lot de limites puisque certains utilisent plusieurs identifiants différents. D'un autre côté, retrouver un hacker utilisant le même identifiant dans plusieurs forums à l'aide de recherches en source ouverte pourrait indiquer une préoccupation à bâtir une meilleure réputation auprès de la communauté virtuelle.

Stratégie d'analyse

Étant donné les lacunes dans la littérature actuelle et la nature des données disponibles, la démarche employée dans cette étude sera plutôt exploratoire. Une telle méthode permettrait d'identifier des tendances sur un sujet peu documenté en criminologie. Ainsi, des recherches plus exploratoires et générales au sujet des botmasters permettraient de soulever des pistes à approfondir davantage pour des recherches futures (Dufour, 2017). Pour se faire, une analyse de contenus de la section « Introduction » du forum Dark0de a été privilégiée, car ce type de méthode favorise l'identification de thèmes importants. À partir de ces observations préliminaires, il a ensuite été possible de bâtir une grille de codification, permettant de quantifier les contenus et ainsi d'avoir une vue d'ensemble plus synthétique et de faciliter les analyses subséquentes.

Afin de répondre à l'objectif de recherche, il sera question de dresser un portrait global des types de botmasters en ce qui concerne leur place au sein de la communauté de pirates et des marchés de botnets, ainsi que leurs profils de compétences. Pour se faire, il sera surtout question de mener des analyses quantitatives descriptives à partir des données codifiées tirées des contenus du forum. Ensuite, pour les cas qui se distinguent, une analyse plus qualitative sera privilégiée. Avant de procéder aux analyses, les botmasters seront catégorisés en fonction des rôles qu'ils occupent au sein du marché de botnets.

Les catégories de botmasters

Selon les observations faites lors d'une analyse préliminaire des introductions publiées par les botmasters, ceux-ci ont été divisés en sept catégories distinctes : les codeurs, les commerçants, les distributeurs, les opérateurs, ceux qui monétisent les réseaux, les curieux et les pirates affirmant avoir de l'expérience en matière de botnets. Certaines de ces catégories ont été identifiées dans la littérature comme les auteurs de codes malveillants (Binsalleeh et coll. 2010), les distributeurs du réseau (Thomas et Martin, 2006), les opérateurs qui mènent des activités criminelles (Auray et Kaminsky, 2006; Abu Rajab et coll., 2006; Ghernaouti-Hélie, 2009; Li et coll., 2009; Brenner, 2010), et ceux qui monétisent les botnets (Auray et Kaminsky, 2006; Stone-Gross et coll., 2011; Wall, 2015; Zhuang et coll., 2008). Les données ont permis de distinguer aussi des catégories de commerçants, de curieux et d'individus expérimentés. Cependant, les activités de maintien

du réseau (John et coll., 2009; Stone-Gross et coll., 2011) ont été incluses avec celle de la distribution et de la propagation des botnets. Chacune des catégories de botmasters identifiés sera définie de la sorte :

1. Les codeurs : ces individus font de la programmation et créent les codes ainsi que les logiciels malveillants qui serviront à la création de botnets.
2. Les commerçants : ils comprennent les vendeurs et acheteurs. Ceux-ci peuvent offrir différents types de transactions telles la vente ou la location. Les vendeurs favorisent la prolifération du marché des botnets en revendant les outils ou en louant des services liés à l'opération de botnets, satisfaisant ainsi la demande élevée pour tous les produits associés. Les acheteurs peuvent ainsi se procurer aisément ces logiciels soit pour s'en servir ou encore pour les modifier et les revendre à nouveau.
3. Les botmasters qui propagent les botnets : dans cette catégorie sont inclus les individus qui ont pour fonction la distribution des logiciels malveillants par moyens de pollupostage, ou encore à travers des sites internet infectés, servant ainsi à corrompre des machines et à agrandir le réseau de botnets. Cette catégorie inclue aussi les individus qui offrent des services complémentaires à cet aspect. Cela inclus donc l'hébergement de botnets, le cryptage, ou encore l'appropriation de bots venant d'autres réseaux. Bref, tout ce qui permet d'agrandir et de maintenir un réseau de botnet.
4. Les opérateurs de botnets : ces individus opèrent les réseaux pour commettre des délits en ligne. Ils contrôlent leurs botnets par un centre de Commande et Contrôle (C&C) et vont utiliser ce réseau pour passer à l'action : vol de données, fraude, hameçonnage, attaques distribuées, etc. Cette catégorie concerne alors plus spécifiquement l'action de la prise de contrôle dans le but de commettre des activités illicites. Ceci dit, cette catégorie n'inclut pas encore l'étape de monétisation, même si certaines activités comme le vol de renseignements bancaires impliquent la conversion de données en argent.
5. Ceux qui monétisent ces réseaux : Dans le cadre de cette étude, une nuance est apportée par rapport aux commerçants. Effectivement, la participation à la vente ou location de services et d'outils reliés aux botnets est un moyen de monétisation. Cependant, les botmasters visés par cette catégorie sont les pirates qui ont les

capacités nécessaires pour rentabiliser l'utilisation des botnets. Souvent, ceux-ci ont les compétences et contacts requis pour convertir leurs activités criminelles en revenus, que ce soit par l'utilisation de mules, de mise en relations entre clients et opérateurs, ou encore de techniques de blanchiment d'argent. Dans le cadre de cette étude, les individus qui monétisent les botnets sont alors responsables de l'étape de la conversion des données en profits, plutôt que celle de l'acquisition de ces renseignements.

6. Les curieux : cette catégorie comprend les pirates informatiques qui indiquent porter un intérêt sur les botnets. Ces individus pourraient être en processus d'apprentissage de techniques ou d'expertises particulières en lien avec les botnets, ou bien sont simplement curieux. Cependant, il est difficile d'évaluer si ceux-ci ont déjà manipulé des botnets, ou encore quels types de rôles les intéressent plus particulièrement.
7. Les individus affirmant avoir de l'expérience en matière de botnets : les observations de conversations a permis d'identifier nombreux individus affirmant avoir de l'expérience en ce qui a trait aux botnets et avoir été impliqués dans certains projets. Malgré que la nature exacte de leur participation soit inconnue, ils n'ont pas été exclus de l'étude et ont plutôt été catégorisés de la sorte. Dans le cadre des analyses, ils seront considérés comme un groupe de botmasters quelconque, sans distinction de leurs rôles dans le marché de botnets.

Les variables

Pour chaque catégorie de botmasters, trois aspects distincts seront explorés : le statut et la réputation, le niveau d'activité ainsi que l'expertise. Une fois ces analyses menées, les différents types de botmasters seront comparés entre eux afin d'évaluer si des différences significatives peuvent être soulevées.

Le statut et la réputation

Les membres du forum sont répartis en fonction de leurs statuts et se voient attribuer une cote de réputation numérique en fonction de leurs activités dans le forum. L'attribution de cotes de réputation se fait par la distribution de points de réputation par les membres, possiblement suite à des transactions et échanges entre eux. Plus la cote est élevée, plus un

pirate a bonne réputation. Tous les membres du forum ont une cote qui leur est attribuée, à l'exception des individus ayant un statut de *guests* (ou invités). Dans la population à l'étude, les scores de réputation varient de 1281 à 2095. Cependant, les modes précis d'attribution de points n'ont pas pu être identifiés avec les données disponibles.

Quant aux statuts des membres, ceux-ci sont accordés par les administrateurs du forum, en fonction de leur influence et leur importance au sein du forum. Les différents statuts des botmasters identifiés sont définis comme suit :

- *Fresh Fish* : les *fresh fish* comprennent les nouveaux membres. Ils doivent faire leurs preuves avant de pouvoir monter dans les rangs. Ils ont peu d'accès dans le forum. On dénombre 138 membres au total ayant ce statut dans Dark0de.
- *Level 1* : les membres identifiés comme *Level 1* sont des membres de confiance. Ils ont plus d'accès dans le forum, dont un accès aux sections de commerce. Ils peuvent ainsi faire des transactions avec leurs pairs et bâtir davantage leur réputation. Les pirates de Niveau 1 comprennent 55 membres.
- *Level 2* : les Niveaux 2 sont les membres les plus dignes de confiance. Il s'agit des pirates qui ont le plus d'influence au sein de cette communauté. Ils ont d'ailleurs le potentiel de devenir administrateurs. On n'en retrouve que 16 membres.
- Administrateurs : cinq administrateurs et un modérateur sont en charge des règles et de la gestion de conflits dans le forum. Ce sont les membres les plus influents et les plus respectés de cette communauté.
- *Guests* : cette catégorie mériterait davantage d'attention. Les invités ne semblent pas avoir de statut particulier au sein du forum, cependant ils participent à une grande part du commerce et des activités de Dark0de. Il n'est pas possible de les quantifier dans la base de données complète, cependant ils constituent 43% de la population de botmasters à l'étude dans le présent travail. Il est important de noter aussi que certains de ces invités peuvent être des membres du forum et qui utilisent un identifiant différent dans certaines conversations. Un ancien administrateur du forum, par exemple, aurait utilisé cette fonction de *guest* afin de continuer ses activités dans le forum.

- *Unknown* : le statut de ces individus est inconnu à cette étape-ci puisqu'ils sont encore en attente de réponse quant à leur candidature. Ces individus ont publié dans la section d'introduction du forum et attendent ainsi que la communauté prenne une décision au sujet de leur adhésion dans Dark0de. Cependant, ils ont tout de même une cote de réputation qui leur est attribuée, possiblement due à leurs contacts déjà présents dans la communauté (puisque ce forum fonctionne par un système d'invitation).
- *Suspended* : les membres qui ont été bannis et suspendus du forum se voient attribuer une telle mention.

L'activité

Deux facteurs sont pris en compte dans l'évaluation du niveau d'activité des botmasters : la quantité de publications qu'ils écrivent dans Dark0de, ainsi que leur présence dans d'autres forums. Dans le cadre de travail, plus un pirate informatique a un nombre élevé de publications dans le forum, plus celui-ci est considéré « actif » au sein de sa communauté. Il en va de même pour la présence des botmasters dans d'autres forums que Dark0de : un individu présent dans plusieurs forums sera considéré plus « actif » qu'un pirate inscrit dans peu de forums.

Des limites doivent toutefois être relevées par rapport à ces mesures d'activité. Tout d'abord, en ce qui concerne les publications, ces dernières ne sont pas précisées lorsqu'il est question des botmasters invités (*guest*). Cela signifie alors 43% des données de publications des pirates informatiques concernés par cette étude ne sont pas disponibles. Ensuite, mesurer la présence dans des forums autres que Dark0de peut aussi s'avérer problématique pour de nombreuses raisons. Premièrement, les pirates informatiques utilisent souvent des noms d'identifiants différents d'un forum à l'autre, cela signifie qu'il faudrait préalablement connaître les nombreux alias de ces individus afin de les retrouver dans les autres forums. À l'inverse, il est aussi possible que différents individus aient le même nom d'utilisateur d'un forum à l'autre. Ensuite, la recherche de données s'est faite à partir de mots-clés sur le web 2.0, ce qui ne permet pas l'exhaustivité des résultats. De plus, certains individus identifiés dans des forums par cette méthode ne s'y retrouvent plus lorsque la recherche est faite à l'intérieur même du forum. C'est le cas justement des forums

HackForums qui ne montre plus de résultats précédents 2016 et Blakhatworld qui n'affiche pas les résultats retrouvés sur Google. Ainsi dans le cadre du présent travail une marge d'erreur sera tolérée. Cependant, il devient pertinent de se questionner sur la faciliter à retrouver certains botmasters dans de nombreux forums. Il n'est pas possible à cette étape de déterminer s'il s'agit d'un manque de compétence ou d'une préoccupation moindre pour la sécurité de leur identité, ou encore s'il s'agit d'un souci de maintenir et d'améliorer plus aisément leur réputation en gardant le même identifiant d'un forum à l'autre. Dû à ces nombreuses limites, la variable « activité » sera étudiée seulement à titre indicatif afin de se donner une idée approximative au sujet de la présence d'autres forums que Dark0de.

Expertise

Cette variable comprend toutes les compétences et expériences nommées par les botmasters dans leurs introductions, qui ne sont pas nécessairement reliées aux botnets, qu'il s'agisse d'expertises techniques ou criminelles. Ces expertises ont été par la suite divisées en secteurs d'activités :

- Programmation et outils : cette catégorie comporte tout ce qui a trait au codage et à la programmation en général, à l'écriture de logiciels malveillants et éléments affiliés, ainsi que la production d'outils « malveillants », tels que des *crypters*[7], des *keyloggers*[8] ou encore des *stealers*[9].
- Maintenance d'infrastructures : y sont inclus les services d'hébergement, de proxys, de maintien de réseaux, et de conception Web.
- Services publicitaires : tout ce qui relève du trafic, des cookies, et de publicité.
- Activités criminelles : cette catégorie comprend les activités criminelles du type piratage et exploitation de vulnérabilités, *carding*, vol de données, contrefaçon de passeports, pollupostage, fraude, blanchiment d'argent et ingénierie sociale.
- Commerce : cette catégorie comprend les marchés de produits et services autres qu'en matière de botnets.

[7] *Crypter*: logiciel qui permet de crypter et de dissimuler des données et de manipuler certains logiciels malveillants pour en éviter la détection (Trend Micro, s. d.).
[8] *Keylogger*: cet outil permet de voler les mots de passe d'usager en enregistrant les touches du clavier utilisées (Kaspersky Labs, s. d.).
[9] *Stealer*: un logiciel malveillant qui collecte des données relatives à des mots de passe (Wordnik, s.d.)

- Partenariat : cette catégorie comprend les pirates cherchant à établir des partenariats et relations professionnelles avec d'autres membres du forum.

La variable « expertise » permet une interprétation limitée. En effet, étant donné la nature des données récoltées, il n'a pas été possible de mesurer la qualité des compétences de ces pirates. Il n'est donc pas possible d'établir jusqu'à quel point les botmasters sont doués dans les diverses expertises qu'ils nomment. Étant donné cette limite, il sera question uniquement d'évaluer la nature et la diversité des compétences énumérées.

Limites

Plusieurs limites ont été identifiées au cours de cette étude. Tout d'abord, cette étude se veut plutôt exploratoire et tente d'examiner différents thèmes en lien avec les compétences et les rôles de botmasters, plutôt que d'analyser en profondeur un ou deux aspects précis. Ensuite, puisque les données proviennent d'un seul forum, il sera difficile de généraliser les conclusions obtenues pour tous les botmasters à l'échelle internationale. De plus, cette étude ne permettra pas de comparer empiriquement la population de botmasters à celle des pirates informatiques en général. Étant donné les limites au niveau du temps et des ressources allouées pour cette étude, il ne sera pas possible d'évaluer scientifiquement si les botmasters se distinguent réellement des hackers ou s'ils constitueraient une sous-catégorie à part entière des pirates; une tentative de réponse sera toutefois entreprise à la suite des analyses. Cette étude permettra principalement de décrire et de mieux comprendre les botmasters, ainsi que de les comparer entre eux, en fonction des rôles qu'ils occupent dans le marché des botnets.

Des lacunes ont aussi été identifiées par rapport aux types de données à l'étude. Puisqu'il s'agit de captures d'écran, il a été difficile de chercher des données complémentaires aux introductions dans la base de données globale. Ensuite, étant donné les formats des images enregistrées, les couleurs du forum (noir, gris, rouge) ainsi que de la qualité des images, il n'a pas été possible de concevoir de logiciel de reconnaissance visuelle de mots-clés à l'intérieur même des fichiers. Des informations telles les types de publications, ou encore les dynamiques des marchés et transactions n'étaient pas possibles à trouver avec les ressources et le temps disponible. Pour se faire, il aurait fallu codifier la totalité des 5000 images (et plus) à la main.

D’autres limites concernant les données se sont avérées importantes dans la réalisation de cette étude. Tout d’abord les botmasters ayant un statut de « *Guest* » posent problème. Il n’y aucune indication par rapport à leur réputation, ni sur comment ils ont obtenu ce statut. Cela fait en sorte que 43% des sujets à l’étude comportent des données manquantes sur leur sujet. D’ailleurs, il est arrivé que dans certains cas, des administrateurs utilisent un identifiant d’invité pour intervenir dans le forum. Ainsi on retrouve des membres avec des statuts et des compétences variables dans cette catégorie. Il en va de même pour les individus qui indiquent avoir de l’expérience en matière de botnets. Ceux-ci affirment dans leur introduction être expérimentés dans ce domaine et d’avoir été participés à des projets impliquant des botnets. Cependant, la nature de leur contribution est inconnue. Ces individus constituent 36% des sujets à l’étude, faisant en sorte que pour plus du tiers des sujets, leurs rôles dans le marché des botnets sont inconnus.

En ce qui concerne les hackers avec des identifiants multiples et ceux utilisant le même identifiant d’un forum à l’autre, un certain degré d’incertitude est présent. Puisque Dark0de est considéré comme un forum regroupant l’élite des hackers anglophones, il est possible d’assumer que ceux-ci seraient plus soucieux de dissimuler leur identité en utilisant divers noms d’usagers d’un forum à l’autre. Lorsque ces différents identifiants étaient mentionnés dans le forum, des recherches sur le web 2.0 étaient faites avec ces nouveaux identifiants. Cette méthode comprend toutefois des risques, dont un manque d’exhaustivité ainsi que la supposition que l’on fait affaire avec le bon pirate alors qu’il pourrait s’agir d’un autre individu. Des recherches sur le web 2.0 ont d’ailleurs été menées avec tous les botmasters, ce qui a permis d’identifier encore plus de sujets ayant le même identifiant dans divers forums (à une majuscule ou minuscule près, ou à encore un chiffre différent). Ces résultats indiquent alors que pas tous les pirates doués se préoccupent de leur anonymat comme la littérature pourrait le laisser penser. Cependant, le même risque d’avoir affaire avec un individu autre que le sujet persiste. Pour contrer cette limite, des recherches additionnelles ont été faites pour trouver des concordances avant de faire le lien entre les divers profils (date de naissance, profil de compétence similaire ou utilisation des mêmes outils). Un certain degré d’incertitude a été toléré.

Chapitre IV – Analyses et discussion

Afin de réaliser la présente étude, des analyses exploratoires portant sur le statut, la réputation, l'activité ainsi que l'expertise des botmasters seront menées. Cet exercice sera fait pour chaque type de botmaster identifié au cours de l'étude, soient les codeurs, les commerçants, les distributeurs, les opérateurs, ceux qui monétisent, les curieux ainsi que les individus affirmant avoir de l'expérience dans le domaine.

Afin de mieux comprendre les relations possibles entre les différents rôles identifiés dans les observations à la lumière de la littérature, l'organigramme suivant a été développé:

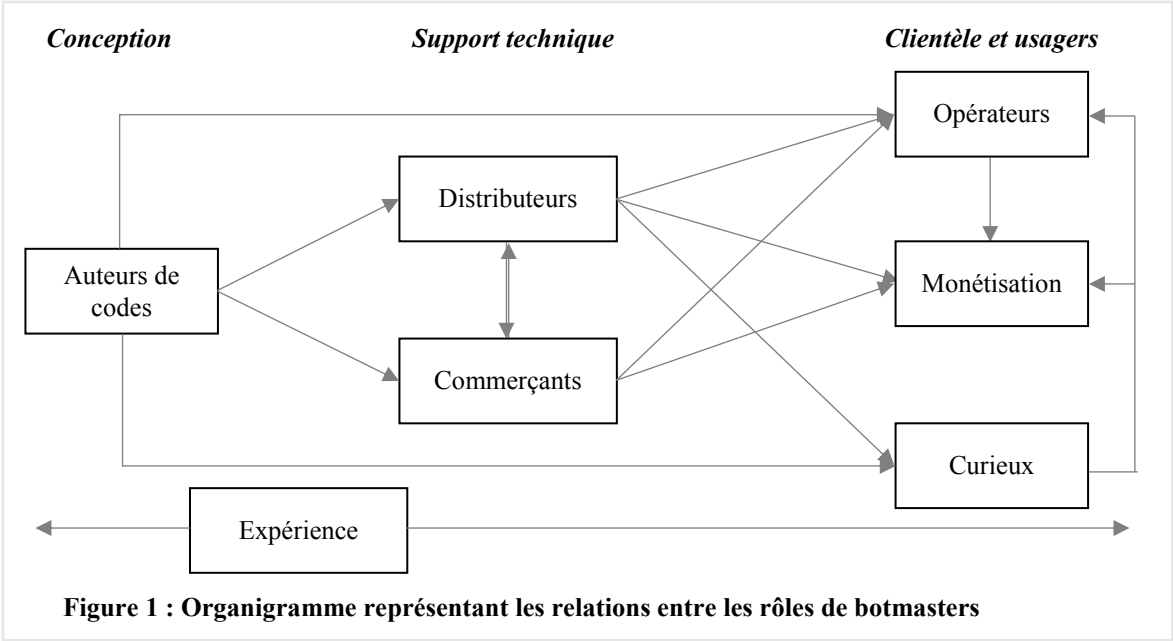


Figure 1 : Organigramme représentant les relations entre les rôles de botmasters

Trois niveaux de rôles ont été suggérés dans la création de cet organigramme, les niveaux de : conception, support technique et clientèle. Au niveau de la conception on retrouve les auteurs de codes. Ceux-ci sont les individus clés dans le processus, c'est grâce à leur expertise technique que sont créés les botnets. Ils servent de point de départ de ce marché illicite. Plusieurs options s'offrent à eux : s'ils ont les contacts appropriés, ils peuvent les vendre directement à des distributeurs (qui vont bâtir et agrandir les réseaux de botnets), ou faire affaire directement avec des opérateurs. Ils peuvent aussi les vendre aux curieux qui d'intéressent au marché des botnets. Si les auteurs n'ont pas les connexions nécessaires, ils peuvent faire affaire avec des vendeurs qui vont servir d'intermédiaires. En théorie, les auteurs pourraient ensuite propager et opérer leurs propres botnets. Ils pourraient vendre

ou louer à n'importe quelle étape du processus, ou encore monétiser leurs activités. Cependant, tel qu'indiqué dans la littérature, chaque étape du processus de développement d'un botnet ainsi que sa mise en marché, requiert des compétences techniques, financières et sociales différentes. Ainsi, il est peu fréquent qu'un individu à lui seul puisse posséder toutes ces expertises (Décary-Hétu, 2011; Dupont, 2010; Dupont, 2012).

Au second niveau on retrouve les distributeurs et les commerçants. Ensemble, ils permettent le soutien technique et commercial des réseaux d'ordinateurs corrompus. Les distributeurs sont les acteurs qui favorisent le support technique nécessaire au bon fonctionnement des réseaux de botnets. On y inclut l'agrandissement de réseaux, les services d'hébergements, le cryptage des outils, etc. Ainsi ces individus bâtissent les réseaux de machines corrompues afin de les présenter « clé en main » et prêts à être opérés. Les distributeurs peuvent ensuite les revendre directement aux opérateurs et ceux qui monétisent, ou encore les vendre à des curieux. Lorsqu'ils n'ont pas les contacts appropriés, ils peuvent eux aussi faire affaire avec des commerçants et vendre leurs produits finaux. Les commerçants, quant à eux, servent de ponts entre les acteurs qui veulent vendre ou acheter des produits et services relatifs aux botnets. Ils servent d'intermédiaires et permettent la prise de contact entre des partis intéressés.

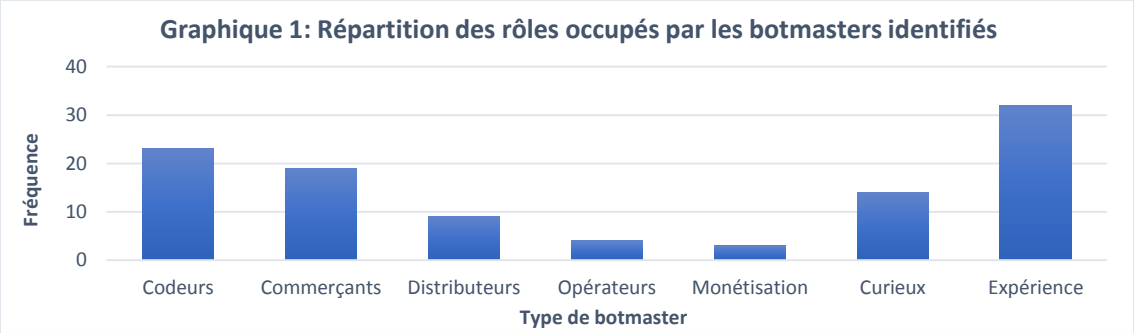
Le troisième niveau comprend les opérateurs, les curieux ainsi que les individus qui monétisent les botnets. Ceux-ci seraient les usagers finaux de la chaine de distribution de botnets. Ce sont les individus qui vont utiliser les botnets afin de mener des activités criminelles en ligne et/ou s'enrichir. Les opérateurs prennent contrôle du botnet et mènent des activités illicites de leur choix et à grande échelle. Ils peuvent mener des campagnes de pollupostage, faire de la fraude ou encore mener des attaques distribuées. Ils peuvent aussi monétiser directement leurs activités soit par la vente ou la conversion de données volées, ou encore faire affaire avec un spécialiste. Les opérateurs peuvent aussi se procurer un botnet clé en main, tout comme ils peuvent acheter des codes et bâtir eux-mêmes leur réseau. Les individus qui monétisent peuvent, de même, envoyer des commandes aux botnets afin de voler des données et convertir eux-mêmes ces données en liquidité. Cependant, les botmasters capables de monétiser peuvent avoir des compétences de blanchiment d'argent ou encore des contacts avec des mules, ce que certains opérateurs ne

possèderont pas. En ce qui concerne les curieux, si l'on considère dans le cadre présent que ceux-ci sont en quête d'apprentissage en ce qui a trait aux botnets, ceux-ci se situeraient au niveau de clientèle. L'hypothèse suggérée ici est qu'il est nécessaire de manipuler un botnet et de l'étudier dans sa forme finale avant d'être en mesure de le développer. Ainsi les curieux pourraient se procurer de tels réseaux auprès de commerçants ou de distributeurs, ou encore se procurer des codes directement des auteurs.

Étant donné que les individus indiquant avoir de l'expérience en matière de botnets ne précisent pas la nature de leur contribution, il sera considéré que ceux-ci peuvent se situer à n'importe quel niveau du marché des botnets. Au final, il n'y a pas une seule et unique façon de diviser le travail entre ces différents acteurs, cependant cela donne une indication quant à la compréhension des diverses tâches que la mise en œuvre d'un botnet peut nécessiter.

Les botmasters dans Dark0de

Afin de mesurer la prévalence de ces différents types de botmasters parmi la population de pirates informatiques de Dark0de, les 88 individus identifiés comme botmasters sont présentés ci-dessous en fonction des rôles qu'ils occupent. Puisque 17% d'entre eux (n=15) se trouvent à occuper plus d'un rôle, ceux-ci ont été comptabilisés plusieurs fois.



Parmi les botmasters identifiés dans Dark0de, 26% d'entre eux (n=23) auraient des compétences en codage et programmation de logiciels de botnets, un chiffre qui semble plutôt élevé si l'on se base sur la littérature. En effet, cela fait près du quart des botmasters qui occuperaient ces fonctions, alors que la littérature suggère que ces individus forment la minorité auprès de leur communauté et qu'ils sont bien souvent sollicités par des pairs moins compétents (Chu et coll., 2010; Holt & Lampke, 2010; Holt et coll., 2008; Honeynet

Research Alliance, 2003; et Thomas et Martin, 2006, cités dans Holt et coll., 2012). Un autre 22% de botmasters sont impliqués dans le commerce de botnets (n=19), qu'il s'agisse de vente (n=7), location (n=1) ou achat de botnets (n=12). Le dixième des individus est impliqué dans la distribution et propagation du réseau, et un total de sept botmasters opèrent et rentabilisent les botnets. Puisque les botnets sont des outils tant convoités dans les communautés de piratage informatique, il semble assez surprenant que si peu d'individus contrôlent et tirent profit des botnets de la sorte. Ce graphique semblerait indiquer qu'il y a plus d'offres que de demandes, et ainsi plus de personnel qualifié pour fournir des produits que d'individus qui utilisent ces produits. Ces résultats semblent contre-intuitifs étant donné que la littérature indique qu'un faible nombre de codeurs fournissent les logiciels à une quantité énorme de pirates ayant moins de compétences techniques. La plateforme à l'étude est toutefois un forum très spécialisé où, en théorie, seule l'élite des pirates informatiques peut y adhérer. Il est important de rappeler cependant que l'on analyse la section introduction du forum Dark0de, plutôt que le forum de marché où on aurait potentiellement retrouvé un bassin plus grand d'individus à la recherche de botnets, en comparaison au nombre de codeurs.

Pour finir, la catégorie la plus importante en termes de nombre est celle qui tient compte de l'expérience des botmasters avec 32 individus. Ainsi, plus du tiers de ces pirates affirment avoir déjà participé à des projets ou avoir de l'expérience en matière de botnets. Cependant, le type de contribution pour cet échantillon d'individu est inconnu ce qui apporte donc une limite importante à l'étude. Treize individus indiquent aussi porter un intérêt en ce qui a trait aux botnets. Encore une fois, il est difficile d'évaluer concrètement quel est leur apport dans ce marché illicite, cependant on pose l'hypothèse qu'ils ne sont pas tout à fait compétents ou encore en phase d'apprentissage, ou alors qu'ils tentent de développer des expertises en ce qui a trait à ce marché.

Les rôles multiples

Parmi les botmasters identifiés dans les introductions de Dark0de, 17% (n=15) occupent plus d'un rôle relatif aux botnets. Ceux-ci sont présentés dans la figure suivante :

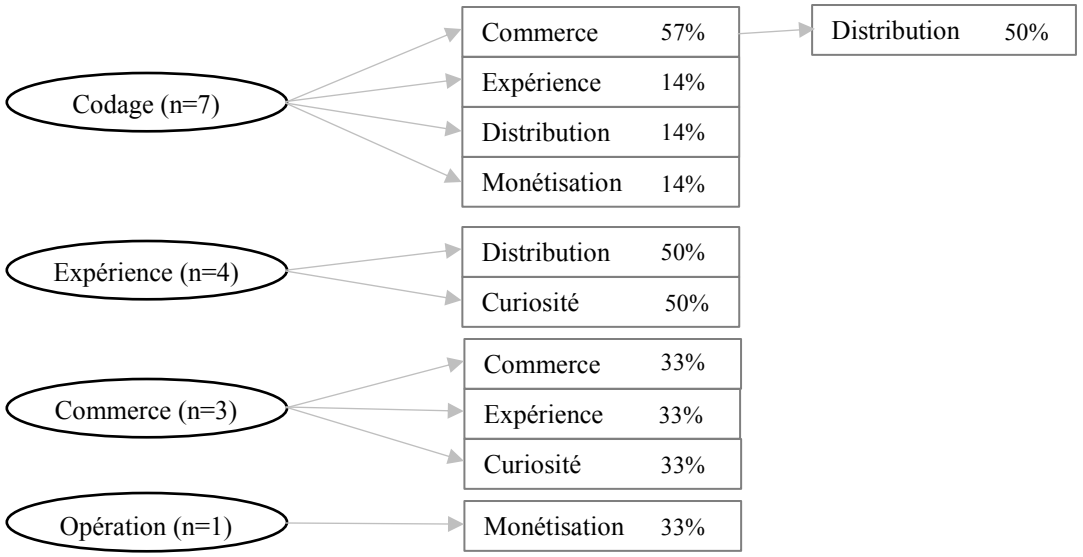


Figure 2: Représentation graphique des botmasters ayant des rôles multiples

La figure 2 indique que les individus qui occupent le plus de rôles relatifs aux botnets en même temps sont les codeurs (n=7). Ils sont impliqués dans le commerce de botnets (56% des codeurs), leur distribution (43%), ainsi que leur monétisation (14%). Seuls les codeurs indiquent occuper jusqu'à trois fonctions en lien avec les botnets. Ils seraient alors les botmasters avec les compétences les plus nombreuses et diversifiées. Les expérimentés (n=4), sont soit des curieux (50%), soit impliqués dans la distribution et propagation de réseau (50%). Les commerçants (n=3) quant à eux, n'ont pas de seconds rôles définis, ils affirment être des curieux ou encore avoir été impliqués dans des projets en lien avec les botnets. Pour finir, un seul individu indique opérer et monétiser ses réseaux de botnets par lui-même. Ainsi la plupart des botmasters n'occuperaient qu'une seule fonction relative aux botnets (83%). Pour ce qui est du reste, ces derniers seraient plus polymorphes, et plus particulièrement les codeurs qui occupent jusqu'à trois fonctions différentes.

Les catégories de botmasters

Pour mieux comprendre les dynamiques entre ces différents rôles ainsi qu'en savoir plus sur ces pirates, chaque catégorie de botmasters sera étudiée plus en détail. Les variables telles que le statut et la réputation, l'activité au sein du forum, ainsi que les expertises seront abordées pour chaque catégorie de botmasters identifiés. Dans le cadre de cette étude,

chaque catégorie de botmaster qui sera étudiée comportera aussi les individus qui ont des rôles multiples. Ils seront ainsi comptés à plusieurs reprises, selon les fonctions qu'ils occupent. Pour conclure, les catégories à l'étude seront ensuite comparées entre elles.

Les codeurs

La section qui suit porte sur le statut et la réputation des codeurs, sur leur niveau d'activité tant au sein du forum que dans la communauté de piratage, ainsi que sur leurs diverses expertises.

Tableau 1: Données statistiques sur le statut, la réputation et les publications des auteurs de code dans Dark0de	
Distribution des statuts des codeurs	
Statut Dark0de	**Fréquence relative (n=23)**
Fresh Fish	13,04 %
Guest	52,17 %
Suspended	4,35 %
Unknown	30,43 %
Total	100,00 %
Données statistiques sur la réputation des codeurs	
	Réputation (n=11)
Moyenne	1817,27
Minimum	1520,00
Maximum	1928,00
Écart-type	105,97
Manquant (n=12)	52,17 %
*Moyenne générale totale (n=50)**	*1796,12*
Données statistiques sur les publications des codeurs	
	Publications (n=11)
Moyenne	10,6
Minimum	1,0
Maximum	30,0
Écart-type	10,2
Manquant (n=12)	52,17 %
*Moyenne générale totale (n=50)**	*63,4*
*Parmi les 88 botmasters à l'étude, 38 ont été identifiés en tant que *Guests*. Ainsi les informations par rapport à leurs statuts, réputations et publications sont disponibles pour 50 botmasters.	

Statut et réputation

Les résultats du tableau 1 montrent que plus de la moitié des codeurs sont des *guests* du forum. Ils ne semblent pas avoir de statuts précis au sein de Dark0de, ce qui pose une limite importante dans l'interprétation des résultats. Cette absence de statut pose problème, surtout lorsque l'on sait que certains administrateurs du forum ou encore des pirates haut placés ayant déjà un statut utilisent parfois un identifiant d'invité lorsqu'ils interagissent

avec leurs pairs. Il est difficile d'affirmer s'il s'agit d'une technique pour préserver davantage leur anonymat, cependant, un tel statut au sein de Dark0de empêche d'avoir des informations sur le pirate, tels sa réputation ou encore le nombre de publications. Ainsi, pour ce 52% de botmasters codeurs, il ne sera pas possible d'évaluer leur réputation dans le cadre de cette étude. Près de 15% des codeurs sont des *Fresh Fish*, donc des nouveaux membres qui se trouvent habituellement plus bas dans la hiérarchie, et ayant un accès limité aux contenus du forum. Finalement, le tiers des codeurs ont un statut inconnu, c'est-à-dire en attente d'approbation pour adhérer au forum. Ainsi, selon les données disponibles, aucun botmaster de niveaux 1 ou 2 ne se consacre au codage de botnets. Ces résultats semblent inattendus étant donné que le codage requiert une certaine expertise au niveau technique, faisant en sorte que les codeurs seraient des membres plus sollicités, et qui pourraient ainsi avoir un meilleur statut au sein de leurs communautés.

En ce qui concerne la réputation, en moyenne, les auteurs de codes ont une réputation juste un peu plus élevée (1817.27) que la moyenne de tous les botmasters identifiés dans cette étude (1796.12). Comme la littérature l'indique, la réputation d'un botmaster ne se bâtit pas uniquement sur ses compétences, mais aussi sur son activité au sein du forum, le nombre de jours passés dans les forums, l'échange et le partage de connaissances, les références de nouveaux membres ou encore l'appartenance à des groupes exclusifs (Décary-Hétu et Dupont, 2013). Ainsi, leur faible activité au sein du forum (qui sera abordée un peu plus tard) entre autres aurait possiblement un impact sur la réputation de ces individus.

Il est surprenant de constater que les codeurs n'ont pas de statuts élevés au sein de Dark0de, et que leur réputation est un peu plus élevée que la moyenne de la population à l'étude. Il faut tout de même être prudent dans l'interprétation de ces résultats puisque la moitié des données ne sont pas disponibles. En effet, les informations sur les *guests* ne sont pas affichées, qu'il s'agisse de leur réputation ou encore de leur réel statut.

Activité

L'activité est ici définie par la quantité de publication dans le forum Dark0de ainsi l'adhésion à d'autres forums de piratages. Le tableau 1 indique que ces individus publient peu en moyenne (10.6 publications), comparativement à 63 publications pour les

botmasters en moyenne. Si l'on considère les codeurs comme les piliers dans de tels milieux, ces résultats contrediraient en partie la littérature en ce qui concerne les le transfert d'information et l'activité au sein de tels forums. En effet, les membres les plus compétents solliciteraient moins d'informations auprès de leur communauté, mais seraient beaucoup plus actifs dans les fils de discussion en ce qui a trait à fournir des informations à leurs pairs et au maintien du bon fonctionnement du forum (Zhang et coll., 2012). Ainsi selon la typologie de Zhang et coll. (2012), les codeurs ressembleraient davantage aux *pirates occasionnels*, car ils sont moins actifs et ont une réputation moindre que les membres les plus centraux et compétents du forum. D'un autre côté, il serait aussi possible d'émettre l'hypothèse que ces individus, ainsi que leurs produits, sont tellement recherchés qu'il n'est plus nécessaire pour les codeurs de participer autant aux discussions du forum. Ils seraient moins dépendants de cette communauté puisque la conception et diffusion de leurs produits occupent déjà une bonne part de leur temps. Toutefois, il faut tout de même rester prudent dans l'interprétation des résultats, puisque plus de 50% des données sont manquantes. De plus, il est important de rappeler que la majeure partie des interactions se font généralement en messagerie privée. Ainsi cette variable ne prend en compte que les messages publiés qui sont accessibles à tous les membres du forum.

En ce qui concerne l'adhésion à d'autres forums de piratages, les recherches en sources ouvertes ont révélé que près du tiers de ces botmasters n'ont été identifiés que dans Dark0de. Ils n'ont pas pu être détectés ailleurs avec leur identifiant de Dark0de. Ensuite, 26% ont été trouvés dans un forum additionnel et un autre 26% dans deux autres forums différents. Seulement trois membres ont été retrouvés dans plus de trois forums. Un de ceux-ci a été identifié dans trois forums et un autre dans cinq (voir le tableau 8 en annexe). Un dernier codeur, B24, a même été retrouvé dans plus de 9 forums de piratage avec un seul identifiant, dont plusieurs sont des forums russes ainsi que des forums dédiés aux jeux en ligne. B24 était encore en attente d'acceptation auprès du forum, et sa réputation était un peu plus élevée que la moyenne des autres botmasters. De telles données pourraient permettre de suggérer certaines hypothèses : certains pirates sont plus soucieux que d'autres de protéger leur identité en ligne et vont utiliser différents noms d'usagers d'un forum à l'autre, alors que certains vont garder le même identifiant d'une communauté à l'autre et ainsi bâtir et maintenir leur réputation.

Donc en somme, les auteurs de codes sont peu actifs dans Dark0de, ils ont en moyenne 10 publications par personne, et l'individu ayant le plus publié n'en avait que 30. Au niveau de l'activité dans les autres forums, trois individus se distinguent avec leur présence dans plus de trois forums, dont un dans plus de neuf forums. Il y a cependant trop de limites pour permettre une véritable conclusion. Ce qu'il serait intéressant d'explorer davantage aussi serait la nature des publications produites par les codeurs. En effet, ont-ils tendance à publier surtout des annonces pour vendre leurs produits? Ou bien n'est-ce pas si nécessaire étant donné la forte demande associée à de tels produits? Il ne sera pas possible de répondre à cette question dans le cadre de cette recherche étant donné la difficulté de retrouver ces publications dans la base de données à l'étude.

Expertises

Cette section porte sur les autres compétences informatiques que les auteurs de codes affirment posséder dans leurs introductions. Tous les individus de cette catégorie indiquent avoir des compétences générales en codage, ce qui n'est pas surprenant étant donné que ces individus écrivent des codes reliés aux botnets. Plus de la moitié des botmasters codeurs (56.5%) auraient des expertises uniquement en lien avec la programmation, qu'il s'agisse de codage de logiciels malveillants ou d'outils complémentaires, de développement d'outils de cryptage, de *rootkits*[10] et *exploit packs*[11], ou encore de *reverse engineering*[12]. Par contre, 17% (n=4) auraient une expertise additionnelle au codage. Parmi eux, la moitié offrirait des services d'hébergement et du maintien de serveurs. L'autre moitié indique être des acheteurs. Un autre 17% (n=4) auraient deux expertises additionnelles. Le premier est un vendeur et acheteur. Les deux suivants indiquent explicitement faire des activités de piratage en plus d'être acheteur dans un cas, et fournir du trafic web dans l'autre. Le dernier, quant à lui, aurait comme expertise l'ingénierie sociale, et aurait un intérêt marqué pour le vol de données et l'espionnage. Cet individu, B06, mentionne d'ailleurs dans son

[10] Collection de logiciels et programmes permettant au pirate d'avoir un accès privilégié à une machine et d'en dissimuler l'intrusion, en plus de corrompre les autres machines du même réseau (TechTarget, s. d.).
[11] Réfèrent à des outils de piratage utilisés par des cybercriminels afin d'exploiter des vulnérabilités dans des systèmes dans le but d'y distribuer des logiciels malveillants ou simplement de mener des activités criminelles (Trend Micro, s. d.).
[12] Action d'analyser des logiciels afin de les reproduire, créer un logiciel similaire, exploiter leurs failles ou encore de les améliorer (Techopedia, s. d.).

introduction que la raison pour laquelle il bâtit son botnet est pour mener ce genre d'activités illicites. Pour finir, 8.7% des individus (n=2) affirment avoir trois expertises additionnelles au codage. Le premier, en plus de coder, est impliqué dans des activités de *carding*[13], est un acheteur de trafic et est à la recherche de partenaires pour mener à bien ses activités. Le dernier est gestionnaire de serveurs, en plus d'avoir une expertise en pollupostage et de faire de la vente de produits.

Somme toute, une bonne partie des codeurs mènent des activités plus ou moins diversifiées au niveau de leurs expertises, étant donné que plus de la moitié ne font que des activités liées au codage. Cependant, les types de codages varient énormément. De même pour les langages de programmation, certains de ces pirates affirment savoir coder jusqu'à sept langues de programmation. Une autre constatation a été faite à la lumière des analyses : de façon générale lorsque les codeurs occupent plusieurs fonctions dans le marché des botnets, ils s'adonnent à peu d'activités non liées. Au contraire, ceux qui ont des expertises nombreuses et diversifiées dans d'autres sphères que les botnets (hacking, commerce, support technique) ne s'impliquent que dans le codage de botnets.

Conclusion

En somme, les auteurs de codes relatifs aux botnets dans Dark0de sont des individus n'ayant pas de statuts prestigieux au sein de Dark0de et une réputation un peu plus élevée que la moyenne des botmasters, ce qui ne semble pas concorder avec la littérature actuelle. Cependant, il ne faut pas oublier qu'à priori, les membres de ce forum prestigieux sont déjà des pirates théoriquement compétents et reconnus au sein des communautés de piratage. Ainsi, ce ne serait qu'auprès de leurs pairs dans Dark0de que les codeurs se démarquent moins en ce qui concerne leurs statuts et réputations. Ils semblent peu actifs dans les forums publics de Dark0de puisqu'ils publient peu et seulement trois d'entre eux ont été identifiés dans plus de trois forums additionnels. En ce qui concerne leurs expertises, la moitié d'entre eux ne font que des activités en lien avec la programmation alors que l'autre moitié mène des activités plus diversifiées.

[13] Activité illégale qui consiste en l'exploitation et au commerce de données bancaires et personnelles d'individus (Goudey, 2004).

Les commerçants

La section suivante porte sur les individus qui affirment participer au commerce de botnets dans Dark0de, qu'il s'agisse de services de vente, d'achat ou de location. Le statut et la réputation, l'activité et les expertises de ces individus seront abordés.

Tableau 2: Données statistiques sur le statut, la réputation et les publications des commerçants				
Répartition des types de commerçants en fonction de leur statut dans Dark0de				
Statut Dark0de	**Fréquence relative (n=19)**	**Acheteurs (n=12)**	**Vendeurs (n=7)**	**Location (n=1)**
Fresh Fish	26,32 %	4	0	1
Guest	42,11 %	4	5	0
Level 1	10,53 %	2	0	0
Level 2	10,53 %	2	0	0
Unknown	10,53 %	0	2	0
Total	100,00 %	12	7	1
Données statistiques sur la réputation des commerçants				
Réputation	**Valeur totale (n=19)**	**Acheteurs (n=12)**	**Vendeurs (n=7)**	**Location (n=1)**
Moyenne	1762,27	1750,38	1858,00	1666,00
Minimum	1281,00	1281,00	1832,00	N/A
Maximum	2095,00	2095,00	1884,00	N/A
Écart-type	209,39	241,53	36,77	N/A
Manquant	42,11%	33,33%	71,43%	0,00%
Moyenne générale totale				*1796,12*
Données statistiques sur les publications des commerçants				
Publication	**Valeur totale (n=19)**	**Acheteurs (n=12)**	**Vendeurs (n=7)**	**Location (n=1)**
Moyenne	97,45	119,25	41,00	36,00
Minimum	1,00	1,00	3,00	N/A
Maximum	558,00	558,00	79,00	N/A
Écart-type	166,37	192,71	53,74	N/A
Manquant	42,11%	33,33%	71,43%	0,00%
Moyenne générale totale				*63,4*

Statut et réputation

Plus de 40% des commerçants sont des *guests*. Le quart des commerçants comprend de nouveaux membres, et seulement 20% représentent des pirates de niveaux 1 et 2. C'est parmi les acheteurs que se retrouvent ces statuts plus élevés, ainsi que les statuts de nouveaux membres. Les vendeurs quant à eux, ont des statuts encore inconnus ou sont des *guests*. Il n'est donc pas possible de développer davantage sur les vendeurs et leurs positions dans le forum. Les acheteurs, par contre, comprennent des botmasters de statuts très variables. Cela indique alors que n'importe quel individu, peu importe le statut, peut être un acheteur de produits relatifs aux botnets.

Les vendeurs ont, en moyenne, une meilleure réputation que les acheteurs, que l'individu qui loue ses botnets et que la population totale. Ce qui ne concorde pas tout à fait avec les résultats trouvés précédemment en ce qui concerne le statut des individus. Cependant, il faut être prudent avec ces données puisqu'une part importante de ces pirates sont des *guests* (71%), ainsi les informations en ce qui concerne leur réputation sont inconnues. Les acheteurs cependant, malgré leur réputation moyenne inférieure à celle de tous les botmasters, ont des cotes de réputation très variables (près de 800 points d'écart entre les extrêmes), tout comme leurs statuts.

Activité

Les acheteurs publient beaucoup plus que les vendeurs, et que les autres pirates du forum en moyenne. Encore une fois, il faut rester prudent, car le nombre de publications des invités n'est pas disponible. Ces résultats sont tout de même peu attendus, il aurait été logique de penser que les vendeurs publieraient plus afin de vendre plus facilement leurs produits et services. Sans information disponible sur le contenu des publications dont il est question, il est difficile de mener de conclusions pour expliquer une telle différence. Il se pourrait que ces acheteurs publient plus, dans l'hypothèse où ils seraient plus actifs en ce qui a trait à laisser des commentaires suites aux transactions effectuées. Ainsi ils partageraient à la communauté leurs expériences commerciales avec les vendeurs.

En ce qui a trait à leur présence dans d'autres milieux de la communauté de piratage, plus de 40% n'ont été identifiés que dans le forum à l'étude, 31% dans un forum de plus et 21% dans deux forums additionnels. Seul un commerçant a été retrouvé dans trois forums différents de Dark0de (se référer au tableau 8 en annexe). Ainsi, on constate que les commerçants sont moins facilement identifiables dans la communauté de piratage informatique avec leur identifiant unique. Tout comme les codeurs, il est possible que ces individus utilisent des noms d'usagers différents d'un forum à l'autre, ou encore qu'ils soient moins actifs dans la communauté que l'on pourrait imaginer. Il serait possible d'ailleurs d'émettre l'hypothèse que ces individus sont moins soucieux de maintenir une bonne réputation, cela concorderait ainsi avec leurs scores de réputations moyennes obtenues, inférieures à celles du reste des botmasters.

Expertises

Chez les commerçants, 42% indiquent faire de la programmation ou du développement de logiciels malveillants et autres outils complémentaires en plus de faire du commerce (n=8). Ensuite, 21% indiquent être impliqués dans des activités illicites (n=4) tels le *carding*, le piratage, le pollupostage et la participation au marché de faux documents d'identité. Les autres (n=6) sont impliqués dans marchés divers de produits et de services informatiques. Qu'il s'agisse de fournir des services de proxy ou d'hébergement de domaines, d'outils d'exploitation, de trafic, ou encore d'acheter différents produits comme des bases de données, du trafic, des logiciels de cryptage, etc. Un seul individu ne semble pas avoir d'autre expertise que l'achat ou la vente de botnet si l'on se fie à son introduction au forum. Donc une part importante des commerçants auraient tout de même des compétences en codage et développement d'outils. Le tiers ne ferait que du commerce (achat et vente de produits et services variés) et un cinquième commettrait des activités virtuelles illicites.

Conclusion

Les acheteurs du forum ont, à première vue, de meilleurs statuts au sein du forum que leurs pairs commerçants et ils publient beaucoup plus que le reste des botmasters, malgré leur score de réputation moins élevé. Ces disparités au niveau des statuts et de la réputation pourraient être dues à des situations de conflits découlant de transactions problématiques. Des défauts de paiement, des négociations trop acharnées ou encore des échanges de produits défectueux sont des situations communes dans les forums de piratage, ainsi les membres trompés auraient la possibilité d'attribuer ou de retirer des points de réputation, ce qui expliquerait ces variations de scores. Aussi, puisque de nombreux membres invités sont présents parmi les commerçants, il faut interpréter avec prudence ces résultats. Il en va de même pour les cotes de réputations : bien que les vendeurs aient obtenu de meilleures cotes, étant donné le manque de données au sujet des *guests*, ils se sont classés mieux que les acheteurs, qui ont pourtant des membres avec des statuts très élevés. Au niveau de l'activité, bien que les commerçants publient beaucoup, ils semblent moins présents dans les autres communautés de piratage. Ils utiliseraient possiblement différents usagers ou seraient plus soucieux de la protection de leur identité. Pour finir, les commerçants ont des expertises assez variées, incluant le codage ou encore des activités illicites en ligne.

Distributeurs de botnets

Les distributeurs de réseaux de botnets sont les individus qui permettent la propagation de logiciels malveillants, et qui offrent des services associés au maintien de ces réseaux tout comme l'hébergement ou le cryptage, entre autres.

Tableau 3: Données statistiques sur le statut, la réputation et les publications des botmasters en charge de la propagation des réseaux	
Répartition des distributeurs en fonction de leur statut dans Dark0de	
Statut Dark0de	**Fréquence relative (n=9)**
Fresh Fish	11,11 %
Guest	66,67 %
Unknown	22,22 %
Total	100,00 %
Données statistiques sur la réputation des distributeurs de botnets	
	Réputation (n=3)
Moyenne	1889,00
Minimum	1832,00
Maximum	1983,00
Écart-type	82,02
Manquant (n=6)	66,67 %
Moyenne générale totale (n=50)	*1796,12*
Données statistiques sur les publications des distributeurs	
	Publications (n=3)
Moyenne	2,67
Minimum	1,00
Maximum	4,00
Écart-type	1,53
Manquant (n=6)	66,67 %
Moyenne générale totale (n=50)	*63,4*

Statut et réputation

Les résultats du tableau 3 indiquent que la grande majorité des pirates responsables de la distribution du réseau (67%) sont, encore une fois, des membres invités de Dark0de. Deux individus sont encore en attente d'approbation au forum, et un seul distributeur est un nouveau membre. Ainsi, ces résultats indiquent qu'à première vue, ces botmasters n'ont pas de statuts nécessairement élevés. Toutefois, puisque les statuts réels de ces individus sont inconnus pour 89% de ceux-ci, il n'est pas concevable de poser des conclusions précises.

En ce qui a trait à la réputation des distributeurs, étant donné que la plupart sont des invités (67%), il y a beaucoup d'informations manquantes quant à la réputation de ceux-ci.

Cependant, pour les trois botmasters restants, la moyenne de leurs scores de réputation est élevée par rapport à celle de la population totale des sujets à l'étude. D'ailleurs, même la cote la plus faible (réputation de 1832) est supérieure à la cote générale. En somme, malgré leurs statuts, ces individus semblent avoir obtenu une bonne réputation au sein du forum. Cela signifierait ainsi qu'ils seraient potentiellement appréciés par leurs pairs de Dark0de.

Activité

Le tableau 3 indique aussi que les distributeurs sont peu actifs au sein de leur communauté. En effet, ces individus auraient 1 à 4 publications produites dans le forum Dark0de. Il s'agit d'un nombre très faible, surtout lorsque l'on sait que ces individus sont bien réputés et qu'ils offrent des services très spécialisés. D'ailleurs, un individu, B78, n'aurait émis qu'une seule publication, ce qui signifie que l'unique publication qu'il ait faite serait son article d'introduction. Cet individu n'a qu'une seule publication étant donné qu'il est encore en attente d'acceptation auprès du forum, cependant sa réputation est déjà très élevée. Une aussi bonne réputation pour un individu qui à priori ne fait pas encore partie du forum Dark0de semble particulière. D'autant plus que son introduction n'a pas suscité d'intérêt auprès des autres membres du forum, malgré une « bonne » introduction et des compétences très diversifiées. Le second membre en attente d'adhésion au forum, B03, a lui aussi une bonne réputation à priori et trois publications (toutes dans son introduction), mais celui-ci dévoile dans son introduction être un codeur qui vend son propre botnet, ce qui pourrait contribuer à augmenter sa réputation. Somme toute, il serait aussi possible de suggérer que ces botmasters offrent des services tellement spécialisés et peu souvent offerts (seulement n=9 pour diverses expertises en lien avec la propagation) qu'ils sont ainsi très convoités. Ils n'auraient alors pas besoin de publiciser autant leurs services auprès de leurs pairs.

Les recherches en source ouverte ont permis d'identifier 67% des distributeurs dans un forum différent de Dark0de (n=6). Un seul n'a été retrouvé dans aucun autre forum avec cette méthode, un autre a été identifié dans deux forums et un dernier dans trois autres forums (se référer au tableau 8 en annexe). Encore une fois, on suppose que ces individus utilisent peu souvent le même identifiant d'un forum à l'autre. Mais la plupart, dans ce cas-ci, l'utilisent au moins deux fois : une fois dans Dark0de et une autre fois ailleurs.

Expertises

Les distributeurs indiquent avoir des compétences diversifiées dans leurs introductions. Six parmi eux affirment coder et programmer, et la moitié de ceux-ci occupent encore d'autres fonctions telles le commerce (n=2) ou encore du piratage et de la fraude (n=1). Quatre distributeurs mènent des activités commerciales, en plus de coder (n=2) et de mener des activités illicites en ligne (n=1) et de faire de la conception graphique (n=1). Et au total, trois individus conduisent des activités illicites du type piratage, *carding*, contrefaçon, vol de données, etc. Seuls quatre individus ne mènent qu'une seule activité : trois ne font que du codage, et un gère des serveurs. En somme, ces individus possèdent des compétences assez diversifiées et nombreuses, différentes de leurs activités relatives aux botnets. Ils semblent plus polyvalents que les catégories étudiées jusqu'à présent. Un individu en particulier se démarque, B78 qui a été nommé précédemment, il admet avoir des compétences en fraude, introduction par effraction, piratage, contrefaçon, conception web et détection de vulnérabilités, entre autres.

Conclusion

Les distributeurs n'ont pas de statuts précis pour la plupart et publient très peu. Cette dernière remarque est due au fait que les individus ayant des informations disponibles ne sont pas encore admis au forum et n'ont pu publier uniquement dans la section d'introduction. Cependant, ils ont une très bonne réputation au sein de la communauté malgré cela. L'hypothèse suggérée ici est que ces individus ont démontré qu'ils sont très polyvalents dans leurs introductions. Aussi, les distributeurs se retrouvaient, pour la plupart, dans au moins un forum différent avec le même identifiant. D'ailleurs ces individus possèdent aussi de nombreuses compétences diversifiées autres que celles relatives aux botnets.

Opérateurs de botnets

La section qui suit porte sur les opérateurs de botnets. Ces individus prennent contrôle de ces réseaux de machines infectées pour commettre des activités illicites telles que mener des attaques distribuées, faire des campagnes de pollupostage, ou encore voler des données. Une faible partie de la population de botmasters à l'étude ont affirmé être opérateurs de botnets. En effet, seulement quatre parmi eux s'adonnent à cette activité. Malgré leur faible proportion, leurs statuts, réputations, activités et expertises seront tout de même évalués.

Tableau 4: Données statistiques sur le statut, la réputation et les publications des opérateurs de botnets dans Dark0de	
Répartition des opérateurs en fonction de leur statut dans Dark0de	
Statut Dark0de	**Fréquence relative (n=4)**
Fresh Fish	25,00 %
Guest	50,00 %
Level 2	25,00 %
Total	100,00 %
Données statistiques sur la réputation des opérateurs de botnets	
	Réputation (n=2)
Moyenne	1885,50
Minimum	1707,00
Maximum	2064,00
Écart-type	252,44
Manquant (n=2)	50,00%
Moyenne générale totale (n=50)	*1796,12*
Données statistiques sur la quantité de publications des opérateurs de botnets	
	Publications (n=2)
Moyenne	159,50
Minimum	13,00
Maximum	306,00
Écart-type	207,18
Manquant (n=2)	50,00%
Moyenne générale totale (n=50)	*63,4*

Statut et réputation

Peu d'opérateurs ont été identifiés dans la population à l'étude, ce qui limite l'interprétation possible des résultats. De plus, la moitié des opérateurs sont des membres invités (n=2), ainsi les informations à leurs sujets ne sont pas disponibles. Par conséquent, seulement deux individus pourront être étudiés pour représenter les opérateurs : un est membre de niveau 2 (B85), donc bien placé dans la hiérarchie du forum, et l'autre est un nouveau membre (B84). En ce qui a trait à leurs scores de réputation, B85 a obtenu une excellente cote (2064) alors que le nouveau membre a une réputation inférieure à la moyenne des

botmasters à l'étude. Cette répartition de la réputation est peu surprenante étant donné les statuts de ces individus.

Activité

L'opérateur le mieux réputé publie énormément (306 publications), contrairement à B84, pour qui la quantité de publications se situe aussi sous la moyenne de celle de la population (13 publications). Ces opérateurs ont été étudiés un peu plus en détail afin de voir si d'autres facteurs que le nombre de publications ou le statut auraient un impact sur leur réputation. La durée de leur présence dans le forum a aussi été observée (Décary-Hétu et Dupont, 2013). Il a été surprenant de constater que B84 a plus de sept mois d'ancienneté que B85, alors que ce dernier a plus de publications et une meilleure réputation. Dans ce cas-ci, il est évident que l'ancienneté des membres n'a pas eu d'influence sur la réputation de ceux-ci ni sur leur activité.

En ce qui concerne leur présence dans d'autres forums, les quatre opérateurs à l'étude ont été identifiés dans plus de deux, trois et même six forums avec les mêmes identifiants. Le membre le moins réputé a été identifié dans plus de six forums, alors que celui qui est mieux placé, B85, ne se retrouvait que dans deux autres forums (se référer au tableau 8 en annexe). Cela laisse à suggérer que ce dernier se préoccupe plus de son anonymat que le nouveau membre. Il serait plus actif et réputé dans Dark0de, mais serait moins présent dans d'autres forums. En fait il est pertinent de préciser qu'il a été retrouvé à l'aide d'un second identifiant (qu'il a divulgué lui-même dans son introduction). En ce qui a trait à un des invités, B81, ce dernier ne se soucie pas de son identité. En effet, les recherches en sources ouvertes ont permis de récolter énormément de données personnelles à son sujet, soit son nom complet, son CV (LinkedIn), sa ville de résidence, des photos de sa famille, etc. Il est surprenant alors qu'un pirate informatique d'élite, accepté auprès de la communauté privée de Dark0de, soit aussi ouvert et présent sur les réseaux sociaux, et peu discret par rapport à sa vie privée. Si l'on considère cet élément, celui-ci pourrait contribuer à l'attribution d'une faible cote de réputation au sein du forum.

Expertises

Deux de ces opérateurs sont impliqués dans l'achat et la vente de produits et services divers. L'un d'eux, B85, mentionne uniquement faire du « business » sans préciser exactement dans quel genre de commerce il participe. Les deux derniers par contre, possèdent des compétences plus diversifiées. Ils font du codage et mènent des activités illicites, l'un impliqué dans des activités de *carding*, alors que l'autre se spécialise dans le piratage de jeux en ligne. Ce dernier aurait en plus de tout cela une expertise en ce qui concerne les systèmes « *adsense*[14] », alors que l'autre ferait du commerce et serait à la recherche de potentiels partenaires.

Conclusion

Il n'est pas possible de généraliser les résultats obtenus dans cette section. Cependant, deux opérateurs très différents ont été analysés : le premier a un statut élevé et une excellente réputation, est très actif au niveau des publications, et se soucie de son anonymat en utilisant d'autres identifiants d'un forum à l'autre. Le second, au contraire se trouve au bas de la hiérarchie du forum avec un statut de nouveau membre et une réputation inférieure à la moyenne de la population entière à l'étude. Il est peu actif dans Dark0de, mais son identité est facilement identifiable en ligne. Pour ce qui est d'un troisième individu, tout aussi intéressant, bien que ses données sur Dark0de ne soient pas disponibles, ses informations privées ont été aisément trouvées à l'aide de recherches par mot-clé en source ouverte. Ainsi, nous sommes en présence de trois individus très différents qui se trouvent à occuper les mêmes fonctions dans un marché et un forum très spécialisés.

Dans un autre ordre d'idées, la moitié des opérateurs ont des compétences variées non reliées aux botnets. En somme, il serait intéressant d'étudier davantage ce groupe de botmasters en particulier afin de mieux les comprendre. Un échantillon supérieur à deux ou quatre serait nécessaire pour avoir une meilleure vue d'ensemble.

[14] Service de placement publicitaire offert par Google, qui génère des revenus lorsque les pages sont visitées (TechTarget, s. d.)

Monétisation des botnets

Les individus qui monétisent les botnets sont très peu nombreux dans la population à l'étude. La section suivante tentera tout de même de dresser un portrait général par rapport à ce qui touche leur réputation, leur niveau d'activité et leurs expertises, à l'aide des données disponibles.

Tableau 5: Données statistiques sur le statut, la réputation et les publications des botmasters en charge de la monétisation des botnets	
Répartition des pirates qui monétisent leurs botnets en fonction de leur statut dans Dark0de	
Statut Dark0de	**Fréquence relative (n=3)**
Fresh Fish	33,33 %
Guest	33,33 %
Unknown	33,33 %
Total	100,00 %
Données statistiques sur la réputation des botmasters qui monétisent leurs botnets	
	Réputation (n= 2)
Moyenne	1817,50
Minimum	1707,00
Maximum	1928,00
Écart-type	156,27
Manquant (n=1)	33,33%
Moyenne générale totale (n=50)	*1796,12*
Données statistiques sur les publications des botmasters qui monétisent leurs botnets	
	Publications (n=2)
Moyenne	7,00
Minimum	1,00
Maximum	13,00
Écart-type	8,49
Manquant (n=1)	33,33%
Moyenne générale totale (n=50)	*63,4*

Statut et réputation

Parmi les trois individus à l'étude, seulement un d'entre eux a un statut de *fresh fish*, alors que pour les deux autres, il n'est pas défini. Le nouveau membre a une faible réputation (1707), tandis que le pirate en attente de réponse pour devenir membre a obtenu une cote élevée (1928), supérieure à celle de la moyenne de tous les botmasters. Il est peu surprenant que le *fresh fish* ait une cote de réputation sous la moyenne, cependant avoir une réputation inférieure à un individu qui ne fait pas encore partie du forum semble contre-intuitif. Cet individu en question, B09, est en fait un auteur de codes de botnets. Bien qu'il ait obtenu une aussi bonne réputation, il a systématiquement été refusé par un des administrateurs du forum, ce qui mène à se questionner sur les mécanismes d'attribution de réputation.

Activité

En ce qui concerne leur activité dans le forum, pour les deux botmasters dont les informations sont disponibles, la fréquence de publication est basse. Ce résultat est normal pour le membre en attente d'adhésion au forum, puisque son unique publication est son message d'introduction. En ce qui concerne leur présence dans d'autres forums, seul le *fresh fish* a été identifié dans trois autres forums avec son identifiant. Les deux autres n'ont pas été identifiés ailleurs, et même avec d'autres identifiants (se référer au tableau 8 en annexe). Ce qui est davantage étonnant est que le *guest* de cette section possède sept identifiants connus cependant, aucun d'entre eux n'a permis de le retrouver dans d'autres forums.

Expertises

Parmi ces individus, deux sont impliqués dans des activités de codage, un d'entre eux est aussi impliqué dans d'autres activités illicites : piratage, vente de passeports volés. Le dernier membre est commerçant, et opère ses botnets dans le but de les monétiser.

Conclusion

Seulement trois individus indiquaient savoir monétiser les botnets. On retrouvait parmi eux un *fresh fish* avec une faible réputation et peu de publications. Il affirme aussi opérer des botnets, ainsi qu'être un commerçant prêt à vendre et acheter divers produits et services. Cet individu a d'ailleurs été identifié dans trois autres forums que Dark0de avec ce même identifiant. Un second individu a été identifié en tant que membre invité, les données relatives quant à sa réputation et son activité au sein du botnet sont donc inconnues, cependant cet individu indique avoir de nombreuses expertises diversifiées, comme le codage, de piratage ou encore la revente de passeports volés. Fait intéressant, cet individu a sept identifiants différents connus, mais aucun d'entre eux n'a pu être identifié dans d'autres forums par des recherches en source ouverte. Le dernier individu de cette section était en attente d'approbation au moment où la base de données a été enregistrée. Il n'a pu avoir qu'une seule publication alors, et même s'il n'a pas encore pu bâtir sa réputation au sein du forum, celle-ci était tout de même plus élevée que la moyenne des botmasters à l'étude. Ce dernier est aussi un codeur et développeur en plus de savoir monétiser les

botnets. Une limite importante de l'étude de ces individus est que ceux-ci ne précisent pas de quelle façon ils monétisent ces réseaux, car les diverses techniques requièrent différentes compétences. Il aurait été intéressant d'en savoir plus, et d'avoir un plus grand échantillon d'individus aussi pour avoir une vue d'ensemble plus généralisable quant au profil de ces individus.

Les curieux

La catégorie des curieux comprend les individus affirmant porter un intérêt pour tout ce qui a trait aux botnets et leurs activités complémentaires. Dans le cadre de cette étude, ils seront considérés comme des individus en quête d'apprentissage par rapport à la création, au développement et à l'utilisation de botnets.

Tableau 6: Données statistiques sur le statut, la réputation et les publications des botmasters appelés « curieux »	
Répartition des curieux en fonction de leur statut dans Dark0de	
Statut Dark0de	**Fréquence relative (n=13)**
Fresh Fish	23,08 %
Guest	46,15 %
Level 1	15,38 %
Unknown	15,38 %
Total	100,00 %
Données statistiques sur la réputation des curieux	
	Réputation (n=7)
Moyenne	1756,43
Minimum	1634,00
Maximum	1847,00
Écart-type	75,62
Manquant (n=6)	46,15 %
Moyenne générale totale (n=50)	*1796,12*
Données statistiques sur les publications des curieux	
	Publications (n=8)
Moyenne	58,57
Minimum	1,00
Maximum	259,00
Écart-type	92,94
Manquant (n=6)	46,15 %
Moyenne générale totale (n=50)	*63,4*

Statut et réputation

Les analyses du forum Dark0de ont permis d'identifier 13 curieux parmi les botmasters à l'étude. Près de la moitié des individus sont des *guests*, il est donc difficile d'évaluer réellement qui sont ces individus. Le tableau 6 indique aussi que 15% de ces individus ont un statut inconnu, ainsi leur application pour devenir membre était encore en attente au moment de la sauvegarde de la base de données. Un autre 15% de ce groupe comprend des membres de niveau 1, et pour finir, les *Fresh Fish* comptent pour 23% de cette catégorie.

En ce qui concerne la réputation du groupe, celle-ci est inférieure à la moyenne de la population totale à l'étude, et cela, malgré la présence de membres de niveau 1. On

comprend ainsi que le statut n'influence pas autant la réputation que l'on pourrait imaginer. Cependant, puisque l'attribution de réputation et celle du statut ne se font pas par les mêmes acteurs, il n'est pas improbable de constater de tels écarts. De plus, puisque l'on considère que ces individus sont en situation d'apprentissage de nouvelles compétences relatives au botnets, il se pourrait que cela ait un impact sur leur réputation et statut, mais en même temps, ils se trouvent à priori dans Dark0de, un forum qui ne regroupe que l'élite des pirates informatique. D'ailleurs, qu'il s'agisse de Dark0de ou d'un autre forum, il y a une énorme variété de compétences qui sont mises en valeur dans les communautés de piratage, et l'apprentissage est un passage important dans le cheminement d'un pirate informatique. Il n'est donc pas possible à cette étape de déterminer si le fait de ne pas maîtriser les compétences nécessaires pour bâtir ou manipuler un botnet aurait un impact significatif sur le statut ou la réputation d'un pirate qui aurait potentiellement d'autres expertises.

Activité

Ce groupe est peu actif dans le forum Dark0de. Les curieux publient en moyenne 51 publications, ce qui est inférieur au botmasters en général (63.4 publications). Cette moyenne est toutefois gonflée à la hausse étant donné qu'un seul de ces individus se démarque quant à son activité avec 259 publications à son actif. Pour les autres, cette activité varie entre 1 et 82 publications, où les individus avec une seule publication à leur actif n'ont pas encore été admis dans le forum et n'ont alors que leur introduction comme unique publication. En somme, ces botmasters sont peu actifs au sein de Dark0de.

Pour ce qui en est de leur activité dans des forums autres que Dark0de, la plupart ont pu être identifiés dans différents forums. À l'exception des quatre membres qui ont uniquement été retrouvés dans Dark0de, cinq ont été identifiés dans un seul autre forum, deux dans deux autres forums, un dans trois forums et le dernier dans quatre forums (se référer au tableau 8 en annexe). Les membres identifiés dans le plus de grand nombre de forums étaient un *Fresh Fish* et un *Guest*.

Expertises

Les curieux ont des compétences plutôt diversifiées : huit prennent part à des échanges commerciaux de toute sorte, six font du codage et de la programmation de maliciels et

d'outils similaires, quatre sont impliqués dans des activités illicites de piratage, de pollupostage et de contrefaçon, et finalement deux font de la conception web. Un des curieux affirme même être un joueur de jeux de hasard. Un dernier encore, B95, qui mène des activités de piratage, rajoute être un employé dans une compagnie d'hébergement et fait des tests d'intrusion web. Ces individus font donc différentes activités, et cherchent à diversifier leurs expériences en acquérant des notions relatives aux botnets.

Conclusion

Bien que ces individus affirment porter un intérêt sur certains aspects du développement de botnets, ceux-ci sont tout de même intéressants à étudier puisqu'on pourrait les considérer en tant que botmasters en voie d'apprentissage. Ils proviennent de statuts différents, et ont une réputation moyenne inférieure à celle de la population totale. Ils publient peu d'ailleurs, à l'exception d'un seul individu. De plus, la plupart ont été identifiés dans un autre forum que Dark0de ou nulle part ailleurs. Peu nombreux sont ceux qui ont été retrouvés dans plus de deux autres forums. Pour finir, ils se diversifient au niveau de leurs expertises nombreuses.

Expérience

La catégorie de botmasters qui affirment avoir de l'expérience pose un peu problème dans le cadre de l'étude en question, au niveau de l'interprétation des résultats. En effet, ces individus ne précisent pas la nature de leur contribution dans le marché des botnets. Cependant, la même méthode sera appliquée pour ce groupe qui sera qualifié comme une catégorie plus générale, comprenant des botmasters de toutes expertises confondues.

Tableau 7: Données statistiques sur le statut, la réputation et les publications des individus ayant de l'expérience en matière de botnets	
Répartition des pirates affirmant avoir de l'expérience en matière de botnets en fonction de leur statut dans Dark0de	
Statut Dark0de	**Fréquence relative (n=32)**
Fresh Fish	25,00 %
Guest	40,63 %
Level 1	9,38 %
Level 2	3,12 %
Suspended	3,12 %
Unknown	18,75 %
Total	100,00 %
Données statistiques sur la réputation des botmasters	
	Réputation (n=19)
Moyenne	1784,47
Minimum	1553,00
Maximum	1999,00
Écart-type	125,23
Manquant (n=13)	40,63%
Moyenne générale totale (n=50)	*1796,12*
Données statistiques sur les publications des botmasters d'expérience	
	Publications (n=19)
Moyenne	44,26
Minimum	1,00
Maximum	300,00
Écart-type	69,28
Manquant (n=13)	40,63%
Moyenne générale totale (n=50)	*63,4*

Statut et réputation

Il est possible d'observer plus de variété au niveau des statuts dans cette catégorie de botmasters. On y retrouve une bonne part de *guests* (40%), et de botmasters en attente d'adhésion (19%). Ensuite, le quart de ce groupe comprend des *fresh fish*, donc de nouveaux membres au sein de Dark0de. Des membres de niveau 1 (9%) et de niveau 2 (3%) s'y retrouvent aussi, ainsi que des membres qui ont été suspendus du forum (3%). Il est

peu surprenant de constater autant de variété dans les statuts de ces individus étant donné la diversité de compétences possibles de botmasters dans cette catégorie. La réputation moyenne de ce groupe (1784) se trouve légèrement sous la moyenne des botmasters en général.

Activité

Ces botmasters sont moins actifs que la moyenne au sein de leur forum. Ils ont en moyenne 44 publications. Un botmaster se démarque cependant quant à son niveau d'activité. B49 aurait publié 300 messages sur Dark0de, en plus d'avoir la cote de réputation la plus élevée de ce groupe. Cet individu de niveau 1 affirme seulement avoir été impliqué dans des projets de botnets, sans donner davantage d'informations. Il a d'ailleurs été identifié dans cinq forums différents de Dark0de avec son identifiant. Cela pourrait indiquer une préoccupation moindre pour son anonymat, ou encore une priorité de préserver un bon statut dans les communautés de piratage.

En ce qui concerne les autres membres de ce groupe quant à leur présence dans d'autres forums, neuf n'ont pas été identifiés ailleurs que dans Dark0de. Dix ont été retrouvés dans un autre forum, cinq dans deux autres forums, trois dans trois autres forums, et le reste dans plus de quatre autres forums, dont un qui a été identifié dans plus de dix forums différents de Dark0de (se référer au tableau 8 en annexe). Ces cinq individus sont principalement des *fresh fish*, des *guest*s, ainsi qu'un membre de niveau 1. On peut suggérer que plus de la moitié sont plus préoccupés par la préservation de leur identité en utilisant, probablement, plusieurs identifiants différents, qui ne sont pas connus.

Expertises

Bien que leurs expertises en matière de botnets ne soient pas connues, ces individus ont tout de même des spécialisations variées. Plus de la moitié mènent des activités de codage et de développement d'outils et logiciels malveillants (n=19), dont six qui ne font qu'exclusivement ça. Une autre part importante d'individus sont impliqués dans des activités commerciales (n=17, dont trois qui le font exclusivement). Le tiers de ce groupe mènent aussi des activités illicites comme le *carding*, le pollupostage et autres activités criminelles (n=12). Cinq botmasters affirmant avoir de l'expérience possèdent des

compétences en matière de maintien de serveurs, ou de conception web (un seul ne fait que cela). Trois individus sont impliqués dans des activités publicitaires et de commerce de trafic, et finalement trois autres indiquent être à la recherche de partenaires. La plupart ont jusqu'à deux ou trois types d'expertises différentes parmi celles qui ont été énumérées, dont un qui en a quatre. Ainsi, on peut constater que la plupart de ces individus ne sont pas spécialisés. Seul le tiers indique se concentrer uniquement sur une seule expertise.

Conclusion

Outre les *guests* et les membres en attente d'attribution de statut, les botmasters d'expérience se composent principalement de *fresh fish*, et quelques niveaux 1 et 2. Leur réputation se situe dans la moyenne de la population à l'étude, mais ils publient moins que celle-ci. La grande majorité n'a été retrouvée que dans un autre forum autre que Dark0de ou uniquement dans ce dernier. En ce qui concerne leurs autres expertises, près du tiers se spécialisent dans une activité uniquement, alors que les autres ont des compétences variées (jusqu'à quatre catégories d'expertises en ligne). Il aurait été intéressant d'en savoir plus sur la nature de leur contribution dans le marché des botnets.

Comparaison

La partie suivante mettra en évidence des éléments comparatifs des variables à l'étude entre les différents rôles de botmasters. À titre de référence, un tableau comparatif des données sur le statut, la réputation et les publications se trouve en annexe (voir tableau 9).

En commençant par le statut, on constate que des membres de statuts variés se trouvent parmi les commerçants et les individus d'expérience. On retrouve tant des *fresh fish* que des membres de niveau 1 et 2. Pour ce qui est du reste des catégories de botmasters, les pirates en attente d'approbation au forum ainsi que les *fresh fish* composent l'essentiel des membres. Les membres invités aussi se retrouvent en majorité dans toutes les catégories, et comptent d'ailleurs pour 43% de la population totale à l'étude.

Ensuite, les opérateurs ainsi que les distributeurs se sont avérés être les botmasters ayant obtenu les meilleures cotes de réputation parmi leurs pairs (1885 et 1882 respectivement), suivis des codeurs et des pirates qui monétisent les botnets (1817 chacun). Ces quatre catégories de botmasters se situent au-dessus de la réputation moyenne du groupe. Les individus d'expérience se situent le plus près de la moyenne avec un écart de 12 points, et les catégories les moins appréciées sont les commerçants et les curieux (1762 et 1756 respectivement). Certains de ces résultats sont inattendus. On aurait pu s'attendre à ce que les codeurs aient obtenu de meilleurs résultats étant donné qu'ils sont à l'origine du marché et qu'ils possèdent des connaissances techniques très spécifiques, tout comme les commerçants puisqu'ils occupent un rôle important et central dans le marché des botnets. Il est donc d'autant plus surprenant de constater que les opérateurs aient atteint de meilleures cotes que leurs pairs, puisque n'importe quel individu pourrait prendre le contrôle d'un botnet sans avoir besoin de compétences particulières. Finalement, les curieux ont obtenu la réputation la plus faible de la population, ce qui ne surprend pas étant donné qu'on les considère comme des pirates en apprentissage en ce qui a trait aux botnets, ou peut-être encore des amateurs qui font perdre du temps aux professionnels. Il est important de préciser qu'il faut interpréter ces résultats avec prudence, puisqu'à priori les membres de Dark0de sont considérés comme l'élite des pirates informatiques du monde anglophone. De tels résultats indiqueraient aussi qu'il est important de s'attarder davantage aux mécanismes d'attribution de points de réputation.

Au niveau de l'activité au sein du forum à l'étude, on constate que les membres qui publient le plus sont les opérateurs, les commerçants et les curieux (160, 98 et 60 respectivement). Alors que les pirates d'expérience, les codeurs, les individus qui monétisent ainsi que les distributeurs sont moins actifs en ce qui concerne leurs publications (44, 11, 7 et 3 respectivement). Il ne faut pas négliger l'impact des conversations en messageries privées qui ont souvent lieu dans tels milieux, ni même qu'une part importante des individus à l'étude n'avait pas accès encore au forum et ne pouvait publier que leur introduction (18%). Ces deux facteurs pourraient avoir un énorme impact sur l'interprétation de ces données. Il aurait d'ailleurs été intéressant de pouvoir étudier les contenus de ces publications afin de comprendre davantage la distribution de ces résultats, mais dans le cadre de ce travail, cette analyse n'a pas pu être réalisée.

En ce qui concerne la présence des membres dans d'autres forums, les résultats ont permis de constater que la majorité du temps, ceux-ci étaient identifiés dans un seul forum, ou nulle part ailleurs que Dark0de. Cela pourrait indiquer que ces individus un souci de prudence quant à leur présence trop évidente dans d'autres forums. Ces individus utiliseraient possiblement de nombreux identifiants variés d'un forum à l'autre. Toutefois, de rares individus ont pu être identifiés à l'intérieur de plus de 10 autres forums de piratage à l'aide de recherches par mots-clés. Il serait possible de suggérer que dans ces cas-ci, certains pirates accorderaient plus d'importance quant au maintien et au développement de leur réputation. La relation entre la présence des individus dans les forums et leur réputation n'a pas été étudiée de plus près pour confirmer cette hypothèse, dans le cadre de ce travail. Cette piste serait toutefois intéressante à explorer davantage pour des recherches éventuelles.

Pour finir, les expertises des botmasters ont aussi été étudiées afin de voir si ces individus ont tendance à se spécialiser ou diversifier leurs connaissances. Les résultats indiquent que plus de la moitié des codeurs se spécialisent en matière de codage et de programmation d'outils variés, et pas seulement en lien avec les botnets. Mais pour la plupart de ces codeurs, ils seraient impliqués dans diverses activités relatives aux botnets (distribution, commerce, etc.). De plus, parmi les individus qui affirment avoir de l'expérience avec les botnets, le tiers indiquait se spécialiser dans une seule expertise. Pour les autres botmasters

à l'étude, la plupart indiquent avoir des intérêts et compétences assez diversifiés, allant de deux à quatre type d'expertises non relatives aux botnets. Ces individus sont donc assez polyvalents quant à leur savoir-faire, certains mentionneront même avoir certaines compétences applicables au monde physique, et non seulement virtuel.

Chapitre V – Dimension d'intégration en criminalistique

L'utilisation d'Internet dans la commission de délits par les cybercriminels a pour avantage d'enregistrer une quantité abondante de données numériques laissées par ces individus, d'un point de vue forensique (Casey, 2011). Ces traces permettent d'observer les activités des cybercriminels, qu'il s'agisse de connexions aux serveurs, d'adresses IP utilisées, de noms d'identifiants, de publications, d'envoi de communications, de trafic, ou même de données personnelles, pour n'en nommer que quelques-uns (Casey, 2011). La pérennité de ces traces virtuelles en permet l'utilisation dans le cadre d'enquêtes. Il suffit qu'un pirate informatique commette une seule erreur, comme utiliser le même nom d'usager dans divers forums, comme dans le cas de B81, pour permettre aux forensiciens numériques de monter une enquête contre cet individu qui mènerait ensuite à son arrestation.

Parmi les formes de traces numériques, il serait pertinent de tenter d'identifier, à l'aide des ressources disponibles, des types de traces qui découleraient spécifiquement d'activités liées à l'opération ou à la création de botnets. En d'autres mots, il serait intéressant de voir dans le discours des botmasters s'ils privilégient l'utilisation de certains outils spécifiques ou encore s'ils partagent leur savoir-faire avec leurs pairs. Idéalement, cet exercice pourrait servir aux forensiciens numériques dans leurs investigations portant sur les botmasters, et plus particulièrement à détecter des patterns en ce qui a trait aux moyens de création et d'opération de ces réseaux. En effet, il deviendrait possible d'orienter certaines recherches en traces numériques grâce aux analyses de profils généraux de ce type d'auteur, en l'occurrence leurs expertises informatiques, et à la détection de patterns au niveau de leurs modes d'opération et de leurs lieux de convergence dans le cyberespace. Par exemple, à l'aide des conversations disponibles sur le forum, il est possible de lier des individus avec les outils qu'ils ont conçus. Ensuite, en faisant des analyses plus poussées sur les mécanismes d'opération de ces outils, il devient possible pour les experts de trouver des signatures ou traces particulières dans les codes de ces outils et ainsi d'estimer en partie leurs fréquences d'utilisation sur Internet. De cette façon, les forensiciens pourront identifier quels individus contribuent le plus au marché des botnets. D'ailleurs, les informations qui peuvent être extraites de ces outils permettraient aussi, à l'inverse, d'en

identifier les auteurs. Le style d'écriture ou encore les modes opératoires sont des exemples de types d'informations qui peuvent être mobilisables par les analystes numériques.

Il est d'autant plus pertinent d'étudier ces traces dans un forum privé comme Dark0de, car ce dernier regroupe 500 pirates de haut calibre, contrairement à un forum ouvert à tous les niveaux et qui peut comporter plus de trois millions de membres (Hackforums par exemple contient plus de 3 696 734 membres[15]). Non seulement l'étude de forums spécialisés permet aux services d'enquête de se concentrer sur les pirates les plus influents et compétents, mais aussi facilite l'identification de ces individus lorsqu'ils sont 500 plutôt que perdre du temps à les retrouver parmi une population de trois millions de pirates.

En plus de combler une lacune dans la recherche en criminologie, l'étude des botmasters amènerait une seconde contribution au sein de la communauté forensique numérique. Dans les cas où les sujets à l'étude publient, volontairement ou non, des détails personnels, tels leur localisation ou encore des intérêts spécifiques, qui s'avèreraient exacts, ces informations permettraient aux experts de cibler leurs recherches et éventuellement retrouver des botmasters. Ces traces laissées dans les forums deviennent alors une source d'information non négligeable pour l'investigation numérique.

[15] Source : https://hackforums.net/. Site web consulté le 31 août 2017.

Conclusion

Les botnets posent une menace importante dans le cyberespace. Dans les dernières années, les mécanismes d'infection ainsi que les conséquences de tels réseaux ont été documentés. Cependant, les individus responsables de telles attaques sont toujours dans l'ombre. Un écart important est constaté en ce qui concerne les connaissances sur les sujets des botnets et des botmasters. Ainsi, dans une perspective criminologique, il est nécessaire d'en savoir davantage sur les individus concernés par de telles activités. Le but principal de cette étude exploratoire était de pallier à ces lacunes en se centrant sur les rôles des botmasters dans le marché des botnets. Plus spécifiquement, les variables ciblées dans cette étude comprenaient le statut et la réputation de ces individus, leur activité au sein du forum et de la communauté de piratage en général, ainsi que les expertises diverses de ces individus. Par conséquent, il a été tenté de dresser des profils de ces caractéristiques pour chaque catégorie de botmasters prélevé dans le forum de piratage Dark0de, soient les codeurs, commerçants, distributeurs, opérateurs, curieux, ainsi que les individus qui monétisent les réseaux et ceux qui affirment avoir de l'expérience.

Les résultats préliminaires se sont avérés intéressants, et ce, malgré les nombreuses limites associées aux méthodes employées ainsi qu'aux données disponibles. À commencer par les codeurs, ces individus se classent bien au niveau de leur réputation, malgré qu'ils soient peu actifs au sein de leur communauté et que leurs statuts ne soient pas particulièrement bons. Plus de la moitié se spécialiseraient uniquement en codage et programmation, alors que le reste possèderait des compétences informatiques plus variables. Les commerçants quant à eux, ont obtenu des scores de réputation moins élevés, cependant des botmasters de statuts variés s'y trouvent. D'ailleurs, ils sont plus actifs tant au sein de Dark0de que dans la communauté de piratage, et ont aussi des compétences diversifiées. Les distributeurs ainsi que les opérateurs ont obtenu les meilleurs scores de réputation, et cela malgré de bas statuts. D'ailleurs dans ces deux catégories, ces individus indiquent avoir d'autres expertises non reliées aux botnets. Là où ces groupes se distinguent, est au niveau de leur activité, alors que les opérateurs publient énormément dans Dark0de et peuvent se retrouver dans plusieurs autres forums de piratage, les distributeurs publient moins et pour

la nette majorité ils ne participent qu'à un seul autre forum. Les botmasters qui monétisent ont eux aussi une bonne réputation malgré de faibles statuts et peu d'activité tant au sein de Dark0de que dans les autres forums de piratage. Les curieux, quant à eux, ont obtenu la cote de réputation la plus faible, bien qu'ils soient plus actifs et possèdent plusieurs expertises variées. Pour finir, les individus qui affirmaient avoir de l'expérience avec les botnets comprenaient des sujets provenant de statuts variés et ont obtenu une réputation correspondant à la moyenne de la population à l'étude. Bien qu'ils soient assez actifs dans Dark0de, près de 60% de ceux-ci se trouvaient dans un autre forum ou moins. De plus, le tiers de ces individus auraient indiqué avoir un seul type de spécialisation, alors que les autres avaient des expertises plus nombreuses et diversifiées.

Il s'agit là d'une première étude en son genre, qui se focalise uniquement sur les botmasters. La prochaine étape est alors de comprendre davantage pourquoi ces catégories de botmasters sont aussi différentes, et comment la réputation ou les statuts sont réellement attribués. Même si certaines hypothèses ont été suggérées tout au long de l'analyse, il reste encore beaucoup de pistes inexplorées, à commencer par la relation entre les botmasters et les *hackers*. Suite aux analyses menées dans le contexte de cette étude, on se rend compte finalement qu'il est complexe d'appliquer des typologies de pirates basées sur les compétences de ceux-ci aux botmasters à l'étude. En effet, les sujets de cette recherche étaient considérés a priori comme des pirates déjà compétents et de haut niveau. Puisque l'on conclut aussi que les botmasters ne sont pas forcément des individus qui ont tendance à se spécialiser, et que l'on sait que les pirates informatiques en général peuvent avoir des expertises variables, il est possible d'affirmer que les botmasters ne seraient pas si différents des hackers finalement. L'hypothèse proposée ici est que les botmasters, tout comme les pirates, s'adonnent à diverses activités illicites en ligne et sont en quête de nouveaux apprentissages. Au final, la question de relation entre les botmasters et les pirates est-elle réellement pertinente? Peu importe leur véritable relation, à l'intérieur même des types de cybercriminels, les compétences techniques et les secteurs d'activités illicites virtuelles sont extrêmement variables. Ainsi, même si les botmasters appartenaient à une sous-catégorie de pirates informatiques ou bien constituent un groupe à part, la pertinence d'étudier de tels individus persiste à l'heure actuelle.

Parmi les limites principales rencontrées, un obstacle de taille se réfère à la situation des *guests* qui comptent pour 43% des sujets ce qui implique donc que 43% des données sont manquantes quant à leur réputation, la réelle nature de leur statut ainsi que leur activité au sein deDark0de. Un problème est aussi survenu quant au contenu des publications et échanges des individus, puisque l'étude a été menée seulement à partir des messages d'introduction de ces individus. La section de marchés aurait été intéressante à étudier davantage pour réduire cette limite. On constate tout de même qu'il reste encore beaucoup d'inconnu, même pour l'interprétation des résultats actuels et même encore pour la proposition d'hypothèses plausibles.

Étant donnée la nature exploratoire de la présente étude, plusieurs pistes de réflexion intéressantes ont été relevées pour des projets futurs sur la question des botmasters. Tout d'abord, des recherches similaires à celle-ci pourraient être proposées pour étudier les botmasters issus d'autres milieux, tels les forums russes, qui ont la réputation d'inclure les meilleurs pirates informatiques, ou encore des forums moins élitistes pour voir s'il existe des variations plus marquées quant aux compétences. D'ailleurs, il aurait été utile de s'attarder davantage aux expertises des botmasters, surtout au niveau de la qualité, à savoir si ces individus sont réellement doués dans les compétences qu'ils indiquent maitriser. Des approches méthodologiques différentes pourraient également être adoptées. Ainsi des entrevues et des études longitudinales pourraient être employées afin de tenir compte d'aspects motivationnels et psychologiques, en plus de traiter de notions d'apprentissage et de transfert de savoirs, ainsi que de l'évolution sociale de ces individus. D'un point de vue plus forensique, des études complémentaires seraient pertinentes. Dans un premier temps, il serait utile d'étudier davantage les familles de botnet et d'observer s'il existe une corrélation entre celles-ci et les profils de botmasters. On pourrait encore essayer de traquer la signature de code permettant la création de botnet et de suivre sa progression et ainsi observer comment il est distribué, vendu, transformé et utilisé. Pour finir, des analyses de réseaux de botmasters qui tiennent compte des rôles occupés par ceux-ci seraient d'autant plus pertinentes pour des services de mise en application de la loi. Somme toute, nous en avons encore beaucoup à apprendre sur ces individus. Ces pirates polymorphes restent une menace réelle dans le cyber espace, c'est pourquoi il est primordial de mieux les comprendre, surtout dans une perspective de lutte efficace contre les botnets.

Annexe I

Tableau 8: Distribution des botmasters selon leur présence dans des forums différents de Dark0de							
Nombre de forums autres que Dark0de	**Codeurs (n=23)**	**Commerçants (n=19)**	**Distribution (n=9)**	**Opérateurs (n=4)**	**Monétisation (n=3)**	**Curieux (n=14)**	**Expérience (n=32)**
0	34,8 %	42,1 %	11,1 %	0,0 %	66,7 %	28,6 %	28,1 %
1	26,1 %	31,6 %	66,7 %	0,0 %	0,0 %	42,9 %	31,3 %
2	26,1 %	21,1 %	11,1 %	25,0 %	0,0 %	14,3 %	15,6 %
3	4,3 %	5,3 %	11,1 %	50,0 %	33,3 %	7,1 %	9,4 %
4	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	7,1 %	3,1 %
5	4,3 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	6,3 %
6	0,0 %	0,0 %	0,0 %	25,0 %	0,0 %	0,0 %	0,0 %
7	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	3,1 %
8	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %
9	4,3 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %
10	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	3,1 %

Tableau 9: Tableau comparatif sur les données de réputation, publications et statuts des botmasters dans Dark0de							
	Codeurs	**Commerçants**	**Distributeurs**	**Opérateurs**	**Monétisation**	**Curieux**	**Expérience**
Réputation	1817,28	1762,27	1889	1885,5	1817,5	1756,43	1784,47
Publications	10,70	97,45	2,67	159,50	7,00	58,57	44,26
Statuts							
Fresh Fish	13,04 %	26,32%	11,11%	25,00%	33,33%	23,08%	25,00%
Guest	52,17 %	42,11%	66,67%	50,00%	33,33%	46,15%	40,63%
Level 1	0,00%	10,53%	0,00%	0,00%	0,00%	15,38%	9,38%
Level 2	0,00%	10,53%	0,00%	25,00%	0,00%	0,00%	3,12%
Suspended	4,35 %	0,00%	0,00%	0,00%	0,00%	0,00%	3,12%
Unknown	30,43 %	10,53%	22,22%	0,00%	33,33%	15,38%	18,75%

Références

Abbasi, A., Li, W., Benjamin, V. A., Hu, S., & Chen, H. (2014, September). Descriptive Analytics: Examining Expert Hackers in Web Forums. In *JISIC* (pp. 56-63).

Abu Rajab, M., Zarfoss, J., Monrose, F. et Terzis, A. (2006, Octobre). *A multifaceted approach to understanding the botnet phenomenon*. Dans Proceedings of the 6th ACM SIGCOMM conference on Internet measurement. ACM.

Auray, N., Kaminski, D., (2006). Les trajectoires de professionnalisation des hackers : la double vie des professionnels de la sécurité. *Working papers in economics and social sciences*, Télécom Paris.

Barber, R. (2001). Hackers profiled—who are they and what are their motivations?. *Computer Fraud & Security*, *2001*(2), 14-17.

Benjamin, V., & Chen, H. (2012, June). Securing cyberspace: Identifying key actors in hacker communities. In *Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on* (pp. 24-29). IEEE.

Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M. et Wang, L. (2010). On The Analysis Of The Zeus Botnet Crimeware Toolkit. *Privacy Security And Trust*. Ottawa, Ontario, p.31-p.38.

Blanchard, F., Fortin, F. (2013). Nouveaux habits de la vieille fraude: une vision «écosystémique» des fraudeurs, de leurs instruments et de leurs victimes. Dans F. Fortin (dir.), *Cybercriminalité: Entre inconduite et crime organisé* (p. 237-258). Québec, Canada: Presses internationales polytechniques.

Boutin, E. (2003). Méthodologie relationnelle d'extraction de connaissances à partir de données provenant d'un forum de discussion. *International Journal of Info & Com Sciences for Decision Making*, (9), 2-10.

Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, CA: Praeger.

Brenner, S., Schwerha, J. (2004). Cybercrime: A Note on International Issues. *Information Systems Frontiers, 6*(2), 111-114.

Cooke, E., Jahanian, F., & McPherson, D. (2005). The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets. *SRUTI*, *5*, 1-6.

Décary-Hétu, D. (2011). Les botmasters : Mythe ou réalité? *Chaire de recherche du Canada en sécurité, identité et technologie*, Note de recherche 12, pp. 1-26.

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global crime*, *14*(2-3), 175-196.

Donohue, B. (2013, 28 février). How much does a botnet cost? Repéré à: https://threatpost.com/how-much-does-botnet-cost-022813/77573/

Dufour, C. (2014). SCI6060 – Méthodes de recherche en sciences de l'information. Repéré à : http://reseauconceptuel.umontreal.ca/rid=1HZKGLHZ9-R7ZQMG-82Q/sci6060a_carte.cmap

Dupont, B. (2010). L'évolution du piratage informatique: de la curiosité technique au crime par sous-traitance. *Le respons@ ble*, *2*, 63-81.

Dupont, B. (2012). Nouvelles technologies et crime désorganisé: incursion au cœur d'un réseau de pirates informatiques. *Sécurité et stratégie*, *11*(4), 25-37.

Dupont, B. (2014). La régulation du cybercrime comme alternative à la judiciarisation. Le cas des botnets. *Criminologie, 47*(2), 179-201.

Dupont, B. (2014). Skills and trust: A tour inside the hard drives of computer hackers. Dans C. Morselli (dir.), *Illicit networks*, Oxford: Routledge, pp. 195-217

Europol. (2015, 15 juillet). Cybercriminal Darkode forum taken down through global action. Repéré à: https://www.europol.europa.eu/newsroom/news/cybercriminal-darkode-forum-taken-down-through-global-action

Fortin, F., Gagnon, B. (2013). Tendances de la cybercriminalité. Dans F. Fortin (dir.), *Cybercriminalité: Entre inconduite et crime organisé* (p. 347-366). Québec, Canada: Presses internationales polytechniques.

Freyssinet, É. (2015). *Lutte contre les botnets: analyse et stratégie* (Doctoral dissertation, Université Pierre et Marie Curie).

Ghernaouit-Hélie, S. (2009). *La cybercriminalité: le visible et l'invisible*. Lausanne: Presses polytechniques et universitaires romandes.

Ghernaouti, S. (2013). *Cyber power: crime, conflict and security in cyberspace*. Crc Press.

Goudey, H. (2004) Watch the money go round, watch the malware go round. *Proceedings of the Virus Bulletin Conference*. Chicago, USA

Graham, L. (2017, 7 Février). Cybercrime costs the global economy $450 billion: CEO. Repéré à: https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html

Holt, J. T., Strumsky, D., Smirnova, O. et Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology, 6*(1), 891-903.

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

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

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). *Data Thieves in Action: Examining the International Market for Stolen Personal Information*. Springer.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). The Marketing and Sales of Stolen Data. In *Data Thieves in Action* (pp. 19-43). Palgrave Macmillan US.

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

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology*, *6*(1), 891.

Hutchings, A., & Holt, T. J. (2014). A crime script analysis of the online stolen data market. *British Journal of Criminology*, azu106.

John, J. P., Moshchuk, A., Gribble, S. D., & Krishnamurthy, A. (2009, April). *Studying Spamming Botnets Using Botlab*. Dans NSDI (9), pp. 291-306.

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

Lavoie, P.-É., Fortin, F. et Tanguay, S. (2013). Problèmes relatifs à la définition et à la mesure de la cybercriminalité. Dans F. Fortin (dir.), *Cybercriminalité: Entre inconduite et crime organisé* (p. 3-20). Québec, Canada: Presses internationales polytechniques.

Lavoie, P.-É., Fortin, F., Ouellet, I. (2013). Usages problématiques d'Internet. Dans F. Fortin (dir.), *Cybercriminalité: Entre inconduite et crime organisé* (p. 53-74). Québec, Canada: Presses internationales polytechniques.

Li, C., Jiang, W. et Zou, X. (2009, décembre). *Botnet : Survey and Case Study*. Dans le 2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC). IEEE Computer Society.

Marcoccia, M. (2004). L'analyse conversationnelle des forums de discussion: questionnements méthodologiques. *Les Carnets du Cediscor. Publication du Centre de recherches sur la didacticité des discours ordinaires*, (8), 23-37.

Radware (s. d.). DDoS Attack Definitions – DdoSPedia – Botmaster. Repéré à: https://security.radware.com/ddos-knowledge-center/ddospedia/botmaster/

Ramsbrock, D., Wang, X., et Jiang, X. (2008, Janvier). A first step towards live botmaster traceback. Dans R. Lippmann, E. Kirda et A. Trachtenberg (dir.), *Recent Advances in Intrusion Detection* (pp. 59-77). Springer Berlin Heidelberg.

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital investigation*, *3*(2), 97-102.

Rounds, M., & Pendgraft, N. (2009, August). Diversity in network attacker motivation: A literature review. In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 3, pp. 319-323). IEEE.

Rouse, M. (2012, mai). Zeus Trojan (Zbot). Repéré à : http://searchsecurity.techtarget.com/definition/Zeus-Trojan-Zbot

Shakarian, J., Gunn, A. T., & Shakarian, P. (2016). Exploring malicious hacker forums. In *Cyber Deception* (pp. 261-284). Springer International Publishing.

Steinmetz, K. F. (2015). Craft(y)ness: An Ethnographic Study of Hacking. *British Journal of Criminology, 55*, 125-145.

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C. et Vigna, G. (2009, Novembre). *Your botnet is my botnet: analysis of a botnet takeover*. Dans Proceedings of the 16th ACM conference on Computer and communications security. ACM.

Stone-Gross, B., Holz, T., Stringhini, G., & Vigna, G. (2011). The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. *LEET*, *11*, pp. 1-8.

Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. Psychology press.

The Associated Press. (2016, 20 avril). SpyEye creator nets prison time for malware that bilked $1B globally. Repéré à: http://www.cbc.ca/news/world/spyeye-creator-sentenced-1.3545773

Thomas, R. et Martin, J. (2006). The Underground Economy: Priceless. *Login, 31*(6), pp. 7-16.

Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review*, *23*(1), 8-23.

U.S. Department of Justice. (2015, 15 juillet). Major Computer Hacking Forum Dismantled. Repéré à: https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/major-computer-hacking-forum-dismantled

Van Eeten, M., Bauer, J. M. (2009). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. *Journal of Contingencies and Crisis Management, 17*(4), 221-232.

Wall, D. (2007). Policing cybercrimes: situating the public police in networks of security within cyberspace. *Police Practice and Research*, *8*(2), pp. 183-205.

Wall, D. (2015). Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime. *The European Review of Organised Crime*, *2*(2).

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. *Information Systems Frontiers*, *17*(6), 1239-1251.

Zhuang, L., Dunagan, J., Simon, D. R., Wang, H. J., Osipkov, I., & Tygar, J. D. (2008). Characterizing Botnets from Email Spam Records. *LEET*, *8*, pp. 1-9.