Council Special Report No. 83
November 2018

Zero Botnets

Building a Global Effort to Clean Up the Internet

Jason Healey and Robert K. Knake

COUNCIL on FOREIGN RELATIONS

Rapport spécial du Conseil n° 83
Novembre 2018

Zéro Botnets

Mettre en place un effort mondial pour nettoyer l'internet

Jason Healey et Robert K. Knake

Le Council on Foreign Relations (CFR) est une organisation indépendante et non partisane, un groupe de réflexion et un éditeur qui se consacre à être une ressource pour ses membres, les responsables gouvernementaux, les chefs d'entreprise, les journalistes, les éducateurs et les étudiants, les dirigeants civiques et religieux, et d'autres citoyens intéressés, afin de les aider à mieux comprendre le monde et les choix de politique étrangère auxquels sont confrontés les États-Unis et d'autres pays. Fondé en 1921, le CFR remplit sa mission en maintenant une diversité de membres, avec des programmes spéciaux pour promouvoir l'intérêt et développer l'expertise de la prochaine génération de leaders en politique étrangère ; en organisant des réunions à son siège à New York et à Washington, DC, et dans d'autres villes où de hauts fonctionnaires, des membres du Congrès, des leaders mondiaux et d'éminents penseurs se réunissent avec les membres du Conseil pour discuter et débattre des grandes questions internationales ; le soutien d'un programme d'études qui encourage la recherche indépendante, permettant aux chercheurs du CFR de produire des articles, des rapports et des livres et d'organiser des tables rondes qui analysent les questions de politique étrangère et formulent des recommandations politiques concrètes ; la publication de *Foreign Affairs*, la revue la plus importante sur les affaires internationales et la politique étrangère des États-Unis ; le parrainage de l'association Independent Affairs.Le CFR publie Foreign Affairs, la plus importante revue sur les affaires internationales et la politique étrangère des États-Unis, parraine des groupes de travail indépendants qui produisent des rapports contenant à la fois des conclusions et des recommandations politiques sur les sujets de politique étrangère les plus importants, et fournit des informations et des analyses actualisées sur les événements mondiaux et la politique étrangère américaine sur son site Web, CFR.org.

Le Council on Foreign Relations ne prend aucune position institutionnelle sur les questions politiques et n'a aucune affiliation avec le gouvernement des États-Unis. Toutes les opinions exprimées dans ses publications et sur son site Web relèvent de la seule responsabilité de l'auteur ou des auteurs.

Les rapports spéciaux du Conseil (CSR) sont des notes politiques concises, produites pour fournir une réponse rapide à une crise en cours ou contribuer à la compréhension par le public des dilemmes politiques actuels. Les CSR sont rédigés par des auteurs individuels - qui peuvent être des boursiers du CFR ou des experts reconnus de l'extérieur de l'institution - en consultation avec un comité consultatif, et sont censés prendre soixante jours entre leur conception et leur publication. Le comité sert de caisse de résonance et fournit des commentaires sur un projet de rapport. Il se réunit généralement deux fois - une fois avant la rédaction d'un projet et une autre fois lorsqu'un projet est soumis à l'examen ; toutefois, les membres du comité consultatif, contrairement aux membres du groupe de travail, ne sont pas invités à signer le rapport ou à l'approuver d'une autre manière. Une fois publiés, les CSR sont affichés sur CFR.org.

Pour de plus amples informations sur le CFR ou ce rapport spécial, veuillez écrire au Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, ou appeler le bureau des communications au 212.434.9888. Visitez notre site Internet, CFR.org.

Pour soumettre une lettre en réponse à un rapport spécial du Conseil en vue de sa publication sur notre site web, CFR.org, vous pouvez envoyer un courriel à publications@cfr.org. Vous pouvez également nous envoyer vos lettres par courrier à l'adresse suivante : Département des publications, Council on Foreign Relations, 58 East 68th Street, New York, NY 10065. Les lettres doivent inclure le nom de l'auteur, son adresse postale et son numéro de téléphone en journée. Les lettres peuvent être éditées pour des raisons de longueur et de clarté, et peuvent être publiées en ligne. Veuillez ne pas envoyer de pièces jointes. Toutes les lettres deviennent la propriété du Council on Foreign Relations et ne seront pas renvoyées. Nous regrettons de ne pas pouvoir répondre à toutes les lettres en raison de leur volume.

Ce rapport est imprimé sur du papier certifié FSC ® Chain-of-Custody par un imprimeur certifié par BM TRADA North America Inc.

SOMMAIRE

AVANT-PROPOS

Le cyberespace ressemble de plus en plus à l'ancien Far West américain, sans véritable shérif et avec les botnets comme hors-la-loi armés. Les botnets, ou groupes d'ordinateurs infectés par des logiciels malveillants et contrôlés comme un seul réseau, sont à l'origine d'une grande partie de la cybercriminalité sur l'internet. Ils permettent en effet à ceux qui contrôlent le réseau d'exploiter la puissance des superordinateurs à des fins malveillantes. Les botnets sont utilisés pour diffuser des spams, envoyer des courriers électroniques de phishing, deviner des mots de passe, casser des cryptages et lancer des attaques par déni de service distribué. Malgré les efforts importants déployés pour éliminer les botnets, leur nombre n'a cessé d'augmenter.

Comme le soutiennent Jason Healey et Robert K. Knake dans ce nouveau rapport spécial du Conseil, l'idée reçue selon laquelle les botnets sont un problème à gérer vise trop bas. Les botnets peuvent causer de graves dommages en permettant à des gouvernements étrangers d'étouffer la liberté d'expression à l'étranger et en leur permettant de fermer les réseaux nationaux des pays, voire l'internet dans son ensemble. En outre, le préjudice économique causé par les botnets est susceptible d'augmenter considérablement au fil du temps, à mesure que le nombre d'appareils connectés à Internet augmente. Les responsables politiques devraient donc redoubler d'ambition et chercher à débarrasser le monde des botnets. Bien que l'objectif de zéro botnet soit impossible à atteindre, les auteurs concluent qu'il est nécessaire de fixer un objectif aussi ambitieux pour orienter les politiques.

Les auteurs proposent plusieurs prescriptions politiques innovantes. Ils suggèrent que les décideurs politiques s'efforcent d'établir le principe selon lequel les États sont responsables des dommages que les botnets basés à l'intérieur de leurs frontières causent aux autres. Les fournisseurs d'accès à Internet devraient se tenir mutuellement responsables du mauvais trafic qui quitte leurs réseaux. Des mesures incitatives devraient être mises en place pour que les fabricants d'appareils connectés à l'internet prennent des mesures pour sécuriser leurs appareils. Les composants de l'écosystème de l'internet qui sont

utilisés par les botnets devraient être poussés à se surveiller eux-mêmes et à empêcher que leurs services ne soient utilisés à des fins criminelles. Enfin, un effort international pour démanteler les botnets peut s'avérer nécessaire si ces mesures ne parviennent pas à stopper leur croissance.

La prévalence des botnets et les problèmes qu'ils causent prouvent une fois de plus que bon nombre des défis du XXIe siècle ne peuvent être contenus dans les frontières ou traités au niveau national. Au contraire, pour minimiser la capacité de nuisance des botnets, les pays devraient appliquer le concept d'obligation souveraine, c'est-à-dire la notion selon laquelle les États souverains ont non seulement des droits mais aussi des obligations vis-à-vis des autres pays. Les gouvernements auraient l'obligation non seulement d'éviter de se livrer à des activités interdites, mais aussi de faire tout ce qui est en leur pouvoir pour empêcher d'autres parties de mener ces activités à partir de leur territoire. Si les pays devaient assumer de telles responsabilités, le monde se rapprocherait de l'objectif de zéro botnet, ce qui serait dans l'intérêt de toute entité ayant un programme bénin.

Richard N. Haass
Président
Conseil des relations extérieures
Novembre 2018

REMERCIEMENTS

Nous tenons à remercier notre comité consultatif d'avoir partagé ses décennies d'expérience. Bien que nous soyons responsables du contenu et des recommandations de ce rapport, de nombreuses idées et sources ont d'abord été présentées par les membres du comité consultatif. Spamhaus a fourni un accès inestimable à ses données sur les réseaux de zombies, et Justin Haner, de l'université North-eastern, a su les exploiter. Nous tenons également à remercier Matt Carothers et Gabriel Ramsey pour avoir apporté leurs points de vue et leur expérience approfondie.

Jason Healey et Robert K. Knake

INTRODUCTION

Les botnets sont le fléau de l'internet. Les criminels utilisent ces groupes d'ordinateurs infectés par des logiciels malveillants pour propager du spam, envoyer des courriels hameçons, deviner des mots de passe, se faire passer pour des utilisateurs et casser des cryptages. Leur utilisation la plus pernicieuse, cependant, est de mener des attaques par déni de service distribué (DDoS). Les attaques DDoS exploitent la puissance des ordinateurs individuels qui composent le botnet pour envoyer le trafic Internet vers une cible, bloquant ainsi le trafic légitime. Jusqu'à 30 % de l'ensemble du trafic Internet peut être attribué aux botnets, et la plupart de ce trafic provient d'attaques DDoS. [1]

La plupart des attaques DDoS sont de nature criminelle, souvent utilisées par des entreprises pour mettre hors service les sites Web ou les serveurs de leurs concurrents. Cependant, la Chine, la Russie et l'Iran ont tous exploité des réseaux de zombies à des fins géopolitiques. La Chine a mené des attaques DDoS contre le *New York Times*, le Falun Gong et des églises chrétiennes chinoises aux États-Unis. La Russie a mené des attaques DDoS par l'intermédiaire de mandataires contre l'Estonie en 2007, à la suite du retrait par l'Estonie d'une statue commémorant les soldats russes à Tallinn, et en 2008, dans le cadre des opérations militaires russes contre la Géorgie. De 2011 à 2013, l'Iran a mené une série d'attaques soutenues et à grande échelle contre le secteur financier américain en réponse aux mesures que les États-Unis auraient prises contre son programme nucléaire. Ces attaques auraient coûté à certaines banques plus de 20 millions de dollars par mois pour maintenir leurs sites Web à la disposition des clients.

La sagesse conventionnelle veut que les botnets et les problèmes qu'ils créent doivent être "gérés" - que les botnets et les dommages qu'ils causent, bien que constituant un problème, font simplement partie d'un Internet ouvert et mondial. Les interventions visant à réduire les infections par les botnets finiront donc par nuire au dynamisme de l'internet, à l'innovation et à la liberté. Ce point de vue est erroné pour trois raisons.

Premièrement, elle ne prend pas au sérieux le préjudice causé à la société lorsque des gouvernements étrangers s'attaquent directement aux libertés protégées en étouffant la liberté d'expression aux États-Unis. Le fait que le gouvernement américain semble impuissant à faire quoi que ce soit pour les arrêter devrait être très préoccupant. Lorsque le site web du journaliste technologique Brian Krebs a été mis hors ligne par une attaque DDoS, Krebs n'a pu le remettre en ligne que lorsque Google a pris le relais et absorbé l'attaque grâce à son programme Project Shield. Le fait de s'en remettre à une société privée à but lucratif pour protéger la liberté d'expression aux États-Unis, et dans le monde, suscite des inquiétudes.

Deuxièmement, un acteur étatique motivé pourrait facilement exploiter des millions de systèmes pour mettre hors service les réseaux nationaux des pays ou cibler l'infrastructure Internet centrale et mettre hors service l'Internet au niveau mondial. Pour les gouvernements étrangers, il existe certainement des scénarios dans lesquels ils pourraient juger que de telles actions sont à leur avantage.

Enfin, si les préjudices économiques peuvent être gérables aujourd'hui, ils ne le seront probablement plus demain. La cybercriminalité coûte aujourd'hui à l'économie mondiale 600 milliards de dollars par an, dont une grande partie est liée aux réseaux de zombies, et ces pertes ne peuvent qu'augmenter. 3 L'internet des objets (IoT) entraîne une croissance massive du nombre d'appareils connectés à l'internet. Souvent, ces appareils ne sont pas conçus dans une optique de sécurité et sont rarement mis à jour une fois installés, ce qui entraîne des vulnérabilités connues qui peuvent être exploitées par des adversaires mais qui sont peu susceptibles d'être corrigées. Ils sont donc plus susceptibles d'être vulnérables à une prise de contrôle dans le cadre d'un botnet, et l'infection a moins de chances d'être découverte et corrigée. En 2016, le botnet Mirai a mis hors ligne le fournisseur de services de noms de domaine Dyn, ainsi que nombre de ses clients, dont Airbnb, Amazon, GitHub, HBO, Netflix, PayPal et Twitter. Les criminels ont mené l'attaque avec seulement une fraction des bots qu'ils avaient sous leur contrôle.

L'exploitation d'un pourcentage même minime d'appareils IoT vulnérables donnerait à un acteur malveillant la possibilité d'inonder Internet d'un trafic susceptible de perturber les fonctions essentielles. À mesure que les trois milliards de personnes restantes qui ne sont pas encore connectées à Internet se connectent, les taux d'infection des appareils IoT de ces utilisateurs sont susceptibles d'être élevés. Environ seize milliards d'appareils sont connectés à l'internet aujourd'hui, et tant ce nombre que celui des appareils vulnérables et infectés devraient doubler au cours des cinq prochaines années. Même si seule une infime partie de ces appareils est infectée par des réseaux de zombies, les acteurs malveillants disposeront d'un énorme potentiel de perturbation. Il est donc nécessaire de se fixer un objectif ambitieux : zéro botnet.

Pour atteindre cet objectif, les experts en sécurité de l'information doivent d'abord mieux mesurer l'activité actuelle des botnets et fixer des objectifs progressifs de réduction. Les nations et les institutions internationales devraient ensuite

s'efforcer d'établir le principe selon lequel les États sont responsables des dommages que les botnets basés à l'intérieur de leurs frontières causent aux autres. Lorsque les gouvernements ne peuvent ou ne veulent pas être responsables, d'autres États peuvent être fondés à prendre des mesures, dans ou hors du cyberdomaine, pour contrecarrer les effets transfrontaliers. De même, au niveau des fournisseurs d'accès à Internet (FAI), les bons gestionnaires des espaces en ligne doivent tenir les autres FAI responsables du mauvais trafic qui quitte leurs réseaux. Les fabricants d'appareils susceptibles de faire partie de réseaux de zombies doivent être incités à sécuriser leurs appareils, et les revendeurs de ces appareils doivent utiliser leur influence pour les tenir responsables. Les fournisseurs d'hébergement, les bureaux d'enregistrement des noms de domaine et les autres composants de l'écosystème Internet utilisés par les réseaux de zombies doivent être incités à se surveiller et à empêcher que leurs services ne soient utilisés à des fins criminelles. Enfin, lorsque ces mesures ne parviennent pas à enrayer la croissance des réseaux de zombies, un effort international continu est nécessaire pour les démanteler.

LA PUISSANCE DE ZÉRO

Le zéro est un concept puissant souvent utilisé comme un outil pour galvaniser l'action politique. Fixer un objectif de zéro pour les résultats indésirables signifie que toute occurrence est inacceptable. Au fur et à mesure que des progrès sont réalisés, les événements deviennent des exceptions qui déclenchent des réponses énergiques pour comprendre ce qui n'a pas fonctionné et empêcher que les mêmes schémas ne se reproduisent.

Dans le secteur de l'aviation, aucun passager d'une compagnie aérienne commerciale immatriculée aux États-Unis n'avait été tué à la suite d'un crash ou d'un accident depuis plus de neuf ans, jusqu'au récent décès d'un passager du vol 1380 de Southwest en avril 2018. Cet incident a déclenché un examen approfondi de la sécurité des moteurs et des protocoles par lesquels la sécurité des moteurs est confirmée. Pour le public volant, les régulateurs, les actionnaires des compagnies aériennes et les opérateurs, zéro est le seul nombre acceptable d'incidents de sécurité.

Les décideurs politiques adoptent une approche similaire dans des domaines tels que les accidents de la route et la politique de santé publique. Les maires de Los Angeles, de New York, de Washington DC et de trente autres villes mettent en œuvre des programmes dits "Vision zéro" pour les accidents de la route et les décès de piétons. Ces efforts s'inspirent d'un programme lancé en Suède il y a vingt ans. Dans le domaine de la santé publique, de nombreux efforts de vaccination visent à atteindre l'objectif de zéro infection dans le monde. Les efforts de vaccination contre la variole ont permis d'atteindre l'objectif de zéro nouvelle infection en 1978. Les efforts de lutte contre la poliomyélite ont abouti à seulement vingt-deux nouvelles infections dans le monde en 2017.

Bien sûr, l'élimination complète des botnets est probablement un objectif impossible à atteindre. De même, il est peu probable que le monde parvienne un jour à éliminer les armes nucléaires (l'objectif du mouvement "Global Zero" adopté par le président Barack Obama en 2009), tout comme il est peu probable que la Suède, la ville de New York et la ville de Washington, DC, n'enregistrent aucun décès dû à la circulation (l'objectif de la "Vision zéro"). Mais parfois, un objectif extrême est nécessaire pour orienter les politiques. Comme le montrent les données, des taux d'infection extrêmement faibles (moins de 0,1 pour cent

aux États-Unis aujourd'hui) peuvent encore permettre de constituer de puissants botnets. Par conséquent, les taux d'infection doivent être ramenés bien en dessous de ce chiffre pour être effectivement nuls.

MESURER LE ÉTAT ACTUEL D'INFECTIONS PAR BOTNET

Les infections par botnet varient considérablement à travers le monde, avec des taux d'infection extrêmement faibles dans les pays non développés, des taux élevés dans les pays en développement, et des taux d'infection faibles et en progression dans le monde développé. Dans le monde développé, certains pays ont pris des mesures actives pour réduire à presque zéro les infections par botnet. La Finlande, notamment, a mis en place un partenariat actif et volontaire avec ses fournisseurs d'accès à Internet afin d'informer les propriétaires de systèmes infectés et, si nécessaire, de les mettre en quarantaine. La Finlande affiche régulièrement l'un des taux d'infection les plus bas parmi les pays développés. D'autres efforts nationaux ont été moins efficaces. Le Japon a créé son Cyber Clean Center en 2008 pour réduire les taux d'infection mais, selon la plupart des indicateurs, il continue à avoir un problème important de botnet. L'Allemagne a mené un effort pluriannuel pour réduire les infections de botnets domestiques, mais son approche est loin d'être aussi efficace que celle de la Finlande. Les États-Unis, qui n'ont pas d'approche nationale coordonnée ni d'obligation légale, se comparent favorablement à de nombreux autres pays qui ont de telles approches ou obligations. Les données fournies par Spamhaus, une organisation internationale qui suit les activités des réseaux de zombies, placent les États-Unis au quatorzième rang sur la liste des pays qui comptent le plus d'infections par des réseaux de zombies (voir tableau 1).

Tableau 1. PAYS AYANT LE PLUS GRAND NOMBRE D'INFECTIONS PAR BOTNET

Rank (most to least infected)	Country	Average number of bots
1	China	1,976,804
2	India	1,689,265
3	Brazil	606,216
4	Iran	566,353
5	Vietnam	560,720
6	Russia	506,982
7	Thailand	419,979
8	Turkey	412,390
9	Mexico	360,876
10	Indonesia	317,988
11	Pakistan	201,315
12	Philippines	166,177
13	Venezuela	156,718
14	United States	154,719
15	Egypt	148,298
16	Algeria	145,273
17	Japan	142,461
18	Italy	115,546
19	Argentina	113,470
20	Malaysia	101,093

Source : Spamhaus, 2018.

Cependant, par habitant, les réseaux américains sont parmi les plus propres du monde. Parmi les pays de l'Organisation de coopération et de développement économiques (OCDE), les États-Unis ont le huitième réseau le plus propre (voir tableau 2), ce qui peut s'expliquer par des taux plus faibles de logiciels piratés ou non pris en charge et par la prévalence des logiciels antivirus. L'Allemagne arrive en douzième position sur la liste, le Japon en seizième. [4]

Pourtant, à la lumière des dommages passés et potentiels causés par les botnets, même des taux d'infection bien inférieurs à un dixième de 1 % sont trop élevés, compte tenu du nombre important et croissant de systèmes sur Internet. Bien que les États-Unis aient un taux d'infection parmi les plus bas au monde, le pays était également l'un des cinq principaux pays sources d'attaques DDoS à chaque trimestre de 2017 (voir tableau 3). [5] Ainsi, la gestion du problème des botnets nécessite de conduire le nombre absolu d'infections à zéro ou presque.

Tableau 2. CLASSEMENT DES TAUX D'INFECTION PAR BOTNET DANS LES DIFFÉRENTS PAYS DE L'OCDE

Rank (least to most infected)	Country	% of IP addresses infected
1	Denmark	0.0258%
1	Finland	0.0258%
2	Switzerland	0.0353%
3	Netherlands	0.0549%
4	France	0.0574%
5	United Kingdom	0.0583%
6	Canada	0.0608%
7	Belgium	0.0627%
8	United States	0.0629%
9	Estonia	0.0816%
10	New Zealand	0.0830%
11	Sweden	0.0835%
12	Germany	0.1039%
13	Austria	0.1079%
14	Korea	0.1123%
15	Iceland	0.1171%
16	Japan	0.1204%
17	Luxembourg	0.1430%
18	Slovakia	0.1447%
19	Czech Republic	0.1509%

Source : Spamhaus, 2018.

Tableau 3. PRINCIPALES SOURCES DE CONTREFAÇON POUR LES ATTAQUES DE DDoS, 2017

Q4 2017		Q3 2017		Q2 2017		Q1 2017	
Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs
Germany	30% 128,350	Germany	22% 58,746	Egypt	32% 44,198	United States	44% 594,986
China	28% 118,716	United States	14% 38,628	United States	8% 11,113	United Kingdom	13% 177,579
United States	8% 36,441	India	7% 19,722	Turkey	5% 7,049	Germany	7% 87,780
Ecuador	3% 14,685	China	6% 15,323	China	4% 5,711	Canada	5% 60,581
Austria	3% 13,503	Mexico	5% 13,501	India	4% 5,224	Brazil	3% 43,863

Source : McKeay, "État de l'Internet / Sécurité : Q4 2017 Report".

POURQUOI LES BOTNETS PERSISTENT

Malgré des efforts très médiatisés pour lutter contre les botnets, le nombre de ces derniers et de systèmes infectés ne cesse de croître. Les efforts passés ont été décousus et se sont concentrés séparément sur les notifications des FAI aux propriétaires de systèmes infectés ou sur les efforts coordonnés des forces de l'ordre pour arrêter les "botmasters" et perturber l'infrastructure qu'ils utilisent pour contrôler leurs botnets.

La Commission fédérale des communications (FCC) a collaboré avec les principaux FAI dans le cadre du Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications (CSRIC) pour produire le Code de conduite anti-bot en 2012.[6] Ce code est un effort volontaire visant à éduquer les clients sur les botnets, à détecter les activités des botnets, à notifier les clients en cas de suspicion d'infection et à fournir des informations sur la façon de remédier aux infections des botnets. Si de nombreux FAI ont adopté les pratiques préconisées dans le code de conduite, leur efficacité reste incertaine.

En avril 2013, le FBI a annoncé l'opération Clean Slate, dont l'objectif déclaré était de réduire ou d'éliminer les botnets qui menaçaient la sécurité économique des États-Unis et la vie privée de ses citoyens. [7] Bien que le FBI ait connu une série de succès en fermant certains botnets, ces efforts n'ont pas conduit à une réduction mesurable du nombre de botnets, du nombre d'appareils infectés ou des dommages causés par les botnets.

Une approche plus globale, allant au-delà de la répression, de la notification et de la mise en quarantaine par les FAI, est nécessaire pour s'attaquer au problème à partir de vecteurs multiples. Les défis liés à l'élimination des réseaux de zombies relèvent de trois catégories : les technologies existantes et nouvelles, les questions opérationnelles, organisationnelles et de processus, ainsi que la politique et l'économie.

La facilité de l'usurpation d'identité. Les criminels qui mènent des attaques DDoS profitent de toutes les occasions pour brouiller les pistes et rendre difficile l'identification de la source de l'attaque par les intervenants. Étant donné que les attaques DDoS ne nécessitent pas de communication bidirectionnelle et qu'elles se contentent d'inonder la victime de trafic, les botmasters programment souvent leurs logiciels malveillants pour "usurper", ou falsifier, l'adresse de protocole Internet (IP) d'où proviennent les paquets de données - c'est-à-dire faire croire que les données proviennent d'une adresse différente - afin qu'il soit difficile d'identifier les sources de l'attaque. Les États-Unis ont le plus grand nombre de blocs d'adresses IP usurpables, mais ceux-ci ne représentent que 4,8 % de toutes les adresses IP dans les données de l'échantillon. Dans de nombreux pays en développement, 100 % des blocs IP peuvent être usurpés. À la fin des années 1990, les membres de la communauté de la sécurité Internet ont développé un protocole pour résoudre ce problème, appelé Best Common Practice 38. Le protocole demandait aux FAI de mettre en œuvre un "filtrage de sortie", dans lequel tous les paquets prétendant provenir d'adresses IP qui ne leur ont pas été attribuées sont bloqués.

Hébergement à l'épreuve des balles. Les fournisseurs d'hébergement à l'épreuve des balles sont ceux qui hébergent des activités criminelles que les sociétés d'hébergement légitimes ne toléreront pas. Aucun système amélioré de signalement des abus ne changera la façon dont les hébergeurs à l'épreuve des balles opèrent. Ils sont souvent situés dans des pays où l'application de la loi est faible, où le niveau de corruption est élevé et où les relations avec l'Occident sont mauvaises. Offrant souvent des services à bas prix, ces fournisseurs affirment qu'ils ne disposent pas des ressources nécessaires pour contrôler le contenu des utilisateurs ou répondre à chaque signalement d'abus. Étant donné qu'ils hébergent presque toujours des entreprises légitimes attirées par des services à bas prix, leur fermeture pure et simple ou l'arrêt de tout trafic en provenance de ces sites n'est pas une réponse appropriée.

La croissance de l'IdO. Les technologies IoT rendent la gestion du problème des botnets plus difficile. En raison du nombre d'appareils, même un faible taux d'infection peut permettre aux acteurs malveillants d'accéder à un nombre incroyablement élevé d'appareils compromis. De plus, la nature "prête à l'emploi" de ces appareils signifie que les propriétaires sont moins susceptibles d'installer des mises à jour logicielles ou de sécuriser leurs appareils. La croissance prévue des appareils IoT s'explique en grande partie par leur faible coût, ce qui entraîne de mauvaises pratiques de développement et donc des appareils moins sécurisés. En outre,

60 pour cent de toutes les applications Internet contiennent des composants à code source ouvert présentant des vulnérabilités logicielles connues. [9]

L'émergence des crypto-monnaies. Une grande partie de la valeur que les criminels tirent de l'exploitation de botnets et de systèmes d'extorsion DDoS provient de crypto-monnaies telles que le bitcoin et l'ethereum. Les criminels lancent une attaque DDoS et demandent ensuite un paiement en crypto-monnaies pour l'arrêter - généralement bien moins que ce que demanderait une entreprise d'atténuation des DDoS. Les crypto-monnaies permettent aux criminels d'exiger des paiements de rançon qui ne sont pas facilement traçables par le système financier - l'époque des mallettes non marquées contenant des billets de 100 dollars non séquentiels est révolue. Bien que toutes les transactions en bitcoins soient publiquement enregistrées dans la blockchain associée, les personnes associées à ces transactions sont inconnues par conception. Le développement de services de "tumbling" qui combinent des transactions non criminelles en crypto-monnaies avec des transactions criminelles rend difficile pour les forces de l'ordre de cibler les points vulnérables restants dans le système, comme lorsque les criminels cherchent à convertir des monnaies virtuelles en monnaies fiduciaires. Des monnaies plus récentes comme le monero, le zcash et le dash semblent avoir été conçues expressément pour les transactions criminelles. [10]

QUESTIONS OPÉRATIONNELLES, ORGANISATIONNELLES ET DE PROCESSUS

La complexité du démantèlement des botnets. Le démantèlement coordonné des réseaux de zombies par les forces de l'ordre, les fournisseurs d'accès à Internet, les éditeurs de logiciels, les sociétés de sécurité et les universités peut réduire considérablement le nombre de machines infectées dans le monde et les maux qui y sont associés. Pourtant, il s'est avéré difficile de maintenir des efforts soutenus dans le temps. Le démantèlement des botnets n'est pas un travail à plein temps. Sur une période de dix ans, vingt-trois démantèlements partiels ou totaux de botnets ont eu lieu (voir tableau 4). Les démantèlements se font par à-coups : quatre démantèlements de botnet ont eu lieu en 2012, puis trois en 2013, un en 2014, trois en 2015, un en 2016 et deux en 201711. Les démantèlements les plus efficaces font appel à un large éventail de parties qui agissent de concert pour attaquer le botnet sous plusieurs angles : des ordonnances judiciaires sont utilisées pour saisir des serveurs et des domaines Web dans le monde entier, les forces de l'ordre arrêtent des membres connus et accessibles de l'organisation criminelle à l'origine du botnet, les fournisseurs d'accès à Internet drainent le trafic, les fournisseurs de logiciels diffusent des correctifs et, sous l'autorité des forces de l'ordre, des experts techniques tentent de prendre le contrôle ou de supprimer le logiciel malveillant sous-jacent en une seule fois.

La direction de ces efforts a été diffuse. Aucune organisation n'est responsable de la coordination des démantèlements. À lui seul, Microsoft a mené plus d'une douzaine d'actions. Des entreprises de cybersécurité comme Crowd-Strike, FireEye, Lastline, Symantec et TrendMicro ont mené d'autres actions. Le FBI, le ministère américain de la justice et le Secret Ser-vice ont également coordonné leurs efforts. Des tiers formels et informels

Tableau 4. PRINCIPAUX DÉMANTÈLEMENTS DE BOTNETS AU COURS DE LA DERNIÈRE DÉCENNIE

Date	Botnet
November 2008	McColo
November 2009	Mega D
December 2009	Mariposa
February 2010	Waledac
September 2010	Pushdo
November 2010	DNSCHanger
March 2011	Rustock
April 2011	Coreflood
November 2011	Rove Digital
March 2012	Zeus Botnet
July 2012	Grum
September 2012	Nitol
December 2012	Butterfly Bot
February 2013	Bamital
June 2013	Citadel
December 2013	Sirefef/ZeroAccess
June 2014	Gameover Zeus
February 2015	Ramnit
April 2015	Simda
December 2015	Dorkbot
December 2016	Avalanche
April 2017	Kelihos Botnet
December 2017	Gamarue/Andromeda

Source : Recherche des auteurs.

Des organisations telles que le Centre européen de lutte contre la cybercriminalité d'Europol, l'Internet Systems Consortium, le Malware Anti-Abuse Working Group, le Mariposa Working Group, la National Cyber Forensics Training Alliance et Spamhaus ont coordonné des opérations de démantèlement. Ces efforts font appel à un nombre limité de techniciens et mettent à rude épreuve les ressources des organisations qui y participent. En bref, le démantèlement des botnets n'est pas un travail de tous les jours.

Les processus de signalement des abus sont défaillants. Les processus de signalement des attaques DDoS, des autres activités malveillantes et des systèmes vulnérables sont défaillants. Les fournisseurs d'hébergement et les FAI ignorent souvent les rapports d'abus ou ne les traitent que lentement. Le signalement efficace des abus repose souvent sur un réseau informel - et pas toujours efficace - de personnes travaillant dans des entreprises réparties dans le monde entier. Les efforts d'une victime de Mirai illustrent bien ce problème : Alors que l'attaque contre ProxyPipe, un fournisseur de services d'atténuation des attaques DDoS pour les serveurs Minecraft, se poursuivait, Robert Coelho, vice-président de la société, n'a pas pu maintenir l'accès aux serveurs de ses clients. Il s'est résolu à déposer des plaintes pour abus auprès des fournisseurs d'hébergement et des FAI qui soutenaient le serveur de commande et de contrôle du botmaster qui dirigeait l'attaque. M. Coelho a conclu que le serveur de contrôle était géré par un fournisseur d'hébergement à l'épreuve des balles bien connu en Ukraine. Ce fournisseur, BlazingFast, n'a pas répondu aux rapports d'abus de Coelho, pas plus que le service d'atténuation des DDoS de BlazingFast, Voxility. M. Coelho a ensuite contacté quatre FAI en amont qui n'ont fourni aucune assistance avant qu'un cinquième FAI, le finlandais TeliaSonera, ne réponde à sa demande et ne coupe la connectivité du serveur de contrôle sur son réseau. "L'action de Telia a réduit la taille des attaques lancées par le botnet à 80 Gbps", un niveau de trafic que ProxyPipe pouvait gérer. [12]

Pourtant, un système plus rapide et automatisé de signalement des abus pourrait créer ses propres problèmes. Même pour les entreprises qui ont l'intention d'être de bons gestionnaires du cyberespace, un tel système pourrait donner lieu à l'équivalent du "swat-ting" en ligne, où les systèmes de signalement des abus sont utilisés abusivement pour mettre fin à une activité légitime. [13] Certaines entreprises ont développé des réseaux vérifiés entre des parties de confiance pour automatiser ce processus. Les hébergeurs et les fournisseurs d'accès à Internet qui ne sont pas réactifs ne subissent que peu de répercussions. En l'absence de tout recours de tiers, les victimes d'activités malveillantes doivent se débrouiller seules pour travailler avec des sociétés souvent indifférentes et hostiles.

Mécanismes insuffisants pour la coopération internationale. Le rôle des équipes nationales d'intervention en cas d'urgence informatique (CERT) est mal défini au sein de l'écosystème Internet : seules certaines d'entre elles ont la capacité de fournir une assistance aux gouvernements et aux entreprises étrangers. Dans les pays disposant de fournisseurs de télécommunications nationaux et de lois favorisant la notification et la mise en quarantaine, les CERT nationales jouent un rôle utile. Aux États-Unis, la Computer Emergency Readiness Team n'a qu'une capacité limitée d'assistance en cas d'attaque DDoS.

La difficulté d'identifier les propriétaires des systèmes infectés. Lorsque les défenseurs du réseau sont en mesure de remonter la piste des systèmes infectés ou vulnérables jusqu'à l'auteur de l'infection, il est difficile d'identifier le propriétaire du système.

En raison de la complexité des réseaux sur lesquels ils se trouvent, ils ne peuvent souvent pas aller plus loin que le FAI qui leur fournit le service. Aux États-Unis, les FAI ne sont pas autorisés à partager les informations relatives à leurs clients avec des tiers, conformément à la loi sur la confidentialité des communications électroniques (Electronic Communications Privacy Act, ECPA). Cette interdiction s'étend aux agences gouvernementales, sauf si une assignation à comparaître est émise. Au niveau international, l'identification des propriétaires de systèmes est également entravée par des lois locales telles que le règlement mondial sur la protection des données (GDPR) de l'Union européenne. Entrant maintenant en vigueur, le GDPR considère les adresses IP comme des données personnelles devant être protégées. Ainsi, les efforts visant à notifier le propriétaire du système et à encourager les mesures correctives doivent s'appuyer sur le FAI (à moins que le système ne se trouve sur le réseau d'une grande entreprise disposant de son propre espace d'adressage). De nombreux FAI ont été réticents à informer activement leurs clients des infections en raison des coûts et des problèmes de confidentialité.

QUESTIONS POLITIQUES ET ÉCONOMIQUES

Des incitations économiques qui favorisent l'attaquant. Selon l'expert en cybersécurité Jim Lewis, "un botnet qui ne coûte que 60 dollars par jour peut infliger jusqu'à 720 000 dollars de dommages aux organisations victimes, et les pirates qui contrôlent les botnets bénéficient d'une marge bénéficiaire de plus de 70 % lorsqu'ils louent leurs services à d'autres criminels".[14] Il convient d'identifier et de mettre en œuvre des interventions qui augmenteront le coût de ces attaques et réduiront les profits.

Incitations perverses pour l'atténuation des DDoS. Les entreprises qui fournissent des services d'atténuation des attaques DDoS ne souhaitent pas que les attaques cessent, mais qu'elles se poursuivent à des niveaux gérables. Comme l'a dit M. Coelho, vice-président de ProxyPipe, dans un échange de texte avec le botmaster à l'origine de Mirai, "Nous voulions simplement que les attaques deviennent plus petites" - il n'a pas dit qu'il voulait que les attaques cessent. [15]

L'atténuation des attaques DDoS est un secteur en pleine expansion. Des sociétés comme Akamai et Cloudflare proposent des services forfaitaires qui agissent comme une police d'assurance et alignent correctement les incitations afin que les fournisseurs de services d'atténuation aient intérêt à nettoyer l'écosystème. Les boucles de rétroaction entre les victimes de DDoS et les sources des botnets pourraient finir par réduire à zéro le nombre de ces derniers, mais il s'agit encore d'un travail en cours.

Coûts indirects des botnets. Les botnets causent généralement des dommages non pas aux systèmes qu'ils infectent, mais à des tiers. L'utilisation par les botnets des ressources informatiques et

La bande passante ne semble pas être une préoccupation importante pour les propriétaires et les opérateurs de la plupart des systèmes infectés. Certains individus ne s'inquiètent pas du vol de leurs informations personnelles et remarquent à peine l'impact sur les performances de leur ordinateur lorsqu'ils exploitent des crypto-monnaies pour d'autres. Certaines entreprises ferment les yeux sur le vol de leur propriété intellectuelle. Pourtant, bien que les botmasters extraient toute la valeur qu'ils peuvent des systèmes infectés, le véritable intérêt de maintenir un botnet est de l'utiliser pour cibler des tiers.

Les préoccupations relatives à la vie privée et le manque d'incitations économiques à l'action des FAI. Dans le passé, la neutralité du réseau a contribué à l'approche non interventionniste des FAI, ces derniers soutenant qu'en tant que transporteurs publics, ils sont obligés de transmettre le trafic à moins qu'il ne cause un préjudice direct à leurs propres systèmes, et non aux autres FAI ou aux utilisateurs finaux plus en aval. Avec la fin des règles de neutralité du réseau par la FCC, la crainte des FAI de violer la neutralité du réseau en bloquant l'activité des botnets a été prise en compte. En outre, les modifications apportées à l'ECPA par la loi sur la cybersécurité de 2015 accordent aux FAI de larges exemptions de responsabilité pour le blocage du trafic malveillant. Le problème plus général reste que de nombreux FAI ne considèrent pas la lutte contre les botnets comme faisant partie de leur modèle économique ; filtrer le trafic DDoS pour les clients ou fournir une bande passante supplémentaire aux victimes est une bonne affaire. Il est peu probable que les FAI acceptent de bloquer l'accès de leurs clients à Internet, du moins sur le marché américain. Une approche plus prometteuse, que AT&T et CenturyLink sont en train de tester, n'essaie pas de nettoyer les infections mais perturbe leur commande et leur contrôle sur le réseau de sorte que le botmaster ne puisse pas diriger les activités des bots, ce qui rend la menace qu'ils représentent inerte.

RECOMMANDATIONS

Dans le décret 13800, le président américain Donald J. Trump a demandé au ministère du Commerce et au ministère de la Sécurité intérieure de collaborer avec le secteur privé pour trouver des moyens de "réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées (par exemple, les botnets)". Le rapport qui en a résulté, intitulé "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats", publié en mai 2018, est une ressource inestimable pour définir le problème, et nombre de ses recommandations inspirent celles qui suivent. [16] Ce qui manque à cet effort qui a été informé par des dizaines d'organisations ayant un intérêt à réduire la menace des botnets est un objectif clair et mesurable. L'établissement d'un objectif mondial de zéro botnet est la première étape de la lutte contre ce problème.

À partir de là, il convient de chercher à obtenir des engagements nationaux pour parvenir à zéro botnet au sein des réseaux nationaux. Il est essentiel de fixer des objectifs intermédiaires et de mettre en place des systèmes permettant de mesurer les progrès accomplis dans la réalisation de ces objectifs. Ces objectifs pourraient être abordés principalement dans les limites nationales. Les objectifs devraient être fixés sur des périodes spécifiques en fonction du nombre d'appareils connectés dans un pays. Les pays développés devraient avoir des exigences plus strictes et des délais plus courts, tandis que les pays en développement devraient avoir des exigences initiales moins contraignantes.

FIXER UN OBJECTIF GLOBAL ET MESURER LES ÉTATS PAR RAPPORT À CET OBJECTIF

Pour parvenir à zéro botnet, il est nécessaire de fixer des objectifs intermédiaires et de mesurer les progrès réalisés par rapport à ces objectifs. Les objectifs en matière de botnets doivent être approuvés par les dirigeants politiques, ainsi que par la société civile et les dirigeants des entreprises mondiales. Fixer ces objectifs et obtenir l'accord des principaux partenaires est la première étape la plus importante pour créer un mouvement.

Ces objectifs devraient commencer par un accord visant à atteindre l'objectif de zéro botnet par les principaux FAI, ce qui pourrait être aussi simple qu'une poignée de main sur le podium par les présidents des États-Unis et de la Chine. Une communauté plus large peut ensuite élaborer des mesures, des normes et une mise en œuvre plus concrètes. Les personnes concernées pourront rectifier le tir au fur et à mesure qu'elles constateront les succès et les échecs dans la réalisation de ces objectifs, et tirer les leçons des pays et des entreprises qui ont réussi. Il sera difficile de se mettre d'accord sur les paramètres et de mesurer le succès par rapport à ceux-ci. Spamhaus et d'autres organisations suivent depuis des années les botnets et les taux d'infection par pays. [17] De même, la Cyber Green Initiative s'efforce de suivre scientifiquement les réseaux de zombies. [18] Ces groupes peuvent mesurer la progression vers l'élimination des botnets.

ÉTABLIR LE PRINCIPE DE LA RESPONSABILITÉ DE L'ÉTAT POUR LES PRÉJUDICES CAUSÉS PAR LES RÉSEAUX DE ZOMBIES

Alors que les défis du XXIe siècle tels que le terrorisme, la prolifération nucléaire et la pollution sont devenus des enjeux de sécurité nationale, les notions de souveraineté nationale ont également changé. Au lieu d'être un droit absolu des États, la souveraineté s'accompagne désormais d'une responsabilité souveraine envers les citoyens des États et d'obligations souveraines envers les autres États. Les botnets causent du tort aux individus, aux entreprises et aux États, mais ce n'est que lorsque le tort est transfrontalier qu'il devient un problème de politique internationale, dans lequel l'État qui cause le tort a une obligation souveraine envers les autres États de le résoudre20. [20] Selon ce raisonnement, les États pourraient choisir d'autoriser des taux élevés d'infections par les botnets tant que le préjudice qu'ils causent est limité à leur propre territoire. Ils devraient cependant être tenus responsables par le système international.

pour tout préjudice causé aux autres États s'ils ne travaillent pas de manière proactive et coopérative pour y répondre.

ENCOURAGER LA COOPÉRATION ET L'ACTION INTERNATIONALES

Les États devraient être incités à la fois par la carotte et le bâton à prendre des mesures pour réduire la prévalence des botnets sur leurs réseaux nationaux. Il peut être utile de situer les États sur une échelle de responsabilité. Tout d'abord, les États qui utilisent activement les botnets pour contraindre d'autres États devraient être spécifiquement visés par les institutions internationales. Viennent ensuite les États qui abritent les entreprises criminelles à l'origine des opérations des botnets. Les États qui sont tout simplement incapables de contrôler ce qui se passe à l'intérieur de leurs frontières se situeraient au bas de l'échelle.

Dans ce cadre, des mesures incitatives pourraient être utilisées pour aider ceux qui se situent en bas de l'échelle à réduire leurs activités. Des sanctions telles que l'humiliation, la limitation des investissements et des sanctions pourraient cibler les États qui utilisent activement les réseaux de zombies ou qui hébergent ceux qui le font. Les pays développés devront aider les pays en développement à réduire l'activité des réseaux de zombies, notamment en les aidant à résoudre des problèmes de longue date dans l'écosystème, tels que la prévalence des logiciels piratés. Le gouvernement des États-Unis, les nations partageant les mêmes idées et les entreprises intéressées par la réduction de l'activité des botnets devraient financer un rapport annuel rédigé par une organisation tierce indépendante afin de suivre les succès obtenus par les États dans la réduction des botnets.

Une fois les obligations internationales établies, l'absence de réponse pourrait constituer un motif raisonnable pour les nations de prendre des mesures limitées pour prévenir, de la manière la plus étroite possible, le préjudice sans en causer davantage en retour. Par exemple, si un pays ne parvient pas à mettre en place des mécanismes permettant de recevoir et de traiter les plaintes pour abus en temps utile, un gouvernement étranger pourrait autoriser le démantèlement d'un serveur de commandement et de contrôle. De telles actions ne doivent être entreprises qu'en dernier recours, car les États pourraient les percevoir comme une violation de la souveraineté et une action hostile, aussi limitée soit-elle.

CRÉER DES VES INCENTI POUR LES ISP AFIN DE NETTOYER LES RÉSEAUX

Certains fournisseurs d'accès détectent lorsqu'un client est infecté par un logiciel malveillant, en informent la personne par texto, puis la dirigent vers un "jardin clos" où elle ne peut accéder à l'internet en général jusqu'à ce que son ordinateur soit nettoyé, parfois avec l'aide du fournisseur d'accès. Il est important de noter que ce n'est pas la personne qui est exclue de l'internet, car cela limiterait la liberté d'expression, mais plutôt les personnes suivantes

l'appareil qui cause du tort à autrui. Pourtant, bien que cette pratique existe depuis plus de dix ans, elle n'est pas considérée comme une responsabilité commune des fournisseurs d'accès à Internet.

Bien que les FAI se méfient de la réglementation dans ce domaine, les FAI, en tant que communauté, pourraient s'autosurveiller. Les FAI pourraient convenir d'une norme selon laquelle, par exemple, un FAI ayant cent millions d'appareils ou un pétaoctet de trafic par mois pourrait être autorisé à avoir un certain pourcentage d'appareils infectés, ou d'émissions. S'il en a plus, il devra payer une taxe ou acheter des crédits auprès d'un réseau plus propre jusqu'à ce qu'il parvienne à ramener le nombre d'appareils infectés en dessous du seuil.

DÉFINIR DES NORMES POUR EMPÊCHER QUE LES DISPOSITIFS NE SOIENT FACILEMENT COMPROMIS

Comme le conclut le rapport au président, "des bases de capacités de sécurité basées sur les performances - qui identifient des suites de normes, de spécifications et de mécanismes de sécurité volontaires représentant la combinaison des meilleures pratiques de sécurité du cycle de vie pour un environnement de menace particulier - sont nécessaires pour accélérer le développement et le déploiement de dispositifs et de systèmes IoT moins vulnérables à la compromission tout au long de leur cycle de vie."[21] Ce que le rapport ne fait pas, c'est identifier qui devrait élaborer ces normes ; pourtant, le National Institute of Standards and Technology (NIST) a déjà effectué une grande partie du travail préliminaire pour produire de telles normes et a d'excellents antécédents de collaboration avec l'industrie. Le président ou le secrétaire d'État à la communication devrait demander au NIST d'établir rapidement des normes pour la sécurité des dispositifs IoT. Ces normes devraient inclure les éléments suivants.

- Éliminer les vulnérabilités connues au moment de la production. Les composants open-source doivent être les versions les plus récentes, et les fabricants d'appareils doivent rechercher les vulnérabilités dans le code qu'ils écrivent.
- Suivre les meilleures pratiques pour le renforcement des dispositifs. Les normes devraient également exiger des fabricants qu'ils mettent en place des mesures qui rendent plus difficile la compromission des dispositifs par les adversaires.
- Faire en sorte que les appareils puissent être mis à jour. Les nouvelles technologies opérationnelles sont susceptibles de persister dans l'environnement bien plus longtemps que les technologies de bureau, il est donc crucial que les appareils IoT aient la capacité d'effectuer des mises à jour automatiques et à distance pour corriger les failles de sécurité. Ces mises à jour doivent être automatisées par défaut, les utilisateurs pouvant choisir de tester les mises à jour avant le déploiement.

- Tenir à jour une "nomenclature" des composants logiciels. Au fur et à mesure que des vulnérabilités sont découvertes dans les composants open-source, les propriétaires de la technologie doivent savoir si le logiciel a été construit avec des composants sûrs.

- Fournir des mots de passe uniques pour chaque appareil. Des séries entières de production d'appareils IoT utilisent souvent les mêmes mots de passe par défaut. Modifier cette procédure permettrait d'éliminer la méthode la plus facile que les attaquants utilisent pour prendre le contrôle des appareils. [22]

UTILISER LA PRESSION DU MARCHÉ POUR INCITER LES FABRICANTS DE DISPOSITIFS À RESPECTER LES NORMES

Tout comme les voitures ne peuvent être vendues si elles polluent excessivement, les revendeurs devraient refuser de vendre des produits dont la sécurité n'a pas été démontrée. *Consumer Reports* et d'autres organisations sont en train d'élaborer des cotes de cybersécurité pour les appareils électroniques. [23] Cet effort prendra du temps pour arriver à maturité, mais c'est le bon mécanisme pour réduire la propagation des appareils non sécurisés. S'il est bien fait, il peut mieux aligner les marchés et les incitations à faible coût mais avec un grand effet.

Au-delà de la transparence, les détaillants devraient refuser de vendre des produits qui ne répondent pas aux normes du NIST. Walmart et Amazon sont déjà les "régulateurs" les plus puissants sur une foule de questions : ils spécifient la taille des conteneurs et la forme des emballages qu'ils autorisent. Exiger que les appareils IoT répondent aux normes de sécurité ferait plus que toute autre action pour réduire la prévalence des botnets. La décision de BestBuy de cesser de vendre le logiciel antivirus de Kaspersky Lab après que le gouvernement américain a affirmé qu'il était lié à l'espionnage du Kremlin est un préambule à une telle action.

Des actions similaires sur les appareils non sécurisés pourraient avoir un effet significatif. Les banques, souvent victimes d'attaques DDoS, devraient faire pression sur les fabricants et les revendeurs de dispositifs en refusant de prêter aux entreprises qui ne respectent pas les normes. Les régulateurs des infrastructures critiques devraient interdire les appareils qui ne respectent pas la norme. Bien que, dans le climat politique actuel, il soit peu probable que de nouveaux pouvoirs réglementaires soient accordés, les régulateurs disposant d'une autorité existante devraient fixer cette exigence.

DÉNONCER LES FACILITATEURS DE L'ACTIVITÉ DES BOTNETS

Les campagnes réussies qui emploient le concept de zéro (par exemple, dans les accidents de la route ou les accidents d'avion) mesurent activement les progrès et font connaître

les succès et les échecs dans la tentative d'atteindre cet objectif. Une telle transparence pourrait contribuer à faire pression sur les responsables de l'activité des botnets.

Les cybercriminels se tournent souvent vers les principaux services de cloud computing lorsqu'ils ont besoin de ressources informatiques pour le commandement et le contrôle des attaques DDoS. En 2017, OVH, la cible d'attaques DDoS menées par Mirai, a hébergé le plus grand nombre de serveurs de commande et de contrôle de botnet au monde ; Amazon en a hébergé le deuxième. [24] La plupart de ces serveurs de commande et de contrôle ont été créés en achetant simplement les services de l'entreprise, généralement avec des numéros de carte de crédit volés achetés sur le dark web. Le bureau d'enregistrement américain NameCheap est l'endroit le plus populaire auprès des opérateurs de botnets pour acheter des adresses web pour le commandement et le contrôle (les botnets doivent contacter les domaines web pour recevoir des instructions). Name-Cheap a comptabilisé 11 878 enregistrements pour l'exploitation de botnets en 2017, soit un quart de tous ces enregistrements.

Les forces de l'ordre, les actionnaires et les clients pourraient faire pression sur les vendeurs d'informatique en nuage et de domaines Web privilégiés par les cybercriminels pour qu'ils rendent l'exploitation des botnets beaucoup plus difficile. L'identification et la suppression rapides des comptes impliqués dans cette activité criminelle sont tout à fait dans les capacités techniques de ces entreprises mais, en l'absence de pression, ce n'est pas dans leur intérêt financier. Les États-Unis et leurs alliés devraient également faire pression sur les pays où cette activité se développe, en désignant et en dénonçant les botnets et les services qui leur permettent de fonctionner, en imposant des sanctions et en engageant des poursuites pénales à leur encontre.

Si les fournisseurs de services légitimes se surveillent eux-mêmes et obligent ainsi les groupes criminels à utiliser des fournisseurs qui ferment sciemment les yeux, il sera possible d'isoler et de punir ces groupes. Les fournisseurs d'accès à Internet ont, par le passé, bloqué l'accès à de grandes parties de l'Internet à de tels fournisseurs. Toutefois, il ne sera possible de prendre ces mesures à plus grande échelle que lorsque ces groupes se distingueront davantage du niveau élevé actuel d'activités malveillantes. Les FAI expérimentent déjà des moyens mécanisés pour éliminer le mauvais trafic.

METTRE EN PLACE UNE ORGANISATION INDÉPENDANTE POUR LE DÉMANTÈLEMENT DES BOTNETS

Même lorsque les takedowns donnent des résultats incroyables, le succès est généralement le résultat d'un niveau de travail exceptionnel. Cette situation devrait être modifiée de manière à ce que les démantèlements puissent se produire à grande échelle, les avantages l'emportant sur les coûts. Comme l'explique un rédacteur dans un blog de TechTarget, "si nous déterminons qu'un botnet envoie des millions de messages par jour - les serveurs de commande sont en Russie, une partie de l'infrastructure est en Espagne, et les bots

sont en Amérique du Nord - il doit y avoir un moyen pour tous ces groupes de coopérer en temps réel, ou très rapidement. Car lorsque vous détruisez un botnet, si vous ne détruisez pas toute la structure en même temps, il est très facile pour ces personnes de prendre le contrôle et de rediriger tout le trafic ailleurs. "[25]

Le démantèlement d'un botnet implique un travail technique de haut niveau et de longue haleine, et n'est pas un travail à plein temps. Mais elles devraient l'être. Une possibilité serait de créer des organisations de collaboration en cas de cyberincident (CICO). [26] L'un de ces groupes pourrait se concentrer sur chaque grand type d'incident, comme la lutte contre les DDoS ou la lutte contre les logiciels malveillants. Le CICO de lutte contre les réseaux de robots serait "mondial et dirigé par le secteur privé, avec des membres comprenant les organisations mondiales qui ont joué le plus grand rôle dans les démantèlements, comme Microsoft, FireEye et le ministère de la Justice". Ce groupe travaillerait avec les CICO connexes contre les logiciels malveillants et les attaques DDoS, car ils sont souvent liés. Ces groupes "ne peuvent pas simplement être une nouvelle organisation avec des frais généraux supplémentaires. L'objectif d'un CICO devrait plutôt être de rationaliser le processus de réponse actuel pour un type d'incident, de fournir un cadre pour faciliter ce travail ou de l'étendre "[27].

Une organisation relativement petite, financée à hauteur de 10 millions de dollars par an sur une période de cinq ans, serait probablement capable de procéder à plusieurs démantèlements par an. Cette organisation pourrait également mesurer les botnets au niveau mondial et fournir une assistance technique aux pays et aux entreprises qui s'efforcent de réduire leur taux d'infection. Le financement d'une telle organisation pourrait être un défi, mais compte tenu des coûts engendrés par les attaques DDoS, le soutien d'une organisation qui réduit la menace serait dans l'intérêt du secteur financier, du secteur des télécommunications, des fournisseurs d'informatique en nuage et des agences gouvernementales.

Ces groupes devraient être internationaux dès leur naissance, et non des excroissances des bureaucraties nationales de la cybersécurité. Les CERT nationales devraient être impliquées, mais l'agilité et la facilité de coordination transfrontalière requises seront probablement trop difficiles à réaliser directement par les gouvernements.

CONCLUSION

La menace que représentent les réseaux de zombies pour la santé de l'internet et l'économie numérique moderne qui en dépend ne cesse de croître. Des milliards de nouveaux appareils devant rejoindre l'internet au cours de la prochaine décennie, il est temps de mettre en place un régime international qui permette d'empêcher les appareils vulnérables d'accéder à l'internet, d'atténuer les effets des appareils infectés et de répondre aux problèmes causés par les appareils infectés. En l'absence d'efforts soutenus et organisés pour lutter contre ce problème, les réseaux de zombies et les acteurs malveillants qui les contrôlent prendront une part toujours plus grande de la valeur créée par l'internet et les systèmes qui y sont connectés.

Zéro botnet est un cri de ralliement efficace pour motiver la coalition disparate de fabricants de technologies, de fournisseurs d'accès à Internet, de consommateurs, d'entreprises de cybersécurité, d'organisations à but non lucratif et d'organismes chargés de l'application de la loi, qui est nécessaire pour réduire les infections par botnet à des niveaux tels qu'elles ne constituent pas une menace pour le fonctionnement continu d'Internet ou des organisations qui y opèrent. Si elle est correctement motivée, une telle coalition pourrait, au fil du temps, faire baisser les taux d'infection des botnets, augmenter les coûts d'exploitation des acteurs malveillants et les priver de toute valeur ajoutée.

ENDNOTES

1. Joy Ma et Tim Matthews, " The Underground Bot Economy : How Bots Impact the Global Economy ", Imperva Incapsula, 5 juillet 2016, http://incapsula.com/blog/how-bots-impact-global-economy.html.
2. " Project Shield ", Google, consulté le 21 mai 2018, http://projectshield.withgoogle. .com/public.
3. James Lewis, " Economic Impact of Cybercrime-No Slowing Down ", Center for Strategic and International Studies et McAfee, février 2018, http://mcafee.com /enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf.
4. Les données des tableaux 1 et 2 ont été fournies par Spamhaus pour 2018 ; l'analyse des données a été réalisée par Justin Haner, Northeastern University.
5. Martin McKeay, éd. " État de l'Internet / Sécurité : Q4 2017 Report ", Akamai, http://akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state - of-the-internet-security-report.pdf.
6. *Rapport final : U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)*, Communications Security, Reliability and Interoperability Council (Federal Communications Commission : Washington, DC, 2012), http://m3aawg.org/system /files/20120322-wg7-final-report-for-csric-iii_5.pdf.
7. *Taking Down Botnets*, 113e Congrès. (2014) (déclaration de Joseph Demarest, directeur adjoint de la division Cyber, FBI), http://fbi.gov/news/testimony/taking-down -botnets.
8. Spoofer, " Country Stats for Last Year of Data ", Center for Applied Internet Data Analysis, dernière modification le 8 juin 2018, http://spoofer.caida.org/country_stats.php.
9. Black Duck Software, "2017 Open Source Security and Risk Analysis", http:// blackducksoftware.com/sites/default/files/images/Downloads/Reports/USA /OSSRA17_Rpt_UL.pdf.
10. Kieran Corcoran, " Law Enforcement Has a Massive Problem With These 3 Cryptocurrencies ", *Business Insider*, 27 février 2018, http://businessinsider.com /law-enforcement-problems-with-monero-zcash-dash-cryptocurrencies-2018-2.
11. Recherche des auteurs.

12. Brian Krebs, " Who Is Anna-Senpai, the Mirai Worm Author ", *Krebs on Security* (blog), 17 janvier 2018, http://krebsonsecurity.com/2017/01/who-is-anna-senpai - the-mirai-worm-author.
13. Urban Dictionary, s.v. "Swatting", par Droct, 27 août 2014, http://urbandictionary. .com/define.php?term=Swatting.
14. Lewis, "Impact économique de la cybercriminalité".
15. Krebs, "Qui est Anna-Senpai".
16. Département du commerce des États-Unis, Département de la sécurité intérieure des États-Unis, " A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats ", 22 mai 2018, http://commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800 _botnet_report_-_finalv2.pdf.
17. CBL (Composite Blocking List), " CBL Breakdown by Country, Highest by Count ", Spamhaus, consulté le 24 avril 2018, http://abuseat.org/public/country.html.
18. CyberGreen Institute (site web), consulté le 21 mai 2018, http://cybergreen.net.
19. Voir Richard Haass, *A World in Disarray : La politique étrangère américaine et la crise de la Old Order* (New York : Penguin Press, 2017).
20. Jason Healey et Hannah Pitts soulignent que cette tension entre la souveraineté de l'État et l'obligation internationale a été abordée dans le droit international de l'environnement "par l'articulation de la responsabilité limitée de l'État pour certains actes qui ont leur origine sur le territoire d'un État et qui causent des dommages à un autre État ou à ses citoyens". Jason Healey et Hannah Pitts, "Applying International Environmental Legal Norms to Cyber Statecraft," (en anglais)
I/S : A Journal of Law and Policy for the Information Society 8, no 2 (2012).
Le principe de l'obligation souveraine est représenté en droit de l'environnement par des affaires telles que l'affaire Trail Smelter, dans laquelle un différend transfrontalier entre les États-Unis et le Canada concernant la pollution a contribué à établir le principe selon lequel les États ont l'obligation, en vertu du droit international, de prévenir les dommages à leurs voisins. Voir Catherine Prunella, "An International Environmental Law Case Study : The Trail Smelter Arbitration ", *International Pollution Issues*, décembre 2014, http://intlpollution.commons.gc.cuny.edu /an-international-environmental-law-case-study-the-trail-smelter-arbitration.

21. Département du commerce des États-Unis, Département de la sécurité intérieure des États-Unis, "A Report to the President".

22. Ces recommandations s'inspirent des travaux de I Am the Cavalry, une organisation à but non lucratif qui se consacre à l'amélioration de la sécurité des dispositifs IoT. Voir http://iamthecavalry.org ; pour

    Pour une discussion plus complète, voir "Renforcer la résilience de l'Internet" : "Action 1.1. À l'aide de processus inclusifs menés par l'industrie, établir des bases de capacités IdO applicables au niveau international et prenant en charge la sécurité du cycle de vie pour les applications domestiques et industrielles, fondées sur des normes internationales volontaires et pilotées par l'industrie."

23. " Consumer Reports lance une norme numérique pour protéger la sécurité et la vie privée des consommateurs sur un marché complexe ", communiqué de presse, *Consumer Reports* Media Room, 6 mars 2017, http://consumerreports.org/media-room/press-releases/2017/03 /consumer_reports_launches_digital_standard_to_safeguard_consumers_security _and_privacy_in_complex_marketplace.

24. Spamhaus Malware Labs, " Spamhaus Botnet Threat Report 2017 ", Spamhaus, 1er janvier 2018, http://spamhaus.org/news/article/772/spamhaus-botnet-threat -report-2017.

25. Kathleen Richards, "Botnet Takedowns : A Dramatic Defense", *Search Security* (blog), TechTarget, mars 2013, https://searchsecurity.techtarget.com/feature/Botnet -takedowns-A-dramatic-defense.

26. Jason Healey, " Innovation sur la collaboration cybernétique : Leverage at Scale ", Conseil atlantique, mai 2018, http://atlanticcouncil.org/images/publications/Innovation-Cyber -WEB.pdf.

27. Ibid.

À PROPOS DES AUTEURS

Jason Healey est chercheur principal à la School for International and Public Affairs de l'université Columbia, spécialisé dans les cyberconflits, la concurrence et la coopération. Auparavant, il était le directeur fondateur de la Cyber Statecraft Initiative au Conseil de l'Atlantique, où il est toujours membre senior. Il a travaillé pour Goldman Sachs, notamment en tant que directeur exécutif à Hong Kong. En tant que directeur de la protection des cyber-infrastructures à la Maison Blanche de 2003 à 2005, il a conseillé le président George W. Bush et coordonné les efforts des États-Unis pour sécuriser le cyberespace et les infrastructures critiques. De 2001 à 2003, il a été vice-président du Financial Services Information Sharing and Anal-ysis Center. M. Healey a commencé sa carrière dans l'armée de l'air américaine, où il a obtenu deux médailles du service méritoire pour ses premiers travaux sur les cyberopérations au quartier général de l'armée de l'air au Pentagone et en tant que membre fondateur de la Joint Task Force-Computer Network Defense, la première unité de cyber-guerre conjointe au monde. Il a été chargé de cours en cyberpolitique à l'université de Georgetown et en études de cybersécurité nationale à la School of Advanced International Studies de l'université Johns Hopkins.

M. Healy est l'éditeur de *A Fierce Domain : Cyber Conflict, 1986 to 2012* et co-auteur de *Cyber Security Policy Guidebook*. Ses articles et essais ont été publiés par des groupes de réflexion, notamment l'Aspen Strat-egy Group, l'Atlantic Council et le National Research Council, ainsi que par des revues universitaires des universités de Brown et Georgetown, entre autres. Il est membre de la Task Force on Cyber Deterrence du Defense Science Board et président de la Cyber Conflict Studies Association. M. Healy est diplômé de l'Académie de l'armée de l'air américaine en sciences politiques, de l'université Johns Hopkins en arts libéraux et de l'université James Madison en sécurité de l'information.

Robert K. Knake est chargé de mission pour la cyberpolitique au Council on Foreign Relations (CFR). Il est également chercheur principal à l'Institut de résilience mondiale de l'université Northeastern. Knake a occupé de 2011 à 2015 le poste de directeur de la politique de cybersécurité au Conseil national de sécurité. À ce titre, il était responsable de l'élaboration de la politique présidentielle en matière de cybersécurité et a construit et géré les processus fédéraux de réponse aux cyberincidents et de gestion des vulnérabilités. Avant de rejoindre le gouvernement, Knake était chargé des affaires internationales au CFR.

Parmi les publications de M. Knake figurent *Cyber War : The Next Threat to National Security and What to Do About It* et le rapport spécial du CFR Council intitulé *Internet Governance in an Age of Cyber Insecurity*. Il a témoigné devant le Congrès sur le partage des informations en matière de cybersécurité et sur le problème de l'attribution dans le cyberespace, et a écrit et donné de nombreuses conférences sur la politique de cybersécurité. M. Knake est titulaire d'un diplôme de premier cycle en histoire et en administration du Connecticut College et d'une maîtrise en politique publique de la Harvard Kennedy School.

COMITÉ CONSULTATIF
Zéro Botnets

Sanjay Parekh
Prototype Prime

Mira Patel
Initiative Chan Zuckerberg

Jonathan Sondik Perelman
Partenaires ICM

Neal A. Pollard
PricewaterhouseCoopers LLP

Brendan P. Shields
Chambre des représentants des États-Unis

Megan Stifel
Silicon Harbor Consultants, LLC

Michael Sulmeyer
L'école Harvard Kennedy
Centre Belfer pour la science
et Affaires internationales

Frederick H. Tsai
salesforce.com, inc.

Ira Winkler
Secure Mentem

Evan D. Wolff
Crowell & Moring LLP

Travail de JD
L'école de l'Université de Columbia
des affaires internationales et publiques

Cover photo: Empty cabinets in the data center of T-Systems, the largest German information technology company, on July 1, 2014, in Biere, Germany.
(Thomas Trutschel/Photothek via Getty Images)

Council on Foreign Relations
www.cfr.org

58 East 68th Street
New York, NY 10065
tel 212.434.9400

1777 F Street, NW
Washington, DC 20006
tel 202.509.8400