Livre blanc technique sur l'industrie

17 juillet 2017

RÉSUMÉ

Le 11 mai 2017, le président Trump a signé le décret 13800, Renforcer la cybersécurité des réseaux fédéraux et des infrastructures critiques, chargeant le ministère du Commerce et le ministère de la Sécurité intérieure de mener un processus ouvert et transparent pour identifier les moyens d'améliorer la résilience de l'écosystème de l'internet et des communications et de réduire les menaces perpétuées par les botnets, notamment les attaques par déni de service distribué. Dans ce livre blanc technique, le secteur des communications décrit le problème des botnets du point de vue des fournisseurs de services Internet (FSI), identifie certains défis et opportunités, puis propose plusieurs recommandations préliminaires ou mesures réalisables que les participants de l'écosystème, y compris les FSI, devraient envisager pour atténuer les menaces associées aux botnets et aux attaques automatisées.

Conseil de coordination du secteur des communications

Table des matières

Résumé exécutif

Un bot est un code utilisé pour prendre le contrôle d'un ordinateur ou d'un appareil afin de former un réseau de machines infectées, appelé botnet. De nombreux botnets sont des réseaux auto-répandus et auto-organisés de machines compromises qui peuvent être utilisés pour réaliser des activités malveillantes de manière coordonnée via des canaux de commande et de contrôle (C&C). Si les bots ne sont pas nouveaux, le déploiement croissant des dispositifs de l'Internet des objets (IoT) amplifie leur capacité à créer une menace de sécurité mondiale à grande échelle.

Conscient de cette menace mondiale croissante, le 11 mai 2017, le président Trump a signé le décret 13800, *Renforcer la cybersécurité des réseaux fédéraux et des infrastructures critiques*[1], chargeant le ministère du Commerce (DoC) et le ministère de la Sécurité intérieure (DHS) de mener un processus ouvert et transparent pour identifier les moyens d'améliorer la résilience de l'écosystème de l'internet et des communications et de réduire les menaces perpétuées par les bots et les botnets.

Dans ce livre blanc technique, le secteur des communications, plus précisément les fournisseurs de services Internet (FSI) dans ce contexte, cherche à informer ce processus en décrivant les responsabilités partagées des principaux participants de l'écosystème Internet pour atténuer les menaces posées par les botnets. Il est faux de croire qu'une seule composante de l'écosystème Internet est en mesure d'atténuer la menace que représentent les botnets et autres systèmes automatisés. Si les FAI, en tant que propriétaires et exploitants d'infrastructures, jouent un rôle important dans cet écosystème, il en va de même pour les fabricants d'appareils, les développeurs de logiciels, les intégrateurs de systèmes, les fournisseurs de périphérie, les fournisseurs de services en nuage, etc. Il faudra l'effort concerté de tous les membres de cet écosystème pour répondre pleinement aux menaces que représentent les bots et les botnets.

Depuis des années, l'écosystème Internet travaille en collaboration pour neutraliser les menaces que représentent les bots et les botnets. Dans ce document, le Conseil de coordination du secteur des communications (CCSC) identifie un certain nombre de défis liés à l'atténuation des réseaux de zombies, ainsi que des possibilités de collaboration et de coopération accrues entre les membres de l'écosystème de l'internet pour résoudre ce problème, notamment :

- Améliorer l'efficacité du processus d'application de la loi pour démanteler les réseaux de zombies ;

[1] Bureau du secrétaire de presse de la Maison Blanche, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (11 mai 2017), disponible à l'adresse https://www.whitehouse.gov/the-press- office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

- Partage d'informations exploitables sur les cybermenaces ;
- Réduire la dépendance à l'égard de l'utilisation des fonctions de traduction d'adresses réseau (NAT) ;
- Atténuation du trafic des réseaux de zombies provenant de pays étrangers ;
- Gestion des notifications des utilisateurs finaux en cas d'infection par des logiciels malveillants ;
- Se défendre contre les dispositifs IoT non sécurisés ;
- la lutte contre l'utilisation de serveurs de noms de domaine (DNS) à flux rapide par les réseaux de zombies pour dissimuler leur infrastructure ; et
- Coordonner la gestion du réseau de réseau à réseau.

Dans le cadre du processus ouvert et transparent du DoC et du DHS, le CSCC propose également les recommandations préliminaires suivantes ou des mesures réalisables que les participants à l'écosystème, y compris les FAI, devraient envisager pour atténuer les menaces associées aux bots, aux botnets et aux attaques automatisées :

- Rationaliser le processus d'application de la loi pour démanteler les réseaux de zombies ;
- Encourager la poursuite de la migration vers IPv6 ;
- Veiller à ce que les informations partagées sur les cybermenaces soient exploitables et adaptées aux besoins des destinataires ;
- Les opérateurs de réseaux et les utilisateurs finaux devraient inclure des dispositions pré-négociées pour le filtrage du trafic dans les accords de transit et d'échange de trafic ;
- Encourager l'ICANN (Internet Corporation for Assigned Names and Numbers), les registres et les bureaux d'enregistrement à adopter les techniques de réduction des flux rapides recommandées par le SSAC (Security and Stability Advisory Committee) ;
- Améliorer la détection des botnets en encourageant l'adoption et l'utilisation de techniques d'apprentissage automatique ;
- Assurez-vous que tous les points finaux, y compris les dispositifs IoT, respectent les normes de sécurité développées par l'industrie ;
- s'assurer que les points d'extrémité exécutent des logiciels à jour ; et
- Les dispositifs IoT doivent utiliser des techniques d'isolation du réseau et/ou de filtrage basé sur le réseau pour toute communication avec des services basés sur le cloud.

Secteur de l'écosystème Internet et des communications

L'écosystème qui soutient l'internet, y compris les membres du secteur des communications qui fournissent des services d'accès à l'internet, est complexe, diversifié et interdépendant. Pour bien comprendre les menaces que représentent les botnets, il est important de comprendre l'écosystème et les relations entre les parties prenantes. Cette section présente un résumé de l'écosystème de l'internet et explique comment le secteur des communications s'intègre dans l'écosystème plus large de l'internet pour protéger les infrastructures critiques des menaces que représentent les bots et les botnets.

Ecosystème Internet

L'écosystème de l'internet est un système diversifié et hautement intégré, composé de nombreuses parties prenantes. L'Internet Society (ISOC) décrit le vaste écosystème de l'internet comme étant composé de six communautés principales, comme indiqué ci-dessous. [2]

[2] Internet Society, *Who Makes the Internet Work : The Internet Ecosystem* (3 février 2014), disponible à l'adresse http://www.internetsociety.org/who-makes-internet-work-internet-ecosystem (consulté le 16 juillet 2017).

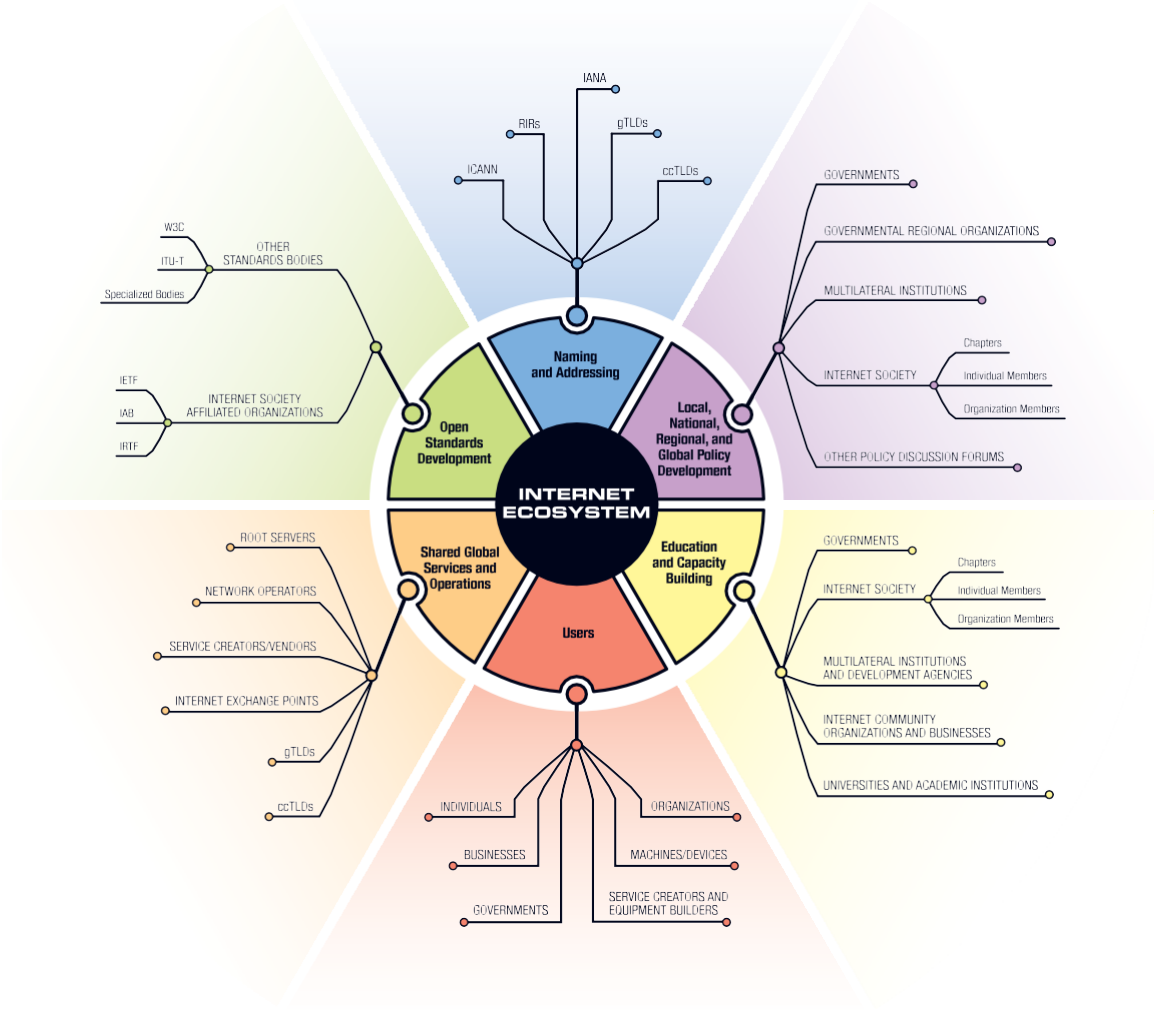


Figure 1 Écosystème Internet Source :

Internet Society

Les opérateurs de réseau, qui font partie du secteur des communications, fournissent les "services et opérations mondiaux partagés" illustrés à la figure 1. Vu sous le seul angle du réseau, l'écosystème Internet ressemble davantage à la figure 2.

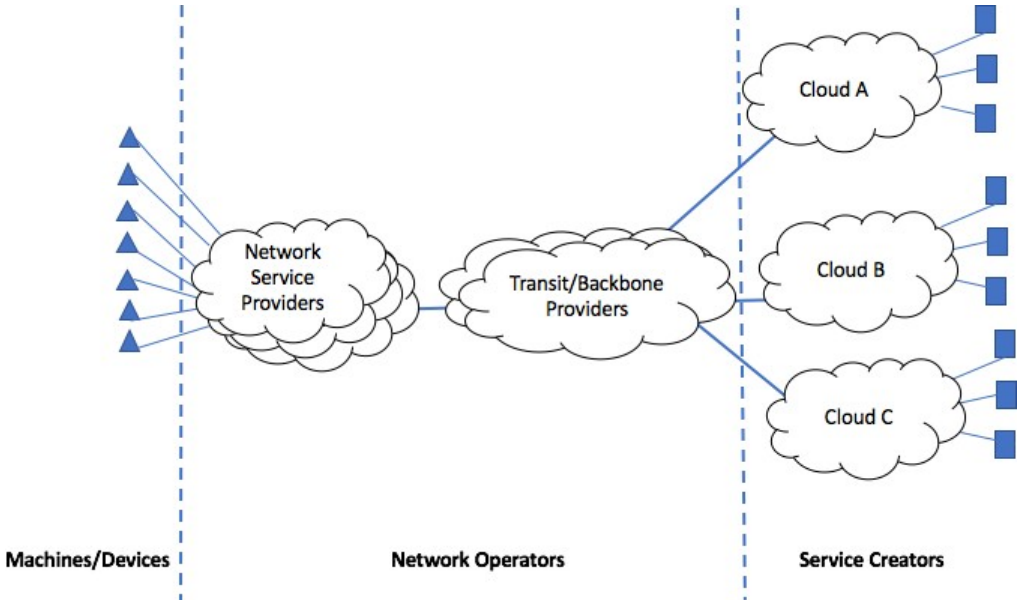


Figure 2 Vue en réseau de l'écosystème Internet

Dans ce contexte, l'écosystème internet est composé de nombreuses machines/appareils (par exemple, smartphones, ordinateurs de bureau, dispositifs IoT, etc.) qui se connectent à des fournisseurs de services réseau. Les fournisseurs de services réseau utilisent une combinaison de transit et d'échange de trafic3 pour fournir une connectivité internet aux créateurs de services (par exemple, hébergement, commerce électronique, médias sociaux, entreprises, etc.)
De nombreux créateurs de services sont basés sur l'informatique dématérialisée, ce qui signifie qu'ils exploitent un réseau de machines travaillant ensemble pour fournir un service. Toutes ces parties travaillent ensemble pour fournir ce que l'on appelle communément l'internet.

Secteur des communications

Les propriétaires et les exploitants d'infrastructures de communication (radiodiffusion, câble, satellite, sans fil et filaire) constituent le secteur des communications. Le secteur des communications est l'un des 16 secteurs d'infrastructures critiques/ressources clés (CI/KR) identifiés dans le plan de protection des infrastructures nationales (NIPP) du DHS. Ce secteur comprend les opérateurs de réseau qui fournissent des services d'accès à Internet. Dans le cadre d'un partenariat public/privé avec le DHS, le secteur des communications utilise le Conseil de coordination du secteur des communications (CSCC) et le Comité d'information sur les communications (CIC).

[3] Remarque : l'annexe B contient un glossaire qui fournit de plus amples informations sur les termes techniques utilisés dans ce document.

(Comm-ISAC) pour aider à sécuriser les réseaux de communication CI/KR.

Le secteur des communications a une longue histoire de coopération au sein de ses membres et avec le gouvernement fédéral en ce qui concerne la sécurité nationale et la préparation aux situations d'urgence. Cette histoire distingue le secteur des communications de la plupart des autres secteurs critiques identifiés dans le plan national de protection des infrastructures (NIPP). Le secteur est un exemple de coopération et de relations de confiance qui ont permis de fournir des services essentiels en cas d'urgence ou de catastrophe. Ce lien solide existe en grande partie grâce à trois organisations qui ont été créées en réponse à des menaces antérieures sur les infrastructures critiques de la nation.

Politique - Le National Security Telecommunications Advisory Committee (NSTAC). Le NSTAC (wwwncs.gov/nstac/nstachtml) a été créé en 1982 par le décret 12382. Il
constitue un exemple très réussi de la manière dont l'industrie contribue à orienter les décisions gouvernementales en matière de communications liées à la sécurité nationale et à la préparation aux situations d'urgence (NS/EP). Le NSTAC est composé d'un maximum de 30 dirigeants de grandes entreprises de télécommunications, de fournisseurs de services réseau et d'entreprises de technologie de l'information, de finance et d'aérospatiale. Par le biais d'un processus de délibération, ils fournissent au président des recommandations destinées à assurer des liaisons de télécommunications vitales lors de tout événement ou crise, et à aider le gouvernement américain à maintenir une posture de communication nationale fiable, sécurisée et résiliente. Les principaux domaines d'intérêt du NSTAC sont les suivants : le renforcement de la sécurité nationale, l'amélioration de la cybersécurité, le maintien de l'infrastructure mondiale des communications, la garantie des communications pour les interventions en cas de catastrophe et la prise en compte des interdépendances des infrastructures essentielles.

Planification - Conseil de coordination du secteur des communications (CSCC). Le CSCC a été créé en 2005 pour : aider à coordonner les initiatives visant à améliorer la sécurité physique et la cybersécurité des actifs du secteur ; faciliter le flux d'informations au sein du secteur, entre les secteurs et avec les agences fédérales désignées ; et aborder les questions liées à la réponse et au rétablissement après un incident ou un événement. Les plus de 40 membres du CSCC représentent largement le secteur et comprennent des câblo-opérateurs, des diffuseurs commerciaux et publics, des fournisseurs de services d'information, des fournisseurs de services par satellite, des fournisseurs de câbles sous-marins, des fournisseurs de services de télécommunications, des intégrateurs de services, des vendeurs d'équipements, des propriétaires et des exploitants de réseaux sans fil et filaires et leurs associations professionnelles respectives.

Opérations - Centre national de coordination des télécommunications (NCC)

Centre d'analyse et de partage des informations sur les communications (Comm-ISAC). En 1982, les responsables du gouvernement fédéral et de l'industrie des télécommunications ont identifié le besoin d'un mécanisme commun pour coordonner le lancement et le rétablissement des services de télécommunications de sécurité nationale et de préparation aux situations d'urgence. En 1984, l'Executive Order 12472 a créé le NCC. Le partenariat unique de cette organisation entre l'industrie et le gouvernement favorise la collaboration sur les questions opérationnelles 24 heures sur 24, 7 jours sur 7, et coordonne les réponses des NS/EP en temps de crise. Depuis 2000, le Centre d'analyse et de partage des informations sur les communications (Comm-ISAC) du NCC, composé de 51 entreprises membres de l'industrie, a facilité l'échange d'informations entre les participants du gouvernement et de l'industrie concernant les vulnérabilités, les menaces, les intrusions et les anomalies affectant l'infrastructure des télécommunications. Les représentants de l'industrie et du gouvernement se réunissent chaque semaine pour partager des informations sur les menaces et les incidents. En cas d'urgence, les représentants de l'industrie et du gouvernement participant aux efforts d'intervention se rencontrent quotidiennement, voire plus fréquemment.

Bots, botnets et menaces associées

> *Bot - programme installé sur un système afin de permettre à ce système d'exécuter automatiquement (ou semi-automatiquement) une tâche ou un ensemble de tâches, généralement sous le commandement et le contrôle d'un administrateur distant (alias bot master ou bot herder).* [4]
>
> *Botnet - réseau de dispositifs informatiques d'utilisateurs finaux connectés à l'internet, infectés par des logiciels malveillants et contrôlés à distance par des tiers à des fins malveillantes.* [5]

Les bots ne sont pas un phénomène nouveau. Il est important de noter que tous les bots ne sont pas mauvais et que tous les réseaux de bots ne sont pas utilisés à des fins néfastes. Il existe de bons bots dans des environnements tels que les jeux et l'Internet Relay Chat (IRC). Toutefois, dans le cadre de cet article, toute mention des bots et des réseaux de zombies suppose qu'ils sont de nature malveillante ou potentiellement malveillante.

Un "botnet" est un réseau de robots travaillant ensemble et capables d'agir sur des instructions générées à distance. Un botnet typique peut compter de quelques milliers à plusieurs centaines de bots.

---

[4] Federal Communications Commission (FCC), Communications Security Reliability and Interoperability Council (CSRIC) III, *U.S. Anti- Bot Code of Conduct (ABCs) for Internet Service Providers*, (Mar. 2012), disponible sur https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf (consulté le 20 juin 2017).

[5] *Id.*

des milliers, voire des millions de bots. Les bots et les réseaux de bots sont hautement personnalisables et peuvent être programmés pour faire de nombreuses choses, notamment : le vol d'informations personnelles et d'autres informations sensibles, le spam, la récolte d'adresses électroniques, les attaques par déni de service distribué (DDoS), l'enregistrement de clés, l'hébergement de contenu illégal et la fraude au clic. Ces types de cyber-attaques sont décrits plus en détail dans la suite de ce document.

Les premiers bots utilisaient IRC pour communiquer avec leurs serveurs C&C. Au fil du temps, les bots et les botnets sont devenus plus sophistiqués. Par exemple, ils sont devenus plus résistants en intégrant des architectures et des protocoles peer-to-peer (P2P), des algorithmes de génération de noms de domaine, le protocole de transfert hypertexte (HTTP) vers des localisateurs de ressources uniformes (URL) spécifiques dans des sites Web légitimes, des infrastructures C&C sophistiquées et hiérarchisées et le cryptage. Chacune de ces améliorations a rendu plus difficile l'identification et l'isolation du mauvais trafic du trafic réseau légitime.

Historiquement, les bots infectaient les ordinateurs de bureau et les serveurs, ce qui entraînait leur détection et leur suppression à l'aide de logiciels antivirus. En revanche, les appareils IoT sont souvent dépourvus d'interface utilisateur, sont conçus pour fonctionner de manière autonome et sont connectés directement ou indirectement à Internet. Ces appareils ne se prêtent pas bien à certaines protections de sécurité traditionnelles. Ils peuvent se connecter à Internet sans pare-feu et sont généralement placés sur le même segment de réseau local (LAN) que d'autres cibles de grande valeur. Il est peu probable qu'ils utilisent un logiciel anti-virus. En outre, ils peuvent être considérés comme un faible risque de sécurité car ils sont peu coûteux et ne traitent que des données apparemment inoffensives. Cependant, les dispositifs IoT sont en fait des cibles attrayantes pour l'exploitation, car ils fournissent une puissance de calcul qui peut être utilisée par des acteurs malveillants, sans que leurs propriétaires s'en aperçoivent, et sont souvent des équipements "à installer et à oublier".

Les grands réseaux d'appareils IoT peuvent être compromis par des bots lorsqu'ils sont connectés à des connexions Internet à haut débit, ce qui peut causer des dommages importants. L'attaque DDoS du botnet Mirai d'octobre 2016 contre le fournisseur de DNS Dyn est l'un des exemples les plus récents. Le botnet Mirai a exploité la faible sécurité de nombreux appareils IoT en balayant continuellement Internet, à la recherche d'autres appareils IoT protégés par des noms d'utilisateur et des mots de passe par défaut ou codés en dur. [6] Lorsque le botnet Mirai a découvert des appareils IoT vulnérables, il a chargé son malware sur les appareils et a commencé à communiquer avec les serveurs C&C en attendant des instructions. Le botnet Mirai a ensuite

---

[6] Symantec Security Response, *Mirai : what you need to know about the botnet behind recent major DDoS attacks*, Symantec Official Blog (27 octobre 2016), disponible sur https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind- recent-major-ddos-attacks (consulté le 20 juin 2017).

a été utilisé pour lancer une attaque DDoS à grande échelle contre Dyn en demandant à chaque appareil infecté d'inonder les serveurs DNS de Dyn d'un grand nombre de paquets utilisant le port de destination du service DNS (port 53 du protocole de datagramme utilisateur (UDP)) et d'inonder les serveurs faisant autorité de nombreuses demandes de noms de domaine invalides7. [7] L'attaque a empêché un certain nombre de clients de Dyn de pouvoir accéder aux noms de domaine servis par Dyn DNS pendant l'attaque.

L'attaque de Dyn n'était pas un incident isolé. Le pic d'attaque a augmenté de façon spectaculaire en peu de temps, passant de 500 Gbps en 2015 à 800 Gbps en 2016.[8] Le site KrebsonSecurity a également été touché par une attaque en septembre 2016, qui a atteint 620 Gbps. En fait, le botnet Mirai et d'autres botnets IoT existaient déjà depuis un certain temps avant ces attaques et étaient généralement utilisés pour réaliser des attaques DDoS de moindre envergure.

Menaces de botnet

Comme décrit ci-dessus, les bots et les botnets sont hautement personnalisables et peuvent donc être programmés pour faire de nombreuses choses bénéfiques sur Internet. Cependant, ils sont souvent et de plus en plus utilisés pour des activités néfastes telles que les types d'attaques énumérés ci-dessous.

- Les attaques DDoS ;
- Vol de données ;
- Distribution illicite de contenu ;
- Détermination du mot de passe par force brute ;
- Traitement du vol ;
- Cliquez sur la fraude ;
- les pourriels ; et
- Passerelle non autorisée.

Le reste de cette section se concentre toutefois sur les attaques DDoS. Les descriptions des autres types d'attaques énumérés ci-dessus se trouvent à l'annexe B.

---

[7] Scott Hamilton, *Dyn Analysis Summary Of Friday October 21 Attack*, Dyn Blog (26 octobre 2016), disponible sur http://dyn.com/blog/dyn- analysis-summary-of-friday-october-21-attack/ (consulté le 20 juin 2017).
[8] Arbor Networks, *12th Annual Worldwide Infrastructure Security Report*, Arbor Networks Special Report Vol. XII (2016), p. 21, disponible sur https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf (consulté le 30 juin 2017).

Les attaques DDoS - une forme d'attaque très répandue perpétrée par des réseaux de zombies - illustrent certains des nombreux défis à relever pour prévenir les attaques et empêcher les zombies de compromettre les points finaux.

Les attaques DDoS peuvent être réparties en quatre grandes catégories:[9]

- Volumétrique ;
- Application/ressource ;
- l'épuisement de l'État ; et
- Plan de contrôle.

Les attaques DDoS volumétriques consistent en des centaines ou des centaines de milliers de robots qui inondent la victime de paquets, entraînant un déni de service pour les autres. Les attaques peuvent être directes, les bots envoyant les paquets directement à la victime, soit avec leur propre adresse IP source, soit avec une adresse IP source usurpée. Les attaques indirectes s'appuient sur une technique connue sous le nom d'attaque par amplification réfléchie, dans laquelle les robots usurpent l'adresse IP source pour qu'elle soit celle de la cible de l'attaque. Les robots envoient ensuite des paquets de demande à d'autres services tels que le DNS, le Character Generator Protocol (chargen) ou le Simple Service Discovery Protocol (SSDP) afin de tromper les services et d'envoyer des réponses à la victime. Les attaques indirectes ou par réflexion sont souvent conçues pour amener le service à envoyer une réponse beaucoup plus importante que la demande initiale du bot, ce qui donne lieu à une attaque par amplification. Dans certaines circonstances, les amplifications peuvent être des milliers de fois supérieures aux paquets de demande initiale des robots.

Les attaques applicatives ont tendance à être des attaques de trafic de plus faible volume que les attaques volumétriques. Elles se caractérisent par l'envoi, par des robots, de demandes d'apparence légitime au niveau des applications à un système afin de consommer des ressources (par exemple, CPU, accès au disque, consultation de bases de données, etc.

Les attaques par épuisement de l'état tirent parti du fait que des dispositifs tels que les serveurs, les pare-feu et les systèmes de détection des intrusions ont des capacités limitées pour suivre l'état des transactions simultanées. Le site

---

[9] FCC CSRIC IV, *Remediation of Server-Based DDoS Attacks Final Report*, (sept. 2014), disponible à l'adresse https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf (consulté le 20 juin 2017).

[10] Messaging, Malware and Mobile Anti-Abuse Working Group, *M3AAWG Introduction to Reflective DDoS Attacks* (mai 2017), disponible sur https://www.m3aawg.org/sites/default/files/m3aawg-reflective-ddos-attack-intro.pdf (consulté le 20 juin 2017).

Les bots tirent parti de cette limitation et consomment toutes les capacités d'état en ouvrant de nombreuses connexions et en ne poursuivant pas complètement ces connexions jusqu'au bout.

Les attaques au niveau du plan de contrôle tirent parti des limites des protocoles Internet tels que le protocole BGP (Border Gateway Protocol)11, IPv6,[12] et le protocole DNS. [13]

L'identification de tous les types d'attaques DDoS constitue un défi, surtout pour les FAI. Les cybercriminels créent rapidement des réseaux de robots de plus en plus sophistiqués, ce qui rend plus difficile la distinction entre le mauvais et le bon trafic. Les premières formes de bots transmettaient souvent leurs messages en clair, sur des ports bien connus, à des adresses IP codées en dur, ce qui rendait le trafic à la fois facile à identifier et à bloquer. De plus en plus, les bots font passer leur trafic pour du trafic au niveau des applications (par exemple, ils le font ressembler à du trafic web ordinaire ou crypté, utilisent des techniques de pair à pair pour éviter un point de défaillance unique, ou utilisent des VPN pour crypter et tunnelliser leur trafic afin d'échapper à la détection).

L'attaque du botnet Mirai a également tiré parti du fait qu'il existe des millions d'appareils IoT dans le monde entier, et le trafic d'attaque a été généré depuis les coins les plus reculés d'Internet, en s'approvisionnant à l'emplacement des victimes. Level 3 Threat Research Labs a déclaré avoir observé plus d'un million d'appareils IoT participant à des attaques de botnet, et un grand pourcentage d'entre eux étaient situés à Taïwan, au Brésil et en Colombie. [14] La difficulté pour un FAI de détecter et de bloquer ce trafic est qu'il ne provient pas du réseau du FAI et peut ne transiter que par une partie du réseau, si tant est qu'il le transite. Et même si des bots sont à l'origine du trafic sur le réseau, le volume du trafic provenant de ces bots peut ne pas être suffisamment important pour être détecté sur le réseau.

Le trafic des attaques de botnets peut sembler tout à fait normal. Il s'agit en grande partie d'attaques amplifiées réfléchies (qui offrent le meilleur rapport qualité-prix), utilisant fréquemment des services communs bien connus tels que le DNS, le protocole de temps réseau (NTP) et le HTTP.

---

[11] K. Butler, et al, *A Survey of BGP Security Issues and Solutions*, Proceedings of the IEEE 98, no. 1 (Jan. 2010), at p. 100-122 (doi:10.1109/jproc.2009.2034031).
[12] Cisco, IPv6 Extension Headers Review and Considerations [IP Version 6 (IPv6)], (10 oct. 2006), disponible sur http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html(consulté le 30 juin 2017).
[13] Suranjith Ariyapperuma, et Chris Mitchell, *Security vulnerabilities in DNS and DNSSec*, Proceedings of Proceedings of The Second International Conference on Availability, Reliability and Security, ARES 2007, The International Dependability Conference - Bridging Theory and Practice, Austria, Vienna, disponible sur http://web.mit.edu/6.033/www/papers/dnssec.pdf (consulté le 30 juin 2017).
[14] Level 3 Research Labs, *Attack of Things !* , disponible à l'adresse http://www.netformation.com/level-3-pov/attack-of-things-2 (consulté le 20 juin 2017).

Il existe des centaines de types d'attaques différentes au sein des cinq catégories d'attaques DDoS. Mirai lui-même a programmé une douzaine d'attaques DDoS. Le botnet se propage en recherchant les ports Telnet ouverts (port 23 du protocole de contrôle de la transmission). Telnet est un protocole en texte clair, extrêmement peu sûr et qui ne devrait pas être utilisé sur Internet, mais c'est exactement de cette manière que Mirai s'est propagé. Au cours de l'attaque DNS de Dyn, Mirai a utilisé la "torture de l'eau" [DNS15,] qu'il a fait passer par l'intermédiaire de plusieurs résolveurs ouverts bien connus (Google 8.8.8.8, par exemple). L'attaque contre le site Web KrebsonSecurity16 a été conçue pour ressembler au protocole GRE (generic routing encapsulation). [17] Les deux attaques auraient pu être bloquées par les fournisseurs de transit Internet en amont. Dans le cas de l'attaque de Dyn, les fournisseurs de services réseau et le Comm-ISAC ont contacté Dyn pour lui proposer leur aide.

L'attaque de KrebsonSecurity, basée sur GRE, aurait pu être bloquée par la plupart des FAI. Le trafic de Dyn a été relayé par des résolveurs ouverts bien connus, de sorte que la limitation du débit de ce trafic vers les IP de Dyn aurait pu atténuer la plupart des effets de cette attaque. Brobot, qui a touché de nombreux systèmes financiers américains, a utilisé HTTP et HTTPS pour la plupart de ses attaques. Pour le bloquer, il faudrait examiner et filtrer le contenu, ce que les FAI ne font généralement pas et ne peuvent pas faire pour HTTPS sans détenir les clés privées de l'utilisateur final. Le trafic malveillant qui est crypté (par exemple, HTTPS) ne peut pas être filtré.

Les dernières attaques illustrent la sophistication et l'ampleur que les botnets ont atteint. Les botnets sont détectables ; le défi consiste à les arrêter. La meilleure façon de les arrêter est d'empêcher leur propagation. Le véritable défi pour l'écosystème de l'internet face aux menaces des réseaux de zombies est de remédier aux points finaux infectés. Si l'on ne remédie pas à la situation du point final ou si l'on ne déconnecte pas le point final infecté d'Internet, la menace que représente le point final infecté demeure. S'assurer que les points d'extrémité exécutent les derniers logiciels et les derniers correctifs de sécurité est une meilleure pratique reconnue pour atténuer la propagation des bots malveillants et infâmes et les menaces qu'ils représentent.

---

[15] Le DNS water torture est un type d'attaque où de nombreux points finaux envoient des requêtes pour le domaine d'une victime avec une chaîne aléatoire ajoutée au début du domaine, ce qui surcharge le serveur DNS faisant autorité de la victime et rend le domaine de la victime inaccessible.

[16] *Voir,* https://krebsonsecurity.com.

[17] KrebsonSecurity, *KrebsOnSecurity Hit With Record DDoS* (21 septembre 2016), disponible sur http://krebsonsecurity.com/tag/gre-ddos/ (consulté le 16 juillet 2017).

La plupart du trafic des botnets provient de l'extérieur des États-Unis

Le paysage des menaces liées aux botnets continue d'évoluer. Selon les sociétés de renseignement sur les menaces, les tendances notables identifiées dans le paysage des menaces en 2016 sont les suivantes : 1) les dispositifs IoT non sécurisés sont une grande source de trafic d'attaque DDoS ; [18] et 2) la grande majorité du trafic d'attaque provient de l'extérieur des États-Unis. [19]

En 2016, les attaques des dispositifs IoT ont fait les gros titres avec les attaques du botnet Mirai à partir de caméras de sécurité mal sécurisées et de leurs enregistreurs (DVR) de télévision en circuit fermé (CCTV). Comme l'a noté Level 3 Threat Research Labs, un grand nombre de ces caméras et DVR non sécurisés étaient situés à Taïwan, au Brésil et en Colombie. [20] Shodan,[21] un moteur de recherche qui permet à l'utilisateur de trouver des types spécifiques d'appareils IoT et d'autres appareils connectés et visibles sur l'internet public, signale (en juillet 2017) plus de 300K d'appareils Hikvision susceptibles d'être connectés directement à l'internet, la grande majorité de ces appareils étant situés au Brésil (45 000), en Inde (36 000), en Chine (34 000), au Mexique (25 000) et en Colombie du Sud.
Corée (20 000). [22]

S'il est difficile d'attribuer la source exacte des attaques de botnet, il est presque toujours possible de déterminer le pays d'origine du trafic. De nombreux rapports23 indiquent que les principales sources d'attaques sont la Chine et d'autres pays d'Asie du Sud-Est (par exemple, le Vietnam, Taiwan et la Thaïlande). [24]

Ce résultat est conforme à une étude antérieure qui a montré une forte corrélation entre les appareils utilisés pour les attaques de botnet et le pays dans lequel ils résident. Ces appareils utilisent généralement des logiciels dépourvus des derniers correctifs de sécurité. [25] Dans une étude, les chercheurs ont analysé six

---

[18] Akamai, *Rapport sur l'état de la sécurité sur Internet au quatrième trimestre 2016* (hiver 2016), disponible sur https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf (consulté le 20 juin 2017).
[19] Incapsula.com, *Global DDoS Threat Landscape Q1 2017* (printemps 2017), disponible à l'adresse https://www.incapsula.com/ddos-report/ddos- report-q1-2017.html (consulté le 20 juin 2017).
[20] Level 3 Research Labs, *Attack of Things !* , disponible à l'adresse http://www.netformation.com/level-3-pov/attack-of-things-2 (consulté le 20 juin 2017).
[21] *Voir* shodan.io (Shodan scanne l'internet en indexant les dispositifs qui répondent aux scans de port sur les ports 80, 8080, 443, 8443, 21, 22,23,161, 5060, 554 et autres ports connus).
[22] Shodan, recherche de " Hikvision ", disponible sur https://www.shodan.io/search?query=hikvision (consulté le 20 juin 2017).
[23] *Voir l'*annexe A du présent document pour les données provenant de différents rapports sur les menaces.
[24] Incapsula.com, *Global DDoS Threat Landscape Q1 2017* (printemps 2017), disponible sur https://www.incapsula.com/ddos-report/ddos- report-q1-2017.html (consulté le 20 juin 2017).
[25] Hadi Asghari, Michael Ciere, et Michael J.G. Van Eten, *Post-Mortem of a Zombie : Conficker Cleanup After Six Years*, In USENIX The Advanced Computing Systems Association, Proceedings of 24th USENIX Security Symposium, Washington, D.C. (août 2015), disponible sur https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-asghari.pdf (consulté le 20 juin 2017).

des années de données longitudinales provenant du gouffre de Conficker, l'un des plus grands réseaux de zombies jamais vus, pour évaluer l'impact sur l'atténuation des zombies des initiatives nationales de lutte contre les zombies, visant à inciter les utilisateurs finaux à nettoyer les machines infectées. Ils ont constaté que les pics d'infection sont fortement corrélés au piratage de logiciels. Cela implique que les pays comptant un nombre élevé d'utilisateurs finaux utilisant des copies de logiciels sans licence ont tendance à avoir un nombre plus élevé de bots, car ces actifs ont un pourcentage plus faible d'utilisateurs enregistrés obtenant des correctifs de sécurité.

Un schéma similaire a été observé avec le botnet Mirai, qui a exploité le fait qu'une catégorie de dispositifs IoT était livrée avec des identifiants de connexion par défaut bien connus que les utilisateurs finaux modifient rarement.
Les vulnérabilités d'au moins un des fabricants ont été signalées dès 2013.[26] Ce n'est qu'après le signalement de l'attaque du botnet Mirai que le fabricant en question a fourni une mise à jour du micrologiciel pour corriger les vulnérabilités et, même dans ce cas, les utilisateurs finaux de l'appareil ont dû intervenir manuellement pour mettre à jour le micrologiciel, car les appareils ne prenaient pas en charge une méthode automatisée de mise à jour sécurisée de leur logiciel.

Outils et techniques actuels

Application du cadre de cybersécurité contre les botnets

Le cadre de cybersécurité, élaboré par le National Institute of Standards & Technology (NIST)27, [est] un "ensemble de normes industrielles et de meilleures pratiques pour aider les organisations à gérer les risques de cybersécurité". Le cadre est composé de cinq domaines fonctionnels
– 1) Identifier, 2) Détecter, 3) Protéger, 4) Répondre, et 5) Récupérer. Les principaux fournisseurs d'accès à Internet utilisent le cadre dans le cadre de leurs processus globaux de gestion des cyber-risques pour faire face aux menaces que représentent les bots et les botnets pour leurs réseaux.

Identifier

Dans ce cadre, la première étape consiste à **identifier** à la fois ce qui doit être protégé et les cybermenaces. La sécurité des communications de la Commission fédérale des communications (FCC),

[26] Bureau de la cybersécurité et des communications du département de la sécurité intérieure (DHS), *Vulnerability Note VU#800094 - Dahua Security DVRs contain multiple vulnerabilities* (4 déc. 2013), disponible à l'adresse http://www.kb.cert.org/vuls/id/800094 (consulté le 20 juin 2017).
[27] National Institute of Standards and Technology, *Cybersecurity Framework* (25 mai 2017), disponible sur https://www.nist.gov/cyberframework(consulté le 20 juin 2017).

Le rapport final du groupe de travail 4 du Conseil pour la fiabilité et l'interopérabilité (CSRIC) IV, intitulé *Cybersecurity Risk Management and Best Practices*, fournit des conseils de mise en œuvre sur l'utilisation du Cadre pour les fournisseurs de services réseau. Les FAI, qui font partie des infrastructures critiques, ont identifié qu'ils devaient protéger leurs réseaux centraux contre les menaces de cybersécurité telles que les bots et les botnets. Les FAI peuvent également, dans le cadre d'un service de sécurité géré, protéger leurs clients contre les méfaits des cybermenaces.

En plus d'identifier ce qui doit être protégé, les fournisseurs de services réseau utilisent le cadre et d'autres outils pour identifier les menaces. La première étape consiste à identifier les surfaces d'attaque des actifs à protéger, puis les vecteurs d'attaque connus. Ces informations sont continuellement synthétisées avec les données de renseignement sur les menaces afin d'assurer une couverture complète et d'identifier, et finalement de traiter, les nouvelles vulnérabilités. L'obtention de données de haute qualité sur les cybermenaces est l'un des aspects les plus importants de la mise en œuvre et de la gestion d'un solide programme d'atténuation des botnets. Pour que le programme soit efficace, il faut que le nombre de faux positifs soit proche de zéro. Les faux positifs peuvent augmenter considérablement les coûts d'exploitation d'un fournisseur de services réseau, avoir un impact sur la satisfaction de ses clients et nuire à sa marque. Comme le souligne le rapport du groupe de travail 5 du CSRIC V sur le *partage d'informations en matière de* cybersécurité[28], les fournisseurs de services réseau ont mis en place un écosystème de partage d'informations afin d'utiliser et de partager des informations sur les indicateurs de cybermenaces provenant d'un large éventail de sources, afin d'identifier les botnets et les menaces qui y sont associées. Cet écosystème comprend des flux de données provenant de tiers de confiance (TTP), des informations provenant du DHS, y compris son système de partage d'informations automatisé (AIS), et le partage d'informations intersectorielles.

Détecter

Comme le souligne le Cadre, la **détection** des menaces et des attaques est l'étape suivante de la protection des réseaux contre les attaques de botnets. Comme nous l'avons décrit précédemment, les attaques de botnets se présentent sous de nombreuses formes, de sorte que leur détection nécessite un ensemble d'outils et de techniques adaptés à chaque type d'attaque.
Quel que soit le type d'attaque par botnet, les fournisseurs de services réseau utilisent un ensemble de techniques de base, notamment l'échantillonnage des paquets, l'analyse des signatures et l'analyse heuristique ou comportementale.

De nombreux botnets tentent de déguiser leur trafic en trafic Internet normal. Il est donc particulièrement difficile de détecter les botnets hautement distribués ou les botnets à faible volume de trafic, car la

[28] FCC CSRIC V, *Groupe de travail 5 : Partage d'informations sur la cybersécurité*, Rapport final (15 mars 2017), disponible sur https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf (consulté le 20 juin 2017).

sera inférieur aux seuils d'alarme sur le réseau d'un seul opérateur. Par exemple, lors de l'attaque Mirai Dyn DNS waterboarding, les attaquants ont fait passer leurs requêtes par des résolveurs DNS ouverts bien connus. [29]

Protéger

Les fournisseurs de services réseau utilisent diverses techniques pour **protéger** leurs réseaux contre les attaques et prennent des mesures pour aider leurs clients à se protéger contre les attaques.

Les fournisseurs de services réseau utilisent différentes techniques de filtrage pour protéger directement leur infrastructure réseau (par exemple, les routeurs, les serveurs). Les robots usurpent souvent l'adresse IP source dans les paquets d'attaque. C'est ce que l'on observe généralement dans les attaques par réflexion du réseau, mais comme on l'a vu dans les attaques à haut volume telles que le botnet Mirai ou l'attaque Dyn, cela peut être accompli même sans usurpation d'adresse IP.
Quoi qu'il en soit, la plupart des fournisseurs de services réseau, sinon tous, effectuent un filtrage réseau pour les adresses IP usurpées. [30]

Les fournisseurs de services réseau utilisent également une combinaison d'autres techniques de filtrage telles que les listes de contrôle d'accès (ACL), la police du trafic, le black holing et le sink holing dans leurs réseaux pour filtrer le trafic des botnets connus. Ces techniques peuvent être efficaces pour neutraliser le trafic C&C des botnets client-serveur. Elles sont moins efficaces contre les botnets plus avancés qui utilisent une architecture peer-to-peer, le cryptage et/ou des techniques DNS à flux rapide pour leur canal C&C. Le fast-flux est une technique DNS utilisée par les botnets pour dissimuler les sites de phishing et de diffusion de logiciels malveillants derrière un réseau en constante évolution d'hôtes compromis faisant office de proxies.

Les fournisseurs de services de réseau ont également réalisé d'importants investissements dans des systèmes d'épuration DDoS afin d'éliminer les attaques DDoS contre leurs réseaux et leurs clients qui ont acheté des services d'atténuation DDoS. Les systèmes d'épuration DDoS consistent à détourner le trafic *de la victime* à travers l'épurateur "à la demande" pour filtrer le trafic d'attaque du bon trafic, puis à le remettre sur le réseau du fournisseur pour l'envoyer à sa destination initiale. Les fournisseurs de services de réseau utilisent une combinaison de systèmes d'épuration internes et de systèmes d'épuration tiers, par le biais de contrats avec des fournisseurs de services de réseau.

---

[29] Scott Hamilton, *Dyn Analysis Summary Of Friday October 21 Attack*, Dyn Blog (26 oct. 2016), disponible sur http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ (consulté le 20 juin 2017).
[30] P. Ferguson et D. Senie, *Network Ingress Filtering : Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, Best Current Practice (BCP) 38 (mai 2000), disponible sur https://tools.ietf.org/html/bcp38 (consulté le 20 juin 2017) ; F. Baker et P. Savola, *Ingress Filtering for Multihomed Networks*, BCP 84 (mars 2004), disponible sur https://tools.ietf.org/html/bcp84 (consulté le 20 juin 2017) ; et Mutually Agreed Norms for Routing Security (MANRS), *Participants* (6 mars 2015), disponible sur https://www.routingmanifesto.org/participants/ (consulté le 20 juin 2017).

des fournisseurs tiers d'atténuation des attaques DDoS. Cependant, les fournisseurs de services réseau *n'ont pas* la capacité d'épurer tout le trafic en permanence.

Outre l'épuration du trafic, de nombreux fournisseurs utilisent les capacités Flowspec31 de BGP pour bloquer dynamiquement le trafic facilement identifiable sur le routeur. Le trafic est généralement bloqué à l'aide des cinq valeurs de base trouvées dans IPFIX32 (IP source et destination, port source et destination, et protocole). Flowspec est avantageux dans la mesure où les mises à jour BGP peuvent être effectuées et retirées assez rapidement dans le réseau, ce qui permet une atténuation plus rapide.

Les fournisseurs de services réseau peuvent également fournir des outils et des services spécifiques à leurs clients pour qu'ils se protègent, notamment des logiciels antivirus pour les points d'extrémité et des passerelles domestiques avec sécurité intégrée. Les grands fournisseurs d'accès Internet qui exploitent des réseaux secondaires ou des fournisseurs de périphérie peuvent également utiliser une technique d'atténuation des attaques DDoS appelée "Anycast", qui permet à plusieurs hôtes ou points d'extrémité d'avoir la même adresse IP. En répartissant géographiquement ces hôtes, l'ampleur de l'attaque DDoS doit être nettement plus importante pour tenir compte des hôtes répartis et réussir à perturber le site ou le service. Les services Anycast peuvent être déployés par les fournisseurs d'accès ou achetés auprès de partenaires spécialisés dans l'atténuation des attaques DDoS.

Plusieurs fournisseurs de services réseau proposent également un ensemble de services de sécurité gérés, y compris, mais sans s'y limiter, les services d'épuration DDoS mentionnés ci-dessus. Ces services peuvent inclure des fonctionnalités telles que des pare-feu basés sur le réseau, des services de gestion des appareils mobiles, l'analyse des menaces et la détection des événements, une connectivité VPN sécurisée au cloud et la sécurité du web et du courrier électronique.

Répondre et récupérer

Aujourd'hui, comme le souligne le Cadre de cybersécurité, lorsqu'un fournisseur de services réseau détecte un trafic malveillant provenant d'un bot sur son réseau ou vers un point final de son réseau, il **réagit et récupère** si nécessaire. La réponse consiste à atténuer l'impact du trafic malveillant et, si nécessaire, à corriger le point final infecté.

Pour atténuer le trafic malveillant, le fournisseur de services réseau doit d'abord déterminer l'ampleur de l'impact du trafic malveillant. Pour le trafic malveillant qui a un impact sur son réseau ou sa

---

[31] Leonardo Serodio, *Traffic Diversion Techniques for DDoS Mitigation using BGP Flowspec* (mai 2013), disponible sur https://nanog.org/sites/default/files/wed.general.trafficdiversion.serodio.10.pdf (consulté le 7 juillet 2017).
[32] B. Claise, B. Trammell et P. Aitken, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*, IETF Tools (sept.2013), disponible sur https://tools.ietf.org/html/rfc7011 (consulté le 7 juillet 2017).
[33] McAfee, *McAfee Web Gateway*, disponible à l'adresse https://www.mcafee.com/us/products/web-gateway.aspx (consulté le 7 juillet 2017).

le fournisseur de services réseau devra s'efforcer de filtrer le trafic malveillant à l'aide de l'une des techniques de filtrage (par exemple, ACL, black hole, sink hole ou scrub) décrites précédemment. En outre, si le trafic malveillant est entrant dans son réseau, le fournisseur de services réseau peut contacter le réseau en amont et lui demander de filtrer le trafic émanant de ce réseau.

Pour le trafic malveillant dont il est déterminé qu'il émane d'un point d'extrémité du client sur son réseau, le fournisseur de services réseau, comme le recommande le code de conduite anti-bot volontaire pour les fournisseurs de services Internet (ABC pour les ISP)[34], va :

- **Détecter** - identifier et détecter l'activité des botnets dans le réseau du FAI ou au nom des entreprises clientes qui ont acheté des services auprès du FAI afin de déterminer les infections potentielles de bot sur les appareils des utilisateurs finaux ;
- **Notifier** - notifier les utilisateurs finaux, y compris potentiellement les consommateurs et les entreprises clientes, des infections suspectées par des robots ;
- **Remédier** - fournir des informations aux utilisateurs finaux sur la façon dont ils peuvent remédier aux infections par les zombies et/ou aider activement les entreprises clientes à remédier à l'impact des réseaux de zombies ; et
- **Collaborer** - fournir un retour d'information et les expériences acquises aux autres ISP.

Solutions émergentes

L'écosystème de l'internet continue d'améliorer sa capacité à atténuer les attaques des botnets. Des efforts sont en cours pour améliorer les capacités de détection et d'atténuation.

Approches technologiques. Un grand nombre de logiciels malveillants utilisent une technique connue sous le nom d'algorithme de génération de domaine (DGA) pour générer périodiquement un grand nombre de noms de domaine qui peuvent être utilisés comme points de rendez-vous pour leurs serveurs C&C dans le but d'obscurcir la véritable infrastructure du botnet. Actuellement, les enquêteurs de sécurité peuvent travailler à la rétro-ingénierie du DGA utilisé par chaque variante de malware. Ce processus d'ingénierie inverse peut prendre beaucoup de temps et constitue souvent une approche inefficace de type "whack-a-mole". Pour remédier à ce problème, l'industrie a étudié comment appliquer l'apprentissage automatique pour automatiser le processus et travailler en temps réel en tant que

[34] Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG), *ABCs for ISPs*, disponible sur https://www.m3aawg.org/abcs-for- ISP-code (consulté le 20 juin 2017).

le logiciel malveillant enregistre les noms de domaine auprès d'un registre Internet. Des efforts sont en cours pour commercialiser et intégrer l'apprentissage automatique pour la détection des botnets dans les produits de protection des réseaux.

Les botnets les plus récents utilisent souvent le cryptage (par exemple, TLS35) pour dissimuler leur canal C&C. Le projet SSBL36 (Secure Sockets Layer SSL Blacklist) montre que même si le botnet utilise le cryptage, il reste possible de le détecter. Le projet Secure Sockets Layer SSL Blacklist (SSBL)36 montre que même si le botnet utilise le chiffrement, il est toujours possible de le détecter. Il est possible d'identifier le trafic C&C du botnet en inspectant les certificats SSL malveillants pour générer une empreinte SHA-137 unique pour chaque botnet à l'aide de l'inspection approfondie des paquets (DPI). Des efforts sont en cours pour commercialiser cette approche et intégrer les méthodes dans les systèmes de protection des réseaux afin de permettre l'identification et l'atténuation en temps réel des botnets.

En outre, les chercheurs développent l'utilisation de tarpits à l'échelle du réseau pour ralentir la propagation des botnets. [38] Les chercheurs étudient comment transformer l'espace d'adresses IP inutilisées en tarpits de botnets. L'idée de base est d'acheminer tout le trafic entrant adressé aux adresses IP inutilisées vers le tarpit. Le tarpit dispose d'un ensemble de règles programmées sur la manière de réagir, ce qui permet de prolonger le temps nécessaire à un botnet pour remonter la chaîne d'élimination40. En prolongeant ce délai, les cibles de l'attaque ont plus de temps pour déterminer quelles mesures défensives supplémentaires doivent être mises en place pour neutraliser l'attaque, le cas échéant.

Outre les bâches, les fournisseurs de réseaux ont entrepris de déterminer comment tirer parti des caractéristiques des réseaux définis par logiciel (SDN) pour atténuer les attaques des botnets. Les réseaux SDN permettent de créer dynamiquement des réseaux superposés. Lorsqu'ils sont associés à d'autres techniques et technologies de partitionnement du réseau, il devient possible de créer dynamiquement des voies virtuelles pour les différents services basés sur IP. Avec cette approche, les fournisseurs IoT peuvent travailler avec les fournisseurs de services réseau pour créer des voies virtuelles de bout en bout, du dispositif IoT au service basé sur le cloud en passant par le réseau. Ce processus permet de s'assurer qu'un dispositif IoT compromis ne peut pas

---

[35E]. Rescorla et N. Modaugu, *Datagram Transport Layer Security Version 1.2*, IETF Tools (Jan. 2012), disponible à l'adresse https://tools.ietf.org/html/rfc6347 (consulté le 20 juin 2017).

[36] SSL Blacklist, *SSL Blacklist*, disponible à l'adresse https://sslbl.abuse.ch/blacklist/ (consulté le 20 juin 2017).

[37] SHA-1 - Secure Hash Algorithm 1 est une fonction de hachage cryptographique qui génère une clé de hachage de 20 octets utilisée par de nombreuses applications et protocoles de sécurité, notamment TLS et SSL, dans le cadre du cryptage des données.

[38] Labrea, *Tom Liston parle de Labrea*, disponible sur http://labrea.sourceforge.net/Intro-History.html (consulté le 17 juillet 2017).

[39] Les tarpits sont des mesures défensives contre les attaques où le serveur retarde délibérément les connexions entrantes pour rendre le spamming et le balayage large moins efficaces.

[40] Eric Hutchins, Michael Cloppert et Rohan Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, CND Papers (21 nov. 2010), disponible sur http://papers.rohanamin.com/?p=15 (consulté le 7 juillet 2017).

communiquer avec des points d'extrémité non autorisés. En d'autres termes, un appareil compromis ne pourrait pas être utilisé dans une attaque DDoS ou envoyer des informations à des hôtes non autorisés. La fonction de découpage du réseau dans les réseaux 5G en est un bon exemple[41], et des approches similaires sont étudiées pour les réseaux filaires compatibles avec le SDN.

Initiatives de collaboration. Plusieurs initiatives menées par l'industrie sont en cours pour améliorer le partage automatisé des informations sur les cybermenaces. La loi sur le partage des informations en matière de cybersécurité (CISA), promulguée en 2015, et le déploiement ultérieur de la capacité de partage automatisé des informations (AIS) du DHS contribuent à faciliter les initiatives de machine à machine (M2M).

Il existe au moins deux autres initiatives de partage automatisé M2M qui peuvent être utiles pour lutter contre les botnets. Toutes deux ont pour objectif commun de faire en sorte que les informations sur les cybermenaces qui sont partagées soient "exploitables" par le destinataire. Par le passé, le paradigme a souvent consisté pour les réseaux à essayer de mettre en place une meilleure protection à leurs points d'entrée. Ces initiatives permettent de partager des informations avec les réseaux voisins afin d'atténuer la menace aussi près que possible de la source du trafic malveillant.

L'IETF (Internet Engineering Task Force) développe un protocole appelé DDOS Open Threat Signaling (DOTS)[42] pour l'échange en temps réel de télémétrie liée aux DDoS entre les éléments de réseau d'atténuation des DDoS. Le protocole DOTS de l'IETF vise à améliorer la coopération entre les victimes d'attaques DDoS et les parties qui peuvent aider à atténuer ces attaques. Le protocole prendra en charge les demandes de services d'atténuation des attaques DDoS et les mises à jour d'état à travers les frontières administratives inter-organisationnelles (par exemple, de réseau à réseau).

Les membres du groupe d'intérêt spécial DDoS du Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG)43 collaborent à un projet similaire. Le M3AAWG développe une interface de programme d'application (API), un magasin de données et des implémentations de référence open source pour que les fournisseurs de services réseau partagent des indicateurs de menace DDoS dans le but d'identifier les sources de trafic d'attaque DDoS, mais pas pour atténuer les attaques en temps réel. L'approche du M3AAWG permet aux fournisseurs de services réseau de partager les adresses IP sources pour les flux IP entrants que leurs systèmes de détection DDoS identifient de manière anonyme avec le réseau sur lequel l'attaque DDoS

---

[41] *Voir* 5G Americas, *Network Slicing for 5G Networks & Services,* disponible sur http://www.5gamericas.org/files/3214/7975/0104/5G_Americas_Network_Slicing_11.21_Final.pdf (consulté le 7 juillet 2017).
[42] IETF, *DDoS Open Threat Signaling (points)*, disponible sur https://datatracker.ietf.org/wg/dots/about/ (consulté le 20 juin 2017). [43] M3AAWG, *M3AAWG publie de nouveaux documents expliquant la sécurité des mots de passe, l'authentification multifactorielle, l'utilisation du chiffrement et les mesures de protection contre les DDoS ; annonce la direction et les présidents des comités*, communiqué de presse (4 avril 2017), disponible à l'adresse https://www.m3aawg.org/news/rel-leadership-papers-2017-04 (consulté le 20 juin 2017).

l'origine de l'attaque. Cela permet aux opérateurs de réseau de nettoyer les sources du trafic des attaques DDoS. En ne partageant que l'adresse IP source, cette approche est compatible avec la plupart des lois mondiales sur la protection de la vie privée en ce qui concerne le partage d'informations identifiables.

Défis et opportunités

La cybersécurité est une responsabilité partagée. La réduction des menaces que représentent les bots, les botnets et leurs attaques automatisées nécessite la coopération et la collaboration de tous les membres de l'écosystème Internet. Cette section identifie un certain nombre de domaines dans lesquels les menaces présentées par les bots et les botnets peuvent être réduites grâce à une meilleure coopération et collaboration des membres de l'écosystème Internet.

Démantèlement de botnets

Défi - Aucune technique n'est plus efficace que les actions de répression qui conduisent à l'arrestation des auteurs. C'est la seule solution qui s'attaque à la cause profonde du problème, et pas seulement à un symptôme. Malheureusement, l'exécution d'une opération de démantèlement d'un botnet nécessite une importante analyse médico-légale en amont et une coordination minutieuse entre de nombreuses parties prenantes, souvent au-delà des frontières internationales. Le manque de ressources des forces de l'ordre est un facteur limitant la vitesse globale de démantèlement des botnets. L'autre difficulté réside dans le fait que la plupart des botnets sont internationaux par nature, ce qui exige une coopération entre les pays qui demande beaucoup de ressources et de temps.

Opportunité - Des ressources supplémentaires pour l'application de la loi et la rationalisation des processus internationaux faciliteraient le processus global de démantèlement des botnets.

Informations exploitables sur les cybermenaces

Défi - Les fournisseurs de services réseau doivent disposer d'informations précises et exploitables sur les cybermenaces pour être en mesure de neutraliser rapidement les réseaux de zombies. Pour que les informations soient exploitables, l'indicateur de cybermenace doit être corrélé à un point final unique. La plupart des flux de données utilisés et partagés par les entreprises sont des listes de réputation IP à long terme qui ont peu de valeur pour les fournisseurs de services réseau qui exploitent des réseaux avec un grand nombre d'abonnés ayant des adresses IP attribuées dynamiquement avec des baux courts. Cela signifie que l'indicateur de cybermenace doit être opportun et inclure soit l'adresse IP actuelle, soit l'adresse IP et un horodatage de l'activité malveillante.

Il en va de même pour les adresses IP des serveurs C&C du botnet. Souvent, les serveurs C&C n'*ont* pas d'adresse IP statique. Souvent, les serveurs C&C se trouvent sur des hôtes partagés où une seule adresse IP est partagée par plusieurs hôtes. En outre, les serveurs C&C peuvent disposer d'un pool d'adresses IP ou d'hôtes partagés qu'ils utilisent en alternance.

Les fournisseurs de services réseau ont besoin d'une indication unique, très fiable et à court terme qu'une adresse IP a généré du trafic malveillant ou a été scannée pour montrer les services vulnérables exposés, ainsi que les hôtes compromis.

Opportunités - Les experts s'accordent à dire que les informations sur les cybermenaces doivent être opportunes et ciblées pour être efficaces. Les initiatives de partage de cyberinformations du groupe de travail DOTS de l'IETF et du M3AAWG DDoS SIG sont des pas dans la bonne direction. L'AIS44 du DHS offre également la possibilité d'améliorer et de renforcer le partage opportun et adapté des indicateurs de cybermenaces afin de répondre aux besoins des destinataires.

Traduction d'adresses de réseau

Défi - Les FAI filaires exploitant des réseaux IPv4 fournissent généralement à un abonné résidentiel une seule adresse IPv4 publique. L'abonné résidentiel utilise souvent un routeur domestique qui comprend une fonction de traduction d'adresse réseau (NAT), ce qui lui permet de partager son adresse IPv4 publique unique avec plusieurs appareils dans la maison.

Lorsqu'un FAI reçoit des informations sur un abonné résidentiel qui envoie du trafic malveillant, ces informations, au mieux, ne peuvent contenir que l'adresse IPv4 attribuée au client et non celle du point final réel derrière le routeur domestique. L'utilisation de la technologie NAT fait qu'il est difficile pour le FAI d'identifier le dispositif spécifique chez l'abonné qui envoie du trafic malveillant.

Opportunité - L'IPv6 élimine le besoin d'utiliser le NAT pour le partage d'adresses IP, puisque chaque dispositif connecté à l'Internet peut avoir une adresse IPv6 publiquement routable. Bien qu'il ne s'agisse pas d'une panacée, l'élimination des routeurs NAT peut faciliter l'identification des appareils finaux qui transmettent du trafic malveillant dans certaines circonstances, et le filtrage approprié du trafic suspect. À partir de juin

[44] DHS, *Automated Indicator Sharing (AIS),* disponible sur https://www.dhs.gov/ais (consulté le 20 juin 2017).

2017, l'adoption d'IPv6 par les fournisseurs de réseaux était d'environ 19 % à l'échelle mondiale[45], et de 35 % et en progression aux États-Unis.

Trafic hors réseau

Défis - En tant que réseaux mondiaux largement distribués, la plupart des bots et leurs serveurs C&C échappent au réseau et au contrôle administratif du fournisseur de services réseau. En fait, de nombreux rapports montrent clairement que l'écrasante majorité du trafic des réseaux de zombies provient de l'extérieur des États-Unis[46] .

En outre, dans la plupart des cas, seule une petite partie des points finaux d'un fournisseur de services réseau peut être infectée par un seul botnet, et la quantité de trafic générée par le botnet sur le réseau sera minuscule. Ce petit volume de trafic peut être très difficile à détecter car il ne déclenchera pas la plupart des seuils de surveillance du réseau mis en place par le fournisseur de services réseau.

Opportunité - Pour relever ces deux défis, il faut une collaboration entre les fournisseurs de services réseau, car l'une des mesures les plus efficaces consiste à filtrer le trafic au plus près de l'appareil infecté par le bot. Tout accord de transit ou d'échange de trafic doit comporter des clauses relatives à la disponibilité et à l'épuration du trafic afin de permettre aux opérateurs de réseau de demander au(x) fournisseur(s) en amont de filtrer le trafic malveillant.

Notifications aux utilisateurs finaux

Défi - Notifier et faire agir les utilisateurs finaux reste un défi. Les membres de l'écosystème Internet peuvent notifier un utilisateur final de plusieurs manières:[47]

- Courriel ;
- Appel téléphonique ;
- Courrier postal ;

---

[45] Google, *IPv6 Adoption* (18 juin 2017), disponible sur https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6- adoption&tab=per-country-ipv6-adoption (consulté le 20 juin 2017).
[46] Incapsula.com, *Global DDoS Threat Landscape Q4 2016* (Winter 2017), disponible à l'adresse https://www.incapsula.com/ddos-report/ddos- report-q4-2016.html (consulté le 20 juin 2017).
[47] Michael Glenn, *Malware Notification and Remediation Tools and Techniques*, présentation de CenturyLink à l'atelier du NIST : Technical Aspects of Botnet (30 mai 2012), disponible sur https://www.nist.gov/sites/default/files/documents/itl/csd/centurylink_malware_notification_and_remediation.pdf (consulté le 20 juin 2017).

- Un message texte ;
- Notification du navigateur Web ;
- un jardin clos ; et
- Autres méthodes. [48]

Une étude commandée par le M3AAWG pour déterminer l'efficacité de diverses méthodes de notification et de remédiation a montré que les deux méthodes les plus efficaces sont un appel téléphonique à l'utilisateur du dispositif et un courrier postal. [49] L'utilisation croissante des dispositifs IoT dans les foyers présente de nouveaux défis en matière de notification aux utilisateurs finaux. Les dispositifs IoT ont souvent des interfaces utilisateur limitées, ce qui annule un certain nombre de méthodes de notification (navigateur web, walled garden, etc.). Le problème est encore aggravé par le fait qu'un fournisseur d'accès à Internet ne peut que notifier à un utilisateur final qu'"un appareil" de son domicile est infecté, et ne peut pas identifier l'appareil corrompu spécifique.

Opportunités - Diverses mesures existent pour améliorer l'identification des appareils à l'avenir. Des dispositifs IoT mieux conçus et conformes aux normes industrielles telles que celles développées par l'Open Connectivity Foundation (OCF)[50] constituent une solution pour améliorer la sécurité. Et, comme indiqué précédemment, la prise en charge de l'IPv6 par les opérateurs de réseau facilitera l'identification de l'appareil infecté, ainsi que la notification de l'appareil à l'utilisateur.

Fast Flux DNS

Défi - L'utilisation du fast flux51 par les logiciels malveillants et les réseaux de zombies pour cacher leur infrastructure ne cesse de croître. Le fast-flux est une technique DNS dans laquelle de nombreuses adresses IP associées à un seul nom de domaine sont échangées à une fréquence extrêmement élevée. Le fast-flux permet de dissimuler efficacement les ordinateurs ou les serveurs qui exécutent les attaques malveillantes. Le fast-flux rend difficile, voire impossible, la coupure du contact entre les bots et les serveurs C&C par le seul filtrage des adresses IP.

Opportunité - En 2008, le comité consultatif sur la sécurité et la stabilité (SSAC) de l'ICANN a publié un avis de sécurité qui contenait un certain nombre de recommandations d'atténuation pour traiter le problème des DNS à flux rapide.

---

[48] D'autres méthodes peuvent inclure un message sur les médias sociaux, une alerte sur le téléviseur via le décodeur, un message vocal de dépôt direct, etc.
[49] Chercheurs de Georgia Tech, *étude sur la remédiation des changeurs de DNS*, présentation à la 27e réunion générale du M3AAWG, San Francisco, CA (19 février 2013), disponible à l'adresse https://www.m3aawg.org/sites/default/files/document/GeorgiaTech_DNSChanger_Study-2013-02-19.pdf (consulté le 20 juin 2017).
[50] *Voir* Open Connectivity Foundation, disponible sur https://openconnectivity.org/ (consulté le 20 juin 2017).
[51] Comité consultatif sur la sécurité et la stabilité de l'ICANN (SSAC), *SAC 025 SSAC Advisory on Fast Flux Hosting and DNS* (mars 2008), disponible sur https://www.icann.org/en/system/files/files/sac-025-en.pdf (consulté le 20 juin 2017).

techniques. Parmi ses conclusions et recommandations, le SSAC a encouragé l'ICANN, les registres et les bureaux d'enregistrement à prendre en compte les pratiques de réduction des flux rapides dans l'avis.

Depuis, les progrès de l'apprentissage automatique ont été appliqués à la détection des botnets utilisant des techniques de DNS à flux rapide. Les progrès dans l'application de l'apprentissage automatique pour détecter les réseaux de zombies qui apportent des modifications aux entrées DNS permettent l'automatisation et l'intégration dans les systèmes de détection des réseaux de zombies.

Dispositifs IoT non sécurisés

Défi - Comme nous l'avons vu tout au long de ce document, la base installée croissante de dispositifs IoT fait de ces dispositifs des cibles attrayantes pour les cybercriminels qui veulent les infecter avec un code bot. La récente attaque du botnet Mirai en est un bon exemple : des caméras de sécurité IoT non sécurisées et connectées à Internet ont été infectées pour générer une attaque DDoS massive. Ce n'est pas un phénomène nouveau ; le problème existe depuis des années, car pendant des années, de nombreux routeurs domestiques de qualité grand public ont été livrés avec des vulnérabilités connues qui ont été exploitées pour générer des attaques d'amplification DNS à grande échelle.

Les types de vulnérabilités connues52 trouvées dans de nombreux dispositifs IoT sur le marché aujourd'hui comprennent :

- Expédition de dispositifs IoT avec un logiciel obsolète contenant des vulnérabilités connues et ne disposant pas de la capacité de mise à jour logicielle automatisée ;
- Protection uniquement par des noms d'utilisateur et des mots de passe par défaut ou codés en dur ;
- Communications non authentifiées ;
- les communications non cryptées ; et
- Absence d'authentification et d'autorisation mutuelles.

Les dispositifs IoT non sécurisés présentent un défi unique car, une fois qu'ils sont compromis, il est souvent impossible pour l'utilisateur final de détecter qu'ils ont été compromis et, comme indiqué précédemment, il est difficile pour un fournisseur de services réseau d'avertir l'utilisateur final que son dispositif a été compromis. Même une fois que l'utilisateur final est conscient de la compromission, il est souvent impossible d'empêcher la compromission.

52Groupe consultatif technique sur l'Internet à large bande (BITAG), *Recommandations sur la sécurité et la confidentialité de l'Internet des objets* (nov. 2016), disponible à l'adresse http://bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf (consulté le 20 juin 2017).

remédier au problème en raison de l'absence de mise à jour logicielle et/ou de l'absence de mises à jour logicielles automatisées.

Opportunité - Les dispositifs IoT peuvent être mieux sécurisés grâce à l'utilisation de l'isolation du réseau/du chemin. Les techniques d'isolation réseau/chemin (VPN, VLAN, routage à base de règles, découpage du réseau, etc.) peuvent être utilisées pour créer des chemins de trafic logiques indépendants.) peuvent être utilisées pour créer des chemins de trafic logiques indépendants. Ces chemins de trafic logiques indépendants garantissent que le trafic IoT ne peut atteindre que les points d'extrémité désignés. Cela permet d'atténuer les impacts de tout trafic malveillant qu'un dispositif IoT compromis pourrait envoyer.

Avec les progrès de la virtualisation des fonctions réseau (NFV) et des SDN, des opportunités existent pour les fabricants d'IoT de concevoir des appareils pour utiliser des techniques d'isolation réseau/chemin dans le cadre de leur service. En outre, les fournisseurs de services réseau ont la possibilité de proposer l'isolation réseau/chemin en tant que service aux fournisseurs IoT ou aux utilisateurs finaux pour leurs appareils IoT.

Attaques d'amplification

Défi - Une attaque par amplification est un type d'attaque DDoS qui tire parti du fait qu'une petite requête telle qu'une requête DNS peut générer une réponse beaucoup plus importante. Associé à l'usurpation d'adresse source, un attaquant peut diriger un grand volume de trafic réseau vers un système cible. La nature asymétrique des attaques par amplification en fait le choix privilégié pour les attaques DDoS. Les attaques par amplification s'appuient souvent sur des protocoles basés sur UDP, tels que le protocole DNS, le protocole de temps réseau (NTP), le générateur de caractères (CharGEN) et la citation du jour (QOTD).
Environ 15 protocoles Internet sont sensibles aux attaques par amplification. [54] ingénieurs Internet ont développé une extension du protocole DNS, appelée DNS Security (DNSSEC) pour remédier à la vulnérabilité du DNS à l'empoisonnement du cache du DNS. Malheureusement, un effet secondaire de cette correction est que l'extension de sécurité du DNS rend les réponses du DNS beaucoup plus volumineuses et contribue à amplifier davantage l'attaque.

La mise en œuvre de la validation de l'adresse source (SAV)[55] , telle que recommandée dans le document IETF BCP 38/84, permet d'éviter les attaques par amplification avec des adresses sources usurpées. Bien que la plupart des grandes entreprises américaines

---

[53]Cisco, *Network Virtualization--Path Isolation Design Guide* (22 juillet 2008), disponible sur http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/PathIsol.html(consulté le 20 juin 2017). [54]United States Computer Emergency Readiness Team (US-CERT), *UDP-Based Amplification Attacks*, Alert (TA14-017A) (4 novembre 2016), disponible sur https://www.us-cert.gov/ncas/alerts/TA14-017A (consulté le 20 juin 2017).
[55] Le SAV est une bonne pratique des FAI depuis longtemps (voir IETF 2267 publié en 1998), mais en raison de la difficulté à mettre en œuvre le SAV dans certaines situations commerciales, il peut ne pas être entièrement mis en œuvre dans les réseaux des FAI.

Les fournisseurs de services réseau56 ont mis en œuvre la validation de l'adresse source, mais environ 30 % de l'espace d'adressage IP global peut encore être usurpé. [57]

Opportunité - L'utilisation du filtrage IP ou de la validation de l'adresse source (SAV), comme indiqué dans les meilleures pratiques communes (BCP) 38 et 84 de l'IETF pour les adresses IP usurpées, est une technique éprouvée pour atténuer les attaques d'amplification DDoS utilisant des adresses sources usurpées.

Les normes mutuellement acceptées pour la sécurité du routage (Mutually Agreed Norms for Routing Security, MANRS)[58] sont un effort de l'industrie pour codifier un ensemble de valeurs partagées par les opérateurs de réseau dans un ensemble de définitions et de comportements idéaux. MANRS recommande la mise en œuvre d'un filtrage anti-spoofing pour empêcher les paquets avec des adresses IP source incorrectes d'entrer ou de sortir du réseau. À ce jour, plus de 45 opérateurs de réseaux participent à MANRS. La possibilité existe de réduire à presque zéro l'espace d'adresses usurpables si chaque opérateur de réseau participe à MANRS.

Gestion coordonnée de réseau à réseau

Défi - Bien que la gestion du réseau puisse sembler simple et souhaitable, elle n'est pas sans défis, notamment en raison de l'impact négatif sur les utilisateurs finaux d'Internet. Idéalement, les mesures d'atténuation des botnets devraient être rapides et dirigées vers la source de l'attaque. Les progrès réalisés dans l'architecture des réseaux à l'aide des réseaux SDN et l'utilisation du partage M2M automatisé d'indicateurs de cybermenaces commencent à rendre techniquement viable pour les opérateurs de réseaux l'automatisation de la coordination de leurs mesures d'atténuation des botnets et la réduction du temps de réponse lorsqu'un bot malveillant est détecté sur un réseau ou qu'un botnet lance une attaque. Mais il y a des défis à relever, qu'ils soient techniques, contractuels ou politiques.

Les défis techniques concernent à la fois la détection et l'atténuation. En l'absence d'une source de vérité fondamentale sur ce qui est ou n'est pas le trafic des réseaux de zombies, étant donné que ce dernier est souvent conçu pour ressembler au trafic Internet normal, il existe un risque de faux positifs. Même avec une source de vérité fondamentale, les méthodes d'atténuation des botnets varieront d'un réseau à l'autre en raison des différences inhérentes aux éléments suivants

---

[56]MANRS, *Participants* (6 mars 2015), disponible sur https://www.routingmanifesto.org/participants/ (consulté le 20 juin 2017). [57]Center for Applied Internet Data Analysis, *State of IP Spoofing*, disponible sur https://spoofer.caida.org/summary.php (consulté le 20 juin 2017).
[58]MANRS, *Mutually Agreed Norms for Routing Security (MANRS) Document* (8 septembre 2016), disponible sur http://www.routingmanifesto.org/manrs/ (consulté le 20 juin 2017).

la façon dont les réseaux sont conçus et construits, ainsi que les différences dans les accords de niveau de service entre les fournisseurs de services réseau et leurs clients.

La lutte aveugle contre les réseaux de zombies par le biais de l'automatisation comporte de nombreux risques. Il existe de nombreux cas où un serveur de commande et de contrôle n'appartient pas à l'opérateur du bot ou n'est pas entièrement sous son contrôle, par exemple : 1) les serveurs DNS partagés, 2) les IP partagées et 3) les sites Web publics. [59] L'application aveugle d'une méthode d'atténuation des botnets telle que le filtrage de l'adresse IP empêcherait l'accès à tous les services qui partagent la ressource (par exemple, DNS, serveur partagé ou service). Le défi ne se limite pas aux ressources partagées. Sans une connaissance complète de l'accord de niveau de service en place entre le fournisseur de services réseau et le client, un service réseau ne peut pas filtrer aveuglément le trafic vers ce point final.

En outre, dans le secteur des télécommunications/ISP, on observe une tendance émergente à l'adoption du SDN, qui n'en est encore qu'à ses débuts, mais qui décrit généralement l'automatisation de la gestion et de l'orchestration des actifs et des services réseau. En général, cela inclut le couplage de cadres de big data qui tirent parti de l'analyse avancée et de l'apprentissage automatique pour servir de boucles de rétroaction à ces réseaux SDN afin de prédire, recommander et prescrire dans le but d'améliorer la réactivité et la résilience de leurs actifs et services. Ces mises en œuvre varient considérablement en termes de capacité et de maturité entre les fournisseurs et, dans la plupart des cas, elles reflètent une propriété intellectuelle hautement protégée qui offre une expérience et un savoir-faire concurrentiels uniques.
offres. Néanmoins, un tel écosystème pourrait être utilisé comme stratégie d'atténuation des attaques. Le déploiement du SDN et de ces outils a largement dépassé le stade conceptuel ; c'est la complexité et le coût d'une mise en œuvre globale sur des réseaux hautement hétérogènes qui font obstacle à la rapidité des fournisseurs à les mettre en œuvre.

Opportunité - Une meilleure collaboration et coordination peut réduire le temps de réponse aux cybermenaces. Comme nous l'avons mentionné précédemment, l'industrie développe des solutions telles que le DOTS de l'IETF, le pilote de partage d'informations du M3AAWG DDoS SIG et un pilote de partage d'informations dirigé par la CTIA qui réduira le temps de réponse en partageant des informations "exploitables" sur les cybermenaces. En outre, à mesure que les plateformes de partage d'informations sur les menaces gagneront en maturité, elles contribueront à réduire le temps de réponse des opérateurs de réseau.

[59] Les sites web publics comprennent des sites comme Twitter, Amazon AWS, Google Cloud et Rapidshare.

La clé de la réussite de toute gestion coordonnée du réseau contre les botnets est une collaboration et une communication étroites et de confiance entre les parties prenantes.

Recommandations de l'industrie

Le présent document expose certains des problèmes posés par les bots et les botnets ainsi que les défis et les opportunités auxquels sont confrontés les propriétaires et les exploitants de réseaux à large bande. La section suivante se concentre sur les recommandations préliminaires qui peuvent être mises en œuvre non seulement par les fournisseurs de services réseau mais aussi par l'ensemble de l'écosystème Internet pour aider à réduire les menaces que représentent les réseaux de zombies en utilisant la technologie existante. Les recommandations préliminaires sont présentées ici du point de vue de la CSCC. Il est nécessaire de discuter des meilleures pratiques et des capacités de tous les segments de l'écosystème, y compris les développeurs de logiciels ainsi que les fournisseurs d'infrastructures de cloud computing, d'hébergement et d'applications.

Atténuation des attaques

- **Encourager la poursuite de la migration vers le tout IPv6.**

  L'utilisation généralisée de l'IPv6 permettra aux appareils de disposer d'une adresse unique et facilitera, dans certaines circonstances, la recherche de la source d'un trafic malveillant.

- **Veiller à ce que les informations partagées sur les cybermenaces soient exploitables et adaptées aux besoins des destinataires.**

  Les informations sur les cybermenaces qui sont partagées entre les parties prenantes de l'Internet doivent être exploitables par les destinataires. Les participants au pool de partage d'informations doivent adapter les informations qu'ils partagent avec leurs pairs pour qu'elles soient exploitables.

- **Inclure des dispositions pré-négociées pour le filtrage du trafic dans les accords de transit et d'échange de trafic.**

  Les opérateurs de services de réseau de toutes tailles (ISP, entreprises, gouvernements, établissements d'enseignement, etc.) et les utilisateurs finaux doivent s'assurer qu'ils ont mis en place des dispositions avec leurs fournisseurs de services de réseau.

les fournisseurs de transit internet et les réseaux d'échange de trafic pour assurer le filtrage en amont et l'épuration du trafic malveillant.

- **Rationaliser le processus de démantèlement des botnets par les forces de l'ordre.**

  Les forces de l'ordre peuvent jouer un rôle clé dans la neutralisation des botnets. Des efforts sont nécessaires pour rationaliser le processus d'application de la loi afin d'accroître la rapidité et l'efficacité du démantèlement des botnets par les forces de l'ordre.

- **Encourager l'ICANN, les registres et les bureaux d'enregistrement à adopter les techniques d'atténuation du fast-flux présentées dans le document SAC 025 SSAC Advisory on Fast Flux Hosting and DNS.**

  L'écosystème de l'Internet devrait encourager l'ICANN, les registres et les bureaux d'enregistrement à prendre en considération et à adopter les techniques d'atténuation des flux rapides présentées dans l'avis du SSAC.

- **Adapter et appliquer l'apprentissage automatique à la détection des réseaux de zombies.**

  L'écosystème de l'internet devrait renoncer à l'ingénierie inverse manuelle des algorithmes de génération de domaines de botnets et commencer à appliquer l'apprentissage automatique pour automatiser la détection en temps réel des botnets qui utilisent le fast-flux, le cryptage et d'autres techniques pour masquer leur infrastructure.

Prévention des points de terminaison

- **Assurez-vous que tous les points finaux, y compris les dispositifs IoT, respectent les normes de sécurité développées par l'industrie.**

  De multiples efforts menés par l'industrie sont en cours pour développer des normes de sécurité pour les dispositifs IoT. Les fabricants de dispositifs IoT et les fournisseurs de services IoT doivent s'assurer que tous les dispositifs IoT respectent les normes de sécurité de leur secteur respectif et les meilleures pratiques en matière de sécurité IoT.

- **Assurez-vous que les points d'extrémité exécutent des logiciels à jour.**

  Comme le dit le proverbe, "une once de prévention vaut mieux qu'une livre de remède". Cela s'applique également aux points finaux des consommateurs/clients. S'assurer que tous les points finaux (ordinateurs de bureau, mobiles, IoT, etc.) exécutent des logiciels à jour avec les derniers correctifs et mises à jour de sécurité.

contribuera énormément à réduire le nombre de points finaux infectés et compromis sur Internet.

- **Les dispositifs IoT doivent utiliser des techniques d'isolation du réseau et/ou de filtrage basé sur le réseau pour toute communication avec des services basés sur le cloud.**

  L'isolation du réseau et/ou le filtrage basé sur le réseau sont des techniques éprouvées pour réduire la capacité de nuisance d'un point d'extrémité Internet malveillant. [60] Les fabricants de dispositifs IoT et les fournisseurs de services IoT devraient concevoir leurs produits et services de manière à utiliser ces techniques.

Conclusion

La cybersécurité est une responsabilité partagée. La sécurisation de l'Internet contre les menaces que représentent les botnets nécessite la collaboration et la coopération de tous les membres de l'écosystème Internet, tant au niveau national qu'international. Les recommandations préliminaires formulées dans le présent document ne représentent que quelques-uns des nombreux moyens de réduire les menaces des botnets et leur capacité de nuisance grâce à un large engagement des parties prenantes.

À propos des auteurs

Matt Tooley est le vice-président de Broadband Technology à la NCTA - The Internet and Television Association. Il est membre du comité exécutif du Conseil de coordination du secteur des communications. M. Tooley a plus de 30 ans d'expérience dans le secteur de la large bande, dans le développement et le déploiement de la technologie à large bande pour les fournisseurs de services Internet.

Ce document comprend des contributions clés de AT&T, CenturyLink et Cox Communications.

---

[60] BITAG, *Recommandations sur la sécurité et la confidentialité de l'Internet des objets (IoT)* (nov. 2016) à la Sec. 6 (discutant d'" un rôle possible pour la technologie des réseaux domestiques "), disponible sur http://bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf (consulté le 20 juin 2017).

Annexe A - Rapports sur les cybermenaces

Les 10 pires pays pour les botnets		
Rang	**Pays**	**Nombre de bots**
1	Chine	1,375,637
2	Inde	958,814
3	Fédération de Russie	569,463
4	Brésil	429,942
5	Vietnam	380,639
6	Iran, République islamique d'Iran	242,909
7	Argentine	177,701
8	Thaïlande	173,027
9	Mexique	145,516
10	C?*	141,684

Source : Spamhaus à partir du 29 juin 2017. https://www.spamhaus.org/statistics/botnet-cc/

** Spamhaus signale le dixième pays de cette liste comme étant "C ?".*

Les 10 principaux pays attaquant le trafic de botnets		
Rang	**Pays**	**Pourcentage du trafic d'attaque**
1	Chine	50.8%
2	Corée du Sud	10.8%
3	États-Unis	7.2%
4	Égypte	3.2%
5	Hong Kong	3.2%
6	Vietnam	2.6%
7	Taiwan	2.4%
8	Thaïlande	1.6%
9	Royaume-Uni	1.5%
10	Turquie	1.4%

Source : Incapsula Global DDoS Threat Landscape Q1 2017. https://www.incapsula.com/ddos- report/ddos-report-q1-2017.html

Principaux pays par % d'adresses IP de pays participant à des attaques DDoS, Q1 - Q4 201661

Q1 2016		Q2 2016		Q3 2016		Q4 2016	
Pays	% des pays Adresses IP	Pays	% des pays Adresses IP	Pays	% des pays Adresses IP	Pays	% des pays Adresses IP
	IPs source		IPs source		IPs source		IPs source
Turquie	0.282%	Vietnam	0.130%	ROYAUME-UNI.	0.036%	Russie	0.078%
	43,400		20,244		44,460		33,211
Brésil	0.075%	Chine	0.093%	Brésil	0.025%	ROYAUME-UNI.	0.059%
	36,472		306,627		81,276		72,949
Chine	0.035%	Taiwan	0.081%	Chine	0.025%	Allemagne	0.042%
	115,478		28,546		81,276		49,408
Corée du Sud	0.028%	Canada	0.026%	France	0.025%	Chine	0.014%
	31,692		20,601		23,980		46,783
U.S.	0.005%	U.S.	0.006%	U.S.	0.004%	U.S.	0.012%
	72,598		95,004		59,350		180,652

Sources :

Rapport d'Akamai sur l'état de la sécurité Internet au quatrième trimestre 2016. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf

Contributeurs Wikipédia, " Liste des pays selon l'attribution des adresses IPv4 ", *Wikipédia, L'encyclopédie libre*,https://en.wikipedia.org/w/index.php?title=List_of_countries_by_IPv4_address_allocation&oldid=776891748 (consulté le 17 juillet 2017).

[61] Le nombre d'IP sources participant à des attaques DDoS est tiré du rapport Akamai State of Internet Security Report Q4 2016. Les données ont été normalisées pour le pourcentage d'adresses IPv4 attribuées à un pays à partir des données de l'IANA au moment de la rédaction de ce document. Les pourcentages peuvent varier quelque peu par rapport au moment de la rédaction du rapport Akamai.

Annexe B - Menaces des botnets

Fraude au clic

Les sites web sont souvent payés par les annonceurs. Les annonceurs paient en fonction du nombre de "clics" ou de visites sur le site Web de l'annonceur. Si un site Web ou un courtier en publicité est capable de donner l'impression que de nombreuses personnes visitent une annonce, il oblige l'annonceur à payer pour chacune de ces visites. Une façon de générer beaucoup de clics est de commander un botnet pour générer ces visites.

Courriel de spam, de phishing ou de malware

Les botnets sont souvent utilisés pour envoyer des courriers électroniques non sollicités en masse, qui peuvent également inclure la distribution de logiciels malveillants de différents types, tels que des ransomwares, des liens vers des sites de phishing et des logiciels malveillants associés à des bots. Les botnets peuvent également être utilisés pour envoyer de la propagande commerciale non sollicitée plus banale.

Passerelle réseau non autorisée

Les bots situés à l'intérieur des limites d'un réseau protégé, tel qu'un réseau d'entreprise, peuvent devenir des passerelles non autorisées vers ces limites et peuvent être utilisés pour accéder à d'autres ressources (données ou ordinateurs) à l'intérieur des limites protégées (mouvement latéral).

Vol de données

Les robots peuvent voler les données des appareils infectés par des moyens tels que la surveillance du réseau, l'enregistrement des clés ou l'extraction de données de la mémoire ou du disque. Ces opérations sont fréquentes car de nombreux membres de robots se trouvent dans des réseaux privés et d'entreprise, à côté des actifs contenant les précieuses données. Aujourd'hui, une grande partie des vols de données est réalisée par des attaques de "Spear Phishing "[62], dans lesquelles des courriels d'apparence valide sont envoyés à une personne au sein d'une entreprise et ce courriel est utilisé pour voler de la propriété intellectuelle ou des informations bancaires, ou pour héberger des logiciels malveillants. Une attaque typique peut consister en l'envoi par le "méchant" d'un courriel à un assistant administratif ou à un autre employé de niveau inférieur, qui semble provenir d'un cadre supérieur, dans lequel le "cadre" demande au destinataire du courriel de réinitialiser un mot de passe parce qu'une "facture doit être payée" aujourd'hui. Le destinataire réinitialisera le

---

[62] Federal Bureau of Investigation (FBI), *Spear Phishers* (1er avril 2009), disponible sur https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109 (consulté le 17 juillet 2017).

mot de passe en utilisant des liens obfusqués contenant des logiciels malveillants dans l'e-mail. Cela permet à l'infection de commencer et à l'installation du logiciel APT (Advanced Persistent Threat) de mener des activités illégales.

Distribution de contenu illicite

Les bots sont parfois connectés à des réseaux de partage de fichiers peer-to-peer pour aider à stocker et à distribuer des contenus illégaux.

Détermination du mot de passe par force brute

Les botnets sont utilisés pour deviner des mots de passe par force brute. Une méthode consiste à tenter de deviner un mot de passe à grande vitesse en utilisant un algorithme de mot de passe aléatoire, un dictionnaire de mots de passe ou une liste de mots de passe prédéfinis. Tout d'abord, le forçage brutal peut être utilisé par un membre individuel du bot comme méthode de recrutement pour infecter d'autres dispositifs en analysant tous les actifs avec un port exposé ouvert connu, puis en mettant en œuvre l'une des méthodes de force brute expliquées pour "deviner" le mot de passe. Deuxièmement, un robot ou un réseau de robots peut utiliser la force brute pour forcer les identifiants de connexion d'une cible afin d'accéder aux privilèges ou aux données que ces identifiants permettent d'obtenir.

Vol de traitement (par exemple, minage de Bitcoin)

En raison du nombre de membres des botnets et de la hausse du prix de la crypto-monnaie (*par exemple, le* bitcoin), les botnets sont très souvent utilisés pour "miner" des pièces. Le processus d'extraction de bitcoins nécessite la résolution d'équations mathématiques très complexes qui, une fois résolues, permettent au mineur d'obtenir un nombre déterminé de pièces. Pour réussir, un mineur a besoin d'une énorme puissance de calcul pour résoudre ces équations en un minimum de temps. C'est là qu'un botnet peut être extrêmement utile. En exploitant la puissance de calcul d'un grand nombre de bots et en "commandant" ces bots pour qu'ils agissent comme des mineurs, le propriétaire du botnet peut utiliser le traitement combiné de nombreux bots pour rendre l'extraction de bitcoins très lucrative.

Les botnets ont également été utilisés pour exploiter la puissance de calcul des appareils infectés afin d'effectuer du minage de bitcoins ou d'autres activités au profit des acteurs malveillants qui gèrent le botnet et non des propriétaires légitimes des ressources informatiques.

Glossaire

AIS - Automated Indicator Sharing, Le département de la sécurité intérieure (DHS) gère un service gratuit d'échange d'indicateurs de cybermenaces.

Bot - Programme installé sur un système afin de permettre à ce système d'exécuter automatiquement (ou semi-automatiquement) une tâche ou un ensemble de tâches, généralement sous la commande et le contrôle d'un administrateur distant (alias bot master ou bot herder).

Botnet - Réseau de dispositifs informatiques d'utilisateurs finaux connectés à l'internet et infectés par des logiciels malveillants, qui sont contrôlés à distance par des tiers à des fins malveillantes.

Command & Control (C&C) - Un ordinateur distant utilisé pour coordonner les actions des bots.

CTI - L'indicateur de cybermenace est l'information nécessaire pour décrire ou identifier l'attribut d'une menace de cybersécurité.

DDoS - L'attaque par déni de service distribué est une tentative de rendre un service en ligne indisponible en le submergeant de trafic provenant de sources multiples.

DNS - Le système de noms de domaine est le système de dénomination hiérarchique et décentralisé des ressources connectées à l'internet.

Torture de l'eau DNS - Type d'attaque dans laquelle de nombreux points finaux envoient des requêtes pour le domaine d'une victime avec une chaîne aléatoire ajoutée au début du domaine, ce qui surcharge le serveur DNS faisant autorité de la victime et rend le domaine de la victime inaccessible.

DOTS - DDoS Open Threat Signaling est une méthode par laquelle un dispositif ou une application participant à l'atténuation DDoS peut signaler à d'autres dispositifs ou applications des informations relatives au traitement actuel des menaces.

ICANN - Internet Corporation for Assigned Names and Numbers est l'organisation à but non lucratif chargée de coordonner la maintenance et les procédures de l'espace de noms de l'internet.

IRC - Internet Relay Chat est un protocole internet qui facilite la communication en texte en utilisant une architecture client/serveur.

IoT - L'internet des objets est le terme générique qui désigne le développement technologique dans lequel un nombre croissant d'appareils sont connectés entre eux et/ou à l'internet.

IPv4 - Internet Protocol version 4 est la quatrième version du protocole Internet (IP). L'IPv4 est l'un des principaux protocoles et achemine encore aujourd'hui la majeure partie du trafic Internet.

IPv6 - Internet Protocol version 6 est la sixième version du protocole Internet (IP). IPv6 est la version la plus récente et a été développée pour répondre au problème anticipé de l'épuisement des adresses IPv4. L'IPv6 est destiné à remplacer l'IPv4.

Kill Chain - Idée avancée par Lockheed Martin pour décrire les phases d'une cyber-attaque ciblée :
1) reconnaissance, 2) armement, 3) livraison, 4) exploitation, 5) installation, 6) commandement et contrôle, et 7) actions.

NAT - Network Address Translation (traduction d'adresses de réseau) est une méthode permettant de remplacer un espace d'adresses IP par un autre en modifiant l'adresse dans les en-têtes des paquets IP afin de permettre à plusieurs points d'extrémité de partager une adresse lorsqu'ils transitent par un routeur de réseau.

Fournisseur de services réseau - Un fournisseur ou opérateur de services réseau est toute entreprise qui exploite un réseau auquel est attribué un numéro de système autonome (ASN).

Peering - Le peering est l'interconnexion volontaire de deux réseaux séparés dans le but d'échanger du trafic entre les utilisateurs de chaque réseau.

Peer-to-Peer (P2P) - Traditionnellement, les clients des botnets communiquent avec un serveur C&C pour recevoir des commandes. Les botnets P2P fonctionnent sans serveur C&C, chaque bot étant à la fois client et serveur.

Software Defined Networking (SDN) - Approche de la mise en réseau informatique qui permet le contrôle programmatique du comportement du réseau à l'aide d'interfaces ouvertes et le découplage du plan d'acheminement des paquets du plan de contrôle afin de permettre l'utilisation de serveurs standard et de commutateurs Ethernet pour assurer la fonction de routage au lieu de routeurs spécialisés.

SSAC - Le comité consultatif sur la sécurité et la stabilité conseille la communauté et le conseil d'administration de l'ICANN sur les questions relatives à la sécurité et à l'intégrité des systèmes d'attribution de noms et d'adresses de l'Internet.

Tarpit - Un tarpit est un ordinateur qui retarde délibérément les connexions entrantes. Il s'agit d'une mesure défensive visant à ralentir le spamming et le balayage du réseau. Il est analogue à une fosse de goudron dans laquelle les animaux peuvent s'enliser et s'enfoncer lentement sous la surface.

Transit - Le transit Internet est un service qui permet au trafic réseau de "transiter" par un réseau pour atteindre un autre réseau. Les petits opérateurs de réseau et les entreprises achètent du transit Internet pour accéder à l'Internet.

Mars 2012

Rapport final

Code de conduite anti-robot américain (ABC) pour les fournisseurs d'accès à Internet (FAI)

(Un code volontaire)

"Ce code de conduite serait un grand pas en avant et un complément important aux efforts plus larges de l'administration contre les botnets."

Julius Genachowski, président de la FCC
22 février 2012

GROUPE DE TRAVAIL 7 - Remédiation des botnets

Table des matières

1 Résultats en bref

1.1 Résumé exécutif

Un "bot" malveillant est un programme installé sur un système afin de permettre à ce dernier d'exécuter automatiquement une tâche ou un ensemble de tâches, généralement sous la commande et le contrôle d'un administrateur distant malveillant. L'augmentation du nombre de dispositifs d'utilisateurs finaux infectés par des robots1 représente une menace significative pour la vitalité et la résilience de l'internet et de l'économie en ligne.

Les réseaux de zombies sont des réseaux de dispositifs informatiques d'utilisateurs finaux connectés à l'Internet et infectés par des logiciels malveillants de zombies, qui sont contrôlés à distance par des tiers à des fins malveillantes. Les bots et les réseaux de bots peuvent entraîner le vol d'informations personnelles, des attaques contre des réseaux publics et privés, ainsi que l'exploitation de la puissance de calcul et de l'accès à l'internet des utilisateurs finaux.

Le CSRIC III a chargé le groupe de travail 7, Botnet Remediation, de proposer un ensemble de pratiques volontaires convenues qui constitueraient le cadre d'un modèle de mise en œuvre opt-in à suivre par les FAI pour atténuer la menace des botnets. En réponse à cette proposition, le code de conduite anti-bot américain pour les FAI a été élaboré pour répondre à la menace des bots et des botnets dans les réseaux résidentiels à large bande par une participation volontaire. Lors de l'élaboration du code, il a été déterminé que les composantes de l'ensemble de l'écosystème Internet ont un rôle important à jouer dans la lutte contre la menace des botnets et que les FAI dépendent du soutien des autres parties de l'écosystème.

Le Code encourage les ISP à participer à des activités visant à soutenir l'éducation des utilisateurs finaux afin de prévenir les infections par des bots, la détection des bots, la notification des infections potentielles par des bots, la remédiation des bots, ainsi que la collaboration et le partage des informations provenant des participants au Code. Le Code est inclus dans l'annexe.

Le groupe de travail a proposé un ensemble de pratiques volontaires convenues qui constitueraient le cadre d'un modèle de mise en œuvre opt-in pour les FAI afin de contribuer à la lutte contre la menace des botnets. Le groupe de travail recommande des mesures que les FAI offrant un accès Internet résidentiel à large bande peuvent prendre s'ils choisissent d'adopter le code. Le groupe de travail recommande également aux FAI et aux autres fournisseurs de services d'indiquer qu'ils acceptent de participer au code volontaire en contactant l'organisation industrielle qui gère la participation au code. Dans un premier temps, il est suggéré que les FAI et autres fournisseurs de services participants informent l'entité de leur choix de leur participation au code ou s'auto-affirment sur leur propre site Web. Les travaux futurs comprennent la détermination de l'administration à long terme de la participation au code, les mises à jour périodiques du code, l'identification des obstacles à la participation au code, la définition de paramètres et l'identification des meilleures pratiques et des leçons apprises parmi les participants au code et les contributeurs de l'écosystème de soutien.

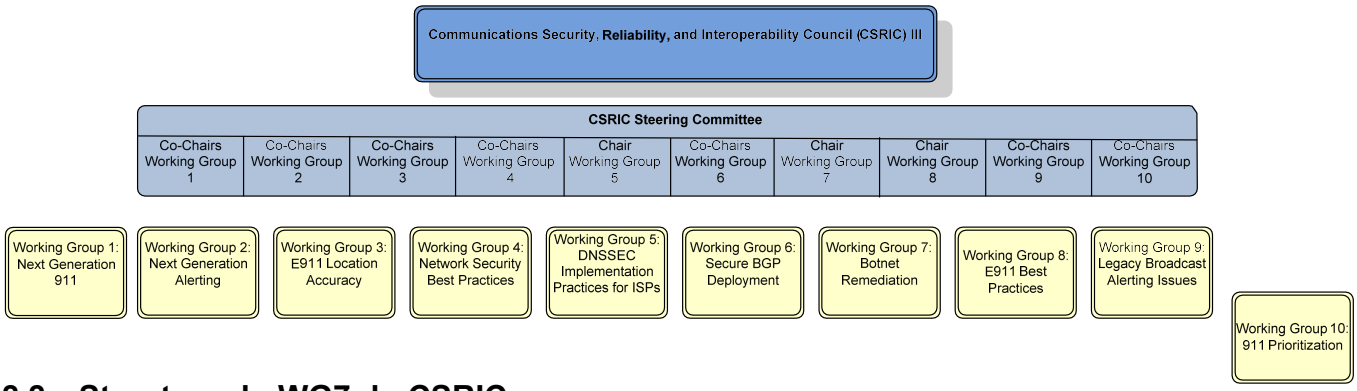
[1] Les termes "bot" et "infection par un bot" sont utilisés indifféremment dans ce document.

2 Introduction

Le CSRIC III a établi le groupe de travail 7 (WG7) pour aborder la remédiation des botnets dans les réseaux à large bande. Le WG7 a étudié les travaux sur la remédiation des botnet qui ont lieu à l'IETF, au Japon, en Australie, en Finlande, en Allemagne et ailleurs afin de déterminer la meilleure approche pour traiter la menace des botnet dans les réseaux à large bande des États-Unis.

Le résultat de ce travail est le code de conduite anti-bot volontaire des États-Unis pour les fournisseurs de services Internet, qui se trouve en annexe.

2.1 Structure du CSRIC



2.2 Structure du WG7 du CSRIC

Le WG7 est présidé par Michael O'Reirdan, président du Messaging Anti-Abuse Working Group (MAAWG), et vice-présidé par le Dr Peter Fonash, Chief Technology Officer, Office of Cybersecurity and Communications, Department of Homeland Security. Les membres du WG7 comprennent des représentants des FAI, des fournisseurs de logiciels et d'équipements de réseau, du monde universitaire, ainsi que d'autres organisations faisant partie de l'écosystème Internet.

2.3 Membres de l'équipe du groupe de travail 7

Le groupe de travail 7 est composé des membres énumérés ci-dessous.

Nom	Entreprise
Michael O'Reirdan - Président	MAAWG
Peter Fonash - Vice-Président	Département de la sécurité intérieure
Neil Schwartzman - Secrétaire	CAUCE
Robert Thornberry - Rédacteur en chef	Bell Labs, Alcatel-Lucent
Paul Diamond - Rédacteur en chef	CenturyLink
Vernon Mosley - Liaison	FCC
Alex Bobotek	AT&T
Adam O'Donnell	Sourcefire
Alfred Huger	Sourcefire
Barry Greene	ISC
Bill McInnis	IID
Bill Smith	PayPal
Brian Done	Département de la sécurité intérieure
Chris Roosenraad	Time Warner Cable
Chris Sills	IID
Craig Spiezle	Alliance pour la confiance en ligne (OTA)
Daniel Bright	EMC
Eric Osterweil	Verisign
Gabe Iovino	REN-ISAC
Greg Holzapfel	Sprint
Gunter Ollmann	Damballa
James Holgerson	Sprint
Jay Opperman	Comcast
Joe St Sauver	Université de l'Oregon et Internet2
Johannes Ullrich	Institut SANS
John Denning	Banque d'Amérique
John Griffin	Telecommunication Systems Inc.
John St. Clair	Verizon
Jon Boyens	Institut national des normes et de la technologie
Kevin Sullivan	Microsoft
Kurian Jacob	FCC
Matt Carothers	Cox
Maxim Weinstein	StopBadware
Merike Kaeo	ISC
Michael Fiumano	Sprint
Michael Glenn	CenturyLink
Robert Mayer	USTelecom
Tice Morgan	T-Mobile
Tim Rohrbaugh	Intersections
Timothy Vogel	Verizon

Tableau 1 - Liste des membres du groupe de travail 7

3 Objectif, portée et méthodologie

2.3 Objectif

Le CSRIC a chargé le groupe de travail 7, Botnet Remediation, de proposer un ensemble de pratiques volontaires convenues qui constitueraient le cadre d'un modèle de mise en œuvre opt-in à suivre par les FAI afin d'atténuer la menace des botnets. En réponse, le code de conduite anti-bot américain pour les FAI a été développé pour répondre à la menace des bots et des botnets dans les réseaux résidentiels à large bande par une participation volontaire.

2.4 Portée

Cette section identifie l'énoncé du problème, la description du groupe de travail, et les livrables décrits dans la charte CSRIC III pour le groupe de travail 7.

Énoncé du problème : La croissance des dispositifs d'utilisateurs finaux infectés par des robots2 représente une menace significative pour la vitalité et la résilience de l'Internet et de l'économie en ligne. Les réseaux de zombies sont des réseaux de dispositifs informatiques d'utilisateurs finaux connectés à l'internet et infectés par des logiciels malveillants, qui sont contrôlés à distance par des tiers à des fins malveillantes. Les bots et les réseaux de bots peuvent entraîner le vol d'informations personnelles, des attaques contre des réseaux publics et privés et l'exploitation de la puissance de calcul et de l'accès à l'internet des utilisateurs finaux.

Afin de réduire les infections par des bots dans les appareils des utilisateurs finaux résidentiels et d'atténuer l'exploitation potentielle des bots, les membres du groupe de travail 7 ont élaboré le code de conduite anti-bot volontaire des États-Unis pour les fournisseurs de services Internet.

Groupe de travail 7 Description : Ce groupe de travail examinera les efforts entrepris au sein de la communauté internationale, tels que le code de pratique australien de l'industrie de l'Internet, et parmi les groupes d'intervenants nationaux, tels que l'IETF et le Messaging Anti-Abuse Working Group, pour leur applicabilité aux ISP américains. En s'appuyant sur les travaux du groupe de travail 8 du CSRIC II sur les pratiques de protection des réseaux des FAI, le groupe de travail sur la remédiation des botnets proposera un ensemble de pratiques volontaires convenues qui constitueront le cadre d'un modèle de mise en œuvre opt-in pour les FAI. Le groupe de travail proposera une méthode permettant aux FAI d'exprimer leur intention d'adhérer au cadre proposé par le groupe de travail. Le groupe de travail identifiera également les obstacles potentiels à la mise en œuvre du code nouvellement rédigé par les FSI et identifiera les mesures que la FCC peut prendre pour aider à surmonter ces obstacles. Enfin, le groupe de travail identifiera des mesures de performance pour évaluer l'efficacité du code à freiner la propagation des infections par les zombies.

[2] Les termes "bot" et "infection par un bot" sont utilisés indifféremment dans ce document.

Livrables du rapport :

1. Code de conduite anti-bot pour les FAI des États-Unis : 22 mars 2012
2. Obstacles à la participation au code : 12 septembre 2012
3. Mesures de performance de la remédiation des bot : 5 décembre 2012

Ce rapport, intitulé U.S. Anti-Bot Code of Conduct for ISPs, est le premier de trois rapports livrables pour le groupe de travail 7.

2.5 Méthodologie

Le groupe de travail 7 a commencé ses recherches sur l'élaboration d'un code de conduite anti-bot volontaire américain pour les FAI en réunissant une équipe d'experts de l'industrie, du gouvernement et du milieu universitaire, représentant diverses parties prenantes dans l'élaboration et la mise en œuvre du code. Le groupe de travail 7 a examiné les efforts entrepris au sein de la communauté internationale, y compris le code de pratique australien de l'industrie de l'Internet et le centre japonais Cyber Clean, et parmi les groupes de parties prenantes nationales, y compris l'Internet Engineering Task Force (IETF) et le Messaging Anti-Abuse Working Group, pour l'applicabilité aux ISP américains. S'appuyant sur les travaux du groupe de travail 8 du CSRIC II, Pratiques de protection du réseau des ISP, le groupe de travail 7 du CSRIC III a établi des conférences téléphoniques bihebdomadaires entre ses membres pour discuter du développement, du contenu et de la pertinence des efforts connexes en vue de l'établissement d'un code de conduite anti-bot américain pour les ISP. Le groupe de travail 7 a coordonné ses efforts d'élaboration du code avec le département du commerce et le personnel de la sécurité nationale de la Maison Blanche par le biais de conférences téléphoniques régulières afin de discuter des domaines d'intérêt commun en matière de remédiation des botnets. Le groupe de travail 7 a organisé deux réunions en face à face avec ses membres, l'une en novembre 2011 pour développer la structure et discuter du contenu des sections du projet de code, et une dernière réunion en face à face en février 2012 pour examiner le projet de code final. Le code de conduite anti-bot américain pour les fournisseurs de services Internet qui en résulte est basé sur la contribution collective des membres du groupe de travail 7 et sur les discussions que ces membres et leurs entreprises ont eues avec d'autres parties prenantes pour réduire l'incidence des infections par les robots.

3 Contexte3

Un "bot" malveillant ou potentiellement malveillant est un programme installé sur un système afin de permettre à ce système d'exécuter automatiquement (ou semi-automatiquement) une tâche ou un ensemble de tâches, généralement sous le commandement et le contrôle d'un administrateur distant malveillant, ou "bot master". Les bots sont également connus sous le nom de "zombies". Ces robots peuvent avoir été installés subrepticement, sans que l'utilisateur comprenne bien ce qu'ils feront une fois installés, à son insu, dans le cadre de l'installation d'un autre logiciel, sous de faux prétextes ou de diverses autres manières.

Les appareils utilisés par les internautes peuvent être infectés par des logiciels malveillants qui peuvent contenir ou installer un ou plusieurs bots sur un appareil. Ils peuvent poser un problème majeur pour plusieurs raisons. Tout d'abord, ces bots peuvent être utilisés pour envoyer du spam, dans certains cas de très gros volumes de spam. Ce spam peut entraîner des coûts supplémentaires pour les FAI en termes de gaspillage de ressources réseau, de serveurs ou de personnel, entre autres.

[3] Voir les recommandations pour la remédiation des bots dans les réseaux des FAI, http://tools.ietf.org/rfc/rfc6561.txt.

de nombreux autres coûts et effets secondaires potentiels. Ces spams peuvent également nuire à la réputation du fournisseur d'accès, de ses clients et de l'espace d'adressage IP utilisé par le fournisseur d'accès (souvent appelé simplement "réputation IP").

En outre, ces bots peuvent servir de plates-formes pour diriger, participer ou mener des attaques sur des infrastructures Internet critiques. Les bots sont fréquemment utilisés dans le cadre d'attaques coordonnées par déni de service distribué (DDoS) pour des motifs criminels, politiques ou autres.

Le rôle des FAI dans la fourniture de services aux utilisateurs d'Internet les place en position de pouvoir tenter de détecter et d'observer les botnets opérant sur leurs réseaux. En outre, les FAI peuvent également être en mesure d'informer leurs clients d'une infection réelle, potentielle ou probable par des bots.

Du point de vue de l'utilisateur final, le fait d'être informé qu'un dispositif infecté se trouve sur son réseau constitue une information importante. Une fois qu'ils le savent, ils peuvent prendre des mesures pour supprimer les bots, résoudre les problèmes qui peuvent résulter de l'infection par le bot et se protéger contre les menaces futures.

Le groupe de travail 7 a élaboré le code de conduite anti-bot volontaire des États-Unis à l'intention des FAI afin de lutter contre la menace des bots et des botnets, décrite ci-dessus, dans les réseaux résidentiels à large bande. L'adoption de ce code par les ISP est volontaire. Elle n'est pas obligatoire.

4 Recommandations

4.1 Recommandations

Le groupe de travail a proposé un ensemble de pratiques volontaires convenues qui constitueraient le cadre d'un modèle de mise en œuvre opt-in pour les FAI afin de contribuer à la lutte contre la menace des botnets. Le groupe de travail recommande des mesures que les FAI offrant un accès Internet résidentiel à large bande peuvent prendre s'ils choisissent d'adopter le code. Le groupe de travail recommande en outre aux FAI et aux autres fournisseurs de services d'indiquer qu'ils acceptent de participer au code volontaire en contactant l'organisation industrielle qui gère en dernier ressort la participation au code. En tant que code de conduite volontaire élaboré par l'industrie et pour l'industrie, l'objectif est qu'un forum industriel neutre reçoive et rassemble les rapports relatifs à la participation au code.
Dans un premier temps, pour indiquer leur participation, il est suggéré aux ISP et autres fournisseurs de services participants de notifier à l'entité de leur choix leur participation au Code ou de s'auto-affirmer sur leur propre site web.

5.1.1 Travaux futurs

Ce rapport, le code de conduite anti-bot volontaire des États-Unis pour les fournisseurs de services Internet, est le premier de trois rapports livrables pour le groupe de travail 7. Il reste à aborder l'administration à long terme du code et les mises à jour périodiques. Ensuite, le groupe de travail identifiera les obstacles potentiels à la participation au code. Enfin, le groupe de travail identifiera les mesures de performance potentielles en matière de lutte contre les robots.

Les travaux futurs devraient porter sur les mécanismes de diffusion des infections par les zombies à partir de sites web et de services d'hébergement infectés et malveillants, afin que les efforts du GT7 deviennent omniprésents et donc efficaces.

5.1.2 Remerciements

Le GT7 souhaite remercier Yurie Ito du CERT japonais pour sa présentation informative et sa discussion sur les leçons tirées du Japan Cyber Clean Center, le programme anti-botnet du Japon. Nous remercions également Ari Schwartz du National Institute of Standards (NIST) pour sa présentation sur la menace des botnets et les stratégies d'atténuation. Le GT7 remercie également Microsoft, le MAAWG et la FCC pour avoir accueilli les réunions du GT7.

Le GT 7 tient à remercier tout particulièrement les membres suivants du groupe dont les efforts soutenus ont contribué massivement au processus d'élaboration du Code :

Robert Thornberry, de Bell Labs, Alcatel-Lucent (éditeur) Paul
Diamond, CenturyLink (éditeur)
Joe St Sauver, Université de l'Oregon et Internet2 (Glossaire) Neil
Schwartzman, CAUCE (Secrétaire)

5 Conclusions

En réponse à la mission confiée par le CSRIC III au groupe de travail 7, le code de conduite anti-bot volontaire américain pour les FAI a été développé pour répondre à la menace des bots et des botnets dans les réseaux résidentiels à large bande par une participation volontaire. Lors de l'élaboration du code, il a été déterminé que les composants de l'ensemble de l'écosystème Internet ont des rôles importants à jouer dans la lutte contre la menace des botnets et que les FAI dépendent du soutien des autres parties de l'écosystème.

Ce rapport du 22 mars 2012, intitulé U.S. Anti-Bot Code of Conduct for ISPs, est le premier de trois rapports livrables pour le groupe de travail 7. Ensuite, le groupe de travail identifiera les obstacles potentiels à la participation au code, avec un rapport à venir en septembre 2012. Enfin, le groupe de travail identifiera les paramètres de performance de l'élimination des botnets et soumettra son rapport sur ce sujet en décembre 2012.

6 Annexe

Code de conduite anti-bot (ABC) des États-Unis à l'intention des fournisseurs de services Internet (FSI) pour lutter contre l'activité des robots dans les réseaux à large bande

Final 22
mars 2012

1. Introduction

La croissance des *dispositifs d'utilisateurs finaux *infectés par des bots représente une menace significative pour la vitalité et la résilience de l'Internet et de l'économie en ligne. Notez que les termes "infection par un bot" et "bot" sont utilisés comme synonymes dans ce document pour désigner un dispositif d'utilisateur final infecté par un logiciel malveillant de type bot. Les réseaux de zombies sont des réseaux d'appareils informatiques d'utilisateurs finaux connectés à Internet et infectés par des logiciels malveillants de zombies.*qui sont contrôlés à distance par des tiers à des fins malveillantes.

Les bots et les réseaux de bots peuvent entraîner le vol d'informations personnelles, des attaques contre des réseaux publics et privés et l'exploitation de la puissance de *calcul et de l'accès à l'internet des utilisateurs finaux. Le public est peu sensibilisé aux bots, à leur impact et aux problèmes de sécurité et de confidentialité qui en découlent. Ce code de conduite volontaire (le "Code") fournit un ensemble de principes et d'activités recommandés que les fournisseurs de services Internet peuvent adopter pour aider à faire face aux menaces présentées par la présence de bots et de botnets dans les réseaux résidentiels à large bande.

Il convient de reconnaître que les bots ont un impact sur l'ensemble de l'écosystème Internet *et que pour réussir à les réduire ou à atténuer leur impact, il faudra une action collective de toutes les parties de cet écosystème, notamment les utilisateurs finaux, les développeurs de logiciels, les fournisseurs de services de recherche, les sites Web, les sites de commerce électronique, etc. Les dispositifs des utilisateurs finaux échappent au contrôle des FAI, c'est *pourquoi tous les participants de l'écosystème Internet doivent travailler ensemble pour résoudre ce problème. Le présent Code vise à jeter les bases d'une future coordination entre les différentes parties prenantes en définissant un ensemble d'actions adaptées au rôle limité que les FAI peuvent jouer pour contribuer à résoudre ce problème important.
Le Code reconnaît la variabilité substantielle de la taille, des ressources, des modèles et environnements commerciaux, de l'expertise et des capacités des FAI aux États-Unis. Le succès des activités des FSI repose sur des efforts similaires de la part des autres acteurs de l'Internet.

Les exigences fondamentales de la participation à ce code sont énoncées à la section 5. Les autres sections de ce document contiennent des informations de base ou des explications supplémentaires.

---

* Définition trouvée dans le glossaire

2. Définitions des termes clés

Note au lecteur :

Toute discussion sur les bots implique inévitablement un vocabulaire technique unique. Sachant que de nombreux lecteurs peuvent ne pas être familiers avec certains de ces termes spécialisés, le Code comprend un glossaire à l'annexe 2. Tout terme apparaissant dans le glossaire sera marqué d'un astérisque "*" dans le corps du texte du Code la première fois qu'il apparaîtra afin d'avertir le lecteur qu'une définition est disponible dans le glossaire.

3. Objectifs et principes

a. Les objectifs de ce code sont les suivants :

1. Fournir un cadre initial permettant aux FAI de mieux comprendre et d'aider à résoudre le problème des bots ; et

2.

• Informez les utilisateurs finaux de la menace que représentent les bots et des mesures qu'ils peuvent prendre pour prévenir les infections par les bots ;

• Détecter les activités des robots ou obtenir des informations, y compris auprès de tiers crédibles, sur les infections par des robots dans leur base d'utilisateurs finaux ;

• notifier aux utilisateurs finaux les infections suspectées par des bots ou aider les utilisateurs finaux à déterminer s'ils sont potentiellement infectés par des bots ; et

• Fournir des informations et des ressources, directement ou par référence à d'autres sources, aux utilisateurs finaux pour les aider à remédier aux infections par des robots.

b. La mise en œuvre du code sera guidée par les principes suivants :

1. Volontaire - la participation est volontaire et encourage les types d'actions à entreprendre par les ISP, cependant ce code n'exige aucune activité particulière.

2. Neutralité technologique - ce code ne prescrit pas de moyens ou de méthodes particuliers.

3. Neutralité de l'approche - ce code ne prescrit aucune approche particulière pour la mise en œuvre d'une partie de ce code.

4. Respect de la vie privée - Les FAI doivent traiter les questions de vie privée d'une manière appropriée et conforme aux lois applicables.

5. Conformité juridique - les activités doivent être conformes au droit applicable.

6. Une responsabilité partagée - Les FAI, agissant seuls, ne peuvent pas répondre entièrement à la menace posée par les bots. Les autres participants de l'écosystème Internet doivent également faire leur part.

7. Durabilité - Les ISP doivent rechercher des activités qui sont rentables et durables dans le contexte de leurs modèles économiques.

8. Partage d'informations - Les FSI doivent indiquer comment ils participent au Code et partager les enseignements tirés de leurs activités avec les autres parties prenantes appropriées. Tout partage d'informations entre les ISP et les autres parties concernées doit être effectué conformément aux lois applicables, y compris, mais sans s'y limiter, les lois antitrust et sur la protection de la vie privée.

9. Efficacité - Les PSI doivent être encouragés à s'engager dans des activités qui ont été démontrées comme étant appropriées et efficaces.

10. Communication efficace - La communication avec les clients *doit tenir compte de diverses questions telles que la langue et s'assurer que les informations sont fournies d'une manière dont on peut raisonnablement penser qu'elle sera comprise et accessible par les destinataires.

4. Champ d'application et rôles

Ce Code a été rédigé spécifiquement pour les ISP et autres fournisseurs de services offrant un service d'accès Internet à large bande aux utilisateurs finaux résidentiels. Les activités de ce Code peuvent être adaptées pour être utilisées par d'autres fournisseurs d'accès Internet et participants.

Ce code n'est pas censé être une approche globale de la sécurité en ligne, mais il est destiné à coexister avec d'autres efforts actuels et futurs. Il prévoit un rôle important pour les autres participants de l'écosystème Internet, y compris, mais sans s'y limiter :

- Vendeurs de logiciels de sécurité
- Développeurs de systèmes d'exploitation
- Organisations axées sur l'utilisateur final
- Fournisseurs de contenu, d'applications et de services Internet

La sécurité en ligne doit inclure une approche flexible et à multiples facettes, utilisant des conseils et des outils provenant de diverses sources réputées.

a. Définition du succès

Le succès initial de ce code sera évalué en fonction de la participation de la communauté des FAI. Cependant, le soutien de l'écosystème Internet dans son ensemble est considéré comme primordial pour le succès final de la lutte contre les bots.

b. Avantages de la participation au code

Les avantages de haut niveau suivants peuvent résulter d'une participation significative des PSI à ce code :

- Sécurité accrue des informations et des appareils des utilisateurs finaux et de l'infrastructure américaine ;
- Sensibilisation accrue des utilisateurs finaux, des fournisseurs d'accès à Internet et des autres acteurs du secteur de l'Internet à la menace des robots et à la manière de la combattre ;

---

* Définition trouvée dans le glossaire

- Notification* et remédiation* de l'activité des robots sur les appareils des utilisateurs finaux infectés par des robots ;
- Création d'un environnement dans les réseaux résidentiels à large bande américains qui est encore plus hostile au déploiement et à l'utilisation des bots ; et
- Développement et utilisation plus large d'architectures et d'outils de notification et de remédiation efficaces chez les utilisateurs finaux et les FAI.

Certains FAI participant au processus d'élaboration du Code et ayant déjà mis en œuvre certains de ses aspects ont obtenu des résultats bénéfiques dans des domaines tels que la diminution du nombre d'appels aux services d'assistance de la part de clients dont les machines sont infectées, la réduction de la consommation de la bande passante en amont par les attaques par déni de service et le spam*une augmentation de la clientèle et une diminution du taux de désabonnement, ainsi qu'une réduction des plaintes liées au spam de la part d'autres FAI. Bien que les résultats individuels puissent varier, les FAI sont encouragés à rechercher les moyens spécifiques par lesquels la participation au Code renforce leur activité globale en matière de large bande, et à partager ces expériences avec d'autres FAI. En outre, la participation des ISP à ce Code peut permettre aux ISP de générer des mesures tangibles relatives à l'impact d'activités spécifiques sur les opérations commerciales à large bande globales des ISP, ce qui peut à son tour soutenir le développement ou le déploiement d'autres activités anti-bot.

* Définition trouvée dans le glossaire

5. Paramètres de participation

La participation à ce code est volontaire.

Exigences de participation au Code de Conduite Volontaire

Pour participer à ce Code, un ISP s'engagera dans au moins une activité (c'est-à-dire qu'il prendra des mesures significatives) dans chacun des domaines généraux suivants :

- Éducation - activité visant à sensibiliser les utilisateurs finaux aux problèmes des botnets et à la manière de prévenir les infections par ces derniers ;
- Détection - activité visant à identifier l'activité des botnets dans le réseau du FAI, à obtenir des informations sur l'activité des botnets dans le réseau du FAI ou à permettre aux utilisateurs finaux de déterminer eux-mêmes les infections potentielles par des botnets sur leurs appareils ;
- Notification - activité destinée à informer les clients des infections suspectes par des robots ou à permettre aux clients de déterminer s'ils sont infectés par un robot ;
- Remédiation - activité destinée à fournir des informations aux utilisateurs finaux sur la façon dont ils peuvent remédier aux infections par des robots, ou à aider les utilisateurs finaux à remédier aux infections par des robots.
- Collaboration - une activité visant à partager avec d'autres PSI le retour d'information et l'expérience acquise dans le cadre des activités du Code du PSI participant.

La notion d'"au moins une activité" dans chacun de ces domaines généraux vise à encourager un certain niveau d'activité dans chacun des cinq domaines susmentionnés dans le cadre d'un processus national global visant à créer un environnement dans les réseaux résidentiels à large bande américains qui soit encore plus hostile au déploiement et à l'utilisation des bots. L'objectif est de soutenir et d'encourager un large éventail d'efforts flexibles pour expérimenter et innover avec diverses méthodes d'éducation, de détection, de notification et de remédiation.*de détection, de notification et de remédiation. Dans le même ordre d'idées, l'obligation de partager le retour d'information avec d'autres FAI ne vise pas à imposer des moyens ou des méthodes spécifiques de partage de ce retour d'information.

* Définition trouvée dans le glossaire

6. Éducation des utilisateurs finaux

a. Vue d'ensemble

Les utilisateurs finaux sont responsables en dernier ressort de la protection de leurs appareils et de l'élimination d'un appareil infecté. Les FAI, comme de nombreux autres participants à l'Internet et acteurs gouvernementaux, peuvent aider à éduquer les utilisateurs finaux sur les menaces présentées par les bots et les mesures que les utilisateurs finaux peuvent prendre pour protéger leurs appareils et remédier aux infections.

b. Action recommandée :

1. Éducation à la prévention du bot*:

Les fournisseurs de services Internet doivent mettre à disposition des informations sur la prévention des infections par les robots et les questions connexes. Au minimum, ces informations devraient inclure :

- Comment et pourquoi les utilisateurs finaux doivent maintenir leurs logiciels à jour pour les ordinateurs et les appareils dont les mises à jour logicielles sont facilement accessibles.
- L'importance d'utiliser un logiciel de sécurité efficace et à jour provenant d'un fournisseur réputé.
- L'importance de sauvegarder les données et les logiciels des utilisateurs et comment le faire efficacement.
- Actions de base de l'utilisateur final pour minimiser l'exposition aux infections par des robots lors de l'utilisation d'Internet.

On s'attend à ce que de nombreux ISP puissent atteindre cet objectif en fournissant ces informations directement à leurs abonnés ou en établissant des liens avec des sources existantes et accessibles au public.

2. Soutien aux efforts de remédiation des bots des utilisateurs finaux :

En plus des informations sur la prévention, les FAI devraient mettre à disposition (par exemple, par le biais de leurs publications, de publications de tiers ou de liens Internet) des informations sur la manière dont les utilisateurs finaux peuvent généralement remédier aux infections par des robots. Dans ce domaine, les FAI devraient être en mesure d'atteindre cet objectif en créant des liens vers des sources d'information existantes et accessibles au public ou en créant de nouvelles sources d'information, soit individuellement, soit en collaboration avec d'autres.

Dans le cadre de leurs activités de notification aux utilisateurs finaux, les FAI devraient inclure dans ces notifications ou par d'autres moyens des informations sur les endroits où le destinataire peut se tourner pour obtenir des informations et une assistance supplémentaires. Ces informations peuvent inclure des liens vers des informations en ligne accessibles au public, des outils de sécurité ou des suggestions pour obtenir l'aide d'un professionnel de l'informatique. Les sujets et références supplémentaires qu'un ISP pourrait souhaiter inclure sont les suivants :

---

* Définition trouvée dans le glossaire

- Risques pour l'utilisateur final et la communauté Internet d'utiliser un appareil que l'on pense infecté,
- Comment identifier et supprimer les formes courantes d'infections par des robots,
- des outils ou des services accessibles au public (gratuits ou payants) pour faciliter la détection et la suppression des infections par des robots, et
- Des conseils pour savoir où trouver une assistance supplémentaire (gratuite ou payante).

3. Directives :

Pour répondre aux exigences ci-dessus, les FAI doivent tenir compte des directives suivantes :

- Offrir des informations et des ressources éducatives directement ou en renvoyant à des services tiers.
- Faites en sorte que le contenu éducatif soit concis et se concentre sur les éléments les plus importants que les utilisateurs doivent connaître.
- S'assurer que les instructions peuvent être suivies par un public d'utilisateurs non techniques.
- Utilisez plusieurs médias, par exemple des images, des vidéos, du texte, des légendes, etc., et, le cas échéant, plusieurs langues pour optimiser la compréhension et l'accessibilité des clients.
- Aidez les utilisateurs finaux à déterminer s'ils sont infectés par un bot en fournissant des informations ou en pointant vers des ressources qui décrivent les comportements anormaux des appareils infectés par un bot et la disponibilité et l'utilisation d'outils ou de services logiciels de détection des bots.

7. Détection de bot

a. Vue d'ensemble

Les outils et techniques utilisés pour détecter les bots évoluent au même rythme que ceux-ci. Le défi de la détection réside dans la polyvalence que le trafic des bots a atteint pour éviter de nombreuses techniques singulières utilisées pour les mécanismes de détection, comme la simple correspondance de motifs. La détection peut être compliquée par le fait que certaines applications Internet, comme les réseaux de diffusion de contenu en cache basés sur l'hôte distribué, les applications de jeux en ligne et d'autres services de ce type, peuvent avoir un comportement similaire à celui des bots malveillants et utiliser des technologies similaires. Les fournisseurs d'accès à Internet doivent veiller à identifier les parties touchées afin de les notifier et d'y remédier.

b. Action recommandée :

Les FAI peuvent s'informer sur les activités malveillantes et les appareils d'utilisateurs finaux compromis par des robots de différentes manières :

1. Recevoir des notifications d'entités externes, notamment celles conçues pour aider à la compréhension globale et à la diffusion en temps réel des données relatives aux bots. Une liste de ressources est présentée à l'annexe 2.

2. Déployer au sein de leurs réseaux des capacités permettant d'identifier les infections potentielles par des robots.

3. Orienter les clients vers des outils, un portail web ou d'autres ressources qui leur permettent d'identifier eux-mêmes une infection potentielle par un bot.

8. Notification à l'utilisateur final d'une infection potentielle par un bot

a. Vue d'ensemble :

De nombreux utilisateurs finaux ne savent pas que leurs appareils sont infectés et fonctionnent comme des robots. Par conséquent, ces utilisateurs et leurs données restent à risque, et les bots peuvent rester actifs indéfiniment. Les fournisseurs de services Internet devraient tirer parti des efforts de détection décrits à la section 7 pour informer les clients des infections actives.

Les notifications doivent être conçues pour aider à limiter les bots et les dommages qu'ils causent. Les notifications peuvent contenir des informations sur ce qu'est un bot, les moyens d'infection, le fait que les bots peuvent ne présenter aucun symptôme visible et la signification de la notification. Les notifications peuvent également contenir ou identifier d'autres ressources telles que des outils, des guides et des services qui facilitent la prévention, la vérification et l'atténuation des infections.*. Elles peuvent également fournir des informations sur un ou plusieurs bots spécifiques détectés.

La notification à l'utilisateur final peut prendre de nombreuses formes différentes. Elle peut être effectuée directement par le FAI ou par des tiers pour le compte du FAI. Les FAI peuvent alerter directement les utilisateurs finaux ou fournir des mécanismes permettant aux utilisateurs finaux de demander et de recevoir des informations sur l'état de leur infection. De même, les FAI peuvent conclure des accords pour que les notifications soient transmises aux utilisateurs finaux par d'autres participants de l'écosystème avec lesquels l'utilisateur final est en relation, comme un fournisseur d'applications ou de services Internet.

Le fournisseur de services Internet devrait envisager des mécanismes qui garantissent que le client peut facilement authentifier l'authenticité des notifications et que ces notifications seront difficiles à falsifier.

Dans la mesure du possible, le PSI peut souhaiter suivre la réception des notifications. Cela peut aider le FAI à mieux comprendre l'efficacité des différents mécanismes de notification.

Chaque fournisseur de services Internet devra évaluer différentes méthodes de notification afin de trouver celle qui est la mieux adaptée à son cas particulier et à la menace que représentent les robots. La méthode de notification choisie devra peut-être s'intégrer aux processus opérationnels et au réseau existants.

---

* Définition trouvée dans le glossaire

l'infrastructure. Des recherches et des analyses peuvent être nécessaires pour développer et maintenir des systèmes et des politiques de notification appropriés.

b. Action recommandée :

Communiquer au client une suspicion d'infection par un bot ou aider les clients à déterminer s'ils sont potentiellement infectés par des bots. De nombreuses méthodes de notification sont décrites dans les références de l'annexe 2 ; toutefois, d'autres méthodes peuvent être utilisées.

9. Remédiation du bot

a. Vue d'ensemble

L'atténuation et l'élimination des zombies sont l'objectif ultime de tout programme de notification d'infection par des zombies et relèvent en fin de compte de la responsabilité de l'utilisateur final. La notification seule peut être suffisante pour les utilisateurs techniques, mais la majorité des utilisateurs ont généralement besoin d'une certaine forme d'assistance pour supprimer les logiciels malveillants de leurs appareils infectés. La remédiation peut toutefois s'avérer difficile et impliquer d'autres fonctions complexes, telles que l'isolement de la source de l'infection parmi de nombreux appareils partageant une connexion Internet, la sauvegarde préalable de toutes les données et de tous les logiciels système de manière à préserver la capacité de récupération de l'utilisateur final (sans toutefois sauvegarder également les fichiers ou programmes infectés) et la garantie que l'utilisateur final dispose de disques sources et d'autres éléments permettant de reconstruire l'image de son appareil si nécessaire au cours du processus de remédiation.

Il est entendu que certains fournisseurs de services Internet ne disposent pas des ressources nécessaires pour fournir ce niveau de service, ni ne sont en mesure de prendre en charge ces activités gratuitement ou même contre rémunération. Dans de nombreux cas, les utilisateurs finaux devront être orientés vers des fournisseurs de services professionnels d'assistance informatique pour remédier complètement à leurs machines. Les notifications des FAI peuvent anticiper ce fait et suggérer aux clients de rechercher l'assistance d'un tiers afin d'éviter de frustrer les utilisateurs finaux avec des services d'assistance limités ou des lignes d'assistance qui ne sont pas capables ou équipés pour résoudre complètement les problèmes de remédiation.

b. Action recommandée :

1. Les bots sont conçus pour être furtifs et difficiles à supprimer. Dans le cadre de la notification, les FAI devraient offrir des conseils, comme décrit ci-dessus. Il peut s'agir de liens vers diverses sources d'information, de logiciels et d'outils en ligne ou provenant de tiers, accessibles au public. Il peut également s'agir de liens vers des services professionnels. Ceux-ci ne doivent pas nécessairement être proposés par le FAI lui-même, mais peuvent l'être par des tiers.

2. Un ISP peut fournir des outils de remédiation à l'utilisateur final, soit pendant, soit après le processus de notification. Cependant, le FAI ne doit pas obliger l'utilisateur final à exécuter les outils de remédiation. Si le FAI fournit des outils à l'utilisateur final, celui-ci doit être autorisé à quitter le processus sans exécuter les outils ou procédures suggérés.

3. Dans le cadre de la procédure de notification, les FAI peuvent souhaiter inclure des indications (en fonction de la nature du bot en question) selon lesquelles les paramètres des équipements de réseau appartenant aux clients, tels que les passerelles et les routeurs domestiques, peuvent avoir été modifiés.

a été altéré et doit être restauré dans un état sécurisé, selon la nature de l'infection par le bot.

c. Directives :

1. Les outils et services de suppression des robots doivent respecter la vie privée des utilisateurs.

2. Les méthodes possibles de remédiation aux infections sont décrites dans les meilleures pratiques du CSRIC II WG 8 et dans le bot remediation IETF RFC qui sont référencés dans l'annexe 2.

10. Collaboration ISP

a. Vue d'ensemble :

L'atténuation et la gestion du bot sont des activités dans lesquelles les FAI, les fournisseurs de recherche, les utilisateurs finaux, les services informatiques, les sociétés d'hébergement, les fournisseurs de blogs, les fournisseurs de sécurité, les chercheurs, les pouvoirs publics, les sociétés de services financiers, les fournisseurs de services en nuage et d'autres parties ont tous un rôle à jouer. Grâce à la contribution et à la collaboration de plusieurs parties prenantes, les résultats seront supérieurs à ceux que l'on pourrait obtenir par des actions indépendantes seules. La participation des FAI à ce code, ainsi que les approches complémentaires et collaboratives adoptées par d'autres segments de l'écosystème Internet, devraient permettre de réduire considérablement la menace que représentent les botnets.

b. Action recommandée :

La participation au code exige une collaboration au sein de l'ISP, de l'industrie ou de forums plus larges par le biais d'activités de collaboration, dont voici quelques exemples :

1. Partager les méthodes de détection, de notification ou d'atténuation prévues ou déployées dans les réseaux des FAI et, le cas échéant, une évaluation de leur efficacité.

2. Partage de renseignements ou de données opérationnelles sur les attaques qui peuvent être utiles à la prévention, à la défense ou à l'élimination des zombies.

3. Identification des données clés ou des ressources techniques qui sont nécessaires de la part des systèmes ou des acteurs au-delà du réseau des ISP.

4. Participation à la définition, au développement ou à l'exploitation de stratégies ou de systèmes de défense intégrés qui dépassent les limites du réseau ISP.

5. Autres activités de collaboration impliquant le partage d'informations avec des parties extérieures au PSI ou de données avec des systèmes extérieurs au réseau du PSI.

Tout partage d'informations entre les FAI et les autres parties concernées sera effectué conformément aux lois applicables, y compris, mais sans s'y limiter, les lois antitrust et les lois sur la protection de la vie privée.

11. Développement ultérieur du présent code

Ce code évoluera au fil du temps en raison de la nature dynamique de la menace des bots et de l'expérience et de l'évaluation des FAI.

12. Informations et ressources supplémentaires

Annexe 1 - Glossaire Annexe 2 -
Références

Annexe 1 - Glossaire :

1. Bot

La définition suivante s'inspire largement des "Recommandations pour la remédiation des bots dans les réseaux des fournisseurs de services Internet" (référencées à l'annexe 2) :

Un "bot" malveillant (ou potentiellement malveillant) (dérivé du mot "robot", ci-après simplement appelé "bot") désigne un programme installé sur un système afin de permettre à ce système d'exécuter automatiquement (ou semi-automatiquement) une tâche ou un ensemble de tâches, généralement sous le commandement et le contrôle d'un administrateur distant (souvent appelé "bot master" ou "bot herder").

Les systèmes informatiques et autres dispositifs d'utilisateur final qui ont été "botté" sont aussi souvent appelés "zombies".

Les robots malveillants sont généralement installés subrepticement, sans le consentement de l'utilisateur ou sans que celui-ci comprenne parfaitement ce que son système pourrait faire une fois le robot installé.

Les bots sont souvent utilisés pour envoyer des courriers électroniques indésirables ("spam"), pour reconnaître ou attaquer d'autres systèmes, pour écouter le trafic réseau ou pour héberger des contenus illégaux tels que des logiciels piratés, du matériel d'exploitation des enfants, etc.

De nombreuses juridictions considèrent l'infection involontaire des hôtes des utilisateurs finaux comme un exemple d'intrusion informatique illégale.

2. Botnet

Les botnets sont des réseaux d'appareils informatiques d'utilisateurs finaux connectés à l'internet et infectés par des logiciels malveillants, qui sont contrôlés à distance par des tiers à des fins malveillantes.
Un botnet est sous le contrôle d'un "botherder" ou "botmaster" donné. Un réseau de zombies peut compter une poignée d'hôtes zombifiés ou des millions.

3. Client (ou "client direct")

La partie qui passe un contrat avec un ISP pour un service. Distinguez le "client" de l'"utilisateur autorisé" : par exemple, un café peut acheter un service Internet à un ISP. Le café serait le client du FSI. Le café peut choisir d'offrir l'utilisation gratuite de sa connexion (si la politique d'utilisation acceptable du FSI l'autorise) à ceux qui lui achètent du café - les acheteurs de café seraient alors des utilisateurs autorisés de la connexion achetée par le café, mais pas le client direct du FSI.

4. Détection

La détection est le processus par lequel un fournisseur de services ou un utilisateur final prend conscience qu'un système ou un appareil particulier a été infecté par un logiciel malveillant. Un fournisseur de services peut détecter qu'un système a été infecté de différentes manières, notamment en recevant des plaintes de tiers concernant des spams, des analyses de réseau ou des attaques provenant de ce système. Les utilisateurs finaux peuvent détecter les infections du système au moyen d'outils logiciels ou d'autres moyens.

5. Écosystème

Ce terme est souvent utilisé pour décrire les relations entre les différents participants à l'internet, à savoir les fabricants de matériel, les développeurs de logiciels, les fournisseurs d'accès à Internet et les fournisseurs de contenu, d'applications et de services internet qui permettent à l'internet de fonctionner et d'être utile aux utilisateurs finaux.

L'écosystème Internet comprend des fournisseurs de systèmes d'exploitation, des organisations axées sur l'utilisateur final, des fournisseurs de contenu, d'applications et de services Internet, des FAI, des fournisseurs de recherche, des utilisateurs finaux, des services informatiques, des sociétés d'hébergement, des fournisseurs de blogs, des fournisseurs de sécurité, des chercheurs, des gouvernements, des sociétés de services financiers et d'autres parties.

L'économie dite "souterraine" est aussi souvent décrite comme un "écosystème", avec de multiples participants remplissant divers rôles spécialisés. Par exemple, certains participants peuvent se spécialiser dans l'écriture de logiciels malveillants, tandis que d'autres peuvent "récolter" des adresses électroniques à partir de pages Web et de listes de diffusion, et d'autres encore peuvent se spécialiser dans la distribution de logiciels malveillants aux adresses électroniques récoltées. L'écosystème des logiciels malveillants comprendra aussi normalement la population des victimes potentielles ciblées et les organismes chargés de l'application de la loi qui luttent contre la cybercriminalité.

6. Utilisateur final

Utilisateur final : dans un contexte informatique et de réseau, l'utilisateur final est la personne qui, en fin de compte, fait un usage autorisé d'un produit ou d'un service.

L'utilisateur final n'est souvent pas la même personne que celle qui a acheté le produit ou le service. Par exemple, le propriétaire d'un café peut acheter de la connectivité pour ses clients ; dans ce cas, ce sont les clients du café, et non le propriétaire, qui sont les véritables "utilisateurs finaux", même s'ils n'ont pas passé de contrat direct avec un FSI pour la connectivité qu'ils utilisent.

Une partie, telle qu'un hacker/cracker qui utilise un produit ou un service sans l'autorisation de l'acheteur, serait normalement considérée comme un cyber-intrus et non comme un "utilisateur final" en soi.

7. ISP

Un fournisseur d'accès à Internet (FAI) est une entreprise qui fournit un accès au détail à Internet pour les membres du public, ou pour les entreprises et autres organisations. Ces connexions peuvent se faire par câble, DSL, satellite, sans fil, par ligne commutée ou par d'autres technologies. Les FAI sont parfois aussi appelés "fournisseurs d'accès".

Une entreprise qui fournit un accès à l'Internet uniquement à ses propres employés ne serait normalement pas considérée comme un FSI. De même, un transporteur de réseau qui ne fournit qu'un accès en gros à l'Internet pour d'autres FSI serait normalement considéré comme un fournisseur de services de réseau (FRS), plutôt qu'un FSI.

8. Logiciel malveillant

"Malware" est l'abréviation de "logiciel malveillant".

Les robots malveillants sont un type de logiciels malveillants. Les autres formes de logiciels malveillants comprennent des catégories de logiciels connues sous le nom de virus, chevaux de Troie, vers, rootkits, crimeware, enregistreurs de frappe, composeurs, logiciels espions, logiciels publicitaires, etc. Les facteurs qui distinguent ces différents types de logiciels malveillants sont moins importants que la compréhension des raisons pour lesquelles les logiciels malveillants peuvent être considérés comme "malveillants".

Les logiciels malveillants violent souvent un ou plusieurs des principes fondamentaux suivants :

(a) Consentement : Un logiciel malveillant peut être installé même si l'utilisateur ne l'a pas demandé sciemment.

(b) Honnêteté : Les logiciels malveillants peuvent prétendre faire une chose, alors qu'ils font en réalité quelque chose de complètement différent.

(c) Vie privée-Respect de la vie privée : Les logiciels malveillants peuvent violer la vie privée d'un utilisateur, par exemple en capturant ses mots de passe ou ses informations de carte de crédit.

(d) Non-intrusivité : Les logiciels malveillants peuvent gêner les utilisateurs en faisant apparaître des publicités, en changeant la page d'accueil du navigateur, en rendant les systèmes lents ou instables et en les rendant susceptibles de tomber en panne, ou en interférant avec les logiciels de sécurité déjà installés.

(e) Inoffensivité : Les logiciels malveillants peuvent être des logiciels qui nuisent aux utilisateurs (par exemple, des logiciels qui endommagent notre système, envoient des spams ou désactivent les logiciels de sécurité).

(f) Respect de la gestion des utilisateurs : Si l'utilisateur tente de supprimer le logiciel, celui-ci peut se réinstaller ou passer outre les préférences de l'utilisateur.

Tout cela se résume à "un logiciel dont les utilisateurs ne veulent tout simplement pas".

Les utilisateurs peuvent installer des logiciels malveillants à leur insu en ouvrant une pièce jointe contaminée reçue par courrier électronique ou en visitant une page web au contenu malveillant. Les systèmes peuvent également être infectés directement par un attaquant à distance, ce dernier ayant ciblé une vulnérabilité connue qui peut être exploitée à distance, ou par l'utilisateur qui monte un CD, un DVD ou une clé USB infectés.

9. Atténuation

L'atténuation est le processus de gestion ou de contrôle des effets associés à un bot. Par exemple, si un système est infecté par un bot de spam et qu'il envoie des courriers électroniques commerciaux indésirables, l'atténuation peut consister à filtrer le spam émis par ce dispositif.

Notez que l'atténuation n'implique généralement pas la correction de la condition sous-jacente (ce serait la "remédiation") ; l'atténuation se contente de gérer les symptômes associés à une condition.

10. Notification

La notification est un processus par lequel les FAI communiquent avec leurs utilisateurs finaux concernant l'infection possible de l'appareil de l'utilisateur final par un bot malware ou la manière dont un abonné peut prévenir ou identifier une telle infection. La notification peut également impliquer un processus par lequel les utilisateurs finaux sont dirigés vers des outils qui leur permettront de découvrir eux-mêmes les infections par des robots. La notification peut prendre différentes formes, notamment une notification directe par le FAI à l'utilisateur final, ou une notification indirecte par le biais des outils d'autodécouverte disponibles ou d'un tiers. La notification peut être effectuée via plusieurs canaux potentiels, notamment (mais pas exclusivement) le courrier électronique, le courrier postal, un appel téléphonique, une notification dans le navigateur, un outil d'autodécouverte en ligne ou un message SMS.

11. Prévention

La prévention consiste à renforcer un système ou un service afin qu'il soit moins vulnérable à la compromission et à l'exploitation. Par exemple, sur de nombreux systèmes, la prévention peut impliquer :

- Mise à jour du système d'exploitation et de toutes les applications avec les correctifs de sécurité disponibles.
- Installation ou activation d'un pare-feu
- Utilisation d'un logiciel anti-virus
- S'assurer que le système est régulièrement sauvegardé
- Utiliser des mots de passe forts
- Désactiver tous les services réseau inutiles
- Encourager les utilisateurs à utiliser les services Internet en toute sécurité (par exemple, le courrier électronique, la navigation sur Internet, etc.)

12. Assainissement

La remédiation est le processus que suit l'utilisateur final pour nettoyer un ordinateur infecté afin qu'il ne le soit plus. Dans les cas simples, il s'agit d'installer et d'exécuter un produit anti-virus. Dans les cas plus difficiles, la remédiation peut impliquer une intervention plus substantielle allant jusqu'à "atomiser et paver" le système - le formater et le réinstaller à partir de zéro, ou au moins à partir de la dernière sauvegarde propre connue. Une fois que le système est propre ou qu'il a été réinstallé, il est normalement renforcé pour le protéger contre la réinfection.

13. Spam

Courriel non désiré et non demandé, souvent de nature commerciale, envoyé normalement à un grand nombre de destinataires sous une forme sensiblement identique. Le spam est souvent envoyé par des "affiliés" qui sont payés par la personne qui gère le programme d'affiliation lorsque les destinataires achètent le produit annoncé par le spam.

Annexe 2 - Références

1. Recommandations sur la manière de gérer les effets des ordinateurs infectés par des bots malveillants : "Recommandations pour la remédiation des bots dans les réseaux des ISP".

http://tools.ietf.org/rfc/rfc6561.txt

2. Groupe de travail 8 du CSRIC II - Meilleures pratiques en matière de protection des réseaux des ISP

http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PRO TECTION_20101213.pdf

3. icode - Code de pratique de l'industrie australienne de l'Internet concernant la cybersécurité

http://iia.net.au/images/resources/pdf/icode-v1.pdf

4. Japan Cyber Clean Center - Projet Anti-Botnet

https://www.ccc.go.jp/en_index.html

5. Centre consultatif anti-botnet allemand - Projet anti-botnet

https://www.botfrei.de/en/

6. Équipe japonaise d'intervention en cas d'urgence informatique

(CERT) http://www.jpcert.or.jp/english/

7. US CERT - Comprendre les menaces cachées : Rootkits et Botnets

http://www.us-cert.gov/cas/tips/ST06-001.html

8. Alliance for Telecommunications Industry Solutions (ATIS)

http://www.atis.org/

9. Département de la sécurité intérieure

http://www.dhs.gov/files/programs/gc_1158611596104.shtm

10. Département de la sécurité intérieure - Équipe de préparation aux situations d'urgence informatique des États-Unis

http://www.us-cert.gov/

11. Union internationale des télécommunications Botnet Mitigation Toolkit

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

12. Institut national des normes et de la technologie (NIST) du département du commerce des États-Unis.

http://www.nist.gov/index.html

13. Demande d'information du ministère du Commerce et du ministère de la Sécurité intérieure - Modèles visant à promouvoir la notification volontaire des entreprises aux consommateurs concernant l'utilisation illicite de matériel informatique par des botnets et des logiciels malveillants connexes

http://www.gpo.gov/fdsys/pkg/FR-2011-09-21/pdf/2011-24180.pdf

14. Commentaires reçus en réponse à la demande d'information du ministère du Commerce et du ministère de la Sécurité intérieure - Modèles visant à promouvoir la notification volontaire des entreprises aux consommateurs concernant l'utilisation illicite d'équipements informatiques par des botnets et des logiciels malveillants connexes

http://www.nist.gov/itl/botnetcomments.cfm

15. Messaging Anti-Abuse Working Group (MAAWG.org) - Code de conduite

http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf

16. Collection de bonnes pratiques du M3AAWG pour les ISP et les opérateurs de réseau

http://www.maawg.org/published-documents

17. Base de données nationale sur les vulnérabilités - National Institute of Standards and Technology

http://nvd.nist.gov/

18. Internet Storm Center

http://isc.sans.edu/index.html

19. Fondation Shadowserver

http://shadowserver.org

20. Liste de blocage de la politique

de Spamhaus

http://www.spamhaus.org/pbl/

21. Liste de blocage composite

http://cbl.abuseat.org

22. OnGuard Online

http://www.onguardonline.gov/default.aspx

23. IETF BCP38 Filtrage de l'entrée du réseau

http://tools.ietf.org/html/bcp38

Un rapport au Président sur

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées et distribuées

---

Transmis par
Le secrétaire au commerce et
Le Secrétaire à la sécurité intérieure

22 mai 2018

Table des matières

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Résumé exécutif

Ce rapport répond au décret du 11 mai 2017 intitulé " Renforcer la cybersécurité des réseaux fédéraux et des infrastructures critiques. " Ce décret appelait à la "résilience contre les botnets et autres menaces automatisées et distribuées", chargeant le secrétaire au commerce, conjointement avec le secrétaire à la sécurité intérieure, de "mener un processus ouvert et transparent pour identifier et promouvoir les actions des parties prenantes appropriées" dans le but de "réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées (par *exemple,* les botnets)."

Les départements du commerce et de la sécurité intérieure ont collaboré à cet effort par le biais de trois approches - l'organisation de deux ateliers, la publication de deux demandes de commentaires et l'ouverture d'une enquête par le biais du comité consultatif présidentiel sur les télécommunications de sécurité nationale (NSTAC) - visant à recueillir un large éventail de contributions d'experts et de parties prenantes, y compris l'industrie privée, le monde universitaire et la société civile. Ces activités ont toutes contribué au processus de collecte d'informations pour les agences qui élaborent les recommandations de ce rapport.

Les ministères ont travaillé en consultation avec les ministères de la Défense, de la Justice et de l'État, le Federal Bureau of Investigation, les agences sectorielles, la Federal Communications Commission et la Federal Trade Commission, ainsi que d'autres organismes intéressés.

Les ministères ont déterminé que les opportunités et les défis à relever pour réduire considérablement les menaces liées aux attaques automatisées et distribuées peuvent être résumés en six thèmes principaux.

1. **Les attaques automatisées et distribuées sont un problème mondial.** La majorité des dispositifs compromis dans les récents réseaux de zombies notables étaient géographiquement situés en dehors des États-Unis. Pour accroître la résilience de l'Internet et de l'écosystème des communications face à ces menaces, dont beaucoup proviennent de l'extérieur des États-Unis, nous devons continuer à travailler en étroite collaboration avec des partenaires internationaux.
2. **Des outils efficaces existent, mais ne sont pas largement utilisés.** Bien que des améliorations soient encore possibles, les outils, les processus et les pratiques nécessaires pour améliorer de manière significative la résilience de l'écosystème de l'internet et des communications sont largement disponibles et sont couramment appliqués dans certains secteurs du marché. Cependant, ils ne font pas partie des pratiques courantes de développement et de déploiement de produits dans de nombreux autres secteurs pour diverses raisons, notamment (mais pas exclusivement) le manque de sensibilisation, l'évitement des coûts, l'insuffisance de l'expertise technique et l'absence d'incitations commerciales.
3. **Les produits doivent être sécurisés à toutes les étapes de leur cycle de vie.** Les appareils qui sont vulnérables au moment de leur déploiement, qui ne disposent pas des moyens de corriger les vulnérabilités après leur découverte ou qui restent en service après la fin de l'assistance technique du fournisseur, facilitent beaucoup trop l'assemblage de menaces automatisées et distribuées.
4. **La sensibilisation et l'éducation sont nécessaires.** Les utilisateurs privés et certaines entreprises n'ont souvent pas conscience du rôle que leurs appareils pourraient jouer dans une attaque de botnet et ne comprennent pas toujours les avantages des contrôles techniques disponibles. Les développeurs de produits, les fabricants et les opérateurs d'infrastructures manquent souvent des connaissances et des compétences nécessaires pour déployer des outils, des processus et des pratiques qui rendraient l'écosystème plus résilient.
5. **Les incitations du marché devraient être mieux alignées.** À l'heure actuelle, les incitations du marché ne semblent pas s'aligner sur l'objectif consistant à "réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées". Les développeurs, fabricants et vendeurs de produits sont motivés par la volonté de minimiser les coûts et les délais de mise sur le marché, plutôt que d'intégrer la sécurité ou de proposer des mises à jour de sécurité efficaces. Les incitations du marché doivent être réalignées pour promouvoir un meilleur équilibre entre sécurité et commodité lors du développement de produits.

6. **Les attaques automatisées et distribuées constituent un défi à l'échelle de l'écosystème.** Aucune communauté de parties prenantes ne peut résoudre le problème de manière isolée.

Les ministères ont identifié cinq objectifs complémentaires et se renforçant mutuellement qui, s'ils étaient atteints, réduiraient considérablement la menace d'attaques automatisées et distribuées et amélioreraient la résilience et la redondance de l'écosystème. Une liste d'actions suggérées pour les principales parties prenantes renforce chaque objectif. Les objectifs sont les suivants :

- Objectif 1 : définir une voie claire vers un marché technologique adaptable, durable et sûr.
- Objectif 2 : promouvoir l'innovation dans l'infrastructure pour une adaptation dynamique à l'évolution des menaces.
- Objectif 3 : promouvoir l'innovation à la périphérie du réseau pour prévenir, détecter et atténuer les attaques automatisées et distribuées.
- Objectif 4 : Promouvoir et soutenir les coalitions entre les communautés de la sécurité, des infrastructures et des technologies opérationnelles au niveau national et international.
- Objectif 5 : accroître la sensibilisation et l'éducation dans l'ensemble de l'écosystème.

Les actions et options recommandées comprennent des activités en cours qui devraient être poursuivies ou étendues, ainsi que de nouvelles initiatives. Aucun investissement ou activité ne peut à lui seul atténuer toutes les menaces, mais les discussions organisées et les commentaires des parties prenantes nous permettront d'évaluer plus avant et de hiérarchiser ces activités en fonction du retour sur investissement attendu et de leur capacité à avoir un impact mesurable sur la résilience des écosystèmes.
Ce rapport demande une mise à jour de la situation qui évaluera le niveau des progrès réalisés par les parties prenantes dans la lutte contre les menaces automatisées et distribuées.

Cet effort ne se terminera pas avec la publication de ce rapport. Il y a encore beaucoup de travail à faire. Cependant, nous ne nous attendons pas à ce que toutes les actions se déroulent simultanément, en raison de considérations telles que les contraintes de ressources dans les communautés de parties prenantes concernées. En outre, certaines actions sont déjà en cours, tandis que d'autres dépendent de facteurs extérieurs. Nous proposons un modèle pour soutenir la coordination et la collaboration pour la mise en œuvre des actions décrites dans la section III, avec un accent particulier sur les exigences fédérales. Bien que certaines actions directement liées au gouvernement fédéral soient clairement appropriées pour que le gouvernement les dirige, ce modèle fournit un moyen pour les parties prenantes de collaborer avec le gouvernement alors qu'ils avancent sur les actions qui sont mieux accomplies grâce au leadership du secteur privé.

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

I. Contexte

Le 11 mai 2017, le président a émis le décret (EO) 13800, "Renforcer la cybersécurité des réseaux fédéraux et des infrastructures critiques", appelant à la "résilience contre les botnets et autres menaces automatisées et distribuées".[1] Le président a demandé au secrétaire au commerce et au secrétaire à la sécurité intérieure de "mener un processus ouvert et transparent pour identifier et promouvoir l'action des parties prenantes appropriées" dans le but de "réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées (par *exemple,* les botnets)".

Ces types d'attaques sont un sujet de préoccupation depuis les premiers jours d'Internet[2] et sont devenus un phénomène régulier au début des années 20003. [3] Les attaques automatisées et distribuées constituent une menace qui dépasse le cadre d'une seule entreprise ou d'un seul secteur. Ces menaces sont utilisées pour diverses activités malveillantes, notamment les attaques par déni de service distribué (DDoS) qui submergent les ressources en réseau, envoient des quantités massives de spam, diffusent des enregistreurs de frappe et d'autres logiciels malveillants ; les attaques par ransomware distribuées par des botnets qui prennent en otage les systèmes et les données ; et les campagnes de propagande informatique4 qui manipulent et intimident les communautés par le biais des médias sociaux. Les techniques traditionnelles d'atténuation des attaques DDoS, telles que la mise en place par les fournisseurs de réseaux d'une capacité excédentaire pour absorber les effets des botnets, sont conçues pour se protéger contre les botnets d'une taille anticipée. Avec les nouveaux botnets qui tirent parti du nombre considérable d'appareils de l'"Internet des objets" (IoT)[5], les attaques DDoS ont atteint une taille de plus d'un térabit par seconde, dépassant de loin la taille prévue et la capacité excédentaire. Par conséquent, le temps de récupération de ces types d'attaques peut être trop lent, en particulier lorsque des services essentiels à la mission sont concernés. En outre, ces techniques d'atténuation n'ont pas été conçues pour remédier à d'autres catégories d'activités malveillantes facilitées par les réseaux de zombies, comme les rançongiciels ou la propagande informatique.

À mesure que de nouveaux scénarios émergent, il est urgent de coordonner et de collaborer avec un ensemble diversifié de parties prenantes. Le gouvernement fédéral a travaillé avec les parties prenantes dans le passé pour faire face aux nouvelles menaces à mesure qu'elles apparaissent. Parmi les efforts antérieurs, citons le Industry Botnet Group, qui a débouché sur les Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace (2012) ; [6] les efforts de partage d'informations et de coordination du secteur des services financiers à la suite des attaques DDoS contre des banques en 2012 et

[1] Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (11 mai 2017), *disponible à l'adresse suivante* . https://www.federalregister.gov/d/2017-10004.
[2] United States v. Morris, 928 F.2d 504 (2d Cir. 1991).
[3] *Voir, par exemple,* Stuart Staniford, Vern Paxson & Nicholas Weaver, How *to 0wn the Internet in Your Spare Time,* Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, Aug. 5-9, 2002, *disponible sur* https://www.usenix.org/legacy/event/sec02/full_papers/staniford/staniford.pdf.
[4] La propagande informatique est "l'assemblage de plateformes de médias sociaux, d'agents autonomes et de big data chargés de manipuler l'opinion publique." Samuel C. Woolley & Philip N. Howard, *Political Communication, Computational Propaganda, and Autonomous Agents-Introduction, 10* Int'l Journal of Commc'n 4882, 4886 (2016), *disponible sur* http://ijoc.org/index.php/ijoc/article/viewFile/6298/1809.
[5] Les exemples d'appareils IoT comprennent (sans s'y limiter) les ampoules connectées, les serrures de porte, les parcmètres, les moniteurs de santé personnels, l'automatisation et les capteurs industriels, et les automobiles.
[6] Industry Botnet Group, *Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace*, https://archive.is/20131015084520/www.industrybotnetgroup.org/principles/ (dernière visite le 4 avril 2018).

[20137] ; le code de conduite anti-bot du Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications (CSRIC)[8] (2013)[9], les rapports sur les pratiques de protection des réseaux des fournisseurs de services Internet (ISP) (2010)[10] et sur la remédiation des attaques DDoS basées sur les serveurs (2014)[11] ; et les travaux actifs et continus du ministère de la Justice et de ses nombreux partenaires sur le traitement et l'élimination de l'infrastructure soutenant ces menaces12. [12] Bien que ces initiatives aient permis de réaliser des progrès, leur impact a été progressif et des défis importants restent à relever. En s'attaquant de manière proactive à ces défis, l'administration et les principales parties prenantes ont la possibilité d'améliorer la résilience du futur écosystème de l'Internet et des communications.

Les attaques DDoS lancées à partir du botnet Mirai à l'automne 2016, par exemple, ont atteint un niveau de trafic soutenu qui a submergé de nombreux outils et services d'atténuation DDoS courants, et ont même perturbé un service de système de nom de domaine (DNS) qui était un composant couramment utilisé dans de nombreuses stratégies d'atténuation DDoS. [13] Cette attaque a également mis en évidence l'insécurité croissante des dispositifs IoT grand public et les menaces qu'ils représentent. En tant que nouvelle technologie, les dispositifs IdO sont souvent construits et déployés sans que d'importantes fonctions et pratiques de sécurité soient en place14. [14] Alors que la variante originale de Mirai était relativement simple, exploitant les mots de passe faibles des appareils, des réseaux de zombies plus sophistiqués ont suivi ; par exemple, le réseau de zombies Reaper utilise des vulnérabilités de code connues pour exploiter une longue liste d'appareils,[15] et l'une des plus grandes attaques DDoS observées à ce jour a récemment exploité une vulnérabilité récemment découverte dans l'appareil relativement obscur

[7] *Evaluating the Security of the U.S. Financial Sector : Hearing Before the Task Force to Investigate Terrorism Financing*, House Committee on Financial Services, 114th Cong. 40-59 (2015) (déclaration de John W. Carlson, Chief of Staff, Financial Services Information Sharing and Analysis Center (FS-ISAC)), *disponible sur* https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg96997/pdf/CHRG-114hhrg96997.pdf.

[8] Le CSRIC est un comité consultatif de la Federal Communications Commission, dont la mission est de faire des recommandations à la Commission pour promouvoir la sécurité, la fiabilité et la résilience des systèmes de communication de la nation. Pour plus d'informations, y compris les efforts passés en matière de sécurité, voir CSRIC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability- council-0 (dernière visite le 4 avril 2018).

[9] Groupe de travail 7 du Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications III, *Final Report on U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs)*, (Mar. 2013), *disponible sur* https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[10] Groupe de travail 8 du Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications, *Rapport final sur les pratiques de protection des réseaux des fournisseurs de services Internet (FSI)*, (déc. 2010), *disponible à l'adresse* http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101 213.pdf.

[11] Groupe de travail 5 du Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications IV, *Rapport final sur la remédiation des attaques DDoS basées sur le serveur*, (sept. 2014), *disponible à l'adresse* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf.

[12] *Voir, par exemple, le* ministère de la Justice des États-Unis, *Avalanche Network Dismantled in International Cyber Operation*, (5 déc. 2016), https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation.

[13] Équipe de préparation aux situations d'urgence informatique des États-Unis, *Alerte (TA16-288A) : Heightened DDoS Threat Posed by Mirai and Other Botnets*, https://www.us-cert.gov/ncas/alerts/TA16-288A (dernière révision le 17 octobre 2017).

[14] The National Security Telecommunications Advisory Committee, *NSTAC Report to the President on the Internet of Things*, (19 nov. 2014), *disponible à l'adresse* https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

[15] Brian Krebs, *Fear the Reaper, or Reaper Madness ?* Krebs on Security (27 oct. 2017, 4:39 PM), https://krebsonsecurity.com/2017/10/fear-the-reaper-or-reaper-madness/.

le logiciel MemCacheD. [16] Ces exemples montrent clairement les risques posés par des réseaux de zombies de cette taille et de cette envergure, ainsi que l'innovation attendue et l'augmentation de l'échelle et de la complexité des attaques futures.

Approche

Les ministères du Commerce et de la Sécurité intérieure ont travaillé conjointement sur cet effort en adoptant trois approches visant à recueillir un large éventail de contributions de la part d'experts et de parties prenantes, notamment du secteur privé, du monde universitaire et de la société civile. Les ministères ont travaillé en consultation avec les ministères de la Défense, de la Justice et de l'État, le Federal Bureau of Investigation, les agences sectorielles, la Federal Communications Commission et la Federal Trade Commission, ainsi que d'autres organismes intéressés.

En juin 2017, l'Administration nationale des télécommunications et de l'information (NTIA) du Département a publié une demande de commentaires (RFC) sur la "promotion de l'action des parties prenantes contre les botnets et autres menaces automatisées".[17] La RFC demandait des commentaires sur "les approches actuelles, émergentes et potentielles pour faire face aux botnets et autres attaques distribuées et automatisées". La NTIA a reçu 47 commentaires, les répondants allant de grandes associations commerciales (représentant des milliers d'entreprises) à des experts techniques individuels. Les commentateurs représentaient également une gamme variée d'industries et de secteurs, y compris des fournisseurs de services Internet, des entreprises de sécurité, des fournisseurs d'infrastructure, des fabricants de logiciels, la société civile et le monde universitaire d'organisations américaines et non américaines.

En juillet 2017, le National Institute of Standards and Technology (NIST) du Département a organisé un atelier sur le thème "Renforcer la résilience de l'écosystème de l'Internet et des communications".[18] Cet atelier a encouragé les parties prenantes à explorer les solutions actuelles et émergentes pour faire face aux menaces automatisées et distribuées de manière ouverte et transparente. Il a attiré 150 participants de diverses communautés de parties prenantes, qui ont identifié un large éventail d'actions coordonnées par toutes les parties prenantes pour faire face à ces menaces.

Conformément à l'Executive Order 13800, un projet de rapport a été publié en janvier 2018, suivi d'un deuxième RFC et d'un atelier, au cours duquel les parties prenantes ont discuté des commentaires publics de fond et des prochaines étapes. Ces activités ont contribué au processus de collecte d'informations pour les agences élaborant les recommandations de ce rapport final. Les commentaires et les discussions de l'atelier éclaireront également de nombreuses actions qui auront lieu après la publication de ce rapport.

La participation du Department of Homeland Security (DHS) à cet effort s'est concentrée sur le sous-comité du President's National Security Telecommunications Advisory Committee (NSTAC) sur la résilience de l'Internet et des communications, qui a finalisé et approuvé le *rapport du NSTAC à l'intention de l*

[16] Lili Hay Newman, *GitHub a survécu à la plus grande attaque DDoS jamais enregistrée*, Wired (1er mars 2018, 11 h 01), https://www.wired.com/story/github-ddos-memcached/.

[17] Des informations supplémentaires, notamment les commentaires publics, sont disponibles à l'adresse suivante : National Telecommunications and Information Administration, *Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats*, (8 juin 2017), https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting- stakeholder-action-against-botnets-and-other-automated-threats.

[18] National Institute of Standards and Technology, *Enhancing Resilience of the Internet and Communications Ecosystem*, https://www.nist.gov/news-events/events/2017/07/enhancing-resilience-internet-and-communications- ecosystem (dernière mise à jour le 10 juillet 2017). Pour un résumé des travaux, voir Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem : A NIST Workshop Proceedings*, (sept. 2017), NIST Interagency/Internal Report No. 8192, *disponible sur* http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8192.pdf.

President on Internet and Communications Resilience le 16 novembre 2017.[19] Lors de l'élaboration de son rapport, le NSTAC a étudié les botnets, ainsi que les formes d'attaques qui peuvent être facilitées par les botnets, telles que les attaques DDoS et les vecteurs qui pourraient être utilisés pour créer des botnets (c'*est-à-dire,* les appareils des utilisateurs finaux et l'IoT). Grâce à son étude, le NSTAC a conclu que les attaques automatisées et distribuées facilitées par les botnets menacent la sécurité et la résilience de l'Internet et de l'écosystème des communications, et à leur tour, les infrastructures critiques de la nation. En outre, le NSTAC a déterminé que les dispositifs IoT compromis seront de plus en plus utilisés par des acteurs malveillants pour lancer des attaques automatisées mondiales.

Thèmes principaux

Les opportunités et les défis auxquels nous sommes confrontés dans le cadre de nos efforts pour réduire considérablement les menaces liées aux attaques automatisées et distribuées peuvent être résumés en six thèmes principaux.

1. **Les attaques automatisées et distribuées sont un problème mondial.** La majorité des dispositifs compromis dans les récents réseaux de zombies notables étaient géographiquement situés en dehors des États-Unis. Pour accroître la résilience de l'Internet et de l'écosystème des communications face à ces menaces, dont beaucoup proviennent de l'extérieur des États-Unis, nous devons continuer à travailler en étroite collaboration avec des partenaires internationaux.
2. **Des outils efficaces existent, mais ne sont pas largement utilisés.** Bien que des améliorations soient encore possibles, les outils, les processus et les pratiques nécessaires pour améliorer de manière significative la résilience de l'écosystème de l'internet et des communications sont largement disponibles et sont couramment appliqués dans certains secteurs du marché. Cependant, ils ne font pas partie des pratiques courantes de développement et de déploiement de produits dans de nombreux autres secteurs pour diverses raisons, notamment (mais pas exclusivement) le manque de sensibilisation, l'évitement des coûts, l'insuffisance de l'expertise technique et l'absence d'incitations commerciales.
3. **Les produits doivent être sécurisés à toutes les étapes de leur cycle de vie.** Les appareils qui sont vulnérables au moment de leur déploiement, qui ne disposent pas des moyens de corriger les vulnérabilités après leur découverte ou qui restent en service après la fin de l'assistance technique du fournisseur, facilitent beaucoup trop l'assemblage de menaces automatisées et distribuées.
4. **La sensibilisation et l'éducation sont nécessaires.** Les utilisateurs privés et certaines entreprises n'ont souvent pas conscience du rôle que leurs appareils pourraient jouer dans une attaque de botnet et ne comprennent pas toujours les avantages des contrôles techniques disponibles. Les développeurs de produits, les fabricants et les opérateurs d'infrastructures manquent souvent des connaissances et des compétences nécessaires pour déployer des outils, des processus et des pratiques qui rendraient l'écosystème plus résilient. Des mécanismes conviviaux permettant d'identifier des choix plus sûrs, analogues à des programmes tels que le programme Energy Star20 ou le classement de sécurité 5 étoiles de la National Highway Traffic Safety Administration (NHTSA)21 sont nécessaires pour sensibiliser les consommateurs et éclairer leurs décisions d'achat.
5. **Les incitations du marché devraient être mieux alignées.** À l'heure actuelle, les incitations du marché ne semblent pas s'aligner sur l'objectif consistant à "réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées". Les développeurs, fabricants et vendeurs de produits sont motivés par la volonté de minimiser les coûts et les délais de mise sur le marché, plutôt que d'intégrer la sécurité ou d'offrir une sécurité efficace.

[19] Le Comité consultatif sur les télécommunications pour la sécurité nationale, *Rapport du NSTAC au président sur la résilience de l'Internet et des communications*, (16 novembre 2017), *disponible sur* https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR.%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

[20] Energy Star, *About Energy Star*, https://www.energystar.gov/about (dernière visite le 4 avril 2018). [21] National Highway Traffic Safety Administration, *Search NHTSA's 5-Star Safety Ratings*, https://www.safercar.gov/Vehicle-Shoppers (dernière visite le 4 avril 2018).

mises à jour. Les incitations du marché doivent être réalignées pour promouvoir un meilleur équilibre entre sécurité et commodité lors du développement des produits.

6. **Les attaques automatisées et distribuées constituent un défi à l'échelle de l'écosystème.** Aucune communauté de parties prenantes ne peut résoudre le problème de manière isolée.

Une note sur les menaces

Le présent document ne fait pas de distinction entre les États-nations, les cybercriminels et les autres acteurs de la menace. Si certaines attaques peuvent être difficiles à attribuer au départ, l'écosystème doit néanmoins s'unir pour atténuer une attaque. Ce processus ouvert et transparent s'est concentré sur les domaines qui susciteraient la plus large participation des parties prenantes de l'ensemble de l'écosystème de l'Internet et des communications concernant les améliorations de la sécurité, ainsi que la coopération avant, pendant et après les attaques, en comprenant que l'identité d'un acteur de la menace donné peut être initialement inconnue. L'évaluation de la menace mondiale 2018 de la communauté du renseignement des États-Unis publiée par le bureau du directeur du renseignement national donne un aperçu du paysage de la cybermenace. [22] Bien que cela dépasse le cadre du présent rapport, il sera important de faire la distinction entre les acteurs de la menace de type État-nation, cybercriminel et autres pour déterminer la meilleure façon d'appliquer un large éventail d'autorités gouvernementales américaines spécifiques à la menace. Certains participants à l'atelier ont également reconnu leurs limites dans le traitement de catégories spécifiques d'acteurs de la menace. Il conviendrait d'accorder une attention particulière à ces questions à l'avenir, en impliquant les parties prenantes de l'écosystème au

II. État actuel de l'écosystème et vision pour l'avenir

Cette section décrit l'état actuel des domaines techniques et politiques de l'écosystème de l'internet et des communications mondiales, et envisage un avenir meilleur. Les domaines techniques de l'écosystème comprennent :

- L'***infrastructure*** qui relie les autres domaines techniques en un seul système ;
- ***Réseaux d'entreprise*** composés de dispositifs connectés localement et dotés d'adresses Internet IP version 4 (IPv4) et IPv6 attribuées par le registre Internet régional (RIR)[23], ainsi que de réseaux sous-locaux (LAN) connectés localement et utilisant un espace d'adressage IP privé ou des protocoles alternatifs (par *exemple,* Bluetooth Low Energy) ;
- les ***dispositifs de périphérie*** tels que les ordinateurs personnels, les dispositifs mobiles, les serveurs de périphérie et les dispositifs IoT et autres dispositifs connectés ; et
- ***Réseaux domestiques et de petites entreprises*** composés de dispositifs utilisant un espace d'adressage IP privé adressable à l'extérieur par le biais de la traduction d'adresses réseau (NAT).

Le domaine de la politique est lié aux domaines techniques, et comprend :

- Les **partenariats public-privé**, y compris les accords de partage d'informations ;

[22] *Voir* Daniel R. Coats, directeur du renseignement national, *Worldwide Threat Assessment of the US Intelligence Community*, déclaration pour le compte rendu à la commission spéciale du Sénat sur le renseignement, (13 février 2018), *disponible sur* https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[23] "Les registres Internet régionaux (RIR) sont des sociétés à but non lucratif qui administrent et enregistrent l'espace d'adressage du protocole Internet (IP) et les numéros de systèmes autonomes (AS) dans une région définie." American Registry for Internet Numbers, *Regional Internet Registries*, https://www.arin.net/knowledge/rirs.html (dernière visite le 4 avril 2018).

- Les **processus d'attestation ou de certification volontaires**, dans lesquels les fournisseurs et les clients acceptent de partager des objectifs et des attentes en matière de sécurité ;
- **Normes et lignes directrices** élaborées dans des forums multipartites ;
- Des **politiques d'approvisionnement**, notamment au sein du gouvernement fédéral, pour créer des incitations au marché ;
- **Les actions réglementaires et législatives** au niveau fédéral et/ou étatique ; et
- Un **engagement international** pour s'appuyer sur des objectifs communs et des meilleures pratiques.

L'amélioration de la résilience face aux attaques automatisées et distribuées nécessitera une collaboration sur des ensembles de solutions techniques, politiques et autres entre les nations, les secteurs et les couches techniques. Des politiques efficaces fourniront des attentes claires pour l'utilisation de normes et de directives qui resteront flexibles et adaptables à mesure que le risque de sécurité évolue. Il n'existe pas de solution ou de cadre unique permettant de faire face à tous les risques, mais une meilleure collaboration entre les domaines améliorera la capacité des membres de l'écosystème à atténuer la menace des botnets.

Domaines techniques

Infrastructure : État actuel

Face aux attaques automatisées et distribuées, l'infrastructure actuelle qui sous-tend l'écosystème numérique a fait preuve d'une résilience remarquable, mais la taille et la portée croissantes des attaques semblent tester les limites de cette résilience. Ces deux perspectives sont apparues après les attaques du botnet Mirai de 2016, qui ont temporairement interrompu les services d'un fournisseur d'infrastructure Internet, perturbant ainsi de nombreux services en ligne et sites Web importants en Amérique du Nord et en Europe. Cependant, les perturbations étaient temporaires et les acteurs clés ont réagi rapidement. Cette réaction souligne à la fois l'interdépendance de l'infrastructure et la capacité des individus et des organisations à apprendre et à s'adapter rapidement.

Dans le présent rapport, le terme "infrastructure" englobe la technologie et les organisations qui permettent la connectivité, l'interopérabilité et la stabilité, allant au-delà des câbles physiques, des émetteurs et récepteurs sans fil et des liaisons par satellite pour inclure le matériel, les logiciels, les outils, les normes et les pratiques dont dépend l'écosystème - par exemple, les routeurs, les commutateurs, les fournisseurs de services Internet, les fournisseurs de DNS, les réseaux de diffusion de contenu, les fournisseurs d'hébergement et de services en nuage. [24] En raison de la complexité de l'infrastructure moderne, avec des outils et des acteurs clés disséminés dans l'écosystème, aucun outil unique ne peut sécuriser l'infrastructure. Traditionnellement, lorsque de nouvelles menaces apparaissent, des sous-ensembles particuliers d'acteurs de l'infrastructure collaborent pour comprendre le risque et les moyens de l'atténuer.

Le filtrage du trafic à l'entrée et à la sortie d'un réseau - technique connue sous le nom de filtrage à l'entrée et à la sortie - est l'un de ces outils. L'usurpation d'adresse IP est une technique couramment employée dans les attaques DDoS, où l'attaquant fabrique l'adresse IP source pour empêcher la victime de filtrer le mauvais trafic en fonction de son origine.
Les fournisseurs de réseaux peuvent limiter l'usurpation d'identité en restreignant le trafic entrant à celui qui provient réellement de son réseau déclaré, en filtrant le trafic qui prétend provenir de l'extérieur de son espace réseau prévu. [25] Le filtrage à l'entrée est reconnu comme une meilleure pratique de longue date par l'Internet Engineering

[24] Alors que la Presidential Policy Directive (PPD) 21 reconnaît les systèmes et les actifs des secteurs des communications et des technologies de l'information comme des infrastructures critiques, le présent document utilise le terme "infrastructure Internet" pour englober les organisations et les pratiques dont dépend l'écosystème Internet.

[25] Le DHS développe et soutient des outils logiciels à code source ouvert pour évaluer et rendre compte du déploiement des meilleures pratiques anti-spoofing de la validation de l'adresse source (SAV). Pour plus d'informations, voir Center for Applied Internet Data Analysis, *Spoofer*, https://www.caida.org/projects/spoofer/.

Task Force (IETF) et d'autres organisations axées sur l'infrastructure. [26] Il peut être complété par le filtrage de sortie, dans lequel une organisation ou un opérateur de réseau déploie des filtres à la périphérie de son réseau pour empêcher le trafic qui ne semble pas provenir de l'intérieur du réseau de sortir sur l'Internet mondial.

Les principaux opérateurs nationaux mettent en œuvre les normes de filtrage à l'entrée dans au moins une partie de leurs réseaux. Cependant, ces normes ne sont pas universellement soutenues dans le monde entier, ni par les petits fournisseurs d'infrastructure nationaux. De nombreux experts techniques et commerciaux se sont opposés aux propositions visant à appliquer le filtrage à l'entrée plus haut dans l'Internet, au niveau des dorsales internationales, parce qu'il serait plus susceptible de bloquer le trafic légitime. [27] Le filtrage à la sortie est préconisé comme une pratique de sécurité courante pour les entreprises,[28] mais il est encore peu répandu dans les petites et moyennes entreprises. Bien qu'il ne soit pas universellement mis en œuvre, le filtrage entrée/sortie du réseau, lorsqu'il est mis en œuvre, est efficace pour atténuer la catégorie d'attaques DDoS qui exploitent l'usurpation d'adresse IP source.

Les fournisseurs d'infrastructures et d'autres entreprises proposent des services anti-DDoS commerciaux, qui peuvent jouer un rôle clé dans la limitation de l'impact des attaques contre des cibles particulières. Cependant, toutes les entreprises clientes n'achètent pas la gamme complète de services anti-DDoS, en raison du coût et de la complexité de l'intégration de ces services dans les autres composants du réseau de l'entreprise. Parallèlement, les attaquants apprennent rapidement à exploiter les failles des services existants. Face à des attaques qui reposent sur le simple volume du trafic, les solutions d'atténuation des attaques DDoS hors site fournissent davantage de capacité réseau ou utilisent la forme du réseau lui-même pour limiter le volume du trafic qui atteint la cible. D'autres attaques visent le serveur web ou l'application elle-même. Les dispositifs et outils sur site d'une entreprise détectent et filtrent ces attaques sur le réseau cible.

Les meilleures pratiques actuelles impliquent l'emploi d'une approche hybride qui utilise à la fois le filtrage local et des outils de défense contre les DDoS qui augmentent la capacité hors site. Cependant, la mise en œuvre des meilleures pratiques peut être coûteuse, difficile à gérer et nécessiter un personnel qualifié. Ces meilleures pratiques sont aussi généralement construites autour de crises passées, ce qui rend difficile, par exemple, de plaider en faveur d'une grande quantité de capacité excédentaire jusqu'à ce que l'on subisse une attaque. Un programme de détection active des menaces qui détecte les vulnérabilités et les tendances des attaques peut compléter ces efforts, en aidant l'organisation victime à réagir en fonction des besoins. Les réseaux de diffusion de contenu (CDN) sont un autre outil qui peut tirer parti de grandes infrastructures privées dédiées pour protéger les clients. À mesure que des attaques différentes apparaissent ou que les adversaires choisissent de nouvelles cibles, les organisations investissent souvent dans des défenses spécifiques aux menaces.

Réagir en temps voulu nécessite une préparation et des connaissances. Compte tenu du grand nombre de contrôles de sécurité nécessaires dans l'Internet moderne, le personnel des petits fournisseurs d'infrastructure ou des entreprises clés n'est pas toujours conscient des avantages du filtrage et des autres outils. De nombreux fournisseurs d'infrastructure émettent des avertissements sur les compromissions et les attaques en cours, mais si les entreprises ignorent ces avertissements, le fournisseur d'infrastructure est moins susceptible de donner suite avec diligence à d'autres avertissements. Les victimes ont souvent du mal à

[26] *Voir, par exemple,* P. Ferguson & D. Senie, *Network Ingress Filtering : Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*, (mai 2000), Internet Engineering Task Force - Network Working Group, *disponible sur* https://tools.ietf.org/html/bcp38 ("BCP 38") ; et F. Baker & P. Savola, Ingress *Filtering for Multihomed Networks, (*mars 2004), Internet Engineering Task Force - Network Working Group, *disponible sur* https://tools.ietf.org/html/bcp84 ("BCP 84").

[27] Les paquets peuvent être acheminés entre les points d'extrémité de l'Internet par des chemins sensiblement différents à différents moments dans le temps pour des raisons légitimes.

[28] *Voir, par exemple*, Chris Brenton, *Egress Filtering FAQ*, SANS Institute, https://www.sans.org/reading-room/whitepapers/firewalls/egress-filtering-faq-1059 (dernière révision le 19 avril 2006).

lorsqu'ils sont confrontés à leur première attaque importante sans plan d'intervention en place, car ils dépendent du réseau même attaqué pour le comprendre et contacter les fournisseurs de services pour obtenir de l'aide.

Vision pour l'avenir des infrastructures

Les fournisseurs d'infrastructure de tous types doivent développer une large compréhension des avantages des approches de défense partagées, et les communautés devraient travailler ensemble pour favoriser l'adoption des meilleures pratiques. Ce travail inclut l'adoption omniprésente du filtrage à l'interface avec les réseaux des clients, y compris les infrastructures multi-tenant telles que les fournisseurs de cloud. Idéalement, les fournisseurs d'infrastructures devraient comprendre les niveaux actuels d'attaques, maintenir une capacité suffisante pour absorber les niveaux de trafic malveillant attendus de manière réaliste, et communiquer ces capacités à leurs clients. Les services des fournisseurs d'infrastructure pour l'atténuation des attaques DDoS devraient s'intégrer aux solutions réseau existantes des clients, quel que soit le niveau de service choisi par le client.

À mesure que de nouveaux produits et outils sont disponibles, les acteurs de l'écosystème doivent comprendre comment leur comportement peut favoriser - ou entraver - leur efficacité. Un réseau de plus en plus intelligent peut segmenter automatiquement différents types de trafic, afin d'isoler ou d'atténuer les applications ou les appareils qui sont des sources et des cibles d'attaques. Les entreprises sont de plus en plus capables de faire face aux attaques au niveau des applications grâce à des outils appropriés, et les fournisseurs de ces outils devraient travailler avec les clients et les fournisseurs d'applications concernés pour rendre les décisions de sécurité plus faciles et plus efficaces.

Une mise en œuvre accrue d'un certain nombre de technologies existantes contribuera à atténuer ces attaques. Une partie de l'infrastructure existante repose sur des protocoles plus anciens, tels que le réseau IPv4 et les anciens protocoles de routage. Une adoption plus large des normes et des meilleures pratiques actuelles apportera des avantages en matière de sécurité. Par exemple, le réseau IPv6 peut mieux permettre la reconnaissance spécifique des appareils sur le réseau afin de détecter les comportements aberrants au niveau des appareils. [29] Les petites et moyennes entreprises devraient intégrer les meilleures pratiques de l'industrie et, à mesure que de nouvelles normes et pratiques d'infrastructure sont nécessaires et éprouvées, les fournisseurs d'infrastructure devraient les adopter efficacement.

Au cœur de l'infrastructure, les acteurs clés partagent déjà des informations sur la nature évolutive des menaces. Si bon nombre de ces organisations emploient des experts qui coordonnent leurs activités avec celles de leurs pairs dans le monde entier, à l'avenir, le partage de l'information devra s'étendre aux acteurs plus petits, moins bien financés ou spécialisés, grâce à de nouveaux outils et pratiques automatisés. Des mesures incitatives pourraient encourager les investissements dans une détection plus efficace du trafic malveillant, ainsi que des engagements publics plus nombreux pour éviter de transporter du trafic malveillant. Ces engagements s'appuieraient sur les relations existantes au sein de la communauté pour aider à construire un réseau mondial plus stable.

Réseaux d'entreprise : État actuel

Les réseaux qui soutiennent les entreprises (*par exemple, les* moyennes et grandes entreprises, les agences gouvernementales et les institutions académiques) constituent un autre domaine technique clé de l'écosystème Internet et des communications. Ces réseaux sont souvent complexes, avec des routeurs BGP (Border Gateway Protocol) appartenant à l'entreprise et exploités par elle, des résolveurs DNS et des applications qui reposent sur un mélange de services locaux et en nuage. Les appareils de périphérie comprennent souvent des serveurs puissants, des appareils informatiques personnels, des téléphones mobiles et des appareils IoT gérés et non gérés par l'entreprise. Les appareils des réseaux d'entreprise peuvent utiliser un mélange de services statiques ou en nuage.

[29] La solution de rechange actuelle pour IPv4, la traduction d'adresses de réseau (NAT), offre des avantages en matière de pare-feu, en particulier au niveau du réseau domestique. Il convient toutefois de noter qu'une fois l'IPv6 mis en œuvre, les attaquants pourraient identifier les adresses spécifiques de dispositifs ciblés qui auraient été auparavant plus difficiles à reconnaître derrière la NAT. Les experts ont également exprimé certaines inquiétudes quant à la sécurité de certaines mises en œuvre d'IPv6.

des adresses attribuées dynamiquement à partir d'une ou plusieurs plages d'adresses IP publiques (par *exemple, des* adresses acquises auprès d'un RIR) ainsi que des adresses attribuées à partir de plages d'adresses IP privées administrées localement. La présence importante de réseaux d'entreprise connectés à l'Internet signifie qu'ils ne sont pas seulement des victimes potentielles mais aussi des sources de risque.

De nombreuses attaques DDoS bien connues, telles que celles qui ont visé des banques américaines en 2012 et 2013, ont ciblé des services en contact avec la clientèle associés à de grandes entreprises. [30] Tout comme les attaques Mirai de 2016 ont permis à certaines entreprises de faire preuve de résilience face à la vulnérabilité, les attaques de 2012-2013 ont incité le secteur financier et ses partenaires à découvrir des faiblesses et à montrer des voies vers une plus grande résilience. Ces attaques ont été perturbatrices, mais le secteur en a atténué les effets grâce à un investissement accru dans la technologie et les ressources, ainsi qu'à une collaboration active au sein de la communauté, y compris avec ses fournisseurs de services réseau et ses partenaires techniques, ainsi qu'avec le gouvernement. Les organisations ont partagé les leçons apprises à mesure que les attaques se poursuivaient, et des institutions telles que le Centre d'analyse et de partage de l'information (ISAC) des services financiers et la Table ronde des services financiers ont facilité le partage de l'information et la coordination avec les principaux fournisseurs de services Internet. L'ampleur des attaques a inspiré un leadership aux plus hauts niveaux de la direction et a favorisé une relation plus durable avec les experts gouvernementaux, ainsi qu'un engagement à investir dans les outils et les services.

Les ressources associées aux réseaux d'entreprise sont également un facteur important dans l'exécution de menaces automatisées et distribuées. Les appareils au niveau de l'entreprise, allant des appareils IoT aux serveurs des centres de données, peuvent être compromis et incorporés dans des botnets. Les ressources d'entreprise mal administrées, telles que les résolveurs DNS ouverts, sont souvent exploitées pour amplifier les attaques. Pour certaines entreprises, il peut être difficile de maintenir tous les systèmes et appareils patchés et mis à jour sur l'ensemble de leurs réseaux mondiaux. Les routeurs exploités par les entreprises qui n'appliquent pas le filtrage à l'entrée et à la sortie ont facilité les attaques par usurpation d'adresse, permettant aux participants du botnet de cacher leur véritable emplacement. Dans le cas des fournisseurs de services en nuage, des ressources d'entreprise ont été louées (généralement avec des cartes de crédit volées) pour constituer rapidement des réseaux de zombies importants. Dans de nombreux pays, les problèmes liés aux systèmes existants sont aggravés par l'utilisation généralisée de logiciels piratés, qui ne sont généralement pas corrigés et sont donc vulnérables aux exploits connus. Les entreprises qui utilisent beaucoup de logiciels piratés sont extrêmement difficiles à protéger, car elles fournissent aux acteurs malveillants un réservoir de systèmes qu'ils peuvent facilement assembler en menaces distribuées.

Les entreprises qui ont été confrontées à des attaques DDoS, ou qui appartiennent à des secteurs largement touchés par ces attaques, intègrent souvent les attaques potentielles dans leur modèle de risque et utilisent une combinaison de mesures d'atténuation des attaques DDoS proposées par les fournisseurs d'infrastructure et de mesures d'atténuation sur site gérées par l'entreprise. Les entreprises qui comprennent les risques et mettent en œuvre ces mécanismes sont l'exception. De nombreuses entreprises à risque n'ont pas conscience de l'impact potentiel des attaques DDoS sur leurs opérations. Ces entreprises peuvent ne pas comprendre pleinement leur capacité à protéger leurs réseaux, à répondre à une attaque et à s'en remettre. Par exemple, elles peuvent ne pas comprendre les limites de leurs contrats avec les fournisseurs d'infrastructure, ou la disponibilité des produits et services pour atténuer les attaques DDoS. Ils peuvent également ne pas comprendre pleinement le coût de la récupération après une telle attaque.

En l'absence d'une attaque en cours, les entreprises se concentrent traditionnellement sur la disponibilité, les fonctionnalités et le coût. En conséquence, les entreprises sont susceptibles de s'appuyer sur des dispositifs existants qui ne peuvent plus être sécurisés de manière adéquate, ou de déployer des dispositifs IoT et autres qui n'ont jamais été conçus pour être sécurisés. Où

[30] *Voir* David Goldman, *Major Banks Hit With Biggest Cyberattacks in History*, CNN (28 septembre 2012, 9:27 AM ET), http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html.

Lorsque les mises à jour de sécurité sont disponibles, les entreprises peuvent avoir des processus extrêmement onéreux pour évaluer les correctifs ou de longues périodes entre les maintenances programmées, ce qui élargit la fenêtre de vulnérabilité. [31]

Alors que les entreprises disposent généralement d'un personnel professionnel chargé des opérations informatiques, l'expertise spécifique à la cybersécurité fait souvent défaut. Cette difficulté est souvent aggravée par un manque de sensibilisation similaire chez les décideurs des organisations, qui sont responsables de l'affectation des ressources aux opérations informatiques au sein de leur organisation ou de la supervision de ces opérations. Les équipes chargées des opérations informatiques ne sont souvent pas conscientes des risques liés aux résolveurs ouverts et aux autres sources d'amplification des attaques, ni de l'importance du filtrage à l'entrée et à la sortie. Lorsque les FAI, par exemple, signalent à leurs clients une compromission potentielle, ils constatent souvent que l'entreprise ne peut pas identifier ou localiser les dispositifs compromis, et même si l'entreprise peut identifier et localiser les dispositifs, elle peut ne pas disposer des outils ou de l'expertise nécessaires pour rétablir un état sécurisé. Les entreprises peuvent avoir du mal à travailler en collaboration avec les fournisseurs de services lorsqu'elles sont attaquées. Si elles ne mettent pas en œuvre des procédures de sauvegarde de base, les entreprises risquent davantage d'avoir du mal à se remettre d'un ransomware distribué par des botnets.

Les entreprises peuvent contribuer à un écosystème plus résilient en combinant les technologies actuelles et émergentes, les politiques opérationnelles et d'approvisionnement, ainsi que la sensibilisation et l'éducation du personnel informatique et des décideurs.

Vision de l'avenir des réseaux d'entreprise

Une étape fondamentale vers cette vision consisterait à accroître l'application par les entreprises des principes contenus dans le cadre de cybersécurité du NIST (CSF). [32] La plupart des actions nécessaires peuvent être attribuées aux cinq fonctions simultanées et continues du cadre :

- **Identifier.** Les entreprises localisent les anciens appareils et les autres appareils qui ne peuvent pas être sécurisés. Dans la mesure du possible, elles retirent ces appareils à haut risque du service et les remplacent par des appareils qui sont intrinsèquement sûrs ou qui peuvent être sécurisés.
- **Protéger.** L'architecture du système fournit des couches de protection supplémentaires à tous les dispositifs à haut risque restants (par *exemple, l'*accès aux dispositifs existants serait limité par l'architecture du réseau). Les entreprises déploient ou se procurent des services d'atténuation des attaques DDoS sur site ou hors site. Les architectures réseau des entreprises limitent l'exposition des dispositifs aux acteurs malveillants et limitent les dommages causés par les attaques DDoS.
  les dispositifs compromis. Des filtres d'entrée et de sortie sont mis en place pour empêcher l'usurpation d'adresse réseau et les amplificateurs d'attaque (*par exemple, les* résolveurs ouverts) sont reconfigurés. Des processus de mise à jour efficaces minimisent la fenêtre de vulnérabilité de tous les dispositifs du réseau. Les infrastructures multilocataires appliquent également un filtrage à l'entrée et à la sortie afin de réduire l'impact des réseaux de zombies basés dans les nuages.
- **Détecter.** Une combinaison de services de détection basés sur les FAI et de surveillance des réseaux et des services exploités par les entreprises permet de détecter le trafic malveillant sortant et les attaques entrantes, et d'identifier les dispositifs compromis en temps quasi réel.
- **Répondre. Les** entreprises disposent de politiques et de procédures pour traiter les dispositifs compromis (par *exemple,* remplacer, atténuer ou patcher un dispositif participant à un botnet) lorsqu'ils sont détectés par l'entreprise ou

[31] *Voir* Dan Goodin, *Failure to Patch Two-month-old Bug Led to Massive Equifax Breach*, Ars Technica (13 sept. 2017), https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch- two-month-old-bug/. *Voir également* Federal Trade Commission, *Mobile Security Updates : Understanding the Issues* (février 2018), https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf.

[32] National Institute of Standards and Technology, *Cybersecurity Framework*, https://www.nist.gov/cybersecurity- framework (dernière visite le 4 avril 2018).

FAI. Les entreprises ont également mis en place des processus pour contacter leur(s) FAI ou d'autres fournisseurs de services anti-DDoS lorsque des attaques sont détectées localement. Les ressources opérationnelles clés continuent de fonctionner avec des ressources limitées.

- **Récupérer.** Les entreprises ont la possibilité de reconstituer les systèmes compromis (par *exemple,* à partir d'une sauvegarde) plutôt que de payer des rançongiciels pour reprendre leurs activités.

Les technologies et les politiques opérationnelles décrites ci-dessus ne sont réalistes que si elles sont soutenues par une combinaison appropriée de politiques d'approvisionnement et d'initiatives de sensibilisation et d'éducation. Le personnel et la direction de l'entreprise doivent être conscients des risques que les menaces distribuées font peser sur les ressources de l'entreprise, ainsi que des options de protection, de réponse et de récupération. Le personnel informatique doit posséder les compétences nécessaires pour mettre en œuvre les options d'atténuation et de prévention retenues. Les politiques d'achat des organisations doivent garantir que les questions relatives au cycle de vie de la sécurité figurent en bonne place dans les décisions d'achat, afin d'éviter que des produits non sécurisés soient ajoutés au système ou y restent connectés. Pour avoir un impact significatif sur l'écosystème, ces changements doivent se produire dans les entreprises à l'échelle mondiale, et pas seulement au niveau national.

Dispositifs de pointe : État actuel

Les appareils constituent un domaine technique diversifié et en pleine expansion de l'écosystème. L'internet prend simultanément en charge des systèmes informatiques multi-utilisateurs, des dispositifs informatiques personnels et mobiles, des technologies opérationnelles (par *exemple,* des systèmes de contrôle et d'acquisition de données [SCADA] dans des environnements industriels ou de fabrication) et des dispositifs IoT dans tout l'écosystème. En règle générale, les périphériques jouent deux rôles diamétralement opposés en ce qui concerne les menaces distribuées : les acteurs malveillants compromettent les périphériques pour créer des menaces distribuées, et les périphériques peuvent également être la cible de la menace (par *exemple*, les attaques de ransomware distribuées par des botnets). Les points d'extrémité mal sécurisés peuvent être à la fois les sources et les victimes des attaques.

Les acteurs malveillants sont motivés pour construire des botnets aussi bon marché et efficaces que possible. Au fil des ans, les cibles ont évolué, allant des machines professionnelles aux appareils domestiques mal sécurisés, en passant par les systèmes vulnérables gérés par les hébergeurs et les fournisseurs de services en nuage et, plus récemment, par les appareils IoT. Ces changements de cibles reflètent les promesses et les défis offerts par ce domaine technique en ce qui concerne la création d'un écosystème plus résilient. Les ordinateurs personnels et les appareils mobiles sont plus sûrs que par le passé. Parallèlement, les appareils connectés ont atteint un niveau de sophistication et de densité qui facilite leur ciblage par un code automatisé, alors que les avantages des outils de sécurité modernes font défaut à ces appareils.

Les dispositifs de bord peuvent être vulnérables à la compromission pour diverses raisons :

- Souvent, les dispositifs n'ont pas été conçus en tenant compte de la sécurité. Les développeurs ne connaissent pas les bonnes pratiques de conception en matière de sécurité, supposent que le dispositif sera inaccessible (*par exemple,* sur un réseau local inaccessible depuis Internet) ou veulent éviter les solutions de sécurité qui imposent des coûts supplémentaires, augmentent le temps de mise sur le marché ou rendent le dispositif plus difficile à utiliser pour les consommateurs. Les choix de conception qui en résultent, tels que les mots de passe administratifs codés en dur, créent des dispositifs intrinsèquement peu sûrs. Dans d'autres cas, des contrôles de sécurité appropriés sont présents mais la facilité d'utilisation et les interfaces utilisateur donnent lieu à des configurations moins sûres.

[33] Gartner, *Gartner Says 8,4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, (Feb. 7, 2017), *disponible à l'adresse* : https://www.gartner.com/newsroom/id/3598917.

- Les techniques courantes de développement de logiciels aboutissent, de manière optimiste, à une faille toutes les 2 000 lignes de code34 - ou plus selon de nombreux autres paramètres. [35] Bon nombre de ces bogues créent des vulnérabilités de sécurité exploitables, telles que des débordements de mémoire tampon.
- Lorsque les bogues sont découverts après le déploiement des produits, il peut être difficile, voire impossible, de les corriger. Ces vulnérabilités sont souvent beaucoup plus faciles à exploiter qu'à corriger.
- Les systèmes livrés avec des paramètres de configuration par défaut inappropriés, tels que des mots de passe codés en dur, sont plus vulnérables en fonctionnement.
- Les systèmes peuvent également être vulnérables parce que le support n'est pas disponible. C'est souvent le cas pour les anciens appareils.
- L'ampleur et la diversité des dispositifs déployés rendent difficile la mise en place de solutions simples et offrent des surfaces d'attaque supplémentaires pour les activités malveillantes.

Un certain nombre de grands développeurs de logiciels ont pris ces leçons à cœur et ont établi de meilleures pratiques actuelles qui peuvent réduire considérablement les vulnérabilités des dispositifs périphériques. Par exemple, le cycle de vie du développement logiciel de Microsoft, ou SDLC, garantit que la sécurité est prise en compte dès le début.
Les outils de développement de logiciels sécurisés, tels que le fuzzing36 ou l'analyse statique37, réduisent le nombre de vulnérabilités dans les logiciels. Les services de mise à jour sécurisés peuvent corriger les vulnérabilités après leur découverte. [38] Les systèmes sont livrés dans des configurations plus sûres, de sorte que les paramètres par défaut n'ont pas besoin d'être modifiés. Par conséquent, les serveurs, ordinateurs de bureau, ordinateurs portables et téléphones intelligents modernes offrent beaucoup moins de possibilités de compromission.
Cela s'applique également à l'environnement en nuage, les dispositifs périphériques plus sécurisés devenant une possibilité pratique. Les racines matérielles de confiance, qui démontrent que les systèmes n'ont pas été altérés, sont une autre innovation qui apparaît dans les systèmes modernes.

Malheureusement, les appareils IoT manquent souvent cruellement de fonctionnalités axées sur la sécurité. Ces systèmes offrent désormais la cible la plus attrayante pour les acteurs malveillants, et constituent un pourcentage de plus en plus important des appareils de l'écosystème. En fait, le rapport sur la mobilité d'Ericsson de novembre 2016 prévoit que les appareils IoT dépasseront les téléphones mobiles en tant que plus grande catégorie d'appareils connectés en 2018.[39] Compte tenu du niveau de sécurité des appareils IoT, il s'agit d'une prédiction décourageante.

---

[34] *Voir Coverity Scan : Open Source Report 2014*, Synopsys, page 4, (2015), http://go.coverity.com/rs/157-LQW- 289/images/2014-Coverity-Scan-Report.pdf.
[35] *Voir, par exemple,* Steve McConnell, *Code Complete : A Practical Handbook of Software Construction*, pages 521, 652, (Microsoft Press, 2e éd. 2004), ISBN : 0735619670.
[36] "Le test fuzz (fuzzing) est une technique d'assurance qualité utilisée pour découvrir les erreurs de codage et les failles de sécurité dans les logiciels, les systèmes d'exploitation ou les réseaux. Il consiste à introduire des quantités massives de données aléatoires, appelées fuzz, dans le sujet du test pour tenter de le faire planter." TechTarget - SearchSecurity.com, définition de fuzz testing (fuzzing), https://searchsecurity.techtarget.com/definition/fuzz-testing (dernière mise à jour en mars 2010).
[37] "L'analyse statique, également appelée analyse statique du code, est une méthode de débogage de programmes informatiques qui se fait en examinant le code sans exécuter le programme." TechTarget - SearchWinDevelopment.com, définition de l'analyse statique (analyse du code statique), https://searchwindevelopment.techtarget.com/definition/static-analysis (dernière mise à jour en novembre 2006).
[38] Le Software Assurance Forum for Excellence in Code (SAFECode), un consortium industriel, a publié un rapport pour codifier ces leçons et offrir des conseils supplémentaires sur le modèle SDLC. Mark Belk et al, *Fundamental Practices for Secure Software Development : A Guide to the Most Effective Secure Development Practices in Use Today*, SAFECode, (2nd ed.) (8 février 2011), *disponible à l'adresse* https://www.safecode.org/wp- content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf.
[39] Ericsson, *Ericsson Mobility Report : On the Pulse of the Networked Society*, (nov. 2016), https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november- 2016.pdf.

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

En outre, ce domaine de l'écosystème n'est pas composé uniquement d'appareils modernes. De nombreux serveurs, ordinateurs de bureau, ordinateurs portables et téléphones mobiles anciens sont utilisés aujourd'hui, et il en sera ainsi dans un avenir prévisible. Les appareils anciens ne sont plus pris en charge par leurs fabricants, de sorte que leurs vulnérabilités ne peuvent être facilement corrigées. [40] Pour aggraver les choses, les outils d'attaque pour ces appareils ou leurs composants de code vulnérables restent largement disponibles.

Enfin, des pourcentages élevés de systèmes informatiques personnels sur Internet utilisent des logiciels piratés ; les statistiques d'une association industrielle pour 2015 allaient de 17 % aux États-Unis à 70 % en Chine et 84 % en Indonésie. [41] Les fabricants limitent généralement la distribution de correctifs de sécurité aux seuls systèmes exécutant des logiciels achetés légalement, de sorte que ces systèmes ne peuvent pas être sécurisés contre les vulnérabilités connues. Bien que l'on ne puisse raisonnablement attendre des fournisseurs qu'ils fournissent une assistance pour les logiciels sans licence, ces systèmes non protégés constituent une autre catégorie de cibles faciles pour les acteurs malveillants, et soulignent la nature internationale de ce défi.

Les dispositifs non sécurisés ne sont généralement pas le résultat des limitations de la technologie sous-jacente. Bien qu'imparfaites, les meilleures pratiques actuelles, lorsqu'elles sont appliquées correctement, sont assez efficaces, permettent d'obtenir des dispositifs raisonnablement sûrs à la livraison et comprennent des outils pour maintenir ce niveau de sécurité tout au long du cycle de vie du dispositif. Les secteurs commerciaux qui ont adopté ces pratiques, comme les développeurs de systèmes d'exploitation, ont démontré des améliorations significatives en matière de sécurité et de résilience. [42] Malheureusement, ces pratiques de sécurité sont mises en œuvre de manière incohérente. De nombreux produits sont livrés avec des bogues connus, ne comportent pas de mécanisme de mise à jour et/ou ne suivent pas les meilleures pratiques actuelles en matière d'accès administratif.

Une partie de ce problème peut être résolue par une sensibilisation et une éducation accrues. Certains développeurs de produits ne savent pas comment exploiter les outils actuellement disponibles pour le développement de produits sécurisés. Les développeurs de produits technologiques opérationnels comprennent leur gamme de produits (*par exemple, les* réfrigérateurs), mais peuvent ne pas comprendre les exigences de sécurité de base pour la connectivité réseau de leurs produits. Les entreprises clientes prennent des décisions d'achat sans tenir compte des coûts du cycle de vie complet, ni des externalités d'un réseau non sécurisé. Les consommateurs finaux ne disposent pas toujours des outils nécessaires pour comprendre comment certaines caractéristiques des produits les protègent des risques de sécurité ou comment leurs appareils peuvent avoir un impact négatif sur l'écosystème.

Les incitations du marché semblent exacerber le problème. Les concepteurs de produits privilégient le délai de mise sur le marché et les fonctionnalités innovantes au détriment de la sécurité et de la résilience. Les caractéristiques de sécurité ne sont pas facilement comprises ou communiquées au consommateur, ce qui rend difficile la création d'une demande.

[40] Par exemple, Microsoft a cessé de prendre en charge Windows XP, vieux de douze ans, en avril 2014. Deux ans plus tard, entre 7,4 et 10,9 % de tous les ordinateurs de bureau fonctionnaient encore sous XP et étaient décrits comme des "canards assis que les cybercriminels pouvaient attaquer." John Zorabedian, *Millions of People Are Still Running Windows XP*, Naked Security (11 avril 2016), https://nakedsecurity.sophos.com/2016/04/11/millions-of-people-are-still-running-windows-xp/.

[41] *Voir* BSA | The Software Alliance, *Seizing Opportunity Through License Compliance : BSA Global Software Survey*, (mai 2016), http://www.bsa.org/~/media/Files/StudiesDownload/BSA_GSS_US.pdf.

[42] *Voir* Steven J. Vaughan-Nichols, *Security 2014 : The Holes Are in the Apps, not the Operating Systems*, ZDNet (28 février 2014, 19:46 GMT), http://www.zdnet.com/article/security-2014-the-holes-are-in-the-apps-not-the- operating-systems/.

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Vision de l'avenir des dispositifs de pointe

De grandes avancées dans le domaine technique des périphériques sont à la fois possibles et essentielles si nous voulons construire un écosystème Internet et de communication plus résilient. Pour être efficaces, ces avancées doivent être mondiales, car la majorité des dispositifs Internet sont situés en dehors des États-Unis. Cette action mondiale nécessitera des normes et des pratiques de sécurité acceptées au niveau mondial, qui devront être solides, largement comprises et appliquées de manière omniprésente. Ces normes doivent être flexibles, s'inscrire dans un calendrier approprié, être ouvertes, volontaires et orientées par l'industrie.

Les appareils doivent pouvoir résister aux attaques tout au long de leur cycle de vie - au moment de l'expédition, pendant l'utilisation et jusqu'à la fin de leur vie. Pour ce faire, la sécurité doit devenir une exigence de conception primordiale. Les fournisseurs ne doivent pas livrer de dispositifs présentant des failles de sécurité graves connues, doivent inclure un mécanisme de mise à jour sécurisé et doivent suivre les meilleures pratiques actuelles (par *exemple,* pas de mots de passe codés en dur, désactivation des fonctions logicielles qui ne sont pas essentielles au fonctionnement) pour la configuration et l'administration du système.
Les fournisseurs doivent communiquer aux clients la durée minimale de l'assistance et les fabricants de dispositifs doivent maintenir des services de mise à jour sécurisés pendant la durée promise. [43]

Les racines matérielles de la confiance et les technologies d'exécution de confiance font désormais partie intégrante de nombreuses plates-formes informatiques prêtes à l'emploi. Les produits futurs devront tirer parti de ces technologies pour démontrer l'authenticité et l'intégrité lors du déploiement initial et tout au long de la période d'utilisation. Les techniques de développement modernes reposent sur une combinaison de composants open source et de composants disponibles dans le commerce. Pour répondre aux futures exigences de sécurité, ces composants doivent être traçables tout au long de la chaîne d'approvisionnement et offrir une plus grande assurance.

Ces progrès nécessiteront des avancées significatives en matière de sensibilisation et d'éducation des développeurs de produits. Tous les développeurs de produits doivent être dotés des connaissances et des compétences nécessaires pour appliquer les outils disponibles pour le développement de produits sécurisés. Les kits d'outils et les composants utilisés par ces fournisseurs doivent refléter les préoccupations en matière de sécurité afin d'atteindre l'échelle et de suivre le rythme de l'évolution de la main-d'œuvre des développeurs, et les partenariats et consortiums à l'origine de la technologie normalisée doivent permettre aux développeurs de prendre et de communiquer des décisions en matière de sécurité. Pendant ce temps, les développeurs de produits technologiques opérationnels doivent ajouter des exigences de sécurité de base à leurs connaissances et compétences spécifiques aux produits. Dans le même temps, les clients doivent disposer de connaissances et d'informations suffisantes pour choisir des produits conçus pour être sécurisés dans leurs environnements, et doivent être conscients des risques présentés par tous les dispositifs, y compris les dispositifs hérités.

Enfin, les incitations du marché devront s'aligner sur ces progrès en matière de sécurité, de sorte que les développeurs de produits qui accordent la même priorité à la sécurité et à la résilience qu'aux délais de commercialisation et aux fonctionnalités innovantes soient récompensés. Des signaux clairs concernant la sécurité et la résilience des produits, accessibles aux clients, contribueront à améliorer ces incitations. Cependant, la proposition de valeur pour une meilleure sécurité commencera probablement dans l'environnement de l'entreprise en raison de ses économies d'échelle ; une fois qu'il existe une posture de sécurité généralement acceptée dans une classe de produits donnée, peu de fabricants seront susceptibles de l'ignorer.

[43] *Voir, par exemple*, le processus multipartite de la NTIA sur la capacité de mise à jour et de correction de la sécurité de l'Internet des objets - Groupe de travail sur la communication de la capacité de mise à jour et l'amélioration de la transparence, *Communiquer la capacité de mise à jour de la sécurité des dispositifs IoT pour améliorer la transparence pour les consommateurs*, (14 juillet 2017), https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-._jul_14_2017_-_ntia_multistakeholder_process.pdf (aider les fabricants à partager les détails des mises à jour de sécurité avec les consommateurs, et donner aux consommateurs les outils pour savoir ce qu'il faut rechercher).

Réseaux domestiques et de petites entreprises : État actuel

Les réseaux des particuliers et des petites entreprises sont de plus en plus complexes. Les appareils informatiques traditionnels interagissent avec le cloud et d'autres fournisseurs de services pour prendre en charge un éventail toujours plus large d'applications professionnelles et personnelles. Les dispositifs IoT prolifèrent déjà en grand nombre dans les foyers des consommateurs, qu'il s'agisse de dispositifs domotiques tels que les lumières, les ouvreurs de portes de garage et les thermostats, d'appareils électroménagers connectés ou de moniteurs de santé et de fitness personnels. Cette prolifération est également le cas dans les petites entreprises, où les entrepreneurs et les dirigeants peuvent chercher à tirer parti de la technologie disponible sur le marché, mais ne disposent pas d'un administrateur ou de stratégies ou politiques informatiques concertées. Selon toutes les estimations, le nombre d'appareils connectés destinés aux consommateurs devrait augmenter.

Malheureusement, ce domaine de croissance est aussi un domaine dans lequel la sécurité fait sérieusement défaut. La grande majorité des particuliers et des petites entreprises ne sont pas conscients des risques de cybersécurité, et beaucoup ne prennent pas les mesures de sécurité les plus élémentaires lorsqu'ils connectent des appareils à leur réseau. Les décisions relatives à la sécurité peuvent être prises sans l'avis ou la connaissance du client si le dispositif est installé et configuré par quelqu'un d'autre en son nom ou si le dispositif utilise un réseau autre que le propre réseau du consommateur (par exemple, un réseau cellulaire). Parallèlement, le partage des informations sur les menaces est un défi pour les petites entreprises, qui ne disposent généralement pas des ressources des grandes organisations pour recevoir et traiter les informations sur les menaces.

Comme dans les domaines détaillés ci-dessus, de nombreux outils existent généralement pour atténuer les risques liés à la cybersécurité, mais il n'est pas réaliste d'attendre de la population générale qu'elle soit capable de s'y retrouver dans l'environnement complexe de la sécurité. Les petites entreprises et les particuliers peuvent être victimes d'attaques DDoS - souvent en échange d'une rançon pour faire cesser les attaques - ou être les hôtes involontaires de dispositifs utilisés dans un botnet. Les produits pour réseaux domestiques ne sont généralement pas conçus de manière à permettre aux utilisateurs de segmenter facilement les réseaux ou de configurer les politiques de sécurité. De nombreux particuliers utilisent des appareils anciens ou des systèmes sans licence. En outre, lorsque l'appareil d'un particulier fait partie d'un botnet, il est souvent difficile pour le fournisseur de réseau de savoir quel appareil transmet, car la fonction NAT, qui permet aux particuliers de partager une seule adresse IPv4 entre de nombreux appareils derrière un routeur domestique, masque l'appareil qui est exploité. [44]

Sur le marché des particuliers et des petites entreprises, la plupart des appareils domestiques ne sont pas gérés et sont donc peu susceptibles d'être mis à jour manuellement, si les fonctions de mise à jour automatique ne sont pas disponibles. Les appareils grand public sont souvent livrés avec des logiciels obsolètes contenant des vulnérabilités connues ou des mots de passe administratifs codés en dur. L'utilisateur type peut ne pas être en mesure de déterminer si le logiciel de l'appareil est mis à jour ou s'il dispose même d'un mécanisme de mise à jour logicielle - ce qui n'est pas le cas de nombreux appareils grand public. L'utilisateur lambda n'est peut-être même pas conscient de l'importance de cet aspect, et n'a peut-être pas accès à des informations substantielles sur le logiciel d'un appareil donné.

Même si le réseau de la maison ou de la petite entreprise est bien architecturé et dispose de contrôles de sécurité solides, certains des appareils pris en charge sont susceptibles d'être mobiles et de se connecter à plusieurs réseaux au cours d'une journée normale. Ces réseaux peuvent ne pas être aussi bien gérés et les appareils peuvent être compromis lorsqu'ils se trouvent sur le réseau extérieur. Ces appareils présentent un risque supplémentaire en matière de cybersécurité, car ils permettent l'introduction de codes malveillants tout en contournant les contrôles locaux.

En général, les particuliers et les petites entreprises n'ont pas facilement accès aux informations dont ils ont besoin pour choisir des produits sûrs, et ils ne disposent généralement pas d'outils pour gérer les produits qu'ils possèdent. Alors que

[44] Nous notons également que la technologie NAT offre certains avantages en matière de sécurité en limitant l'accès du trafic entrant à des points d'extrémité spécifiques. Cela permet d'entraver (mais pas d'éliminer complètement) la menace que représentent les outils d'analyse et d'infection automatisés.

Les passerelles d'entreprise sont plus susceptibles de fournir des offres de sécurité intégrées, mais il est peu probable que les utilisateurs domestiques aient accès au même niveau de service, et pour ceux qui y ont accès, beaucoup ne sont pas conscients des offres de sécurité ou de la raison pour laquelle ces services devraient être mis en œuvre. Les mesures de sécurité fondamentales, telles que la modification du mot de passe par défaut d'un appareil ou l'activation d'un cryptage sécurisé, échappent souvent à la connaissance ou aux capacités des consommateurs. Dans certains cas, une mauvaise application de ces exigences peut contrarier les efforts des utilisateurs pour mettre en œuvre ces pratiques de base.

On craint que les consommateurs ne paient pas davantage pour des appareils offrant une meilleure sécurité. En réalité, les expériences des consommateurs ne sont généralement pas directement affectées par la compromission de leurs appareils ; en fait, le consommateur peut ne jamais savoir que son appareil fait partie d'un botnet. Du point de vue du consommateur, la webcam continue de fonctionner ou le réfrigérateur continue de refroidir. Pour cette raison, il peut être difficile de tenir les propriétaires responsables si leurs appareils sont utilisés dans un botnet. L'absence de conséquences claires de l'infection incite les consommateurs à prendre des mesures pour améliorer la sécurité, par exemple en mettant à jour les appareils qui peuvent l'être.

Vision de l'avenir des réseaux domestiques et des réseaux de petites entreprises

Il n'est pas réaliste d'attendre des utilisateurs privés et des propriétaires de petites entreprises qu'ils deviennent des experts en sécurité. Cependant, il existe des mesures que les acteurs du secteur et d'autres peuvent prendre pour améliorer la situation. Outre les efforts de sensibilisation et d'éducation visant à modifier le comportement des consommateurs, une autre approche consiste à concevoir des appareils en tenant compte du comportement des utilisateurs. Idéalement, les appareils commercialisés auprès des consommateurs devraient être conçus en intégrant la sécurité. Les produits grand public devraient être conçus de manière aussi sûre que possible, inclure des mécanismes de mise à jour automatisés et sécurisés, et n'avoir que peu ou pas d'exigences en matière de gestion des produits.

Dans l'idéal, les consommateurs auront accès à des offres commerciales qui mettent en œuvre les meilleures pratiques actuelles en matière de sécurité, et ils seront en mesure de reconnaître facilement ces offres. De même, les propriétaires de petites entreprises seront en mesure de faire correspondre leurs achats à leurs préoccupations et obligations uniques en matière de sécurité. Ils seront conscients des différents risques liés aux dispositifs IoT non sécurisés et choisiront des dispositifs plus sûrs.
Des organisations à but non lucratif et des entités commerciales ont commencé à évaluer les produits du point de vue de la protection de la vie privée et de la sécurité des données ; des efforts de ce type permettront de sensibiliser le public et, à mesure que la sensibilisation augmentera, les fabricants d'appareils devraient s'intéresser au développement sécurisé. Au fil du temps, il devrait devenir plus facile et moins coûteux pour les fabricants et les intégrateurs d'adopter un cycle de vie de développement sécurisé.

Si les utilisateurs domestiques ne sont pas particulièrement motivés par la crainte que leurs appareils soient utilisés dans un botnet, ils peuvent se sentir plus contraints par la crainte que leur vie privée, leurs données ou leur accès aux services ne soient compromis. De nombreux appareils connectés utilisent des services en nuage pour la gestion et le stockage des informations, ce qui a des implications supplémentaires en matière de sécurité et de confidentialité. Heureusement, la plupart des mesures qu'ils prendraient pour améliorer la sécurité de leur vie privée ou de leurs données et garantir un accès ininterrompu aux services réduiraient également le risque que leurs appareils fassent partie d'un botnet.

Avec des incitations correctement appliquées, les forces du marché peuvent jouer un rôle clé dans l'amélioration de la sécurité des dispositifs. Pour que les consommateurs adoptent largement des dispositifs plus sécurisés, ces derniers ne doivent pas coûter beaucoup plus cher que les dispositifs de sécurité.

[45] Bruce Schneier, *Security Economics of the Internet of Things*, Schneier on Security (10 oct. 2016, 10:26 AM) https://www.schneier.com/blog/archives/2016/10/security_econom_1.html (dernière mise à jour le 17 oct. 2016).
[46] Consumer Reports, *Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security*, (6 mars 2017), *disponible sur* https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating- products-services-for-privacy-and-data-security/.

des appareils non sécurisés. Les produits et services grand public devraient être conçus en intégrant des protections de base en matière de confidentialité et de sécurité. Des guides d'achat faciles à comprendre et fournissant des recommandations pratiques, ciblées sur les besoins spécifiques des particuliers et des petites entreprises, peuvent générer les signaux de marché nécessaires pour récompenser les développeurs et les vendeurs qui investissent dans la sécurité.

Les routeurs et les pare-feu intelligents devraient être largement utilisés pour atténuer les attaques et détecter lorsqu'un appareil a été compromis. À mesure que les appareils IoT des particuliers passent à des adresses IPv6 publiquement adressables, les FAI auront plus de facilité à identifier les appareils finaux transmettant du trafic malveillant. Les réseaux des particuliers appliquent la segmentation des réseaux virtuels. Limiter les capacités des appareils en fonction de leur utilisation prévue - par exemple, limiter les activités d'un grille-pain connecté sur le réseau aux seules activités nécessaires à l'exécution de ses tâches de grillage - limiterait considérablement la capacité des botnets à capturer les appareils domestiques. Un déclin mondial de l'utilisation domestique des produits anciens et des logiciels piratés limiterait aussi considérablement les possibilités des auteurs de botnets.

Les utilisateurs domestiques devraient être en mesure d'identifier les dispositifs de leurs réseaux qui augmentent leur risque de cybersécurité. Des travaux de recherche et développement sont en cours pour aider les consommateurs soucieux de sécurité à mieux gérer leurs réseaux. En 2017, l'IoT Home Inspector Challenge de la Federal Trade Commission (FTC) a décerné son premier prix à une proposition d'outil basé sur une application mobile qui aiderait les utilisateurs à gérer les appareils IoT de leur domicile. L'appli signalerait les appareils dont le logiciel n'est pas à jour et d'autres vulnérabilités courantes et fournirait des instructions sur la façon de mettre à jour le logiciel de chaque appareil et de corriger les autres vulnérabilités. [47]

L'éducation des consommateurs devra devenir plus efficace, même si les appareils sont mieux adaptés au niveau de compétence attendu des consommateurs. Entre-temps, il existe une possibilité de créer une nouvelle main-d'œuvre pour répondre aux besoins des consommateurs et des petites entreprises en matière de réseaux ; ce rôle pourrait devenir une nouvelle vocation, plus proche de celle des électriciens que de celle des ingénieurs électriciens, avec une formation appropriée. Les industries des réseaux et des dispositifs peuvent également rendre le soutien plus facile et moins coûteux grâce à la normalisation et à la coordination.

Gouvernance, politique et coordination

Étant donné que les attaques automatisées et distribuées sur l'internet mondial constituent un problème à l'échelle de l'écosystème, cette question nécessitera une coordination des solutions politiques et de gouvernance entre les secteurs. Aucun acteur ou secteur n'est responsable à lui seul de la gestion de ces risques, et aucune entité ne peut prétendre que ces risques sont le problème de quelqu'un d'autre. Par exemple, si de nombreuses solutions impliquent une coordination active avec les fournisseurs d'accès à Internet, le fait de placer la responsabilité exclusive au niveau du réseau rendrait imprudemment tout le trafic dépendant de cette couche connective pour déterminer à quoi ressemble le "bon" trafic, obligeant les fournisseurs d'accès à décider ce qui est fondamentalement autorisé ou non sur l'Internet. De plus, cette prise de décision des FAI bloquerait invariablement le trafic qui est en fait "bon", et manquerait le trafic qui devrait être bloqué ; le trafic crypté exacerberait le problème.

Étant donné la nature en réseau des risques, une véritable coordination est nécessaire pour comprendre pleinement le problème et identifier des pistes de solutions. Si les secteurs des technologies de l'information et des communications s'emploient activement à comprendre les risques pour la sécurité, certains secteurs éprouvent des difficultés à partager les informations et à se coordonner en dehors de leur propre secteur. Certaines entités coordonnent leur action au niveau national ou régional, mais il est nécessaire de partager davantage d'informations sur les menaces, les solutions, leur adoption et leur efficacité à l'échelle mondiale. Sur le site

[47] Federal Trade Commission, *IoT Home Inspector Challenge*, https://www.ftc.gov/iot-home-inspector-challenge (dernière visite le 4 avril 2018).

Dans de nombreux cas, le manque de clarté concernant les rôles et les responsabilités a entravé l'action collective, entraînant des défaillances en matière de sécurité.

Certains gouvernements s'appuient sur des réglementations trop spécifiques qui deviennent rapidement obsolètes, entravent l'innovation et limitent les avantages pour le consommateur dans les secteurs dynamiques. Les exigences de conformité, ou la mise en place de réglementations spécifiques, peuvent permettre de faire face à certains risques, mais elles peuvent entraîner une charge plus lourde tout en laissant l'écosystème plus large dans l'insécurité ou en envoyant le signal que la conformité à la réglementation est suffisante plutôt que le minimum nécessaire. Le tableau réglementaire est encore compliqué par la réglementation nationale ou locale des dispositifs périphériques, de la technologie opérationnelle et de l'infrastructure. Les solutions spécifiques à certains pays ou juridictions mettent en danger la nature globale d'un écosystème où les bits et les produits circulent avec une relative facilité, et peuvent désavantager les innovateurs locaux.

Ce problème est encore aggravé par la nature inter-domaines de la technologie en réseau. Les frontières se sont estompées entre la technologie grand public, les outils et les dispositifs de niveau entreprise dont dépendent les organisations, et la technologie critique pour la sécurité dont peuvent dépendre des vies. Le même matériel et les mêmes logiciels peuvent être utilisés dans l'ensemble de l'écosystème. Les services d'infrastructure clés peuvent être utilisés aussi bien par un réseau de jeux vidéo que par le réseau d'entreprise d'une société.

Dans le domaine de l'application de la loi, la coopération de l'industrie dans le démantèlement des botnets s'améliore, mais n'est pas encore monnaie courante. Les récents démantèlements réussis de botnets ont nécessité une importante collaboration avec l'industrie dans les cas, par exemple, de Kelihos, Gameover Zeus et Coreflood. Une collaboration active entre les forces de l'ordre et le secteur privé a permis de perturber les activités en saisissant des actifs clés de commandement et de contrôle. Aux États-Unis, en 2016, la règle fédérale de procédure pénale 41(b)(6) a été modifiée pour répondre aux défis uniques des enquêtes sur les activités des botnets, en précisant que les tribunaux peuvent délivrer des mandats autorisant la perquisition de plusieurs ordinateurs lorsque les ordinateurs identifiés sont situés dans plusieurs districts judiciaires. En outre, la capacité des services fédéraux d'application de la loi à obtenir des injonctions civiles - ce qui s'est avéré indispensable dans le cadre de démantèlements antérieurs de botnets - est limitée aux affaires comportant des éléments d'écoute électronique ou certains types de fraude. Le démantèlement des botnets de manière sûre et sécurisée est un processus long et laborieux. En outre, les forces de l'ordre ont du mal à identifier et à poursuivre les acteurs malveillants responsables des botnets, en particulier ceux qui opèrent en dehors des États-Unis.

Vision pour l'avenir de la gouvernance, des politiques et de la coordination

À l'avenir, les acheteurs - qu'il s'agisse de consommateurs finaux ou d'entreprises sophistiquées - devraient être mieux à même de comprendre les risques et les propriétés de sécurité des appareils connectés. Il est nécessaire d'adopter des approches de l'IdO et des dispositifs informatiques qui contribueront non seulement à sensibiliser les consommateurs, mais aussi à stimuler le marché, en augmentant l'adoption générale et l'utilisation de meilleures pratiques de cybersécurité par les fabricants de dispositifs. Cela dit, le risque de sécurité évolue rapidement ; ce qui est considéré comme sûr aujourd'hui peut ne pas l'être demain, et il est peu probable qu'il le soit dans dix ans. Les solutions de transparence du marché peuvent permettre aux acheteurs de prendre de bonnes décisions, mais elles doivent également tenir compte du contexte et de l'échelle de temps du cycle de vie du produit. Les institutions qui se sont appuyées sur des approches qui reflétaient traditionnellement un risque statique, comme les exigences d'achat ou les assurances, devront s'adapter pour refléter la nature évolutive du risque de cybersécurité. Une meilleure transparence des composants logiciels et matériels des systèmes sera utile, tout comme des incitations appropriées pour comprendre les risques pertinents dans un contexte donné et pour l'écosystème dans son ensemble.

Les acteurs de l'infrastructure partageront et analyseront mieux les données afin de favoriser une connaissance commune des réputations dans l'ensemble de l'écosystème et d'évaluer dans quelle mesure les partenaires du réseau traitent les risques de manière évolutive, efficace et décentralisée. Les mécanismes de partage de l'information devraient s'appuyer sur les mécanismes existants.

les mécanismes multipartites et les communautés, créant ainsi de nouvelles possibilités d'engagement au niveau local et mondial.

À mesure que les menaces distribuées évoluent, de nouvelles normes, directives et mesures peuvent être nécessaires pour répondre à des questions nouvelles et émergentes telles que : Comment les tiers peuvent-ils évaluer au mieux les produits pour les avantages des consommateurs d'une manière suffisamment agile pour suivre l'évolution rapide des pratiques de sécurité ? Quelles mesures et quelle visibilité sur les pratiques de gestion des réseaux peuvent nous informer sur les investissements dans les infrastructures ? Des attentes plus formelles mais adaptables en matière de sécurité nous permettront d'introduire une certaine responsabilité dans les pratiques de sécurité. Des mécanismes tels que les cadres volontaires peuvent contribuer à la fois à créer des incitations à une conception plus sûre et à responsabiliser les personnes qui ne prennent pas en compte la sécurité et n'investissent pas dans des dispositifs sûrs. Tout mécanisme de responsabilisation doit récompenser ceux qui prennent de bonnes décisions fondées sur le risque, tout en reconnaissant que la sécurité parfaite n'existe pas.

Pour faire face à l'éventail des menaces, toutes les parties prenantes, nationales et internationales, doivent s'attaquer plus complètement aux attaques automatisées et distribuées. Il s'agit essentiellement de réduire le nombre de dispositifs non sécurisés ayant accès à l'Internet afin de limiter la taille des réseaux de zombies et de mettre au point des mécanismes permettant de partager les informations sur les systèmes compromis et les nouvelles tendances en matière d'attaques, en amont et en aval de la pile de réseaux, avec la ou les parties les mieux placées pour répondre à la menace.

Le déploiement des technologies étant véritablement transnational et les informations circulant au-delà des frontières internationales, rien de tout cela ne peut être accompli sans collaboration internationale. Dans le domaine international, le gouvernement américain plaide vigoureusement en faveur d'approches dirigées par l'industrie et de normes volontaires, fondées sur le consensus. Comme l'indique le rapport du NSTAC, les solutions dépendent à la fois des normes et de l'innovation au niveau des réseaux et de l'infrastructure Internet. Bien qu'il existe une variété de normes, de cadres et de meilleures pratiques pertinents, ils ne sont pas pleinement exploités dans le monde entier.

Les gouvernements peuvent influencer de manière constructive le développement de produits plus sûrs en prenant des mesures telles que le soutien de normes ouvertes, volontaires et axées sur l'industrie, et en prenant leurs propres décisions en matière d'acquisition de technologies et de dispositifs de manière à créer des incitations commerciales en faveur de produits plus sûrs.
La sécurité peut également être favorisée par un engagement multipartite accru entre les communautés de lutte contre les abus et d'infrastructure de réseau mondial, ainsi qu'entre les éléments de cybersécurité et de technologie opérationnelle des industries qui ne sont pas traditionnellement axées sur les TI (par *exemple,* les services publics ou les appareils médicaux). Par exemple, l'engagement opérationnel et multipartite lié aux ressources Internet utilisées par les gestionnaires de botnets pour le commandement et le contrôle est essentiel à la signalisation des menaces pour la gestion des réseaux et la détection des botnets. Les États-Unis devraient accroître leur engagement international dans ce domaine, en particulier avec les pays qui sont déjà actifs sur cette question.

En outre, l'industrie et les services répressifs devraient s'efforcer de trouver des moyens de se coordonner plus souvent et plus tôt pour détecter et prévenir les activités menaçantes, et pour gérer les incidents qui se produisent. De nouveaux outils et processus pourraient améliorer le partage de l'information entre les organismes internationaux d'application de la loi. Les services répressifs et les groupes industriels devraient communiquer plus efficacement sur ce qui est nécessaire pour réussir à perturber les réseaux malveillants et poursuivre les acteurs qui en sont à l'origine, tout en gardant à l'esprit les préoccupations en matière de protection de la vie privée. Les politiques de protection des données, tant aux États-Unis qu'au niveau international, ne devraient pas perturber les outils existants, tels que la base de données WHOIS, largement utilisée pour les données relatives à la propriété des domaines.

Paysage juridique

Certaines parties prenantes ont souligné l'importance de minimiser l'incertitude et le risque juridique pour encourager la collaboration du secteur privé avec les organismes chargés de l'application de la loi, un plus grand partage des informations, la divulgation des vulnérabilités et la capacité à mener des contre-mesures efficaces. Beaucoup ont également souligné la nécessité d'harmoniser les approches juridiques entre les secteurs afin d'éviter un patchwork de lois qui pourrait entraver le marché de l'IdO.

Des efforts sont déjà en cours pour améliorer les relations public-privé. Le Centre national d'intégration de la cybersécurité et des communications (NCCIC) du DHS sert de lieu central où un ensemble diversifié de partenaires du secteur privé et du gouvernement impliqués dans la cybersécurité coordonnent leurs efforts[48], y compris le partage d'informations, la collaboration et l'assistance technique. [49] Le droit fédéral comprend déjà une structure permettant de répondre à une partie de l'incertitude et du risque juridique. La loi de 2015 sur le partage des informations en matière de cybersécurité (CISA), par exemple, accorde une protection en matière de responsabilité et d'autres protections juridiques - telles que des protections antitrust, des exceptions aux lois sur la divulgation et à certaines utilisations réglementaires, et des protections contre les renonciations aux privilèges - aux entités privées qui partagent des indicateurs de cybermenaces et des mesures défensives conformément à la loi. [50] La CISA désigne le NCCIC comme centre de partage des indicateurs de cybermenaces et des mesures défensives avec le gouvernement fédéral. Ces capacités de cybersécurité du NCCIC et les protections juridiques de la CISA s'appliquent à la cybersécurité de l'IdO de la même manière qu'elles s'appliquent à la cybersécurité en général. En outre, rien dans la CISA n'empêche les entités privées de partager avec les forces de l'ordre des informations solides dans le cadre du déroulement normal d'une enquête criminelle ; en effet, la CISA autorise le partage d'indicateurs de cybermenace et de mesures défensives avec les forces de l'ordre - ou toute autre entité fédérale - et, en outre, sa protection en matière de responsabilité s'applique lorsque ces informations sont partagées avec les forces de l'ordre dans certaines circonstances.

De nombreuses parties prenantes ont également souligné l'importance des incitations commerciales pour sécuriser les dispositifs IdO. Certains se sont demandé si un régime de responsabilité fondé sur des normes et des pratiques exemplaires communes pourrait améliorer la responsabilité en matière de sécurité des dispositifs IdO. Bien que le présent rapport ne s'engage pas dans une analyse exhaustive de la responsabilité liée à la sécurité des dispositifs IdO, nous pensons que cette question continuera à susciter de l'intérêt à mesure que l'utilisation des dispositifs connectés - des dispositifs qui peuvent avoir un impact sur le monde physique - augmentera et que des questions concernant les préjudices, les problèmes de confidentialité, la protection des consommateurs, les chaînes de causalité, la gestion des risques et les actions possibles des États et des tribunaux émergeront. La responsabilité est un domaine complexe du droit, tout comme le marché émergent de l'IdO, et il faut veiller à éviter les exigences de conformité statiques et inefficaces, en particulier au milieu d'un paysage dynamique de cybersécurité. Des investissements doivent être réalisés pour faire face aux risques par le biais de pratiques innovantes, et avec des parties prenantes engagées dans une coordination intersectorielle. La pression pour aborder directement cette question augmentera si l'incertitude juridique est endémique et persistante.

Certaines parties prenantes ont noté que tout nouveau régime juridique ou réglementaire pourrait avoir des effetsnégatifs involontaires sur le secteur des TI si des orientations claires ne sont pas incluses concernant ce qu'un fournisseur peut faire pour limiter son exposition. Toutefois, les défenseurs mettent en garde contre les protections générales en matière de responsabilité sans gains sociaux clairs découlant de l'amélioration des processus de sécurité. Certaines parties prenantes, y compris des organisations de la société civile, ont demandé des éclaircissements supplémentaires sur la manière dont les lois existantes dans diverses juridictions s'appliquent dans ce domaine, sur la manière dont ces lois peuvent ou doivent affecter les différentes parties prenantes le long des chaînes d'approvisionnement et de distribution, et sur la manière de traiter correctement les préjudices. Alors que ce domaine continue d'évoluer, il est essentiel que le gouvernement fédéral comprenne mieux l'interaction entre la responsabilité et les incitations du marché, ainsi que la manière dont tout changement proposé pourrait modifier cette dynamique. Il faut veiller à ce que nos lois sur la responsabilité profitent aux consommateurs, protègent les parties prenantes le cas échéant et évitent de freiner l'innovation dans l'environnement numérique actuel. Au fur et à mesure que la collaboration entre les secteurs public et privé se poursuit dans ce domaine, le gouvernement fédéral

devrait continuer à vérifier si la protection contre la responsabilité liée au partage d'informations est suffisante dans l'environnement actuel pour faire face efficacement aux menaces actuelles et nouvelles.

III. Objectifs et actions

Ces objectifs et actions visent à présenter un portefeuille d'actions se renforçant mutuellement qui, si elles sont mises en œuvre, amélioreront considérablement la résilience de l'écosystème. Les actions recommandées comprennent des activités en cours qui devraient être poursuivies ou étendues, ainsi que de nouvelles initiatives. Aucun investissement ou activité ne peut à lui seul atténuer toutes les menaces, mais les discussions organisées et les commentaires des parties prenantes nous permettront d'évaluer plus avant et de hiérarchiser ces activités en fonction du retour sur investissement attendu et de leur capacité à avoir un impact mesurable sur la résilience de l'écosystème. Nous attendons des parties prenantes de l'ensemble de l'écosystème qu'elles collaborent avec le gouvernement pour mettre en œuvre les activités proposées, saisir les occasions de soutien et de leadership, et supprimer les obstacles à la mise en œuvre.

Objectif 1 : définir une voie claire vers un marché technologique adaptable, durable et sûr.

Pour renforcer la résilience de l'écosystème de l'Internet et des communications, il est essentiel que notre marché technologique soutienne et récompense le développement, l'adoption et l'évolution continus de technologies et de processus de sécurité innovants. Lorsque les incitations du marché encouragent les fabricants à présenter les innovations en matière de sécurité comme un complément équilibré aux fonctionnalités et aux performances, cela favorise l'adoption d'outils et de processus qui aboutissent à des produits plus sûrs. Au fur et à mesure que ces caractéristiques de sécurité deviennent plus populaires, la demande accrue stimule la recherche. Au fur et à mesure que ces outils sont perfectionnés, il devient moins coûteux pour les fabricants, les intégrateurs et les propriétaires/exploitants de systèmes d'adopter les composants d'un cycle de développement sécurisé, ce qui encourage davantage de fabricants à différencier leurs produits en fonction de la qualité de leurs fonctions de sécurité et permet ainsi une plus grande concurrence. Cette section identifie les actions que les principales parties prenantes peuvent entreprendre pour établir un marché technologique adaptable, durable et sécurisé.

Action 1.1 : à l'aide de processus inclusifs dirigés par l'industrie, établir des lignes de base de capacités IoT applicables au niveau international pour assurer la sécurité du cycle de vie des applications domestiques et industrielles, sur la base de normes internationales volontaires dirigées par l'industrie.

[48] *Voir* 6 U.S.C. § 148.
[49] *Id.* § 148(c).
[50] *Voir* Consolidated Appropriations Act, 2016, Division N - Cybersecurity Act of 2015 (Pub. L. No. 114-113, 129 Stat. 2242) (codifié à 6 U.S.C. §§ 1501-1510).
[51] La CISA offre une série de protections juridiques pour les indicateurs de cybermenaces et les mesures défensives qui sont partagés avec une entité fédérale conformément à la loi. Par exemple, elle prévoit une protection contre la responsabilité antitrust (6 U.S.C. § 1503(e)) ; les lois fédérales et étatiques sur la divulgation (6 U.S.C. §§ 1504(d)(3) et 1503(d)(4)(B)) ; la renonciation aux privilèges (6 U.S.C. § 1504(d)(1)) ; et l'utilisation réglementaire fédérale et étatique (6 U.S.C. §§ 1503(d)(4)(C) et 1504(d)(5)(D)). Lorsque les indicateurs de cybermenace et les mesures défensives sont partagés avec le NCCIC par le biais de la capacité du gouvernement fédéral et du processus géré par le DHS, ce partage bénéficie également de protections supplémentaires en matière de responsabilité. 6 U.S.C. § 1504(c)(1)(B). Ces protections supplémentaires en matière de responsabilité sont également disponibles pour le partage avec d'autres entités fédérales dans des circonstances limitées. *Voir* 6 U.S.C. § 1504(c)(1)(B)(i) et (ii).

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Les normes de sécurité, les lignes de base et les meilleures pratiques ont évolué au fil du temps pour les dispositifs informatiques traditionnels, augmentant le coût de l'assemblage de botnets avec ces dispositifs. L'augmentation rapide du déploiement de dispositifs IoT non sécurisés a eu l'effet secondaire pernicieux de permettre le développement rentable de botnets extrêmement importants et largement distribués. Par exemple, les botnets Mirai ont compromis des centaines de milliers d'appareils grâce à des mots de passe administratifs codés en dur. Plus récemment, le botnet Reaper a compromis des appareils en ciblant des vulnérabilités logicielles bien connues. Bien qu'il existe des mesures d'atténuation, de nombreux appareils touchés ne peuvent être corrigés. Comme les mots de passe ne peuvent pas être changés et que les vulnérabilités ne peuvent pas être corrigées, ces appareils resteront vulnérables tout au long de leur cycle de vie. Ces vulnérabilités pourraient être atténuées dans les futurs systèmes IdO si les meilleures pratiques actuelles en matière de sécurité pour les appareils informatiques traditionnels, telles que des configurations par défaut sécurisées et des mécanismes efficaces de mise à jour des logiciels, étaient appliquées aux appareils IdO.

L'impact des botnets passés a été atténué par les mesures prises par les fournisseurs d'infrastructure tels que les FAI - principalement des actions de cessation et d'abstention et l'absorption du trafic excessif - mais les mesures d'atténuation passées étaient principalement de nature réactive, et l'augmentation exponentielle des dispositifs et systèmes IoT indique que les rendements de ces stratégies d'atténuation traditionnelles diminuent. L'écosystème doit devenir plus résilient aux menaces distribuées, en commençant par une approche proactive et ciblée sur la réduction des vulnérabilités connues des appareils connectés à l'internet tout au long de leur cycle de vie.

Les 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 d'appareils et de systèmes IoT moins vulnérables à la compromission tout au long de leur cycle de vie. [52] Par exemple, une base de référence pour les environnements domestiques pourrait inclure des mécanismes de mise à jour sécurisés, tels que l'application automatique de correctifs de sécurité et des configurations sécurisées par défaut, qui minimisent la nécessité d'une intervention de l'utilisateur. Une base de référence en matière de sécurité pour une industrie peut supposer un personnel de sécurité dévoué et compétent qui utilise des processus tels que des mises à jour gérées de manière centralisée. Ces lignes de base doivent être suffisamment souples pour s'appliquer lorsque les dispositifs IoT sont à la fois un produit et un service (c'*est-à-dire* lorsque les services en nuage font partie intégrante du fonctionnement du produit) et lorsque les capacités de sécurité sont réparties sur un système de dispositifs IoT.

Lors de l'élaboration de ces lignes de base, nous devons mettre en balance l'investissement dans les exigences de base et les coûts de la non-utilisation des lignes de base (c'*est-à-dire* les coûts pour les personnes potentiellement lésées, les coûts pour le fabricant du produit et les coûts pour les autres parties prenantes). Les lignes de base des capacités doivent être pragmatiques afin de garantir que les fabricants puissent répondre aux exigences de manière rentable, tout en offrant un avantage clair au client et à l'écosystème. Pour atteindre cet équilibre, ces lignes de base doivent être élaborées sous la direction de l'industrie, en collaboration avec le client visé (*par exemple,* un consortium représentant un secteur industriel, ou des groupes de défense des consommateurs et de la société civile représentant les utilisateurs domestiques) et avec la contribution et la participation actives des gouvernements, le cas échéant. La collaboration dans l'élaboration des lignes de base permet aux fabricants de disposer d'un temps d'avance et d'un aperçu précoce des attentes des clients, et augmente la probabilité que des produits conformes soient disponibles en temps voulu. La participation des clients à l'élaboration des lignes de base peut également indiquer au marché que les acheteurs préfèrent des dispositifs IdO conçus pour être sécurisés dans leurs environnements cibles et permettre l'alignement des activités d'éducation décrites ci-dessous. Les capacités spécifiées dans la ligne de base devenant la norme de facto, cela favorisera un marché durable pour des dispositifs plus sûrs.

[52] Les normes fondées sur les performances décrivent *ce qui* doit être réalisé, plutôt que la *manière d'*y parvenir, ce qui réduit ou élimine les impacts négatifs sur l'innovation.

Pour que les coûts d'opportunité d'innovation perdus n'écrasent pas la valeur de la base de référence, les bases de référence de la sécurité de l'IdO qui identifient un petit nombre de capacités de sécurité flexibles doivent imposer des contraintes minimales (le cas échéant) sur la conception et la mise en œuvre. [53] La spécification des capacités en termes de performance plutôt que de conception (c'*est-à-dire* une approche fondée sur les résultats plutôt que prescriptive) aidera à gérer les coûts associés aux programmes d'évaluation correspondants. La limitation de l'ensemble des fonctionnalités présente un avantage supplémentaire : il devient également plus pratique pour les plateformes de développement communes d'intégrer ces ensembles de fonctionnalités dans les composants de l'IdO, ce qui simplifie le développement de produits conformes.

Un fondement pour les futures bases de référence

Plusieurs spécifications ont été publiées récemment et offrent, au minimum, une base solide pour les futures lignes de base des capacités de sécurité de l'IdO. Ces efforts vont de spécifications de haut niveau à des documents extrêmement détaillés et ciblent un éventail d'environnements d'application. Parmi les exemples notables de spécifications de haut niveau axées sur les appareils de qualité grand public, toutes publiées depuis juin 2017, citons le cadre de sécurité IoT de l'Online Trust Alliance[54], la norme numérique (élaborée par une coalition comprenant Consumer Reports, Ranking Digital Rights et le Cyber Independent Testing Lab),[55] et *Secure by Design : Improving the cyber security of consumer Internet of Things56* du ministère britannique du numérique, de la culture, des médias et du sport. Un exemple de spécification de base détaillée est constitué par les *recommandations de sécurité de base pour l'IdO dans le contexte des infrastructures d'information* critiques[57], publiées en novembre 2017 par l'Agence de l'Union européenne pour la sécurité des réseaux et de l'information, qui identifie 83 mesures techniques et bonnes pratiques de sécurité applicables à la sécurité de l'IdO. Un autre exemple est le document "Security Tenets for Life Critical Embedded Systems", élaboré par un groupe de travail intersectoriel composé de membres de la base industrielle de la défense et du secteur des technologies de l'information. [58]

Action 1.2 Le gouvernement fédéral devrait s'appuyer, le cas échéant, sur les lignes de base de capacités développées par l'industrie pour établir des lignes de base de capacités pour les dispositifs IoT dans les environnements du gouvernement américain, afin de répondre aux exigences de sécurité fédérales, de promouvoir l'adoption de lignes de base dirigées par l'industrie et d'accélérer la normalisation internationale.

L'action 1.1 est axée sur le développement, sous la direction de l'industrie, de bases de référence de capacités pour les dispositifs IdO dans différents environnements de menace. Cette approche crée de multiples défis, allant du développement de multiples profils concurrents à l'absence de toute base de référence pour un environnement critique. En outre, lorsque les efforts menés par l'industrie sont axés sur le plan national, il peut être difficile de les faire accepter au niveau international. Le gouvernement fédéral peut accélérer la convergence là où il existe de multiples bases de référence, lancer de nouveaux efforts

[53] Par exemple, une ligne de base peut spécifier une exigence de gestion des correctifs sans surveillance sans préciser un modèle pull ou push, si les correctifs doivent être chiffrés ou le type exact de protection de l'intégrité appliqué au correctif.[54] *Voir* Online Trust Alliance, *Internet of Things*, https://otalliance.org/initiatives/internet-things (dernière visite le 4 avril 2018).
[55] The Digital Standard, *The Standard*, https://www.thedigitalstandard.org/the-standard (dernière visite le 4 avril 2018). [56] Département du numérique, de la culture, des médias et du sport, *Secure by Design : Improving the cyber security of consumer Internet of Things*, (7 mars 2018), *disponible sur* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_. pdf.
[57] Agence de l'Union européenne pour la sécurité des réseaux et de l'information, *Recommandations de sécurité de base pour l'Internet des objets dans le contexte des infrastructures d'information critiques*, (20 novembre 2017), *disponible à l'adresse* https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.
[58] Département de la sécurité intérieure des États-Unis, *Security Tenets for Life Critical Embedded Systems*, https://www.dhs.gov/publication/security-tenets-lces (dernière publication le 12 janvier 2017).

en établissant un projet de discussion lorsqu'il n'existe pas de base de référence, et encourager la normalisation internationale en établissant des bases de référence fédérales en matière d'IdO.

En établissant des bases de référence fédérales pour les capacités de sécurité de l'IdO en coordination avec l'industrie, la société civile et les partenaires internationaux, le gouvernement fédéral peut démontrer le caractère pratique et l'efficacité des capacités spécifiées, contribuer aux incitations du marché et établir une base pour des programmes d'évaluation pratiques (voir actions 5.1 et 5.2). Cette approche garantira également que les bases de référence du gouvernement fédéral reflèteront l'état de l'art et évolueront en fonction de l'évolution de l'industrie et du marché. Le National Institute of Standards and Technology (NIST) est chargé d'élaborer des normes et des lignes directrices en matière de sécurité des informations, y compris des exigences minimales pour les systèmes fédéraux. Le NIST devrait identifier les exigences de sécurité pour les dispositifs et systèmes IdO dans les environnements fédéraux. Lorsque des lignes de base consensuelles dirigées par l'industrie existent, le NIST devrait évaluer leur applicabilité aux exigences de sécurité fédérales et, le cas échéant, élaborer une norme fédérale par référence. Ces bases de référence des capacités fédérales seraient similaires (et suivraient la progression) aux bases de référence industrielles développées dans l'action 1.1. Si une base de référence appropriée n'est pas disponible, le NIST devrait rechercher des partenaires industriels pour le développement d'une base de référence pratique et d'un projet de discussion pour les efforts futurs de l'industrie.

Au fur et à mesure que l'efficacité de ces lignes de base est prouvée, le gouvernement et l'industrie des États-Unis devraient également s'engager conjointement avec les développeurs de normes et de spécifications internationales volontaires dirigées par l'industrie afin d'établir des normes pertinentes à l'échelle mondiale. Au fur et à mesure de l'émergence de ces normes et spécifications, des lignes de base fédérales devraient être créées, mises à jour ou remplacées, le cas échéant.

Le lieu de normalisation de ces lignes de base doit être choisi avec soin. Les lignes de base en matière de sécurité et toutes les normes et spécifications connexes doivent être élaborées par des organismes du secteur privé ouverts à la participation de toutes les parties intéressées. Elles doivent être élaborées de manière transparente, en utilisant des processus équilibrés fondés sur le consensus et en adoptant, dans la mesure du possible, une approche fondée sur les résultats plutôt que sur les exigences. Ces normes fondées sur les performances sont les mieux adaptées pour relever les défis posés par un espace technologique en évolution rapide, tel que l'IdO. Ces processus n'excluent pas la participation du gouvernement, mais garantissent que les intérêts du gouvernement, de l'industrie, de la société civile et des utilisateurs sont tous bien représentés, et que les solutions qui en résultent reflètent l'état de l'art dans cet espace technologique.
La flexibilité de ces processus permet également de mettre à jour les normes à mesure que la technologie, les menaces et les solutions évoluent. La forte concordance entre l'utilisation par les entreprises des normes qu'elles ont contribué à élaborer et le soutien des gouvernements au développement de ces outils facilite l'adoption de ces normes à grande échelle.

Il est important de reconnaître que, compte tenu de l'ampleur de l'espace technologique, aucun organisme de développement de normes ou de spécifications ne peut à lui seul développer toutes les solutions. Les gouvernements du monde entier doivent soutenir la coopération et la coordination entre les organismes de normalisation et de spécification qui disposent de l'expertise et de l'expérience nécessaires et qui développent des produits selon les principes évoqués ci-dessus, afin de garantir des solutions solides, opportunes et adaptées. Aux États-Unis, le NIST devrait continuer à diriger et à coordonner l'engagement des agences fédérales dans les activités de normalisation connexes, y compris l'engagement avec le secteur privé, en explorant une stratégie du gouvernement fédéral à l'appui des normes internationales pour relever les défis des botnets et autres menaces automatisées et distribuées.

Des actions complémentaires de la part du gouvernement américain et du secteur privé pourraient renforcer considérablement les effets de ces bases de référence fédérales en matière de capacités IoT. Le gouvernement fédéral peut utiliser les règles d'acquisition et les directives de passation de marchés pour amplifier le signal du marché en exigeant les capacités de la ou des lignes de base (cf.

Action 2.3) et, le cas échéant, préférer les produits qui sont également conformes à un système d'étiquetage donné du secteur privé (voir actions 5.1 et 5.2).

Action 1.3 L'industrie doit adopter plus largement des outils et des processus de développement de logiciels permettant de réduire considérablement l'incidence des failles de sécurité dans les logiciels commerciaux. Le gouvernement fédéral devrait collaborer avec l'industrie pour encourager l'amélioration et l'application de ces pratiques et pour améliorer l'adoption et la responsabilité du marché.

Les techniques courantes de développement de logiciels produisent des logiciels comportant au moins un bogue pour 2 000 lignes de code[59], et les systèmes modernes comprennent des dizaines de millions de lignes de code. Cela implique des dizaines de milliers de bogues dans un système, dont beaucoup créent des failles de sécurité. Les mécanismes de mise à jour sécurisée (notés comme une caractéristique de base importante dans l'action 1.1) permettent aux fournisseurs de corriger ces erreurs après une période de vulnérabilité relativement brève. Cependant, éviter complètement ces vulnérabilités aurait un impact encore plus important en termes de réduction du risque de sécurité. S'il est possible de développer un code comportant un très petit nombre d'erreurs, lorsque l'importance de la mission mérite une réduction significative de la productivité, le défi consiste à développer des mécanismes qui produisent un code nettement meilleur sans réduire indûment la productivité.

Un groupe de travail interagences (documenté dans le rapport NIST Interagency/Internal Report [NISTIR] 815160) a identifié de nombreuses approches pour développer des logiciels présentant moins de vulnérabilités, en mettant en œuvre trois stratégies de base :

- Arrêter les vulnérabilités avant qu'elles ne se produisent, notamment en améliorant les méthodes de spécification et de construction des logiciels ;
- la découverte de vulnérabilités, notamment par l'amélioration des techniques de test et l'utilisation plus efficace de méthodes de test multiples
- Réduire l'impact des vulnérabilités en construisant des architectures plus résilientes, de sorte que les vulnérabilités ne puissent pas être exploitées de manière significative.

Des outils pour soutenir ces approches sont maintenant disponibles[61] et ont été adoptés par quelques entreprises avant-gardistes[62]. Les développeurs de logiciels devraient commencer à adopter ces outils immédiatement, en se concentrant d'abord sur les produits qui présentent le plus de risques. Le DHS et la FTC offrent également des ressources aux petits développeurs de logiciels. [63]

[59] *Voir Coverity Scan, supra* note 34, à la page 4.

[60] Paul E. Black, Lee Badger, Barbara Guttman et Elizabeth Fong, Dramatically *Reducing Software Vulnerabilities : Report to the White House Office of Science and Technology Policy*, (Nov. 2016), NIST Interagency/Internal Report No. 8151, *disponible sur* http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf.

[61] *Voir, par exemple*, *CWE/SANS Top 25 Most Dangerous Software Errors*, SANS Institute, https://www.sans.org/top25- software-errors/ (dernière mise à jour le 27 juin 2011).

[62] Par exemple, le Software Assurance Marketplace (SWAMP) vise à faciliter le test systématique de la qualité et de la sécurité de ces applications et à apporter un changement transformateur au paysage de l'assurance logicielle en réduisant le nombre de faiblesses déployées dans les logiciels. Pour plus d'informations, voir Software Assurance Marketplace, https://continuousassurance.org/ (dernière visite le 4 avril 2018).

[63] Le DHS a soutenu le développement du SWAMP, qui propose à la fois des outils d'assurance logicielle basés sur le cloud et des outils open source. Pour plus d'informations, voir Software Assurance Marketplace, *About Swamp*, https://continuousassurance.org/about-us/ (dernière visite le 4 avril 2018) ; Federal Trade Commission, *Careful Connections : Building Security in the Internet of Things*, (janvier 2015),

Le gouvernement fédéral devrait soutenir l'adoption de ces outils par l'industrie en améliorant le retour sur investissement ou en créant des incitations commerciales pour les secteurs ou les groupes industriels en retard, comme le NSTAC l'a également recommandé dans son rapport. Le gouvernement fédéral devrait promouvoir le développement d'outils pour des pratiques de codage sécurisées en parrainant ou en effectuant des recherches ciblées (voir Action 1.4), et en parrainant des concours pour des chaînes d'outils sécurisées (processus multi-outils pour le développement de logiciels) afin de démontrer leur efficacité et leur productivité. Le gouvernement fédéral devrait également collaborer avec l'industrie et la société civile pour élaborer des stratégies qui rendent l'adoption de ces approches plus facile et moins coûteuse - y compris l'éducation et la formation abordées en détail ci-dessous - en gardant à l'esprit les exigences des petites entreprises, et travailler avec l'ensemble des parties prenantes pour rendre ce processus observable et vérifiable par des tiers.

À titre d'exemple, les produits modernes utilisent de nombreux composants logiciels, bibliothèques et modules, dont certains peuvent être obsolètes ou vulnérables et ne sont pas toujours suivis de près par les fabricants dans le cadre du cycle de développement rapide. Si la notion de transparence autour des composants logiciels n'est pas nouvelle, elle n'a pas été largement soutenue et adoptée. La NTIA devrait engager diverses parties prenantes dans l'examen des stratégies et des politiques nécessaires pour favoriser un marché pour une plus grande transparence des composants logiciels, y compris l'identification et l'exploration du marché et d'autres obstacles qui peuvent entraver les progrès dans ce domaine. Savoir quels logiciels ont été intégrés dans un produit est une étape fondamentale pour pouvoir le maintenir à jour et atténuer les menaces lorsqu'elles se présentent.

Action 1.4 L'industrie devrait accélérer le développement et le déploiement de technologies innovantes pour la prévention et l'atténuation des menaces distribuées. En conséquence, le cas échéant, les pouvoirs publics devraient accorder la priorité à l'utilisation des fonds de recherche et de développement et aux efforts de transition technologique pour soutenir les progrès en matière de prévention et d'atténuation des DDoS, ainsi que les technologies de base pour empêcher la création de botnets. Le cas échéant, la société civile devrait amplifier ces efforts.

La croissance rapide de la capacité DDoS offerte par les botnets basés sur l'IoT met en péril l'efficacité des techniques actuelles d'atténuation des DDoS. La recherche et le développement de techniques d'atténuation plus proches de la source ou exploitant de nouvelles analyses de données, l'apprentissage automatique ou l'intelligence artificielle (IA) sont nécessaires de toute urgence pour devancer les acteurs malveillants. Des innovations seront nécessaires pour lutter contre d'autres activités malveillantes soutenues par les botnets, telles que les ransomwares et la propagande informatique. Des technologies de base permettant de prévenir, de détecter et de récupérer la compromission et l'incorporation dans un botnet seront nécessaires pour faire face à ces attaques et à celles à venir.

Pour renforcer la résilience de l'écosystème, il faut capitaliser sur les succès de la recherche et du développement par un déploiement agressif. Les technologies innovantes en matière de dispositifs, telles que les racines de confiance matérielles ou les mécanismes améliorés d'authentification des dispositifs, offrent la possibilité de renforcer considérablement la sécurité tout au long du cycle de vie des produits. Les progrès des outils de réseau, tels que la description de l'utilisation par le fabricant (MUD), une norme actuellement en cours de développement au sein de l'IETF[64], pourraient améliorer la résilience du réseau en gérant les communications pour la sécurité et en rendant la gestion granulaire du réseau plus efficace.

---

https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections- buildingsecurityinternetofthings.pdf.

[64] *Voir* E. Lear, R. Droms & D. Romascanu, *Manufacturer Usage Description Specification (*Draft), Internet Engineering Task Force - Network Working Group, https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/ (dernière mise à jour le 19 avril 2018).

moins cher et plus facile. L'adoption accélérée de ces technologies innovantes améliorerait la résilience de l'écosystème, mais la commercialisation et l'adoption de résultats de recherche prometteurs pour créer des produits viables ou des services commercialisables sont notoirement difficiles. La société civile et les groupes à but non lucratif peuvent également amplifier les nouvelles plates-formes ou solutions, comme l'ont fait l'Internet Society et la Global Cyber Alliance pour leurs initiatives respectives de promotion de la sécurité du routage[65,66] et l'American Civil Liberties Union pour son initiative sur la vie privée et la technologie[67]. [67]

En tant que source essentielle de financement de la recherche fondamentale en matière de cybersécurité, le gouvernement fédéral devrait soutenir cette action par un financement ciblé et des activités de transition technologique en collaboration. Les ministères et les agences parrainent également la recherche appliquée à l'appui des exigences de la mission et une variété d'activités de transition technologique. [68] Les agences devraient donner la priorité au développement et au déploiement d'innovations qui augmenteraient la résilience de l'écosystème et coordonner ces investissements par le biais du programme Networking and Information Technology Research and Development (NITRD). [69] Comme pour l'utilisation de toute technique d'atténuation, des mesures doivent être prises pour s'assurer que ces technologies innovantes n'exposent pas les consommateurs à des risques inutiles pour la vie privée. Pour ce faire, on peut utiliser les outils d'évaluation des risques pour la vie privée décrits dans la norme NISTIR 806270 ou procéder à une évaluation des incidences sur la vie privée[71]. [71]

Action 1.5 Les pouvoirs publics, les entreprises et la société civile devraient collaborer pour faire en sorte que les meilleures pratiques, les cadres et les lignes directrices existants en matière d'IdO, ainsi que les procédures visant à garantir la transparence, soient plus largement adoptés dans l'ensemble de l'écosystème numérique. Les risques émergents dans l'espace IoT doivent être abordés de manière ouverte et inclusive.

Plusieurs initiatives antérieures ont donné lieu à des orientations et à des meilleures pratiques concernant les botnets et l'amélioration de la sécurité de l'IdO, mais les botnets restent un problème. Par exemple, les parties prenantes du processus multilatéral de la NTIA sur la mise à niveau et le correctif de la sécurité de l'IdO ont élaboré un ensemble de documents proposant des solutions à la fois pour l'offre et la demande du marché des consommateurs de l'IdO, mais les parties prenantes ont également souligné le rôle partagé dans la promotion de ces idées au sein de la communauté IdO. La publication de documents ne suffit pas : nous devons veiller à ce qu'ils soient largement adoptés par l'écosystème. La communauté de l'IdO doit travailler en collaboration pour identifier et adopter les meilleures pratiques, les cadres et les lignes directrices existants qui sont

[65] *Voir* Internet Society, *MANRS : Mutually Agreed Norms for Routing Security*, https://www.internetsociety.org/issues/manrs/ (dernière visite le 4 avril 2018).
[66] *Voir* Global Cyber Alliance, *Quad9 : quatre étapes simples vers la sécurité, la confidentialité et la performance*, https://www.globalcyberalliance.org/initiatives/quad9.html (dernière visite le 4 avril 2018).
[67] *Voir* ACLU, *Privacy & Technology,* https://www.aclu.org/issues/privacy-technology (dernière visite le 4 avril 2018).
[68] Le projet Distributed Denial of Service Defense du DHS est un exemple de ces recherches. *Voir le* ministère américain de la Sécurité intérieure, *Distributed Denial of Service Defense*, https://www.dhs.gov/science-and-technology/csd-ddosd (dernière visite le 4 avril 2018). *Voir également* National Science Foundation, *Secure and Trustworthy Cyberspace (SaTC)*, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709 (dernière visite le 4 avril 2018).
[69] Le programme de recherche et développement sur les réseaux et les technologies de l'information, https://www.nitrd.gov/ (dernière visite le 4 avril 2018).
[70] Sean Brooks, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman et Ellen Nadeau, An *Introduction to Privacy Engineering and Risk Management in Federal Systems, (*janv. 2017), NIST Interagency/Internal Report n° 8062, *disponible sur* https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
[71] Pour plus d'informations sur un type d'évaluation des incidences sur la vie privée, voir U.S. Department of Homeland Security, *Privacy Impact Assessment Guidance*, https://www.dhs.gov/publication/privacy-impact-assessment-guidance (dernière publication le 13 avril 2018).
[72] NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (dernière mise à jour le 7 novembre 2017).

pertinents pour l'IdO. La communauté de l'IdO devrait également s'efforcer de faire connaître ces meilleures pratiques, cadres et directives. Le rapport du NSTAC fait également état de ce besoin, en lien avec sa recommandation selon laquelle l'industrie devrait travailler avec le DHS et le Commerce pour accélérer l'adoption de directives de sécurité.

Le gouvernement fédéral devrait soutenir l'adoption généralisée des meilleures pratiques en engageant la communauté à déterminer pourquoi les recommandations antérieures n'ont pas été largement mises en œuvre ou ont échoué, à identifier les voies appropriées pour favoriser une mise en œuvre réussie et à se concentrer sur des outils et des leviers pratiques et éprouvés. Par exemple, les pratiques de développement actuelles mettent l'accent sur la réutilisation des logiciels libres et commerciaux, qui peuvent être obsolètes ou vulnérables, mais ces attributs de l'(in)sécurité sont cachés aux développeurs et aux clients. Le processus multipartite de la NTIA sur la transparence des composants logiciels (voir l'action 1.3) peut explorer les moyens d'accroître les garanties qu'aucune vulnérabilité connue n'est livrée avec les produits.

Un problème particulièrement contrariant qui nécessitera la contribution des parties prenantes est la question du code hérité et orphelin, ou "logiciel mort". Les parties prenantes au processus multipartite de la NTIA sur les correctifs ont identifié l'importance de communiquer la période pendant laquelle les mises à jour de sécurité seraient fournies, mais n'ont pas offert d'orientation explicite sur ce qui se passerait lorsque les mises à jour de sécurité ne seraient plus offertes. [73] Comme les biens durables ayant une longue durée de vie sont de plus en plus liés à un code fragile, ce problème va s'amplifier. Un expert en sécurité est même allé jusqu'à préconiser que les logiciels abandonnés soient rendus open source. [74] L'accès au code n'est cependant qu'un obstacle. Les mises à jour doivent encore être écrites et testées. Les fournisseurs en faillite présentent des défis supplémentaires si les certificats de signature ou les fichiers MUD (voir Action 1.4) sont liés aux domaines. L'initiative Core Infrastructure propose un modèle pour traiter les externalités des logiciels insuffisamment pris en charge[75], mais la perspective de faire face systématiquement aux systèmes non maintenus distribués dans le monde entier nécessitera la contribution d'un large éventail de parties prenantes.

Des pratiques transparentes et vérifiables de gestion des actifs logiciels (SAM) peuvent aider les entreprises à identifier les logiciels qui ne peuvent pas être corrigés parce que les mises à jour ne sont plus disponibles ou que les licences ont expiré. Une fois identifiées, les entreprises peuvent remédier à ces vulnérabilités en remplaçant les produits ou en réorganisant les réseaux pour gérer les risques. Les entreprises et les acteurs gouvernementaux devraient adopter des pratiques SAM fondées sur les normes internationales en matière d'approvisionnement et de gestion des actifs, ainsi que des procédures pour atténuer les risques identifiés grâce à ces pratiques.

Des efforts complémentaires visant à sensibiliser et à éduquer les développeurs et les fabricants de produits pourraient renforcer considérablement l'impact de ces meilleures pratiques, cadres et lignes directrices, comme décrit dans les actions 5.3, 5.4 et 5.5.

[73] Le rapport de la FTC sur les mises à jour de sécurité mobile recommande aux entreprises d'envisager la divulgation de la période d'assistance minimale et les notifications avant la fin de la période d'assistance de sécurité. Commission fédérale du commerce, *Mobile Security Updates : Understanding the Issues*, (fév. 2018), https://www.ftc.gov/system/files/documents/reports/mobile- security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf . [74] Dan Geer, discours liminaire à Black Hat USA 2014 : *Cybersecurity as Realpolitik*, (6 août 2014), *disponible à l'adresse* http://geer.tinho.net/geer.blackhat.6viii14.txt (ébauche de livraison nominale). Vidéo disponible à l'adresse : https://www.blackhat.com/us-14/video/cybersecurity-as-realpolitik.html.

[75] Initiative pour une infrastructure de base, https://www.coreinfrastructure.org/ (dernière visite le 4 avril 2018).

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Objectif 2 : promouvoir l'innovation dans l'infrastructure pour une adaptation dynamique à l'évolution des menaces.

Afin d'établir un écosystème Internet et de communication plus résilient, les normes et pratiques qui dissuadent, préviennent et/ou atténuent les réseaux de zombies et les menaces distribuées doivent être continuellement mises en œuvre et améliorées dans tous les domaines de l'écosystème en réponse et en anticipation de l'évolution de la menace. Cette section identifie les actions à la disposition des parties prenantes pour soutenir le développement d'une infrastructure efficace et dynamique.

Action 2.1 Les fournisseurs de services Internet et leurs partenaires d'échange de trafic[76] devraient étendre le partage d'informations actuel afin de parvenir à un partage plus rapide et plus efficace des informations sur les menaces exploitables, tant au niveau national que mondial.

Une fois établis, les botnets sont revendus ou loués à plusieurs clients et redirigés pour attaquer de nouvelles cibles. Cela signifie que de nombreux FAI et leurs partenaires d'échange de trafic seront confrontés à des attaques similaires au fil du temps. Lorsqu'un FAI est confronté pour la première fois à une menace particulière, il doit analyser les comportements anormaux et élaborer des méthodes d'atténuation. Les botnets sont généralement répartis entre de nombreux FAI, chacun d'entre eux pouvant contribuer aux activités d'atténuation si les connaissances sont suffisantes. Le partage des techniques de gestion de réseau et des tactiques défensives efficaces contre des menaces particulières est un autre moyen pour les grands fournisseurs de réseaux d'augmenter la valeur préventive des informations partagées.

Les accords actuels de partage d'informations entre les FAI et leurs partenaires d'échange de trafic sont très efficaces dans leur domaine. En partageant les informations sur les menaces connues, en cours et émergentes, les FAI sont en mesure de réagir plus efficacement. Cependant, les accords actuels de partage d'informations sont souvent motivés par des relations personnelles et ne sont pas complets, en particulier lorsqu'il s'agit de menaces plus nuancées ou plus sensibles. L'évolution du paysage des réseaux et l'évolution de la portée, de l'échelle, de l'orientation et de la diversité des acteurs des réseaux ont également un impact sur l'efficacité des relations de partage. La collaboration entre les FAI et leurs partenaires d'échange de trafic doit être formalisée et inclure le partage de la détection, de la notification et des méthodes d'atténuation prévues ou utilisées au sein du réseau. Lorsque le partage est entravé par des préoccupations d'ordre commercial, les FAI doivent chercher des moyens d'aborder les dispositions de partage et la coordination des réponses dans leurs accords d'échange de trafic et de transit.

L'industrie devrait diriger les efforts visant à étendre la portée et l'utilité du partage d'informations entre les FAI et leurs partenaires d'échange de trafic et à combler les lacunes dans l'opérationnalisation des informations partagées. En particulier, l'industrie doit travailler en collaboration avec la société civile et le gouvernement pour améliorer les réponses coordonnées aux informations exploitables et diriger le développement, le perfectionnement et la normalisation des protocoles de partage d'informations afin d'augmenter la vitesse et de permettre une réponse automatisée. Une attention particulière doit être accordée à l'engagement et à l'inclusion des petits fournisseurs de services Internet et aux développements de protocoles qui améliorent leur participation.

Bien que l'industrie joue un rôle de premier plan, le gouvernement fédéral peut faciliter cette activité à l'échelle nationale par l'entremise du Centre d'analyse et de partage de l'information sur les communications (ISAC) (c*.-à-d.* le Centre national de coordination des communications [NCC]), en forgeant des partenariats avec les groupes d'exploitants de réseaux (NOG), à l'échelle internationale par un engagement continu dans le Forum of Incident Response and Security Teams (FIRST), et en élargissant les accords de partage de l'information avec des pairs internationaux comme Telecom ISAC Japan. Le gouvernement peut jouer un rôle important dans ces discussions, en convoquant

[76] Cela inclut les entreprises qui exploitent leurs propres routeurs BGP et serveurs DNS.

des réunions multipartites si nécessaire, en fournissant une vue d'ensemble et en veillant à ce que le processus soit équitable pour toutes les parties prenantes. Les équipes nationales de réponse aux incidents de sécurité informatique (CSIRT) peuvent également assurer une coordination directe et catalyser la réponse des gestionnaires de ressources et des acteurs de l'infrastructure au niveau local.

Action 2.2 Les parties prenantes et les experts en la matière, en consultation avec le NIST, devraient diriger l'élaboration d'un profil CSF pour la prévention et l'atténuation des attaques DDoS en entreprise.

Les entreprises sensibilisées aux attaques DDoS qui souhaitent atténuer l'impact de futures attaques DDoS et réduire la probabilité que des ressources internes soient incorporées dans des botnets pour attaquer d'autres entreprises constatent que des directives complètes ne sont pas facilement disponibles. Les grandes entreprises sont obligées de consacrer d'importantes ressources en personnel à l'identification et à l'acquisition ou au déploiement de mécanismes appropriés. Les petites entreprises manquent souvent d'expertise ou ne peuvent se permettre de consacrer ces ressources à l'élaboration d'une stratégie anti-DDoS. Les solutions globales sont complexes et nécessitent souvent une combinaison de services commerciaux externes et gérés localement. Il est donc essentiel de communiquer les besoins aux fournisseurs.

Le Cadre pour l'amélioration de la cybersécurité des infrastructures critiques (connu sous le nom de CSF) version 1.0 a été développé par le NIST avec une contribution importante du secteur privé, tout comme la version 1.1, publiée en avril 2018. Le CSF fournit une approche flexible de la gestion du risque de cybersécurité qui intègre les normes et les meilleures pratiques de l'industrie, est suffisamment général pour permettre une large applicabilité dans une variété d'environnements - y compris l'IdO - et a été largement accepté par l'industrie. Le CSF peut être complété par des profils de cadre, qui appliquent les composantes du cadre à une situation spécifique. En particulier, les secteurs industriels peuvent utiliser des profils pour documenter les meilleures pratiques de protection contre des menaces spécifiques. Le CSF est conçu pour évoluer au fil du temps, à mesure que l'environnement de la cybersécurité change.

Les entreprises qui souhaitent améliorer la résilience de leurs propres réseaux contre les attaques DDoS et se protéger contre les botnets qui incorporent leurs ressources bénéficieraient grandement de la disponibilité d'un profil CSF[77] pour la prévention et l'atténuation des attaques DDoS en entreprise. Un effort mené par l'industrie, en consultation avec le NIST, le monde universitaire et d'autres experts en la matière, devrait développer un profil CSF pour la prévention et l'atténuation des attaques DDoS en entreprise, en se concentrant sur l'état souhaité de la cybersécurité organisationnelle pour atténuer les attaques DDoS. Le profil CSF fournirait des conseils aux entreprises et établirait un langage commun pour les discussions concernant les mécanismes de protection contre les attaques DDoS avec les fournisseurs de produits, les FAI et les autres fournisseurs d'infrastructure. Le profil aiderait les entreprises à identifier les possibilités d'améliorer l'atténuation des menaces DDoS et contribuerait à la hiérarchisation des priorités en matière de cybersécurité en comparant leur état actuel avec l'état cible souhaité. Le profil comprendrait probablement plusieurs niveaux pour soutenir les secteurs industriels ayant des exigences de résilience différentes.

Le champ d'application du profil CSF devrait inclure, au minimum, les mécanismes d'atténuation des attaques DDoS sur site et hors site, les fonctions de sécurité du routage (par *exemple, le* filtrage à l'entrée de la meilleure pratique actuelle [BCP] 38/84) et les conseils sur la fermeture des vecteurs de réflexion. Pour une applicabilité maximale, le profil doit être rédigé de manière à couvrir à la fois les grandes entreprises, qui peuvent exploiter les éléments clés de leurs stratégies d'atténuation des attaques DDoS, et les petites entreprises, qui dépendent souvent entièrement des fournisseurs de services.

[77] Les profils CSF sont des compilations de conseils et de meilleures pratiques autour de menaces particulières qui suivent le modèle CSF bien établi.

[78] La Coalition for Cybersecurity Policy & Law (Cybersecurity Coalition) a lancé un effort prometteur, actuellement sous forme de projet. *Voir* Cybersecurity Coalition, *Threat Profile for DDoS Attacks Using NIST Framework*, https://www.cybersecuritycoalition.org/threat-profile-ddos-nist-framework (28 juillet 2017).

Les parties prenantes du gouvernement devraient participer à l'élaboration de ce profil afin de s'assurer qu'il est assez largement applicable pour servir de profil CSF pour la prévention et l'atténuation des DDoS au niveau fédéral. Pour créer des incitations commerciales, cette action devrait être soutenue par une adoption agressive dans l'ensemble du gouvernement fédéral, comme spécifié dans l'action 2.3, soit par l'application directe du profil, soit par l'application des contrôles correspondants en utilisant le processus existant de la loi fédérale sur la modernisation de la sécurité de l'information.

Action 2.3 Le gouvernement fédéral devrait donner l'exemple et démontrer l'aspect pratique des technologies, en créant des incitations commerciales pour les premiers adoptants.

Après la publication des lignes de base pour la sécurité des dispositifs IoT (action 1.1), le gouvernement fédéral devrait établir des lignes directrices pour l'approvisionnement afin de fournir des incitations commerciales aux premiers utilisateurs. De nombreux fournisseurs de produits IoT ont formulé des plans pour améliorer la sécurité de leurs produits, mais les observateurs s'inquiètent du fait que les incitations du marché sont fortement axées sur le coût et le délai de mise sur le marché. S'il n'est pas prouvé que les clients absorberont les coûts supplémentaires liés au développement de produits plus sécurisés, l'industrie pourrait être incitée à une course vers le bas. Bien que les marchés publics fédéraux ne dominent plus le marché, leur pouvoir d'achat et leur influence sont encore forts, et le gouvernement américain peut montrer l'exemple. En élaborant des lignes directrices pour les marchés publics fédéraux fondées sur les bases de sécurité des dispositifs IdO, le gouvernement américain peut mettre en place des incitations commerciales pour les premiers utilisateurs. L'Office of Management and Budget, la General Services Administration (GSA) et le ministère de la Défense peuvent faciliter ces exigences d'approvisionnement par le biais de politiques et de modifications du calendrier de la GSA et des règlements d'acquisition fédéraux. [79]

Dès la publication d'un profil CSF approprié (action 2.2), le gouvernement fédéral devrait mettre en œuvre des mesures de prévention et d'atténuation DDoS de base pour tous les réseaux fédéraux afin de renforcer la résilience de l'écosystème et de démontrer le caractère pratique et l'efficacité du profil. Par le passé, des pirates ont exploité des réseaux fédéraux dans des attaques DDoS en utilisant des résolveurs ouverts et d'autres ressources d'agences pour amplifier leurs attaques. Le gouvernement fédéral doit montrer l'exemple, en veillant à ce que les ressources fédérales ne soient pas des participants involontaires et que les réseaux fédéraux soient préparés à détecter, atténuer et répondre si nécessaire. L'administration devrait rendre obligatoire la mise en œuvre du profil CSF fédéral pour la prévention et l'atténuation des attaques DDoS par toutes les agences gouvernementales dans un délai déterminé après l'achèvement et la publication du profil.

Le gouvernement fédéral devrait évaluer et mettre en œuvre des moyens efficaces pour inciter à l'utilisation d'outils et de processus de développement de logiciels qui réduisent considérablement l'incidence des vulnérabilités de sécurité dans tous les achats de logiciels fédéraux, par exemple par des exigences d'attestation ou de certification. Afin d'inciter le marché à développer des logiciels sécurisés, le gouvernement fédéral devrait établir des règles d'achat qui favorisent ou exigent des logiciels commerciaux développés à l'aide de tels processus, lorsqu'ils sont disponibles. Le gouvernement fédéral devrait également s'assurer que les projets de développement de logiciels financés par le gouvernement utilisent les meilleurs outils disponibles pour obtenir un aperçu de l'impact de ces réglementations.

[79] Le groupe de travail sur la sécurité de l'IdO du Conseil de coordination des technologies de l'information (Information Technology Coordinating Council), dirigé par le DHS, rédige actuellement des conseils à l'intention des responsables des achats sur les questions à poser à leurs clients, à leurs équipes informatiques et de sécurité, ainsi qu'aux fournisseurs, afin de s'assurer qu'un appareil connecté acheté s'inscrit dans la posture de gestion des risques de l'agence. Ces conseils viendront compléter, mais ne seront pas identiques, aux directives de conformité élaborées en fonction des bases de sécurité.

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Action 2.4 L'industrie, les pouvoirs publics et la société civile doivent collaborer avec l'ensemble des parties prenantes pour continuer à améliorer et à normaliser les protocoles de partage des informations.

Pour faire face aux menaces automatisées et distribuées, les parties prenantes doivent partager des informations solides en temps quasi réel. Le rapport du NSTAC indique que la collaboration entre les secteurs public et privé est essentielle pour atténuer les réseaux de zombies. Les protocoles de partage d'informations actuellement utilisés ont été mis au point par le gouvernement fédéral, avec la participation active d'un large éventail de parties prenantes, mais ils ne répondent pas nécessairement aux besoins de toutes les parties prenantes.

Par exemple, les petites entreprises sont sous-représentées ; elles ne contribuent pas à la plupart des accords actuels de partage d'informations et n'en bénéficient pas. Pour répondre aux besoins des petites entreprises, qui ne disposent généralement pas d'une équipe interne solide en matière de cybersécurité, les protocoles devront peut-être permettre une action automatisée. Par exemple, les fournisseurs d'accès à Internet peuvent souvent identifier le réseau client associé à un dispositif compromis, mais n'ont pas la visibilité nécessaire pour identifier des dispositifs spécifiques. Les petites entreprises peuvent ne pas être en mesure d'identifier ces appareils si elles sont contactées par leur FAI. Des protocoles de partage d'informations permettant aux FAI de partager des informations sur les dispositifs compromis détectés avec les routeurs des petites entreprises pourraient permettre une identification automatisée et un contrôle plus solide des clients sur leurs dispositifs en réseau. Les clients pourraient également choisir de partager les résultats de toute mesure d'atténuation avec leurs FAI, de la même manière qu'ils partagent les informations sur les défaillances logicielles avec les fournisseurs.

Pour répondre aux besoins de coordination et de collaboration d'une infrastructure hautement résiliente, ces protocoles de partage de l'information doivent avoir une portée globale, être accessibles à un large éventail d'entreprises et être suffisamment précis pour permettre un traitement et une réponse automatisés. Pour garantir l'atteinte de ces objectifs, l'industrie devrait diriger les efforts, en collaboration avec le gouvernement fédéral et d'autres parties prenantes, afin d'améliorer les protocoles de partage de l'information pour répondre aux besoins des parties prenantes et établir des normes internationales pour faciliter la coordination mondiale.

Action 2.5 Le gouvernement fédéral devrait collaborer avec les fournisseurs d'infrastructures américains et mondiaux pour étendre les meilleures pratiques en matière de gestion du trafic réseau à l'ensemble de l'écosystème.

Si l'on ne peut attendre des fournisseurs de réseaux qu'ils jouent le rôle de gendarmes du trafic et identifient tous les mauvais paquets, les outils et les pratiques, tant courants que nouveaux, peuvent contribuer à filtrer certains types de mauvais trafic. De nombreux acteurs du marché utilisent soit des signaux de réputation informels, soit des accords d'échange de trafic et de transit plus formels pour gérer le trafic. Une large coalition d'experts nationaux et internationaux, issus de l'industrie, du monde universitaire, de la société civile et des pouvoirs publics, devrait examiner dans quelle mesure les accords d'échange de trafic et de transit entre systèmes autonomes et réseaux Internet pourraient améliorer la responsabilité en matière de gestion du trafic, par exemple en ce qui concerne la lutte contre l'usurpation d'identité et le filtrage. La communauté des universitaires et des ingénieurs devrait étudier comment les nouveaux outils et pratiques en cours de développement pourraient également être intégrés et mis en œuvre. L'industrie, le monde universitaire, la société civile et le gouvernement fédéral devraient s'appuyer sur ces résultats pour étendre les politiques constructives et les meilleures pratiques en matière de gestion du trafic réseau à l'ensemble de l'écosystème, en tenant compte des exigences des petites entreprises. Les outils et cadres existants, tels que le code de conduite anti-bots des États-Unis pour les fournisseurs d'accès Internet et les normes volontaires Mutually Agreed Norms for Routing Security (MANRS), devraient être révisés, et de nouvelles solutions devraient être explorées dans le cadre d'un processus multipartite incluant une représentation diversifiée des acteurs du réseau qui correspondent à l'environnement de l'écosystème actuel.

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Objectif 3 : promouvoir l'innovation à la périphérie du réseau pour prévenir, détecter et atténuer les attaques automatisées et distribuées.

Pour établir un écosystème Internet et de communication résilient, les services d'infrastructure conçus pour se protéger contre les attaques devraient être complétés par une détection et une atténuation accrues des dispositifs compromis dans les réseaux domestiques ou d'entreprise, et là où ces réseaux se connectent à l'Internet. Une meilleure connaissance du contexte local peut améliorer la détection, et il peut être plus facile de se contenter de déconnecter ou de mettre en place un pare-feu pour certains appareils ou services au comportement anormal. Cette section identifie les actions que les parties prenantes peuvent entreprendre pour gérer l'impact des dispositifs compromis utilisés dans les attaques automatisées et distribuées.

Action 3.1 L'industrie des réseaux devrait étendre les efforts actuels de développement et de normalisation des produits pour une gestion efficace et sûre du trafic dans les environnements domestiques et d'entreprise.

L'industrie des réseaux cherche à mettre en place divers mécanismes propriétaires ou basés sur des normes pour mieux gérer le trafic au sein des réseaux d'entreprise. Ces mécanismes visent à empêcher les communications avec des systèmes suspects ou à limiter les communications aux hôtes spécifiquement requis pour un fonctionnement correct.
Ces systèmes peuvent tirer parti de l'IA ou de l'apprentissage automatique, des méthodes de détection et d'atténuation des menaces fournies par des services commerciaux externes, ou des informations spécifiques aux appareils. L'industrie devrait étendre ces efforts pour accélérer la fourniture d'une sécurité réseau efficace et rentable pour les environnements domestiques et professionnels.

Les concentrateurs et les passerelles du réseau local80 peuvent jouer le rôle de gestionnaires de trafic, en identifiant et en empêchant le trafic malveillant d'accéder aux dispositifs IoT et en limitant le trafic nuisible émanant des dispositifs du réseau local. Les fournisseurs de services en nuage développent également des solutions qui pourraient être superposées à ces solutions axées sur les passerelles, ce qui pourrait fournir de multiples contrôles et équilibres dans la pile du réseau pour mieux sécuriser l'écosystème IdO. Au fur et à mesure de l'émergence de ces innovations en matière de sécurité, le gouvernement et les parties prenantes devraient s'associer pour sensibiliser les consommateurs, les petites et moyennes entreprises et les partenaires internationaux aux solutions de sécurité. Lorsqu'il existe des obstacles spécifiques à l'adoption ou à l'avancement, le gouvernement et les parties prenantes doivent se réunir pour identifier les obstacles, promouvoir le déploiement des normes émergentes et examiner les politiques de pare-feu pratiques pour l'espace produit plus large.

Action 3.2 Les produits informatiques et IoT domestiques devraient être faciles à comprendre et simples à utiliser en toute sécurité.

Les produits informatiques et IoT domestiques devraient réduire ou éliminer les connaissances requises pour les utiliser en toute sécurité et en privé. Les réseaux d'entreprise bénéficient de l'attention du personnel professionnel chargé de maintenir la sécurité du réseau et des systèmes. Ce personnel est souvent conscient et suffisamment compétent pour configurer ces appareils selon une base de référence sécurisée. Les interfaces d'administration de la plupart des dispositifs informatiques et IoT sont conçues pour le personnel ayant ce bagage et ce niveau de compétence.

Les propriétaires de réseaux domestiques et de petites entreprises sont moins susceptibles de bénéficier d'un tel soutien, avec pour résultat inévitable des réseaux et des produits déployés de manière non sécurisée. Plutôt que d'attendre des consommateurs qu'ils deviennent des experts en sécurité, les secteurs de l'informatique et de l'IdO devraient donner la priorité à des processus de déploiement et de configuration simples et directs pour les appareils commercialisés auprès des particuliers et des petites entreprises. Pour

[80] Les passerelles sont des composants de l'architecture du réseau qui se situent entre les sous-composants du réseau. *Voir la* section II *ci-dessus* pour des discussions sur les passerelles intelligentes, etc.

Par exemple, si le processus d'installation ne force pas la mise à jour des mots de passe administratifs, ces produits continueront d'être des cibles faciles à incorporer dans les botnets. Les configurations par défaut doivent être les plus sûres pour le champ d'utilisation prévu, et les interfaces basées sur le cloud ou les applications doivent être intuitives et reposer sur les meilleures pratiques de conception actuelles. L'installation des correctifs de sécurité doit être automatique ou très facile à gérer (par *exemple, elle* ne doit pas nécessiter de téléchargement sur des lecteurs flash).

Action 3.3 Les entreprises devraient migrer vers des architectures de réseau qui facilitent la détection, la perturbation et l'atténuation des menaces automatisées et distribuées. Elles doivent également tenir compte de la façon dont leurs propres réseaux mettent les autres en danger.

Divers produits et services anti-DDoS efficaces sont actuellement disponibles, et de nouveaux produits innovants (tels que ceux décrits dans l'action 3.1) sont apparus récemment. Cependant, la plupart des entreprises ont conçu leurs réseaux dans un souci de simplicité et de performance plutôt que de sécurité. En combinaison avec le profil CCA pour la prévention et l'atténuation des attaques DDoS, les entreprises ont l'opportunité de ré-architecturer leurs réseaux pour isoler les dispositifs non sécurisés, gérer les flux de communication, et généralement améliorer la résilience de leurs zones de l'écosystème. Par exemple, les entreprises qui dépendent de systèmes anciens doivent architecturer leurs réseaux de manière à ce que ces dispositifs non sécurisés ne soient pas exposés aux attaques de l'Internet général.

Les risques provenant des réseaux d'entreprise vont au-delà du danger des appareils IoT détournés. Certains services basés sur le réseau permettent aux acteurs malveillants d'amplifier une attaque par le biais de " réflecteurs ", ou de services capables d'envoyer de grandes quantités de trafic vers une cible usurpée. S'ils sont mal configurés pour permettre des requêtes depuis n'importe où sur Internet, les services vulnérables tels que les serveurs DNS permettent aux attaquants d'envoyer d'énormes volumes de trafic contre les victimes. En 2018, l'une des plus grandes attaques DDoS observées à ce jour a exploité une vulnérabilité récemment découverte dans le logiciel relativement obscur MemCacheD. [81] Ces failles sont souvent plus problématiques car les systèmes vulnérables se trouvent sur des machines et des réseaux à l'échelle de l'entreprise, avec une haute disponibilité et une bande passante élevée. Les organisations devraient suivre les meilleures pratiques pour les outils orientés vers l'Internet, et s'assurer qu'ils sont à jour.

Une partie de cette évolution vers de meilleures pratiques de réseau peut se produire organiquement, à mesure que les entreprises intègrent davantage de dispositifs IoT dans leurs environnements en réseau et prennent conscience des risques des applications tournées vers l'extérieur. Cependant, les pouvoirs publics, l'industrie et la société civile doivent s'efforcer d'améliorer les connaissances des utilisateurs et des entreprises sur les menaces et les meilleures pratiques de sécurité, par le biais de collaborations telles que des campagnes de partenariat et des activités d'engagement stratégique. Lorsque ces connaissances seront formalisées, on pourra envisager de les inclure dans les futures versions du cadre de cybersécurité du NIST.

Action 3.4 Le gouvernement fédéral devrait étudier comment un déploiement plus large d'IPv6 peut modifier l'économie de l'attaque et de la défense.

L'Amérique du Nord a épuisé les adresses IPv4 inutilisées et facilement distribuables en 2015, mais très peu de consommateurs et de petites entreprises profitent actuellement de l'espace et des capacités des adresses IPv6. Le gouvernement et l'industrie ont planifié et travaillé en vue d'une adoption plus large de l'IPv6, mais ils devraient également considérer comment cela changera l'espace d'attaque potentiel et l'ampleur des attaques automatisées et distribuées.

[81] Lili Hay Newman, *GitHub a survécu à la plus grande attaque DDoS jamais enregistrée*, Wired (1er mars 2018, 11 h 01), https://www.wired.com/story/github-ddos-memcached/.

L'une des difficultés rencontrées pour informer les consommateurs qu'un appareil de leur réseau est lié à une activité malveillante est le grand nombre d'appareils généralement connectés à un réseau domestique ou de petite entreprise. Les routeurs dotés de la fonction NAT, qui peuvent donner l'impression que de nombreux appareils ont la même adresse IP, peuvent entraver la notification. Avec le passage à l'IPv6, les fournisseurs d'accès Internet grand public seront peut-être mieux placés pour observer le mauvais comportement de certains appareils lorsque les adresses IPv6 ne seront pas soumises au NAT. Ces informations peuvent, à leur tour, être mises en correspondance avec d'autres solutions axées sur la périphérie.

La mise en œuvre de routeurs compatibles NAT au niveau des particuliers et des petites entreprises a parfois servi de protection clé pour les points d'extrémité vulnérables. Les outils NAT agissent comme un pare-feu accessoire, empêchant les dispositifs domestiques d'être directement atteints par le type d'outils de balayage de masse qui propagent les logiciels malveillants et conduisent à une infection généralisée ; les caméras de sécurité étaient une cible commune du botnet Mirai parce qu'elles ne se trouvent généralement pas derrière un routeur compatible NAT. Dans les architectures actuelles, un réseau basé sur IPv6 permettrait probablement à chaque appareil d'être adressable. En théorie, l'espace d'adressage IPv6 est si vaste qu'il ne pourrait pas être scanné par les outils existants, mais les experts ont observé que les modèles permettraient aux nouvelles techniques de scannage de découvrir des dispositifs vulnérables.

La NTIA devrait travailler avec les parties prenantes pour identifier les leçons apprises de l'industrie et d'autres pays, en examinant plus en détail les obstacles et les options pour aligner les incitations afin d'encourager les FAI à effectuer une transition complète vers IPv6 plus rapidement. Pour assurer la défense et atténuer les risques, il faudra continuer à innover à la périphérie du réseau. Comprendre cela plus tôt permettra de trouver de meilleures solutions lorsque l'utilisation d'IPv6 se généralisera.

Objectif 4 : Promouvoir et soutenir les coalitions entre les communautés de la sécurité, des infrastructures et des technologies opérationnelles au niveau national et international.

Pour améliorer la résilience de l'internet et des infrastructures de communication, il faut faciliter la mise en œuvre d'actions coordonnées qui dépassent les frontières géopolitiques, publiques-privées, sectorielles et techniques. Cette section identifie des actions clés pour accroître l'engagement entre les communautés de parties prenantes critiques.

Action 4.1 Les FAI et les grandes entreprises devraient accroître le partage d'informations avec les agences gouvernementales et entre elles afin de fournir des informations plus opportunes et exploitables concernant les menaces automatisées et distribuées.

Si bon nombre des actions décrites dans ce rapport augmenteront le coût ou réduiront l'efficacité des attaques automatisées et distribuées, les actions des forces de l'ordre ont un impact unique sur la communauté des botnets. En mettant hors service les systèmes de commande et de contrôle, les forces de l'ordre peuvent rapidement "lobotomiser" une menace distribuée. Les poursuites engagées contre les principaux acteurs de l'économie des botnets ne font pas que ralentir le développement des menaces distribuées par les participants actuels, elles découragent également les développeurs potentiels.

Les forces de l'ordre comptent sur les FAI, grands et petits, les équipes de réponse aux incidents, les sociétés de cybersécurité et de réponse aux incidents, les fournisseurs d'antivirus, les entités commerciales et les sociétés de renseignement sur les cybermenaces pour soutenir les enquêtes en cours et les autres efforts de lutte contre les menaces automatisées en fournissant des informations exploitables sur les menaces et les tendances affectant leurs réseaux et leurs clients. En fournissant des informations encore plus opportunes et exploitables, les FAI et les autres fournisseurs d'infrastructures clés peuvent faciliter, soutenir et accélérer les actions des forces de l'ordre, y compris celles qui touchent les réseaux de zombies distribués sur le territoire de l

globe. Par exemple, les parties prenantes ont suggéré que l'élargissement des rapports d'incidents pour inclure les attaques infructueuses pourrait fournir des alertes précoces et permettre une intervention plus rapide des forces de l'ordre. Ce type de données aiderait également la communauté de la sécurité à mieux comprendre le paysage des risques.

Les services répressifs peuvent identifier de manière proactive les types de données qui les aideront à enquêter et à poursuivre les mauvais acteurs, et travailler avec les fournisseurs d'infrastructures pour rendre le partage de ces informations avec le gouvernement moins coûteux et plus facile, tout en protégeant la vie privée des internautes. [82] L'amélioration du partage des informations sur la cybersécurité reste l'un des éléments clés pour prévenir et atténuer les problèmes actuels et émergents de la cybercriminalité. Pour promouvoir la confiance et des relations plus larges qui se sont avérées utiles, les services répressifs devraient poursuivre leurs efforts de sensibilisation auprès des communautés de la sécurité et des réseaux pour les aider à identifier et à comprendre les bons partenaires au sein du gouvernement.

Les organismes publics, y compris les services répressifs, doivent continuer à améliorer l'actualité et la pertinence des informations de cybersécurité qu'ils partagent afin de prévenir et d'atténuer les cyberincidents. Les forces de l'ordre traitent les entreprises victimes d'une intrusion ou d'une attaque distribuée comme des victimes d'un crime, et mènent leurs enquêtes sur ces crimes signalés avec discrétion pour éviter, dans la mesure du possible, la diffusion injustifiée d'informations concernant l'incident. En outre, les organisations privées doivent partager les informations relatives à la cybersécurité au sein de leur secteur d'activité par l'intermédiaire des organisations de partage et d'analyse de l'information et avec les agences gouvernementales, le cas échéant, tout en identifiant clairement les informations qui doivent être partagées avec d'autres entités pour éviter tout préjudice supplémentaire.

Les RIR et les bureaux d'enregistrement peuvent faciliter l'attribution des mauvais acteurs en maintenant des bases de données WHOIS exactes. En outre, le gouvernement fédéral devrait s'engager auprès de ses homologues européens pour s'assurer que l'accès rapide à aux informations WHOIS est préservé, à mesure que les protections européennes de la confidentialité des données sont appliquées, afin de préserver un outil essentiel pour les efforts nationaux et mondiaux d'investigation des botnets. Les gouvernements peuvent collaborer avec les entités du secteur privé chargées du respect des réglementations relatives à la protection de la confidentialité des données, ainsi qu'avec les entités participant aux enquêtes sur les botnets, afin de s'assurer que les deux équités sont préservées (conformité et enquêtes sur les botnets).

Action 4.2 Le gouvernement fédéral devrait promouvoir l'adoption internationale des meilleures pratiques et des outils pertinents par le biais d'un engagement international bilatéral et multilatéral.

Des améliorations significatives de la résilience de l'écosystème ne peuvent être obtenues par une action nationale seule. Les États-Unis devraient s'engager régulièrement avec des partenaires internationaux sur la cybersécurité, aux niveaux bilatéral, régional et international, en tirant parti de l'expertise des agences fédérales. Pour les questions liées au DNS, la NTIA devrait coordonner son action avec les agences fédérales et représenter les positions américaines dans les forums multipartites, tels que l'Internet Corporation for Assigned Names and Numbers (ICANN) et l'Internet Governance Forum.

La normalisation internationale pourrait être particulièrement bénéfique. Les normes internationales pour les produits et services IoT ainsi que les normes qui pourraient autrement perturber les attaques automatisées et distribuées pourraient élargir le marché des produits qui contribuent à la résilience de l'écosystème. Comme le recommande le rapport du NSTAC, l'industrie et les agences fédérales qui participent à l'élaboration des normes devraient

[82] *Voir, par exemple,* Information Sharing and Analysis Organization (ISAO) Standards Organization, *ISAO SP 4000 : Protecting Consumer Privacy in Cybersecurity Information Sharing v1.0*, (26 juillet 2017), https://www.isao.org/products/isao-sp-4000-protecting-consumer-privacy-in-cybersecurity-information-sharing-v1- 0/.

coordonner une stratégie pour s'engager au sein des organismes internationaux de normalisation appropriés, dirigés par l'industrie, afin de garantir la représentation et le leadership des États-Unis et, grâce à cette participation, défendre une série de normes internationales flexibles et interopérables pour la sécurité de l'IdO.

Action 4.3 Les organismes de réglementation sectoriels, le cas échéant, devraient collaborer avec l'industrie pour garantir une commercialisation non trompeuse et favoriser les considérations de sécurité propres au secteur.

En raison de la complexité et de la diversité du paysage de l'IdO, il est difficile d'envisager un ensemble de règles uniques qui pourraient garantir la sécurité tout en suivant le rythme du changement et la nature dynamique de l'environnement des menaces. Les organismes de réglementation sectoriels peuvent toutefois promouvoir la résilience de l'écosystème en collaborant avec l'industrie pour garantir que la sécurité des produits déployés est adaptée à leur utilisation. Par exemple, la Food and Drug Administration a établi des directives pour les dispositifs médicaux qui dissocient les mises à jour de sécurité de base des régimes de certification des produits existants. [83] Ces lignes directrices sont bénéfiques pour les consommateurs, car les dispositifs médicaux dont ils dépendent deviennent plus résistants aux menaces de cybersécurité, et pour les fabricants, qui bénéficient d'une plus grande clarté quant aux exigences de certification. Les parties prenantes ont souligné que le gouvernement fédéral pourrait bénéficier d'un mécanisme de coordination interagences pour l'IdO afin de promouvoir et de partager ces types de pratiques innovantes et d'enseignements tirés, et d'éviter les conflits réglementaires.

Des mesures d'application judicieuses peuvent profiter aux consommateurs et aux participants honnêtes du marché. La FTC a pris des mesures dans de nombreux cas liés à la vie privée et à la sécurité, les dispositifs IdO figurant dans certaines de ces actions. [84] En arrêtant et en décourageant le marketing trompeur, la FTC peut renforcer la confiance des consommateurs dans les déclarations de sécurité des fournisseurs de technologies IdO et informatiques et soutenir les incitations positives du marché. La FTC a également utilisé son autorité en matière de déloyauté en vertu de la section 5 de la loi FTC pour contester les pratiques de sécurité déraisonnables, y compris dans l'espace IoT. En outre, des agences sectorielles, telles que le ministère américain de la santé et des services sociaux, appliquent les réglementations en matière de sécurité des informations dans les secteurs concernés. Ces politiques peuvent contribuer au débat plus large sur la sécurité des écosystèmes et en bénéficier.

Action 4.4 La communauté doit identifier les points de levier et prendre des mesures concrètes pour perturber les outils et les incitations des attaquants, y compris le partage et l'utilisation actifs des données de réputation.

De nombreuses menaces découlent d'asymétries qui favorisent les attaquants en répartissant l'exploitation entre des acteurs diffus dans l'écosystème. Les défenseurs peuvent utiliser des mesures de partage des données et des informations pour suivre les outils des attaquants et peuvent utiliser l'incidence des dommages pour identifier les outils et les acteurs. Dans certains cas, des efforts de coordination relativement légers devraient permettre de perturber des classes d'attaques plus larges. La section 3.3 souligne l'importance pour les organisations d'identifier les réflecteurs qui amplifient les attaques DDoS. La communauté peut suivre la présence de ces menaces pour aider à cibler la sensibilisation et la réduction des menaces. Ce type de partage a permis de lutter contre des menaces telles que le spam, et peut être exploité contre d'autres vecteurs d'attaque.

[83] Food and Drug Administration, *Postmarket Management of Cybersecurity in Medical Devices*, (28 déc. 2016), *disponible sur* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. [84] *Voir, par exemple,* Federal Trade Commission, *In the Matter of TRENDnet, Inc.* , FTC Matter/File Number 122 3090, https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter (dernière mise à jour le 7 février 2014).

"L'hébergement fast-flux" est la modification automatisée et rapide des adresses IP attribuées aux hôtes dans le DNS pour masquer l'emplacement de sites web soutenant des activités malveillantes, illégales ou criminelles. En 2008, un avis du comité consultatif sur la sécurité et la stabilité (SSAC)85 a examiné les mesures que certains bureaux d'enregistrement et registres mettent en œuvre aujourd'hui : surveillance des modifications apportées aux enregistrements DNS qui indiquent un hébergement fast-flux, restriction de la fréquence des modifications DNS et des plages de valeurs, et surveillance de l'accès aux comptes des titulaires de noms de domaine pour empêcher l'automatisation. Elle a également examiné comment les bureaux d'enregistrement pourraient appliquer ces mesures pour accélérer les processus de suspension des sites web et des noms de domaine illégaux. Ces mesures pourraient faire une différence substantielle dans les efforts visant à réduire l'activité des réseaux de zombies, mais elles n'ont pas été largement mises en œuvre. Les nouvelles avancées des attaquants, notamment les "réseaux à double flux", nécessitent davantage d'innovation et de collaboration au niveau des réseaux. La communauté au sens large, y compris le gouvernement fédéral, devrait plaider au sein des forums multipartites concernés (par *exemple,* l'ICANN et les RIR) en faveur d'une mise en œuvre plus large de ces mesures, ou de mécanismes alternatifs pour atteindre cet objectif.

Certaines menaces pour l'écosystème sont alimentées par des marchés illicites particuliers. Le marché actif des DDoS pour le compte de tiers est florissant dans les communautés de joueurs. La collaboration entre les sociétés de jeux et les processeurs de paiement peut potentiellement permettre de suivre et de punir ceux qui utilisent ces services, ce qui assèche le marché. De même, le marché des justificatifs d'identité volés peut être perturbé en rendant la validation des données plus difficile. [86] L'utilisation d'outils basiques d'anti-automatisation sur le web peut augmenter le coût pour les attaquants de la vérification de la valeur des informations d'identification volées, réduisant ainsi le profit tiré de leur vol et de leur utilisation. Plus généralement, les recherches suggèrent que le fait de cibler les partenaires en amont en les informant des vulnérabilités exposées peut jouer un rôle clé dans la mise en place de mesures correctives. [87]

L'investissement du gouvernement peut être un autre levier. Les agences ont été réceptives aux mesures et à la transparence autour des questions de sécurité telles que l'adoption de HTTPS. [88] Avec un peu d'orientation et de contrôle, la réputation de l'hygiène du réseau pourrait être incluse comme facteur dans le processus d'acquisition du gouvernement. Le gouvernement britannique a commencé à expérimenter cette approche. [89]

Action 4.5 La communauté de la cybersécurité devrait continuer à s'engager auprès de la communauté des technologies opérationnelles pour promouvoir la sensibilisation et accélérer l'incorporation des technologies de cybersécurité.

L'intégration de fonctionnalités de mise en réseau dans les technologies opérationnelles (OT) (*par exemple,* les systèmes SCADA dans les environnements industriels) a introduit de nouveaux défis en matière de cybersécurité qui ne peuvent être relevés que grâce à l'expertise combinée des communautés de la cybersécurité et des OT. Les exigences primaires associées aux cas d'OT sont souvent hors de portée des experts en cybersécurité, et les experts en OT sont souvent peu familiers avec les pratiques de cybersécurité de base.

---

[85] Comité consultatif sur la sécurité et la stabilité de l'ICANN, *SAC 025 : Avis du SSAC sur l'hébergement à flux rapide et le DNS*, (mars 2008), https://www.icann.org/en/system/files/files/sac-025-en.pdf.

[86] *Voir* Timothy Peacock et Allan Friedman, *Automation and Disruption in Stolen Payment Card Markets, (*2014), *disponible sur* http://www.econinfosec.org/archive/weis2014/papers/PeacockFriedman-WEIS2014.pdf.

[87] *Voir, par exemple,* Orcun Cetin, Carlos Gañán, Maciej Korczyński et Michel van Eeten, Make *Notifications Great Again : Learning How to Notify in the Age of Large-Scale Vulnerability Scanning*, (2017), *disponible à l'adresse* http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_17.pdf.

[88] *Voir, par exemple*, Eric Mill, *Tracking the U.S. Government's Progress on Moving to HTTPS*, General Services Administration - 18F, (4 janvier 2017), https://18f.gsa.gov/2017/01/04/tracking-the-us-governments-progress-on- moving-https/.

[89] *Voir* Ian Levy, *Active Cyber Defence-One Year On*, UK National Cyber Security Centre, (5 février 2018), *disponible sur* https://www.ncsc.gov.uk/information/active-cyber-defence-one-year.

Le gouvernement fédéral peut faciliter ce processus en élargissant les engagements actuels qui réunissent les communautés de la cybersécurité et de l'OT pour partager les connaissances et l'expertise, et qui favorisent la sensibilisation et accélèrent l'adoption des technologies de la communauté de la cybersécurité. Les agences sectorielles travaillent en étroite collaboration avec leurs secteurs pour comprendre les risques liés à la cybersécurité, pour mettre les secteurs en relation avec les ressources fédérales et pour promouvoir la planification de la résilience. L'équipe d'intervention d'urgence pour les systèmes de contrôle industriel (ICS-CERT) s'efforce de réduire les risques au sein de tous les secteurs d'infrastructures critiques et collabore avec les équipes d'intervention en cas d'incident informatique (CIRT) internationales et du secteur privé pour partager les incidents de sécurité liés aux systèmes de contrôle et les mesures d'atténuation. La communauté de la cybersécurité du gouvernement fédéral poursuit actuellement des engagements spécifiques aux dispositifs avec des communautés OT spécifiques, sur des sujets tels que les mises à jour sécurisées pour les pompes à perfusion. La communauté des technologies de l'information devrait participer aux actions industrielles citées dans ce rapport afin de trouver des solutions sectorielles aux cyberrisques qui lui sont propres.

Objectif 5 : accroître la sensibilisation et l'éducation dans l'ensemble de l'écosystème.

Pour renforcer la résilience de l'écosystème de l'internet et des communications face aux menaces distribuées, toutes les parties prenantes doivent comprendre leurs rôles et responsabilités et être prêtes à les assumer. Cette section identifie les actions spécifiques aux menaces distribuées qui permettraient de combler les écarts entre les compétences et les responsabilités actuelles.

Ces actions proposées ne remplacent pas les efforts généraux visant à accroître la sensibilisation et l'éducation en matière de cybersécurité. Les parties prenantes ont indiqué que ces initiatives générales de sensibilisation et d'éducation à la cybersécurité sont essentielles pour accroître la résilience de l'écosystème de manière durable. Par exemple, l'importance de commencer l'éducation à la cybersécurité dès la maternelle a été soulignée à plusieurs reprises dans les commentaires publics et les contributions aux réunions et ateliers.

L'initiative nationale pour l'éducation à la cybersécurité90 (NICE), dirigée par le NIST du ministère américain du commerce, est un partenariat entre le gouvernement, le monde universitaire et le secteur privé axé sur l'éducation, la formation et le développement de la main-d'œuvre en matière de cybersécurité. Sa mission consiste à dynamiser et à promouvoir un réseau robuste et un écosystème d'éducation, de formation et de développement de la main-d'œuvre en matière de cybersécurité, en mettant l'accent sur les travailleurs de ce secteur. Les programmes vont de l'enseignement de la cybersécurité de la maternelle à la 12e année et des filières universitaires, telles que les centres nationaux d'excellence académique en cybersécurité91, à l'élaboration et à la gestion de programmes d'évaluation et de formation axés sur les performances. Le ministère de la sécurité intérieure complète les contributions de NICE, en jouant un rôle essentiel dans les efforts de sensibilisation par le biais de la campagne STOP. PENSER. CONNECT. [92].

Les actions suivantes s'appuient sur ces efforts plus généraux de sensibilisation et d'éducation à la cybersécurité, en identifiant les possibilités de sensibilisation et d'éducation spécifiquement liées à l'atténuation ou à la prévention des menaces distribuées.

[90] National Initiative for Cybersecurity Education, National Institute of Standards and Technology, https://www.nist.gov/itl/applied-cybersecurity/nice (dernière visite le 4 avril 2018).
[91] Centres d'excellence académique en cybersécurité, Agence de sécurité nationale, https://www.nsa.gov/resources/educators/centers-academic-excellence/ (dernière visite le 10 avril 2018). [92] Arrêtez-vous. Pensez. Connect, https://www.stopthinkconnect.org/ (dernière visite le 4 avril 2018).

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Action 5.1 Le secteur privé devrait établir et administrer des outils d'information volontaires pour les dispositifs IoT domestiques, soutenus par un processus d'évaluation évolutif et rentable, auxquels les consommateurs peuvent se fier et qu'ils comprennent intuitivement.

Le secteur privé, en consultation avec la société civile et les experts gouvernementaux, devrait concevoir une approche efficiente et efficace d'évaluation et d'étiquetage des dispositifs IoT afin que les consommateurs soucieux de sécurité puissent faire des choix éclairés et créer des incitations commerciales pour le développement de produits sécurisés dès la conception. De nombreux produits IoT disponibles dans le commerce n'ont pas été conçus en tenant compte de la sécurité. Ces appareils créent un risque systémique pour tous les membres de l'écosystème et mettent en danger la vie privée et la sécurité des consommateurs. Dans un monde idéal, les consommateurs préféreraient des produits IoT qui protègent également leur sécurité et leur vie privée, mais les consommateurs soucieux de sécurité ne peuvent pas facilement identifier les produits IoT qui ont été conçus pour être sécurisés.
Sans ces informations, leurs critères de sélection se limitent au prix et à l'ensemble des fonctionnalités.

Le secteur privé est le plus à même de créer et de maintenir des mécanismes légers et agiles, mais il peut souvent bénéficier du pouvoir de convocation du gouvernement. Le gouvernement fédéral devrait réunir les parties prenantes de l'industrie, de la société civile et du gouvernement dans un processus multipartite afin d'explorer les exigences d'une approche viable de l'étiquetage. Cet effort peut s'appuyer sur les succès initiaux de programmes tels que le processus multipartite de la NTIA sur la mise à niveau et les correctifs de sécurité de l'IdO, qui a produit un document détaillant les éléments clés que les fabricants devraient envisager de communiquer aux consommateurs avant et après l'achat. [93] Les parties prenantes devraient examiner si un mécanisme reposant sur l'affirmation du fournisseur est viable et répond aux besoins des consommateurs domestiques. La viabilité d'un tel mécanisme pourrait reposer en partie sur les interdictions existantes en matière de tromperie commerciale. Par exemple, la Federal Trade Commission pourrait protéger l'intégrité du mécanisme d'évaluation en prenant des mesures contre le marketing trompeur (par *exemple, les* fausses déclarations de conformité), sachant que les assurances de sécurité dans cet espace ne peuvent pas offrir des garanties similaires à celles des affirmations de sécurité qui restent statiques dans le temps. Le DHS pourrait également soutenir le programme d'évaluation par le biais de ses activités de sensibilisation existantes, telles que STOP. PENSER. CONNECT. (Voir Action 5.3). [94]

Bien que la sécurité et la confidentialité de l'IdO ne soient pas parfaitement analogues, des mécanismes tels que les programmes NHTSA 5-Star Safety Rating et Energy Star ont réussi à sensibiliser les clients et à créer des marchés pour les véhicules sûrs et les appareils à haut rendement énergétique, ce qui étaye l'hypothèse selon laquelle une approche d'étiquetage bien conçue permettrait de réduire les attaques automatisées et distribuées. Toutefois, le grand nombre de dispositifs IoT différents et la période de vente relativement brève de nombre de ces dispositifs (par rapport aux voitures et aux chauffe-eau) indiquent qu'un mécanisme plus léger et plus agile sera nécessaire. Compte tenu de la nature mondiale des affaires aujourd'hui, le mécanisme d'évaluation devrait, dans la mesure du possible, être basé sur des normes reconnues au niveau international. En outre, toute utilisation d'une approche d'évaluation et d'étiquetage de la sécurité devrait refléter les différences entre les assertions de sécurité, qui restent statiques dans le temps, et les assertions de sécurité, qui ne peuvent offrir des garanties similaires. Le DHS pourrait compléter ces mécanismes d'application générale en explorant les possibilités d'un régime de certification qui pourrait être efficace pour répondre aux besoins des infrastructures critiques.

L'évaluation subjective des dispositifs IdO et de leur facilité d'utilisation joue également un rôle. Les organismes de test orientés vers les consommateurs complètent souvent les analyses basées sur les caractéristiques et les historiques de réparation par des évaluations plus subjectives du confort ou de la convivialité. La facilité d'utilisation des interfaces de gestion de la sécurité est une question particulièrement délicate.

[93] NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (dernière mise à jour le 7 novembre 2017). [94] Arrêtez. Pensez. Connect, https://www.stopthinkconnect.org/ (dernière visite le 4 avril 2018).

problème difficile. En incluant des évaluations réfléchies de la convivialité, les organismes de test orientés vers les consommateurs peuvent aider ces derniers à identifier les produits qui conviennent à leur niveau de compétence.

Action 5.2 Le secteur privé devrait établir des systèmes de labellisation volontaire pour les applications industrielles de l'IdO, soutenus par un processus d'évaluation évolutif et rentable, afin d'offrir une assurance suffisante pour les applications d'infrastructures critiques de l'IdO.

Les infrastructures critiques et les applications industrielles de l'IdO présentent des risques nettement plus élevés pour la nation que les applications domestiques dans le cadre d'attaques automatisées et distribuées. Ces dispositifs sont également déployés dans des environnements très différents, soutenus par des administrateurs professionnels. Le mécanisme volontaire d'évaluation légère envisagé dans l'action 5.1 n'offrirait pas un niveau d'assurance suffisant pour ces clients, et des fonctionnalités supplémentaires seront probablement nécessaires. Les fonctions d'évaluation telles que l'authentification des dispositifs, les racines de confiance matérielles ou les fonctions de mise à jour gérées nécessiteraient une interaction directe avec les produits, voire un examen du code source.

Des exemples de réussite d'un tel processus existent tant dans le secteur public que dans le secteur privé. Par exemple, le programme de validation des modules cryptographiques du NIST fait appel à des laboratoires d'essai indépendants pour évaluer la sécurité des modules cryptographiques par rapport à la norme FIPS 140 (Federal Information Processing Standards) depuis plus de deux décennies. Dans le secteur privé, la société de sécurité et de certification UL dispose d'une variété de systèmes de certification et de conformité pour les marchés commerciaux et de consommation, avec plus de 20 milliards de marques UL apparaissant sur les produits en 2016. Cependant, un étiquetage fragmenté ou trop complexe peut se retourner contre vous. La FTC, qui dispose d'une expertise considérable en matière d'étiquetage, est favorable à des informations claires, mais met en garde contre le fait que "de mauvaises informations, y compris des informations trop détaillées, peuvent en fait empêcher les consommateurs de faire des choix éclairés "[95].

Le secteur privé devrait mettre en place un processus d'évaluation efficace mais solide pour s'assurer que les dispositifs IoT destinés à ces secteurs offrent une résilience renforcée à un niveau d'assurance approprié. L'établissement d'une liste de produits évalués permettra aux entreprises soucieuses de la sécurité de faire des choix éclairés et de créer des incitations commerciales pour des processus robustes de cycle de vie de développement sécurisé.

Action 5.3 Le gouvernement devrait encourager les secteurs de l'enseignement et de la formation à intégrer pleinement les pratiques de codage sécurisé dans les programmes d'informatique et les programmes connexes.

Comme indiqué dans l'Action 1.3, de nombreuses vulnérabilités courantes en matière de sécurité (par *exemple,* les dépassements de tampon) peuvent être évitées ou corrigées pendant le développement du produit en utilisant des outils de développement de sécurité appropriés, tels que les fuzzers, les analyseurs statiques et les langages de programmation sûrs. Bien que les établissements universitaires, les camps d'entraînement au codage et les programmes de reconversion professionnelle créent une main-d'œuvre de codage plus importante, leurs diplômés sont rarement compétents dans ces langages ou aptes à utiliser ces outils de développement. Au lieu de cela, les étudiants acquièrent une expérience significative avec des outils de développement de logiciels qui ne prennent pas en compte la sécurité, et des méthodologies de développement de logiciels qui ne donnent pas la priorité à la sécurité, créant ainsi un état d'esprit de "boulonnage" parmi la main-d'œuvre de développement de logiciels.

Les entreprises qui souhaitent améliorer les pratiques de codage peuvent être dissuadées par une main-d'œuvre non préparée et parfois résistante - les codeurs qualifiés peuvent facilement changer d'emploi s'ils ne sont pas intéressés par l'apprentissage des nouvelles méthodes de codage.

[95] Commission fédérale du commerce, *Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers",* à la page 6, (2017), *disponible sur* https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications- information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.

et peuvent être difficiles à remplacer. En enseignant des méthodologies de conception de logiciels sécurisés et en encourageant l'utilisation de chaînes d'outils de développement de logiciels axés sur la sécurité dans l'ensemble du programme d'études en informatique et en cybersécurité, nous pouvons préparer notre main-d'œuvre à créer des logiciels de meilleure qualité et accroître l'acceptation des chaînes d'outils de développement de logiciels axés sur la sécurité.

Le gouvernement fédéral peut faciliter ces changements grâce aux relations existantes avec le monde universitaire et l'industrie de la formation. En particulier, le NICE devrait s'engager avec le monde universitaire et le secteur privé à intégrer les principes de conception sécurisée et les outils de soutien à chaque étape du cursus. La catégorie "fourniture sécurisée" du cadre des effectifs de cybersécurité de NICE (NICE Framework) comprend les connaissances, les compétences et les aptitudes nécessaires au développement de logiciels et de produits sécurisés. NICE devrait s'associer aux prestataires d'enseignement et de formation pour les encourager à utiliser le NICE Framework comme outil de référence pour l'élaboration du contenu des cours. Autre exemple, la FTC accueille chaque année la conférence PrivacyCon, qui offre une vitrine aux travaux des universitaires et des chercheurs en sécurité sur la vie privée et la sécurité. [96]

Action 5.4 Le secteur universitaire, en collaboration avec l'initiative nationale pour l'éducation à la cybersécurité, devrait faire de la cybersécurité une exigence fondamentale dans toutes les disciplines de l'ingénierie.

L'intégration de l'informatique dans toute la gamme de produits et de services fait apparaître des menaces de cybersécurité dans de nouvelles catégories de produits. Les concepteurs de produits n'ont souvent pas conscience des risques qui peuvent être introduits lors de l'intégration de l'informatique dans les lignes de produits traditionnelles. Il est de plus en plus nécessaire qu'ils comprennent la gestion des risques liés à la cybersécurité, car nous intégrons des capteurs dans de nombreux environnements, notamment le sol, les autoroutes et les bâtiments. Par exemple, les caméras de télévision en circuit fermé (CCTV) sont disponibles dans le commerce depuis 1949, mais n'ont évolué que récemment vers des dispositifs connectés à Internet. En 2016, le botnet Mirai a compromis plus de 100 000 caméras CCTV pour soutenir des attaques DDoS. Dans d'autres cas, des caméras connectées à Internet utilisées comme moniteurs pour bébés ont été piratées en exploitant les mots de passe administratifs par défaut, violant ainsi la vie privée des propriétaires. [97]

Pour s'assurer que les concepteurs de produits sont conscients des risques introduits dans la technologie opérationnelle, les établissements universitaires enseignant l'ingénierie et les disciplines connexes devraient intégrer la cybersécurité de base dans le programme d'études requis. Comme ci-dessus, le NICE devrait s'engager avec le monde universitaire et le secteur privé pour intégrer les principes dans le cursus de l'ingénierie et des disciplines connexes.

Action 5.5 Le gouvernement fédéral devrait mettre en place une campagne de sensibilisation du public pour soutenir la reconnaissance et l'adoption de la base de référence et de la marque de sécurité des dispositifs IoT domestiques.

Pour avoir un impact, la base de sécurité des dispositifs IoT domestiques doit être reconnue et privilégiée par les consommateurs soucieux de sécurité, ce qui renforce la résilience des réseaux domestiques où les dispositifs sont installés et crée des incitations commerciales pour les fournisseurs soucieux de sécurité. Le gouvernement fédéral mène depuis longtemps des campagnes de sensibilisation du public, avec le soutien des parties prenantes, sur des sujets très variés : comment prévenir les feux de forêt, l'utilité de la ceinture de sécurité et l'importance du dépistage du VIH. La campagne Stop. Pensez. Connect. est une campagne nationale de sensibilisation du public, parrainée par le DHS, qui vise à accroître le nombre d'utilisateurs de l'Internet.

---

[96] *Voir* Federal Trade Commission, *PrivacyCon 2018*, https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018 (dernière visite le 4 avril 2018).

[97] *Voir* Darlene Storm, *Hacker Hijacks Wireless Foscam Baby Monitor, Talks and Freaks Out Nanny*, Computerworld (2 février 2015, 12:09 PM PT), https://www.computerworld.com/article/2878741/hacker-hijacks- wireless-foscam-baby-monitor-talks-and-freaks-out-nanny.html.

compréhension des cybermenaces et de donner au public américain les moyens d'être plus sûr et plus sécurisé en ligne. Le gouvernement fédéral devrait envisager de tirer parti de Stop. Think. Connect. ou mettre en place une campagne complémentaire de sensibilisation du public pour alerter les utilisateurs domestiques et les petites organisations sur l'importance de la base de référence des dispositifs IoT domestiques et les éduquer sur la façon d'identifier des produits plus sûrs. Plus généralement, une meilleure sensibilisation des utilisateurs au risque de cybersécurité est essentielle à un écosystème résilient, et le gouvernement devrait accroître son engagement stratégique et son pouvoir de rassemblement avec des communautés d'utilisateurs ciblées et la société civile pour améliorer l'adoption de la sécurité et la sensibilisation, en accueillant toute partie prenante non gouvernementale qui souhaite jouer un rôle plus important.

* * *

Prochaines étapes initiales pour l'action des parties prenantes

La section ci-dessus détaille 24 actions conçues pour atteindre cinq objectifs. Ces cinq objectifs se renforcent mutuellement ; ils doivent tous être atteints pour accroître durablement la résilience de l'écosystème de l'internet et des communications. De nombreuses actions se renforcent également mutuellement par conception, même entre les objectifs, de sorte que l'exclusion ou l'omission d'une action pourrait potentiellement retarder la réalisation de plusieurs objectifs. Cependant, nous ne nous attendons pas à ce que toutes les actions se déroulent simultanément, en raison de considérations telles que les contraintes de ressources dans les communautés de parties prenantes concernées. En outre, certaines actions sont déjà en cours, tandis que d'autres dépendent de facteurs extérieurs. Le gouvernement fédéral ne dirigera pas la mise en œuvre des actions spécifiques à l'industrie. Cependant, comprenant que dans certains cas, il peut falloir du temps au secteur privé pour s'organiser, le gouvernement américain commencera immédiatement à coordonner les étapes initiales décrites ci-dessous.

Élaborer une feuille de route hiérarchisée pour des actions coordonnées visant à accroître la résilience de l'internet et de l'écosystème des communications face aux menaces distribuées.

Afin de s'assurer que les actions les plus importantes sont dotées de ressources adéquates et exécutées efficacement par les parties prenantes, les communautés de parties prenantes ont fortement encouragé le gouvernement fédéral à délimiter clairement les priorités d'action. [98] En particulier, certaines actions n'impliquent pas directement le gouvernement fédéral, mais soutiennent, ou sont soutenues par, des actions qui dépendent de la participation ou du leadership du gouvernement fédéral. En indiquant ses propres priorités, le gouvernement fédéral peut accroître la confiance des parties prenantes dans le fait que les ressources investies dans des actions dirigées par l'industrie et dépendant du gouvernement fédéral donneront des résultats productifs.

En plus des dépendances fédérales, certaines actions ont un ordre temporel naturel : par exemple, les programmes d'évaluation dans les actions 5.1 et 5.2 dépendent de l'établissement de bases de capacités de sécurité appropriées dans l'action 1.1. D'autres actions sont mûres pour la priorisation parce que le travail préparatoire est en cours, tel que le profil CSF décrit dans l'action 2.2. Enfin, certaines actions sont particulièrement urgentes en raison de leur long délai d'exécution (*par exemple, les* actions 1.3, 5.3 et 5.4) ou des développements qui réduisent la possibilité pour les États-Unis d'influencer la direction (action 1.2).

Les ministères du commerce et de la sécurité intérieure, en coordination avec l'industrie, la société civile et en consultation avec les partenaires internationaux, devraient être chargés d'élaborer une feuille de route initiale avec des actions prioritaires dans les 120 jours suivant l'approbation du présent rapport. Cette feuille de route devrait s'aligner sur

[98] Cette demande a été soulignée à la fois dans les réponses des parties prenantes à la demande de commentaires du 5 janvier 2018 et dans l'atelier du 28 février au 1er mars 2018.

Les priorités de l'administration telles qu'elles ont été définies après l'achèvement des tâches assignées en vertu du décret 13800. Le gouvernement et le secteur privé travailleront ensemble pour s'assurer que la feuille de route est mise à jour et maintenue à mesure que les parties prenantes accomplissent les actions identifiées.

Le gouvernement fédéral donnera l'exemple.

Les parties prenantes ont indiqué que le leadership fédéral par l'exemple est essentiel à la mise en œuvre du rapport par les autres parties prenantes. Les parties prenantes ont indiqué que l'adoption par le gouvernement fédéral de pratiques de "bon voisinage" qui profitent principalement à l'écosystème et aux activités d'approvisionnement constituerait une base pour d'autres activités visant à réduire les menaces automatisées et distribuées. En particulier, les mesures prises par les agences fédérales pour mettre en œuvre le filtrage de sortie afin d'empêcher l'usurpation d'adresse réseau, fermer les réflecteurs utilisés pour amplifier les volumes de trafic et mesurer la conformité des agences (et potentiellement nommer et faire honte aux mauvais acteurs) démontreraient la détermination fédérale et encourageraient les actions bénéfiques des autres parties. Le NIST, l'OMB et le DHS devraient étudier les mesures à prendre pour s'assurer que ces meilleures pratiques sont correctement prises en compte dans les politiques, les normes, les directives et la surveillance des agences fédérales.

De même, les activités de passation de marchés fédéraux rendant obligatoire l'acquisition de produits et de services plus sûrs ou plus résilients que ceux couramment disponibles aujourd'hui ont été considérées comme une étape importante vers la mise en place d'incitations commerciales. Les parties prenantes ont suggéré de se concentrer immédiatement sur les actions 1.1, 1.2 et 2.3 pour soutenir les orientations en matière de marchés publics fédéraux. Ce travail de conception peut ensuite conduire à une évaluation des orientations et des normes existantes en matière d'approvisionnement, ainsi qu'à des recommandations spécifiques pour mettre à jour ces orientations afin de refléter les exigences de sécurité.

Encourager le leadership du secteur privé et soutenir la coordination intersectorielle pour suivre la mise en œuvre de la feuille de route.

De nombreuses actions de la feuille de route devraient être dirigées par un secteur industriel, le monde universitaire ou la société civile. L'identification ou l'établissement de structures de gouvernance du secteur privé pour ces activités sera un facteur essentiel pour la durabilité et l'acceptation internationale des produits du travail (par *exemple, les* spécifications techniques ou les systèmes d'évaluation). Lorsque des organismes existants mènent déjà des actions connexes ou représentent déjà des communautés clés, il convient de les encourager à prendre la tête des opérations. Les actions peuvent nécessiter une inclusion au-delà des structures actuelles - par exemple, en ajoutant des participants ou des perspectives de la société civile ou internationale.

Au fur et à mesure que des communautés se forment pour mettre en œuvre ces actions, l'établissement d'un lieu de coordination régulière entre ces communautés sera de plus en plus important. La valeur d'une base de référence pour la sécurité de l'IdO est limitée si un schéma d'évaluation ne peut être établi en temps utile. L'alignement et la coordination des investissements sont nécessaires pour maximiser l'impact sur la résilience de l'infrastructure. Jusqu'à ce qu'une ou plusieurs parties du secteur privé soient identifiées d'un commun accord, le gouvernement fédéral fournira un mécanisme de coordination et de communication pour la poursuite de la mise en œuvre, et convoquera des réunions périodiques des parties concernées.

Fournir au président un rapport d'étape de 365 jours sur la mise en œuvre de la feuille de route.

Pour suivre les progrès accomplis, les ministères du commerce et de la sécurité intérieure élaboreront un rapport d'étape de 365 jours à l'intention du président, qui devra être remis un an après la publication initiale de la feuille de route. Cette mise à jour fera le point :
1) les progrès réalisés par l'ensemble de la communauté par rapport à la feuille de route ; 2) l'impact de ces activités de la feuille de route ; 3) une réévaluation de la menace d'attaques automatisées et distribuées, y compris la question de savoir si la stratégie de l'Union européenne en matière de sécurité et de protection de l'environnement est efficace.

La menace augmente ou diminue, et les raisons connues d'un tel changement ; et 4) si des ajustements doivent être apportés à la feuille de route.

Promouvoir la participation mondiale en renforçant l'engagement des parties prenantes et du gouvernement américain dans l'élaboration des politiques et des normes internationales.

La nature mondiale des menaces distribuées a été fréquemment soulignée au cours du processus exécuté par le Département et la Sécurité intérieure. Les parties prenantes ont souligné l'importance des normes, politiques et meilleures pratiques internationales pour promouvoir la participation et la collaboration internationales. En continuant à préconiser des approches dirigées par l'industrie et en participant activement à l'élaboration de normes internationales volontaires et consensuelles, le gouvernement fédéral peut contribuer à l'élaboration de normes pragmatiques et efficaces fondées sur les résultats qui répondent aux besoins de toutes les parties prenantes. Le gouvernement fédéral est également bien placé pour diriger l'engagement international requis pour établir des politiques et des pratiques exemplaires largement acceptées, et il améliorera la coordination avec les intervenants dans le cadre de ces efforts.

Annexe : Liste des acronymes

AI	Intelligence artificielle
BCP	Meilleure pratique actuelle
BGP	Protocole de passerelle frontalière
CCTV	Télévision en circuit fermé
CDN	Réseau de diffusion de contenu
CIRT	Équipe de réponse aux incidents informatiques
CISA	Loi de 2015 sur le partage des informations relatives à la cybersécurité
CSF	Cadre de cybersécurité du NIST
CSIRT	Équipe de réponse aux incidents de sécurité informatique
CSRIC	Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications
DDoS	Déni de service distribué
DHS	Département de la sécurité intérieure
DNS	Système de nom de domaine
FIPS	Normes fédérales de traitement de l'information
FIRST	Forum des équipes de sécurité et de réponse aux incidents
FTC	Commission fédérale du commerce
GSA	Administration des services généraux
HTTPS	Protocole de transfert hypertexte sécurisé
ICANN	Internet Corporation for Assigned Names and Numbers (Société pour l'attribution des noms de domaine et des numéros)
ICS-CERT	Équipe d'intervention en cas d'urgence cybernétique pour les systèmes de contrôle industriel
IETF	Groupe de travail sur l'ingénierie Internet
IoT	Internet des objets
IP	Protocole Internet
IPv4	Protocole Internet version 4
IPv6	Protocole Internet version 6
ISAC	Centre de partage et d'analyse des informations
ISP	Fournisseur de services Internet
IT	Technologies de l'information
LAN	Réseau local
MANRS	Normes mutuellement acceptées pour la sécurité du routage
MUD	Description de l'utilisation du fabricant
NAT	Traduction d'adresses de réseau
CCN	Centre national de coordination des communications
CCNIC	Centre national d'intégration de la cybersécurité et des communications
NHTSA	National Highway Traffic Safety Administration
NICE	Initiative nationale pour l'éducation à la cybersécurité
NIST	Institut national des normes et de la technologie
NISTIR	Rapport inter-agences/interne du NIST
NITRD	Recherche et développement en matière de réseaux et de technologies de l'information
NOG	Groupe d'opérateurs de réseau

NSTAC	Comité consultatif du Président sur les télécommunications pour la sécurité nationale
NTIA	Administration nationale des télécommunications et de l'information
OT	Technologie opérationnelle
PPD	Directive politique présidentielle
RFC	Demande de commentaires
RIR	Registre Internet régional
SAM	Gestion des actifs logiciels
SCADA	Contrôle de surveillance et acquisition de données
SSAC	Comité consultatif sur la sécurité et la stabilité

Recommandations sur la sécurité et la confidentialité de l'Internet des objets (IoT) RAPPORT DU GROUPE DE TRAVAIL TECHNIQUE SUR L'INTERNET BANDE LARGE (BROADBAND INTERNET TECHNICAL ADVISORY GROUP)

Un rapport d'accord uniforme

Délivré :

Novembre 2016

Droits d'auteur / Avis juridique

À propos du BITAG

Le Broadband Internet Technical Advisory Group (BITAG) est une organisation à but non lucratif, composée de plusieurs parties prenantes, dont l'objectif est de réunir des ingénieurs et des technologues au sein d'un groupe de travail technique (TWG) afin de développer un consensus sur les pratiques de gestion des réseaux à large bande et sur d'autres questions techniques connexes qui peuvent affecter l'expérience Internet des utilisateurs, notamment l'impact vers et depuis les applications, le contenu et les dispositifs qui utilisent l'Internet.

La mission du BITAG comprend : (a) l'éducation des décideurs politiques sur ces questions techniques ; (b) le traitement de questions techniques spécifiques dans le but de minimiser les différends politiques connexes ; et (c) servir de caisse de résonance pour les nouvelles idées et les pratiques de gestion du réseau. Les fonctions spécifiques du TWG peuvent également inclure : (i) l'identification des "meilleures pratiques" des fournisseurs de large bande et d'autres entités ; (ii) l'interprétation et l'application des pratiques de "sphère de sécurité" ; (iii) la fourniture d'autres conseils techniques à l'industrie et au public ; et/ou (iv) l'émission d'avis consultatifs sur les questions techniques liées à la mission du TWG qui peuvent sous-tendre des différends concernant les pratiques de gestion des réseaux à large bande.

Le groupe de travail technique du GTAB et ses différents comités prennent leurs décisions par consensus, les niveaux d'accord correspondants étant représentés sur la couverture de chaque rapport. Chaque représentant du GTT s'efforce de parvenir à un consensus sur les recommandations que son organisation soutient, bien que, même au niveau d'accord le plus élevé, le consensus du GTAB n'exige pas que toutes les organisations membres du GTT soient d'accord avec chacune des phrases d'un document. Le président de chaque comité GTT détermine si un consensus a été atteint. En cas de désaccord au sein d'un comité quant à l'existence d'un consensus, le GTCV dispose d'un processus de vote permettant d'atteindre et d'indiquer plus formellement différents niveaux d'accord. Pour plus d'informations, veuillez consulter le manuel des groupes de travail techniques du GTCV, disponible sur le site Web du GTCV à l'adresse www.bitag.org.

Les rapports des GTT du GTC BITAG portent essentiellement sur des questions techniques, en particulier celles susceptibles d'être interprétées comme anticoncurrentielles, discriminatoires ou autrement motivées par des facteurs non techniques. Bien que les rapports puissent aborder un large éventail de questions liées à une pratique particulière de gestion de réseau, ils ne sont pas destinés à traiter ou à analyser de manière exhaustive les questions économiques, juridiques, réglementaires ou de politique publique que la pratique peut soulever. Le BITAG accueille volontiers les commentaires du public. N'hésitez pas à soumettre vos commentaires par écrit en envoyant un courriel à comments@bitag.org.

Résumé exécutif

Au cours des dernières années, bon nombre des nouveaux appareils connectés à Internet ne sont pas des ordinateurs personnels, mais plutôt une variété d'appareils intégrant une connectivité et des fonctions Internet. Cette catégorie d'appareils a été généralement décrite comme l'*Internet des objets* (IoT) et a entraîné de nouveaux risques pour la sécurité et la vie privée.

Le terme "IoT" a une portée potentiellement large. L'IoT peut faire référence à des déploiements dans les foyers, les entreprises, les installations de fabrication, les industries du transport et ailleurs. Ainsi, l'IdO peut se référer à bien plus que de simples dispositifs destinés aux consommateurs. Aux fins du présent rapport, nous utilisons le terme IdO pour désigner uniquement les appareils grand public et les systèmes logiciels locaux et distants qui leur sont associés, bien que certaines ou l'ensemble de nos recommandations puissent être applicables de manière plus large. Ce rapport s'intéresse aux scénarios dans lesquels les consommateurs installent, configurent et administrent des appareils qu'ils louent ou possèdent.

Le nombre et la diversité des dispositifs IoT grand public augmentent rapidement ; ces dispositifs offrent de nombreuses nouvelles applications aux utilisateurs finaux, et à l'avenir en offriront probablement encore plus. De nombreux dispositifs IoT sont soit déjà disponibles, soit en cours de développement pour un déploiement dans un avenir proche, notamment :

- des capteurs pour mieux comprendre les schémas de la vie quotidienne et surveiller la santé
- des moniteurs et des commandes pour les fonctions de la maison, des serrures aux systèmes de chauffage et d'eau.
- des dispositifs et des appareils qui anticipent les besoins d'un consommateur et peuvent prendre des mesures pour y répondre (par exemple, des dispositifs qui surveillent les stocks et réorganisent automatiquement les produits pour un consommateur).

Ces dispositifs interagissent généralement avec des logiciels fonctionnant ailleurs sur le réseau et fonctionnent souvent de manière autonome, sans nécessiter d'intervention humaine. En outre, lorsqu'ils sont couplés à l'analyse des données et à l'apprentissage automatique, les dispositifs IoT peuvent être en mesure de prendre des mesures plus proactives, de révéler des schémas de données intéressants et utiles, ou de faire des suggestions aux utilisateurs finaux susceptibles d'améliorer leur santé, leur environnement, leurs finances et d'autres aspects de leur vie.

Bien que les consommateurs soient confrontés à des menaces générales en matière de sécurité et de respect de la vie privée en raison de la présence de *tout* appareil connecté à l'internet, la nature de l'IdO grand public est unique en ce sens qu'elle peut impliquer des consommateurs non techniques ou non intéressés, ce qui complique la découverte et l'inventaire des appareils sur les réseaux domestiques des consommateurs, étant donné que le nombre et la variété des appareils prolifèrent, des effets sur le service d'accès à l'internet du consommateur et d'autres qui fonctionnent sur des liens de réseau partagés, et des effets sur d'autres services dans la mesure où, lorsque les dispositifs IoT sont compromis par des logiciels malveillants, ils peuvent devenir une plateforme pour le trafic de données indésirables - comme le spam et les attaques par déni de service - qui peuvent interférer avec la fourniture de ces autres services.

Plusieurs rapports récents ont montré que certains appareils ne respectent pas les meilleures pratiques rudimentaires en matière de sécurité et de confidentialité. Dans certains cas, des dispositifs ont été compromis et ont permis à des utilisateurs non autorisés d'effectuer une surveillance et un contrôle, d'obtenir un accès ou un contrôle, de provoquer des pannes de dispositifs ou de systèmes, et de déranger ou de harceler des utilisateurs autorisés ou des propriétaires de dispositifs.

Parmi les problèmes potentiels contribuant à l'absence de bonnes pratiques en matière de sécurité et de confidentialité, citons : le manque d'expérience de la chaîne d'approvisionnement IoT en matière de sécurité et de confidentialité, le manque d'incitations à développer et à déployer des mises à jour après la vente initiale, la difficulté d'effectuer des mises à jour logicielles sécurisées sur le réseau, les dispositifs dotés de ressources matérielles limitées ou restreintes (empêchant certaines mesures de sécurité de base ou "de bon sens"), les dispositifs dotés d'interfaces utilisateur limitées ou restreintes (qui, si elles sont présentes, peuvent n'avoir qu'une fonctionnalité minimale) et les dispositifs dotés de logiciels malveillants insérés au cours du processus de fabrication.

L'émergence de l'IdO offre des possibilités d'innovation importantes, des maisons intelligentes aux villes intelligentes. Dans de nombreux cas, des modifications simples des processus de développement, de distribution et de maintenance des appareils peuvent empêcher la distribution d'appareils IoT qui souffrent de problèmes importants de sécurité et de confidentialité. BITAG estime que le respect des lignes directrices décrites dans ce rapport peut améliorer considérablement la sécurité et la confidentialité des dispositifs IoT et minimiser les coûts associés aux dommages collatéraux qui affecteraient autrement les utilisateurs finaux et les FAI. En outre, à moins que le secteur des dispositifs IoT - le secteur de l'industrie qui fabrique et distribue ces dispositifs - n'améliore la sécurité et la confidentialité des dispositifs, la réaction des consommateurs pourrait entraver la croissance du marché de l'IoT et, en fin de compte, limiter les promesses de l'IoT.

Observations. À partir de l'analyse faite dans ce rapport et de l'expérience combinée de ses membres en matière de dispositifs de l'Internet des objets, le groupe de travail technique du BITAG formule les *observations* suivantes :

- **Vulnérabilités de sécurité :** Certains dispositifs IoT sont expédiés "d'usine" avec un logiciel qui est soit obsolète, soit le devient avec le temps. D'autres appareils IoT peuvent être livrés avec un logiciel plus récent, mais des vulnérabilités peuvent être découvertes à l'avenir. Les vulnérabilités découvertes tout au long de la durée de vie d'un dispositif peuvent rendre ce dernier moins sûr au fil du temps, à moins qu'il ne dispose d'un mécanisme de mise à jour ultérieure de son logiciel.

- **Communications non sécurisées :** De nombreuses fonctions de sécurité conçues pour des dispositifs informatiques plus polyvalents sont difficiles à mettre en œuvre sur les dispositifs IoT et un certain nombre de failles de sécurité ont été identifiées sur le terrain, notamment des communications non cryptées et des fuites de données provenant de dispositifs IoT.

    - **Communications non authentifiées :** Certains dispositifs IoT fournissent des mises à jour logicielles automatiques. Sans authentification et chiffrement, cependant, cette approche est insuffisante car le mécanisme de mise à jour pourrait être compromis ou désactivé. En outre, de nombreux dispositifs IoT n'utilisent pas l'authentification au cours de la communication.

    - **Communications non cryptées :** De nombreux dispositifs IoT envoient tout ou partie des données en clair, plutôt que sous une forme chiffrée. Les communications en clair peuvent être observées par d'autres appareils ou par un attaquant.

- **Absence d'authentification et d'autorisation mutuelles :** Un appareil qui permet à une partie inconnue ou non autorisée de modifier son code ou sa configuration, ou d'accéder à ses données, constitue une menace. L'appareil peut révéler que son propriétaire est présent ou absent, faciliter l'installation ou l'exploitation de logiciels malveillants, ou faire en sorte que sa fonction IoT principale soit fondamentalement compromise.
- **Manque d'isolation du réseau :** Ces appareils créent également de nouveaux risques et sont susceptibles de faire l'objet d'attaques *à l'intérieur de* la maison. Étant donné que de nombreux réseaux domestiques n'isolent pas, par défaut, les différentes parties du réseau les unes des autres, un appareil connecté au réseau peut être en mesure d'observer ou d'échanger du trafic avec d'autres appareils sur le même réseau domestique, ce qui permet à un appareil d'observer ou d'affecter le comportement d'appareils non liés.

- **Fuites de données :** Les dispositifs IoT peuvent provoquer des fuites de données privées des utilisateurs, à la fois depuis le cloud (où les données sont stockées) et entre les dispositifs IoT eux-mêmes.
  - **Fuites dans le nuage :** Les services hébergés dans le cloud pourraient subir une violation de données due à une attaque externe ou à une menace interne. En outre, si les utilisateurs s'appuient sur des méthodes d'authentification ou de cryptage faibles pour ces services hébergés dans le cloud, les données des utilisateurs peuvent également être compromises.
  - **Fuites depuis et entre les appareils :** Dans certains cas, les appareils situés sur le même réseau ou sur des réseaux voisins peuvent être en mesure d'observer les données d'autres appareils, comme le nom des personnes présentes dans un foyer, l'emplacement géographique précis d'un foyer, ou même les produits qu'un consommateur achète.

- **Susceptibilité à l'infection par des logiciels malveillants et autres abus : Les** logiciels malveillants et autres formes d'abus peuvent perturber le fonctionnement des dispositifs IoT, obtenir un accès non autorisé ou lancer des attaques.

- **Possibilité d'interruption de service :** La perte potentielle de disponibilité ou de connectivité diminue non seulement la fonctionnalité des dispositifs IoT, mais peut également dégrader la sécurité des dispositifs dans certains cas, notamment lorsqu'un dispositif IoT ne peut plus fonctionner sans cette connectivité (par exemple, un système d'alarme domestique se désactivant en cas de perte de connectivité).

- **Possibilité de persistance des problèmes de sécurité et de confidentialité des appareils : Les** problèmes de sécurité des dispositifs IoT sont susceptibles de persister car de nombreux dispositifs peuvent ne jamais recevoir de mise à jour logicielle, soit parce que le fabricant (ou une autre partie de la chaîne d'approvisionnement IoT, ou le fournisseur de services IoT) peut ne pas fournir de mises à jour, soit parce que les consommateurs peuvent ne pas appliquer les mises à jour déjà disponibles.
  - **De nombreux dispositifs IoT ne seront jamais corrigés :** Le déploiement de mises à jour logicielles qui corrigent les vulnérabilités de sécurité critiques est difficile en général. De nombreux vendeurs et fabricants de dispositifs ne disposent pas de systèmes ou de processus permettant de déployer des mises à jour logicielles sur des milliers de dispositifs, et le déploiement par réseau

Il est difficile d'apporter des mises à jour aux appareils qui fonctionnent dans les foyers des consommateurs, car les mises à jour peuvent parfois interrompre le service et ont parfois le potentiel de "briquer" l'appareil, si elles ne sont pas effectuées correctement. En outre, certains appareils peuvent même ne pas être en mesure d'effectuer des mises à jour logicielles.

- **Les mises à jour logicielles ne se limitent pas aux bogues :** Les mises à jour logicielles ne sont pas simplement destinées à corriger des bogues de sécurité ou de confidentialité. Elles peuvent également être destinées à introduire de nouvelles fonctions importantes ou à améliorer les performances et la sécurité.
- **Les consommateurs sont peu enclins à mettre à jour le logiciel des dispositifs IoT :** Peu d'utilisateurs finaux mettent systématiquement à jour le logiciel des appareils de leur propre chef ; il est préférable de supposer que la plupart des utilisateurs finaux ne prendront jamais d'initiative pour mettre à jour le logiciel.

- **Le remplacement du dispositif peut être une alternative aux mises à jour logicielles - pour les dispositifs peu coûteux ou "jetables" :** Dans certains cas, le remplacement complet d'un appareil peut être une alternative aux mises à jour logicielles. Certains dispositifs IoT peuvent être si peu coûteux que la mise à jour du logiciel peut être peu pratique ou non rentable.

Recommandations. Le groupe de travail technique du BITAG dispose également des éléments suivants *recommandations* :

- **Les dispositifs IoT devraient utiliser les meilleures pratiques logicielles actuelles :**
  - **Les dispositifs IoT devraient être livrés avec un logiciel raisonnablement à jour :** BITAG recommande que les dispositifs IoT soient livrés aux clients ou aux points de vente au détail avec un logiciel raisonnablement à jour qui ne contient pas de vulnérabilités graves et connues.
  - **Les dispositifs IoT doivent disposer d'un mécanisme de mise à jour logicielle automatisée et sécurisée :** Les bugs logiciels doivent être réduits au minimum, mais ils sont inévitables. Ainsi, il est essentiel qu'un dispositif IoT dispose d'un mécanisme de mises à jour logicielles automatiques et sécurisées. BITAG recommande aux fabricants de dispositifs IoT ou aux fournisseurs de services IoT de concevoir leurs dispositifs et systèmes en partant du principe que de nouveaux bogues et vulnérabilités seront découverts au fil du temps. Ils devraient concevoir des systèmes et des processus pour assurer la mise à jour automatique des logiciels des appareils IoT, sans exiger ou attendre un quelconque type d'action de la part de l'utilisateur, ni même d'opt-in de sa part.
  - **Les dispositifs IoT devraient utiliser une authentification forte par défaut :** BITAG recommande que les dispositifs IoT soient sécurisés par défaut (par exemple, protégés par un mot de passe) et n'utilisent pas de noms d'utilisateur et de mots de passe courants ou facilement devinables (par exemple, "admin", "password").
  - **Les configurations des dispositifs IoT doivent être testées et renforcées :** Certains dispositifs IoT permettent à un utilisateur de personnaliser le comportement de l'appareil. BITAG recommande aux fabricants de tester la sécurité de chaque appareil avec un éventail de configurations possibles, par opposition à la simple configuration par défaut.

- **Les dispositifs IoT devraient suivre les meilleures pratiques en matière de sécurité et de cryptographie :** BITAG recommande aux fabricants de dispositifs IoT de sécuriser les communications en utilisant la sécurité de la couche de transport (TLS) ou la cryptographie légère (LWC). Si les appareils s'appuient sur une infrastructure à clé publique (PKI), alors une entité autorisée doit être en mesure de révoquer les certificats lorsqu'ils sont compromis, et les fabricants doivent veiller à éviter les méthodes de cryptage, les protocoles et les tailles de clé présentant des faiblesses connues. Parmi les autres bonnes pratiques de cryptage, citons
    - Cryptage des communications de configuration (commande et contrôle) par défaut
    - Communications sécurisées vers et depuis les contrôleurs IoT
    - Cryptage du stockage local des données sensibles
    - Authentifier les communications, les modifications de logiciels et les demandes de données
    - Utilisez des informations d'identification uniques pour chaque appareil
    - Utilisez des informations d'identification qui peuvent être mises à jour
    - Fermer les ports inutiles et désactiver les services inutiles
    - Utilisez des bibliothèques qui sont activement entretenues et soutenues.

- **Les appareils IoT doivent communiquer de manière restrictive plutôt que permissive :** Dans la mesure du possible, les appareils ne doivent pas être joignables par défaut via des connexions entrantes. Les dispositifs IoT ne doivent pas s'appuyer uniquement sur le pare-feu du réseau pour restreindre la communication, car certaines communications entre dispositifs au sein de la maison peuvent ne pas traverser le pare-feu.

- **Les dispositifs IoT devraient continuer à fonctionner si la connectivité Internet est interrompue :** BITAG recommande qu'un dispositif IoT devrait être en mesure d'exécuter sa ou ses fonctions primaires (par exemple, un interrupteur d'éclairage ou un thermostat devrait continuer à fonctionner avec des commandes manuelles), même s'il n'est pas connecté à Internet, car la connectivité Internet peut être interrompue pour des causes allant d'une mauvaise configuration accidentelle à une attaque intentionnelle. Les dispositifs IoT qui ont des implications pour la sécurité des utilisateurs devraient continuer à fonctionner en mode déconnecté afin de protéger la sécurité des consommateurs.

- **Les appareils IoT devraient continuer à fonctionner si le back-end du cloud tombe en panne :** De nombreux services qui dépendent ou utilisent un back-end de cloud peuvent continuer à fonctionner, même dans un état dégradé ou partiellement fonctionnel, lorsque la connectivité au back-end de cloud est interrompue ou que le service lui-même tombe en panne.

- **Les dispositifs IoT doivent prendre en charge les meilleures pratiques d'adressage et de nommage :** De nombreux dispositifs IoT peuvent rester déployés pendant un certain nombre d'années après leur installation. La prise en charge des derniers protocoles d'adressage et de nommage permettra à ces appareils de rester fonctionnels pendant des années.
    - **IPv6 :** BITAG recommande que les dispositifs IoT prennent en charge la version la plus récente du protocole Internet, IPv6.

- **DNSSEC :** BITAG recommande que les dispositifs IoT prennent en charge l'utilisation ou la validation des extensions de sécurité DNS (DNSSEC) lorsque des noms de domaine sont utilisés.

- **Les dispositifs IoT devraient être livrés avec une politique de confidentialité facile à trouver et à comprendre :** BITAG recommande que les dispositifs IoT soient livrés avec une politique de confidentialité, mais cette politique doit être facile à trouver et à comprendre pour un utilisateur type.

- **Divulguer les droits de réduire à distance les fonctionnalités d'un dispositif IoT :** BITAG recommande que si la fonctionnalité d'un dispositif IoT peut être diminuée à distance par un tiers, comme par le fabricant ou le fournisseur de services IoT, cette possibilité doit être clairement indiquée à l'utilisateur au moment de l'achat.

- **L'industrie des dispositifs IoT devrait envisager un programme industriel de cybersécurité :** Le BITAG recommande que l'industrie des dispositifs IoT ou un groupe connexe d'électronique grand public envisage la création d'un programme soutenu par l'industrie, dans le cadre duquel une sorte de logo ou de mention "Secure IoT Device" pourrait figurer sur les emballages de vente au détail des dispositifs IoT. Un ensemble de meilleures pratiques soutenues par l'industrie semble être le moyen le plus pragmatique d'équilibrer l'innovation dans l'IdO avec les défis de sécurité associés à la nature fluide de la cybersécurité, et d'éviter la "mentalité de liste de contrôle" qui peut se produire avec les processus de certification.

- **La chaîne d'approvisionnement IoT devrait jouer son rôle dans la résolution des problèmes de sécurité et de confidentialité de l'IoT :** Les utilisateurs finaux des appareils IoT dépendent de la chaîne d'approvisionnement IoT, du fabricant au détaillant, pour protéger leur sécurité et leur vie privée, et certaines ou toutes les parties de cette chaîne d'approvisionnement IoT jouent un rôle essentiel tout au long du cycle de vie du produit. En plus des autres recommandations de cette section, BITAG recommande que la chaîne d'approvisionnement IoT prenne les mesures suivantes :

    - **Politique de confidentialité :** Les appareils doivent avoir une politique de confidentialité claire et compréhensible, en particulier lorsqu'un appareil est vendu en même temps qu'un service continu.

    - **Mécanisme de réinitialisation :** Les appareils devraient disposer d'un mécanisme de réinitialisation pour les appareils IoT qui efface toute la configuration à utiliser lorsqu'un consommateur retourne ou revend l'appareil. Les fabricants de dispositifs devraient également fournir un mécanisme permettant de supprimer ou de réinitialiser toutes les données que le dispositif respectif stocke dans le cloud.

    - **Système de signalement des bogues : Les** fabricants doivent fournir un système de rapport de bogues avec des mécanismes de soumission de bogues bien définis et une politique de réponse documentée.

    - **Chaîne d'approvisionnement en logiciels sécurisés :** Les fabricants doivent protéger la chaîne d'approvisionnement en logiciels sécurisés afin d'empêcher l'introduction de logiciels malveillants au cours du processus de fabrication ; les vendeurs et les fabricants doivent prendre les mesures appropriées pour sécuriser leur chaîne d'approvisionnement en logiciels.

- **Prise en charge de l'appareil IoT pendant toute sa durée de vie :** Les fabricants doivent prendre en charge un dispositif IoT tout au long de sa durée de vie, depuis sa conception jusqu'au moment où il est mis hors service, en faisant preuve de transparence sur la période pendant laquelle ils prévoient de fournir une assistance continue à un dispositif, et sur ce que le consommateur doit attendre de la fonction du dispositif à la fin de sa durée de vie.
- **Méthodes de contact claires :** Les fabricants doivent fournir des méthodes claires permettant aux consommateurs de déterminer qui ils peuvent contacter pour obtenir de l'aide et des méthodes pour contacter les consommateurs afin de diffuser des informations sur les vulnérabilités des logiciels ou d'autres problèmes.
- **Signaler la découverte et la correction des vulnérabilités :** Les fabricants doivent signaler la découverte et la correction des vulnérabilités logicielles qui menacent la sécurité ou la vie privée des consommateurs.
- **Processus clair de signalement des vulnérabilités : Les** fabricants doivent fournir un processus de signalement des vulnérabilités avec un formulaire de signalement des vulnérabilités bien défini, facile à trouver et sécurisé, ainsi qu'une politique de réponse documentée.

Table des matières

1 Introduction

Au cours des dernières années, bon nombre des nouveaux appareils connectés à l'Internet ne sont pas des ordinateurs personnels, mais plutôt une variété d'appareils intégrant une connectivité et des fonctions Internet. Parmi ces appareils, on peut citer les thermostats, les prises intelligentes et les caméras en réseau. Cette catégorie d'appareils est généralement décrite comme l'*Internet des objets* (IoT), et il est clair que cette nouvelle catégorie d'appareils connaîtra une forte croissance dans les années à venir, avec des estimations variables selon les sources, mais toutes prévoient plusieurs milliards de ces appareils d'ici 2020 [1].

Le nombre et la diversité des dispositifs IoT augmentent rapidement ; ces dispositifs offrent de nombreuses nouvelles applications aux utilisateurs finaux, et en offriront encore plus à l'avenir. De nombreuses solutions IoT sont soit déjà disponibles, soit en cours de développement pour un déploiement dans un avenir proche, notamment :

- des capteurs pour mieux comprendre les schémas de la vie quotidienne et surveiller la santé
- des moniteurs et des commandes pour les fonctions de la maison, des serrures aux systèmes de chauffage et d'eau.
- des dispositifs et des appareils qui anticipent les besoins d'un consommateur et peuvent prendre des mesures pour y répondre (par exemple, des dispositifs qui surveillent les stocks et réorganisent automatiquement les produits pour un consommateur).

En outre, lorsqu'ils sont couplés à l'analyse des données et à l'apprentissage automatique, les dispositifs IoT peuvent être en mesure de prendre des mesures plus proactives, d'exposer des modèles de données intéressants ou de faire des suggestions aux utilisateurs finaux susceptibles d'améliorer leur santé, leur environnement, leurs finances et d'autres aspects de leur vie.

L'émergence de l'IdO offre des possibilités d'innovation importantes, des maisons intelligentes aux villes intelligentes. Malheureusement, de nombreux dispositifs IoT ont été livrés avec de graves défauts de sécurité et de confidentialité [2] ; la section 3 examine en détail de nombreux exemples récents. Ces failles font courir de nombreux risques aux utilisateurs finaux qui achètent les dispositifs et peuvent affecter le service d'accès à l'internet de l'utilisateur des dispositifs et des autres utilisateurs dont le trafic passe par les mêmes liens internet partagés. Les failles créent également des problèmes de sécurité et d'atténuation plus larges pour les cibles des attaques, les fournisseurs d'accès à Internet (FAI), ainsi que d'autres fournisseurs de services - par exemple les services de moteurs de recherche, la messagerie électronique et les sites de jeux - et introduisent de manière importante de nouveaux coûts de support et d'atténuation (qui sont généralement répercutés sur les utilisateurs finaux) [3]. Des coûts supplémentaires peuvent également être imposés aux fabricants de dispositifs eux-mêmes, qui devront peut-être prendre des mesures pour atténuer ces problèmes.

Dans de nombreux cas, des modifications simples des processus de développement, de distribution et de maintenance des appareils peuvent empêcher la distribution d'appareils IoT qui souffrent de problèmes importants de sécurité et de confidentialité. BITAG estime que le respect des lignes directrices décrites dans ce rapport peut améliorer considérablement la sécurité et la confidentialité des dispositifs IoT et minimiser les coûts associés aux dommages collatéraux qui affecteraient autrement les utilisateurs finaux et les FAI. En outre, à moins que le secteur des dispositifs IoT - le secteur de l'industrie qui fabrique et distribue ces dispositifs - n'améliore la sécurité et la confidentialité des dispositifs, les réactions des consommateurs pourraient entraver la croissance du marché de l'IoT et, en fin de compte, limiter les promesses de l'IoT pour les utilisateurs finaux.

2 Qu'est-ce que l'Internet des objets ?

L'internet des objets (IoT) comprend des dispositifs qui fonctionnent comme des capteurs, des actionneurs, des contrôleurs et des enregistreurs d'activité. Ces dispositifs interagissent généralement avec un logiciel fonctionnant ailleurs sur le réseau, par exemple sur un téléphone mobile, un dispositif informatique universel (par exemple, un ordinateur portable), une machine sur l'Internet public (par exemple, dans le "nuage"), ou une combinaison de ces éléments. Les dispositifs IoT fonctionnent souvent de manière autonome, sans nécessiter d'intervention humaine.

Le terme "IoT" a une portée potentiellement large. L'IoT peut faire référence à des déploiements dans les foyers, les entreprises, les installations de fabrication, les industries du transport et ailleurs. Ainsi, l'IdO peut se référer à bien plus que de simples appareils destinés aux consommateurs.

Aux fins du présent rapport, le terme IdO est utilisé pour désigner uniquement les appareils destinés aux consommateurs et les systèmes logiciels1 locaux et distants qui leur sont associés, bien que certaines ou l'ensemble de nos recommandations puissent être applicables de manière plus large. Le présent rapport s'intéresse aux scénarios dans lesquels les consommateurs installent, configurent et administrent des dispositifs qu'ils louent ou possèdent.

2.1 Limites du champ d'application

Le rapport ne prend pas directement en compte les dispositifs destinés à des environnements industriels ou interentreprises, tels que les capteurs des réseaux d'hôtels ou d'aéroports, les villes intelligentes, l'automatisation industrielle, le contrôle des bâtiments commerciaux ou le contrôle des stocks de fabrication. Dans ces contextes, les clients disposent souvent des ressources et des incitations nécessaires pour spécifier et gérer les fonctions de sécurité et de confidentialité des produits qu'ils achètent. En outre, bon nombre de ces appareils utilisent des connexions sans fil commerciales qui ne permettent pas un accès complet à l'Internet. Ceci étant dit, certaines des questions abordées dans ce rapport peuvent également être présentes dans ces environnements.

Le champ d'application de ce rapport est également limité aux dispositifs IoT qui sont à l'origine ou à la fin d'un flux de données. Plus précisément, le rapport ne s'intéresse pas aux dispositifs qui traversent un trafic qui peut contenir des données à destination ou en provenance de dispositifs IoT, parmi d'autres trafics, comme une passerelle domestique, un point d'accès sans fil ou un routeur.

En outre, le rapport se concentre uniquement sur les dispositifs et les systèmes qui utilisent le protocole Internet (IP), qu'il s'agisse d'IPv4 ou d'IPv6 ou des deux. Divers dispositifs IoT utilisent d'autres mécanismes de transport, tels que Zigbee 1.0 [4], X10 [5], etc. Ces appareils ne peuvent pas être connectés à Internet autrement que par l'intermédiaire d'un dispositif qui effectue une conversion de protocole. Ils fonctionnent sur un réseau isolé. Toutefois, les présentes recommandations s'appliquent toujours au dispositif qui effectue la conversion de protocole (par exemple, le concentrateur ou la passerelle domotique).

Ce rapport se concentre sur les problèmes spécifiques aux dispositifs d'un réseau IP local qui peuvent communiquer sur Internet. Les problèmes de confidentialité et de sécurité qui surviennent sur des réseaux isolés qui n'ont pas de connexion à l'Internet public sont hors de portée de ce rapport.

2.2 Dispositifs IoT que les utilisateurs ont modifiés

Le logiciel de certains appareils peut être mis à jour ou remplacé par un logiciel autre que celui prévu par le fabricant, créant ainsi, à bien des égards, un nouveau produit. Par exemple, un utilisateur peut installer un logiciel libre sur un appareil, au lieu d'utiliser le logiciel fourni par le fabricant. Le produit qui en résulte peut être soumis aux considérations et recommandations du présent rapport, mais dans ce cas, le dispositif doit être considéré comme un produit distinct dont l'utilisateur est responsable.

[1] Lorsque BITAG utilise le terme "logiciel", il s'agit d'inclure le micrologiciel du dispositif, qui est une forme de logiciel, et tous les autres

types de logiciels.

3 Pourquoi la sécurité et la confidentialité de l'IdO présentent un intérêt particulier

Les dispositifs IoT sont confrontés aux mêmes types de défis en matière de sécurité et de confidentialité que de nombreux dispositifs conventionnels destinés aux utilisateurs finaux. D'autre part, les dispositifs IoT n'offrent généralement ni contrôles clairs ni documentation pour informer un utilisateur des risques introduits lors du déploiement de ces dispositifs. En outre, des études ont montré que le fait de s'appuyer sur l'utilisateur final pour prendre des décisions en matière de sécurité et de confidentialité est susceptible d'échouer [6, 7, 8].

3.1 Consommateurs non techniques ou non intéressés.

Les utilisateurs finaux ne disposent pas de l'expertise technique nécessaire pour évaluer les implications en matière de confidentialité et de sécurité d'un dispositif IoT particulier, ou bien ils peuvent ne pas avoir envie de le faire [9]. En outre, le plus souvent, les dispositifs déployés ne disposent pas de mécanismes automatisés pour effectuer des mises à jour sécurisées ou appliquer la politique de sécurité [9,10].

3.2 La découverte et l'inventaire des appareils sont difficiles.

Les consommateurs ont déjà du mal à identifier et à dépanner les appareils qui sont actuellement connectés à leurs réseaux domestiques [11]. Les dispositifs IoT vont exacerber cette situation, car les consommateurs connectent une variété de plus en plus grande de dispositifs à leurs réseaux domestiques.
Au fil du temps, les utilisateurs perdront probablement la trace des appareils connectés à l'Internet, ce qui rendra leur sécurisation encore plus difficile. En outre, les FAI auront du mal à aider les consommateurs à identifier les sources des problèmes de sécurité. Bien que les FAI puissent être en mesure de déterminer qu'un dispositif du réseau domestique d'un client est compromis, ils peuvent être incapables d'identifier le dispositif spécifique compromis, en raison de technologies telles que la traduction d'adresse réseau (NAT) et d'autres technologies qui peuvent masquer l'identité des dispositifs individuels.

3.3 Effets sur le service d'accès à Internet.

Les dispositifs IoT compromis par des logiciels malveillants (voir les sections 4.5 et 5.3) peuvent affecter le service d'accès à Internet à la fois de l'utilisateur de ces dispositifs IoT et des autres utilisateurs dont le trafic passe par les mêmes liens Internet partagés. Ces appareils peuvent également présenter une menace pour l'utilisateur et les autres cibles du malware [12]. Ce logiciel malveillant peut être utilisé pour lancer des attaques DDoS [13],

envoyer des spams, attaquer d'autres dispositifs sur le réseau de l'utilisateur ou interférer de manière malveillante avec le service d'accès à Internet de l'utilisateur.

Ces problèmes augmentent les coûts supportés par le FAI, qui doit s'efforcer d'atténuer ces attaques, de fournir un service d'assistance aux utilisateurs qui ne parviennent pas à déterminer pourquoi leur service d'accès à Internet se comporte mal ou anormalement, voire de désactiver le service d'accès à Internet des utilisateurs dont les appareils se livrent à des activités réseau malveillantes. Ces problèmes augmentent également les coûts pour le consommateur en dégradant les performances et en créant un risque de perte d'identifiants. Enfin, ils imposent des coûts à la cible de toute attaque de ce type et aux fabricants de dispositifs IoT eux-mêmes (ou à d'autres parties de la chaîne d'approvisionnement IoT), qui peuvent être amenés à prendre des mesures pour atténuer ces problèmes.

3.4 Effets sur les autres services.

Les appareils IoT compromis par des logiciels malveillants peuvent devenir une plateforme pour le trafic indésirable, comme le spam et les attaques par déni de service - y compris les attaques par réflexion et amplification, par lesquelles un attaquant envoie du trafic à un appareil avec l'adresse source usurpée d'une victime, ce qui amène l'appareil à envoyer de grandes quantités de trafic vers la victime) [14] - ce qui peut interférer avec la capacité d'un fournisseur de services à fournir un service [15]. Les dispositifs compromis peuvent également être utilisés pour écouter le trafic du réseau local ou comme "tremplin" pour attaquer d'autres dispositifs et services sur le réseau local du client, créant ainsi un risque de fuite de données. Les fournisseurs qui proposent des services tels que des moteurs de recherche, des courriers électroniques en ligne et des sites de jeux doivent investir des ressources pour atténuer ces attaques. Les victimes de ces attaques supporteront également des coûts financiers et de confidentialité. Les appareils IoT compromis peuvent aussi occasionnellement affecter le modèle économique d'un fournisseur de services. Le malware DNSChanger, qui permettait aux attaquants d'insérer leurs propres publicités dans les pages web des victimes, en est un exemple [16].

4 De nombreux appareils ne respectent pas les meilleures pratiques en matière de sécurité et de confidentialité

Les dispositifs IoT sont déjà devenus une plateforme d'abus et d'attaques. De nombreux technologues ont découvert divers risques pour la sécurité et la confidentialité associés aux dispositifs IoT disponibles aujourd'hui [17, 18, 19, 20, 21, 22, 23, 24]. Des dizaines de millions de dispositifs IdO supplémentaires seront probablement déployés au cours des prochaines années, ce qui pourrait constituer une vaste plate-forme pour lancer des attaques, à la fois sur d'autres dispositifs au domicile de l'utilisateur et sur l'Internet en général, et pour collecter subrepticement des informations privées sur des utilisateurs finaux ou des groupes d'utilisateurs spécifiques.
Outre les pertes que peuvent subir les consommateurs, les FAI peuvent subir une augmentation des appels à l'assistance technique et des attaques, ce qui augmente le coût des opérations qui est répercuté sur les consommateurs.

Plusieurs rapports récents ont étudié les caractéristiques de sécurité et de confidentialité des dispositifs IoT et ont constaté que certains dispositifs ne respectent pas les meilleures pratiques rudimentaires en matière de confidentialité et de sécurité [25, 26, 27, 28, 29, 30, 31]. Dans certains cas, les dispositifs ont été compromis [32].

Les problèmes potentiels contribuant à ce manque de bonnes pratiques en matière de confidentialité et de sécurité sont les suivants :

4.1 Manque d'incitations à développer et à déployer des mises à jour après la vente initiale.

Pour les appareils IoT grand public vendus par les canaux de vente au détail, les fournisseurs d'appareils peuvent être peu incités à fournir des mises à jour logicielles après la vente initiale. Si le revenu d'un appareil provient uniquement de la vente initiale, alors toute maintenance de l'appareil érode ce revenu initial, diminuant ainsi le bénéfice. Cette structure peut encourager l'obsolescence planifiée, où les fournisseurs donnent la priorité à la vente de nouveaux appareils plutôt qu'au soutien des appareils existants.

4.2 Difficulté des mises à jour sécurisées des logiciels via le réseau.

Les appareils IoT peuvent ne pas être conçus et configurés pour recevoir des mises à jour logicielles sécurisées sur le réseau, ce qui entraîne des processus de mise à jour fastidieux.

4.3 Dispositifs avec des ressources limitées

Les dispositifs IoT vendus dans un environnement de consommation à faible marge peuvent être conçus avec des ressources matérielles limitées. Par conséquent, certaines mesures de sécurité de base telles que le chiffrement, la vérification des signatures logicielles et le contrôle d'accès sécurisé ne sont pas réalisables. Ainsi, les conceptions qui limitent les capacités de traitement et de mémoire d'un appareil peuvent empêcher l'exécution d'un logiciel de sécurité basé sur l'hôte ou empêcher sa mise à niveau en toute sécurité. La section 5.1 aborde cette question de manière plus détaillée.

4.4 Dispositifs à interfaces limitées

De nombreux types de dispositifs IoT ont des interfaces utilisateur limitées ou inexistantes. Même lorsqu'un dispositif expose une interface utilisateur via un dispositif secondaire (par exemple, une application pour smartphone), sa fonctionnalité peut être minimale. Par conséquent, des tâches telles que la configuration d'un pare-feu local ou la désactivation de services distants peuvent être impossibles. Les dispositifs peuvent également ne pas avoir la capacité d'afficher des conditions d'erreur et des alertes significatives pour les utilisateurs qui peuvent utiliser les informations d'erreur pour mieux protéger un dispositif.

4.5 Appareils avec des logiciels malveillants insérés pendant la fabrication.

Les logiciels malveillants peuvent être insérés dans les appareils au moment de la fabrication ou de l'emballage par des employés du fabricant ou d'autres personnes ayant accès à l'environnement de fabrication ou d'emballage. Un dispositif compromis peut souvent sembler fonctionner normalement, auquel cas la violation de la sécurité ou de la vie privée peut persister jusqu'à ce que la compromission soit détectée. Les pare-feu et l'isolation du réseau ne peuvent pas se défendre contre les attaques lancées par ces dispositifs compromis sur d'autres dispositifs internes au réseau isolé. Pour des exemples connus de tels dispositifs compromis et une discussion supplémentaire sur les effets des logiciels malveillants, voir la section 5.3.

4.6 Manque d'expérience des fabricants en matière de sécurité et de confidentialité

De nombreux fabricants d'appareils IoT (et d'autres parties de la chaîne d'approvisionnement IoT) n'ont aucune expérience préalable de la conception, du développement ou de la maintenance des appareils connectés à Internet ou de la manipulation des données des consommateurs. Ces fabricants manquent de cycles de développement sécurisés, d'équipes de réponse aux incidents et d'expérience en matière de confidentialité et d'ingénierie de la sécurité en général.

4.7 Risques dus aux dispositifs vulnérables

Les exemples suivants illustrent la portée et l'étendue des problèmes possibles lorsque les dispositifs IoT deviennent vulnérables aux attaques contre la sécurité et la vie privée. Un utilisateur non autorisé peut être en mesure de :

- **Effectuer une surveillance et un contrôle non autorisés.**
    - savoir si une personne spécifique est à la maison, quelle pièce elle occupe et quand elle entre dans la maison
    - savoir quels autres appareils sont connectés au réseau domestique, et comment les utilisateurs interagissent avec eux
    - activer à distance un microphone ou une caméra sur un appareil pour écouter ou espionner quelqu'un [33].
    - découvrir si une porte ou un garage a été récemment ouvert et fermé afin de déterminer si quelqu'un est à la maison, pour aider à une effraction physique
    - installer un logiciel malveillant sur une caméra IoT pour accéder au flux vidéo de la caméra [34].
- **Obtenir un accès ou un contrôle non autorisé.**
    - éteindre un thermostat pendant les mois d'hiver pour provoquer l'éclatement des conduites d'eau et endommager une maison.
    - d'allumer ou d'éteindre des lumières, par exemple en éteignant l'éclairage du périmètre pour faciliter une effraction physique
    - déverrouiller des portes pour aider à une intrusion physique
    - suppression d'une alarme provenant d'un capteur de porte ou de fenêtre
    - réaffecter un appareil à un usage illicite (par exemple, comme mineur de bitcoins [35])

- **Provoquer des pannes de dispositifs ou de systèmes.**
    - activer des systèmes de climatisation résidentiels pour créer une surtension inattendue sur un réseau électrique dans le but de créer des conditions de brownout ou de blackout
    - subvertir les capteurs de collecte de données de santé pour modifier les données de santé telles que la pression artérielle, la glycémie ou les informations sur le poids qui peuvent être transmises à un service de surveillance de la santé ou à un dispositif médical (tel qu'une pompe à insuline)
    - émuler le logiciel de gestion de l'appareil de manière à ce qu'il semble fonctionner normalement, mais au lieu de cela, désactiver des fonctionnalités importantes ou apporter d'autres modifications de fonctionnement, ce qui entraîne des défaillances importantes de l'équipement ou des systèmes matériels [36] .
    - empêcher un thermostat de contrôler le chauffage ou la climatisation d'un bâtiment, ce qui entraîne une chaleur ou un froid extrême.

- **Déranger ou harceler les utilisateurs.**
    - activer à distance un haut-parleur et se livrer à des menaces verbales ou à du harcèlement
    - activer les détecteurs de fumée ou autres détecteurs de sécurité

Tous ces scénarios créent de sérieux risques pour la sécurité et la vie privée des utilisateurs finaux et pour l'internet dans son ensemble. Certains risques pour la sécurité et la vie privée des utilisateurs finaux pourraient également permettre une nouvelle forme de harcèlement numérique. Dans des cas extrêmes, la subversion de la collecte de données sur la santé pourrait entraîner des blessures ou la mort. Dans le cas d'appareils largement déployés, les risques pour la sécurité peuvent être cumulés sur des centaines ou des milliers d'appareils pour créer des attaques distribuées sur les infrastructures critiques.

Les problèmes de sécurité et de respect de la vie privée liés aux dispositifs IoT pourraient, à terme, limiter la croissance future du secteur IoT. Un petit nombre d'incidents très médiatisés pourrait réduire la demande de dispositifs IoT ou limiter la croissance et le potentiel de l'IoT. Il est donc essentiel de résoudre ces problèmes pour soutenir la santé, le dynamisme et la croissance à long terme du marché de l'IdO.

5 Observations sur les questions de sécurité et de confidentialité de l'IdO

Il n'est pas réaliste d'attendre des fabricants qu'ils créent des produits logiciels exempts de bogues ; tous les logiciels ont des bogues, et produire des logiciels exempts de tels défauts reste un problème non résolu. Par conséquent, certains appareils IoT sortent de l'usine avec des logiciels qui sont ou deviennent obsolètes au fil du temps. Il ne s'agit pas d'expédier des logiciels bogués, ce qui est sans doute inévitable ; le problème est plutôt que les fabricants peuvent expédier des appareils avec des logiciels obsolètes qui contiennent de nombreuses vulnérabilités de sécurité importantes et documentées, dont certaines peuvent être immédiatement exploitables lorsque l'appareil est connecté à Internet pour la première fois [37].

D'autres dispositifs IoT peuvent être livrés avec un logiciel plus récent qui ne contient aucune vulnérabilité de sécurité majeure connue au moment de l'expédition. Même dans ces cas, des vulnérabilités peuvent être découvertes à l'avenir, ce qui peut rendre un appareil moins sûr au fil du temps, à moins qu'il ne dispose d'un mécanisme de mise à jour ultérieure de son logiciel. Malheureusement, de nombreux dispositifs IoT ne disposent pas de mécanismes de mise à jour logicielle sécurisés et automatisés permettant de corriger les vulnérabilités une fois que les dispositifs ont été expédiés et déployés. [2] Sans l'adoption généralisée de méthodes de mise à jour logicielle automatisée et sécurisée, le nombre de dispositifs IoT non sécurisés et compromis risque d'augmenter considérablement dans les années à venir.

Les dispositifs IoT qui sont livrés avec des problèmes de sécurité et de confidentialité ou qui les développent au fil du temps

peuvent créer une nouvelle population de dispositifs qui peuvent être utilisés par des pirates malveillants, par exemple pour mener des attaques par réflexion et amplification [41]. Non seulement ces dispositifs présentent des risques pour leurs propriétaires, mais ils peuvent également être exploités pour abuser d'autres parties. La sécurité des dispositifs IoT intéresse donc non seulement les fabricants (et les autres parties de la chaîne d'approvisionnement IoT) et les clients des dispositifs IoT, mais aussi l'Internet au sens large.

Enfin, bien que ce rapport fournisse de nombreux exemples de dispositifs IoT qui présentent ou ont présenté des problèmes de sécurité ou de confidentialité, dans de nombreux cas, les exemples soulignés ici peuvent avoir été traités par les parties concernées avant la publication de ce rapport.

5.1 Communications réseau non sécurisées

Les dispositifs IoT en général peuvent être assez limités en ressources, n'ayant pas la puissance de calcul et la bande passante des dispositifs informatiques plus conventionnels tels que les téléphones mobiles, les ordinateurs portables et les ordinateurs de bureau, comme nous l'avons vu à la section 4. Par conséquent, de nombreuses fonctions de sécurité conçues pour des dispositifs informatiques plus polyvalents sont plus difficiles à mettre en œuvre sur les dispositifs IoT. Par exemple, le chiffrement à clé publique, qui sous-tend les communications sécurisées modernes basées sur Transport Layer Security (TLS) [42] et Datagram Transport Layer Security (DTLS) [43], peut être difficile à mettre en œuvre sur certains dispositifs IoT aux ressources limitées. Par exemple, les appareils Arduino et Raspberry Pi peuvent prendre plusieurs secondes pour effectuer une opération de chiffrement ou de déchiffrement asymétrique [44,45].

Au-delà des limites inhérentes aux dispositifs IoT et aux plateformes IoT sur lesquelles ils fonctionnent, un certain nombre de failles de sécurité ont été identifiées sur le terrain, notamment des communications non cryptées, des fuites de données des dispositifs IoT et des effets négatifs sur le réseau auquel le dispositif IoT est attaché [25,26,27,46,47].

Par exemple, certaines implémentations de serveurs TLS sont vulnérables aux attaques dites de " downgrade ", par lesquelles un attaquant peut forcer un serveur à utiliser une ancienne version du protocole TLS, qui peut présenter des problèmes de sécurité connus, tels que des vulnérabilités aux attaques de type man-in-the-middle. Dans ces scénarios, la communication entre un dispositif IoT et le service hébergé dans le cloud qui le prend en charge pourrait être compromise.

▪ Communications non authentifiées

Certains dispositifs IoT fournissent des mises à jour logicielles automatiques. Cependant, sans authentification ni chiffrement, cette approche est insuffisante, car le mécanisme de mise à jour pourrait être compromis ou désactivé [48]. Le mécanisme de mise à jour lui-même et tout trafic de commande et de contrôle associé doivent être authentifiés et chiffrés, et l'intégrité des communications entre le dispositif et les autres points d'extrémité doit être protégée. [3] Malheureusement, de nombreux dispositifs IoT n'utilisent pas l'authentification au cours de la communication. Par exemple, le hub Lightwave RF Smart a envoyé du trafic vers un serveur distant sur le réseau à chaque fois qu'il a redémarré et, par la suite, toutes les quinze minutes lors de la vérification des mises à jour logicielles [29]. Si la connexion n'est pas sécurisée, il n'est pas difficile pour un attaquant ayant accès au réseau de mener une attaque de type man-in-the-middle.

▪ Communications non cryptées

De nombreux appareils IoT envoient tout ou partie des données en clair, plutôt que sous une forme chiffrée. Cela signifie que les données peuvent "fuir" et être observées par d'autres appareils ou par un attaquant.

Par conséquent, certains dispositifs IoT laissent échapper des informations sur les utilisateurs (par exemple à un observateur du trafic réseau), ce qui peut permettre d'identifier le ou les dispositifs IoT utilisés, ainsi que de révéler l'activité et le comportement actuels des utilisateurs [17]. [4] Par exemple :

- Un cadre photo numérique transmet l'adresse électronique de l'utilisateur en clair lors de la synchronisation des photos, et l'activité actuelle de l'utilisateur est également affichée en clair [10].
- Une caméra web envoie des fichiers vidéo en clair [29].
- Un assistant personnel audio transporte les commandes audio de l'utilisateur, les relevés des capteurs et les adresses électroniques de l'utilisateur en clair [29].
- Un thermostat transporte des données météorologiques locales avec des informations précises sur la localisation de l'utilisateur en clair, et est clairement identifiable comme un thermostat d'une marque spécifique en fonction des ports utilisés. [5]
- Un hub de dispositif IoT a un profil de trafic en clair qui est si régulier et spécifique que le hub de dispositif peut être identifié simplement en prenant l'empreinte du modèle de trafic en clair [29].
- Certains stimulateurs cardiaques compatibles IoT utilisent des canaux de communication non cryptés [52].

L'envoi de trafic en clair n'est pas le modèle recommandé pour les nouveaux déploiements et crée des problèmes de fuite d'informations personnelles ou autres sur un réseau local ou sur Internet. À ce sujet, par exemple, l'Internet Architecture Board (IAB) a récemment déclaré : " L'IAB exhorte les concepteurs de protocoles à concevoir un fonctionnement confidentiel par défaut... Nous encourageons vivement les développeurs à inclure le chiffrement dans leurs implémentations et à les rendre chiffrées par défaut "[53].

- **Absence d'authentification et d'autorisation mutuelles**

De nombreuses attaques proviennent de derrière un pare-feu, à la frontière d'un réseau, à la maison ou ailleurs. Par conséquent, les communications derrière un pare-feu ne doivent pas nécessairement être considérées comme dignes de confiance. Ainsi, un dispositif doit établir la confiance entre les dispositifs, indépendamment du fait qu'il se trouve sur un réseau local ou sur Internet ; il doit supposer que les autres dispositifs ne sont pas dignes de confiance par défaut et doivent être explicitement authentifiés et autorisés. Un appareil qui permet à une partie inconnue ou non autorisée de modifier son code ou sa configuration, ou d'accéder à ses données, constitue une menace ; l'appareil peut révéler que son propriétaire est présent ou absent, faciliter l'installation ou l'exploitation de logiciels malveillants, ou faire en sorte que sa fonction IoT principale soit fondamentalement compromise.

Heureusement, contrairement aux appareils informatiques polyvalents tels que les ordinateurs portables, qui peuvent communiquer avec de nombreuses destinations Internet, les appareils IoT communiquent souvent avec un petit nombre de destinations bien définies. Par exemple, un appareil peut communiquer régulièrement uniquement avec un serveur de contrôle ou de mise à jour qui a un nom DNS ou une adresse IP bien connus ; une communication importante avec d'autres destinations peut être source d'inquiétude.

- ***Manque d'isolation du réseau***

Outre les risques pour la sécurité et la vie privée que les dispositifs IoT introduisent en dehors du réseau domestique où le dispositif IoT lui-même est installé (voir section 4), ces dispositifs créent également de nouveaux risques et sont susceptibles d'être attaqués *à l'intérieur de* la maison. Étant donné que de nombreux réseaux domestiques n'isolent pas, par défaut, les différentes parties du réseau les unes des autres, un dispositif connecté au réseau peut être en mesure d'observer ou d'échanger du trafic avec d'autres dispositifs sur le même réseau domestique, ce qui permet à un dispositif d'observer ou d'affecter le comportement de dispositifs non liés.

Bien qu'il soit courant d'utiliser des pare-feu pour isoler les appareils d'un réseau les uns des autres, les pare-feu seuls ne peuvent pas toujours protéger les appareils contre les compromissions ou les fuites de données, ni contre les logiciels malveillants sur les appareils déjà présents sur le réseau domestique. Aujourd'hui, un réseau domestique typique n'offre que peu ou pas d'isolation entre les appareils. La section 6 traite plus en détail des pare-feu et des autres mécanismes d'isolation du réseau.

Ce manque d'isolement constitue une menace pour la sécurité et la confidentialité de tous les appareils du réseau, à la fois en raison des actions spécifiques du fabricant (ou des actions d'autres parties dans la chaîne d'approvisionnement de l'IdO) et en raison de la compromission de l'appareil [27,54,55]. Plus précisément, un attaquant peut être en mesure de collecter des renseignements ou des informations personnelles à partir d'autres appareils sur le même réseau. En général, chaque appareil d'un réseau domestique peut voir le trafic des autres appareils qui se trouvent sur le même réseau. Si les appareils transmettent le trafic en clair, un appareil peut être en mesure de découvrir les détails de l'activité d'un autre appareil. Des travaux récents ont montré que même la capacité d'observer des détails plus "grossiers", tels que les consultations DNS et les changements dans les volumes de trafic, peut révéler des informations sur l'activité des appareils et le comportement des utilisateurs [56]. Un attaquant qui compromet un dispositif peut donc être en mesure de déduire des informations importantes sur un utilisateur final, comme les heures d'entrée et de sortie de la maison via des capteurs de porte compromis ou des enregistrements audio et vidéo provenant de microphones et de caméras vidéo intégrés dans des dispositifs IoT. La conception de la sécurité de nombreux réseaux sans fil domestiques permet des attaques de type "stepping stone" [57], par lesquelles un attaquant peut compromettre un dispositif IoT vulnérable et utiliser cette compromission comme mécanisme pour accéder à d'autres dispositifs connectés depuis l'intérieur du réseau. En voici quelques exemples :

- Un produit smartwatch comprenait un serveur DNS fonctionnel que des attaquants externes pouvaient utiliser pour attaquer d'autres appareils sur le réseau auquel la smartwatch était connectée. Le même produit présentait une vulnérabilité qui permettait à des attaquants externes de visualiser le trafic du réseau local [27].

- Une ampoule intelligente pourrait être piégée pour envoyer des informations d'identification de réseau sans fil que des attaquants externes pourraient ensuite utiliser pour contrôler les lumières et visualiser le trafic du réseau local [54].

- Certains fabricants de dispositifs et fournisseurs de services Internet ont exposé des interfaces de gestion à distance non sécurisées de millions de dispositifs et d'équipements d'abonné (par exemple, des modems, des routeurs domestiques) qui partageaient tous la même clé privée connue, exposant ces dispositifs à des attaques man-in-the-middle passives et actives [55].

- Des vulnérabilités dans un certain modèle de téléphone VoIP permettraient à un attaquant de réseau local de fournir des mises à jour malveillantes du micrologiciel du téléphone [58].

- Un fabricant de caméras de sécurité Wi-Fi a conçu ses produits avec un logiciel de mise en réseau peer-to-peer qui "perce" plusieurs trous dans le pare-feu du réseau local et ne peut pas être facilement désactivé. Ce logiciel permettait aux attaquants non seulement de compromettre la caméra elle-même à partir d'une grande variété de points d'accès, mais aussi de lancer des attaques sur d'autres appareils du réseau local [31].

5.2 Fuites de données

L'installation de dispositifs IoT dans la maison crée un potentiel de fuite de données privées des utilisateurs, à la fois depuis le cloud (où les données sont stockées) et entre les dispositifs IoT eux-mêmes.

▪ Fuites dans le nuage

Une grande partie des données que les appareils IoT collectent sont actuellement stockées dans des services de cloud à l'extérieur du domicile ; ces services de cloud pourraient subir une violation des données en raison d'une attaque externe ou d'une menace interne.

En outre, si les utilisateurs utilisent des méthodes d'authentification ou de cryptage faibles pour ces services hébergés dans le nuage, les données des utilisateurs peuvent également être compromises.

En voici quelques exemples :

- Une application web associée à un ours en peluche (qui contient une petite caméra sur son nez) contenait une faille de sécurité qui exposait l'identité des enfants [59].
- La poupée envoyait des chats cryptés entre la poupée et les serveurs hébergés dans le nuage en utilisant une version de TLS qui était vulnérable à une attaque par déclassement, ce qui permettait d'écouter les enregistrements des enfants [60].
- Une violation des données chez un fabricant de jouets pour enfants a exposé les données personnelles de plus de six millions d'enfants [61].
- Des faiblesses dans la configuration du point d'accès Wi-Fi d'un véhicule automobile ont permis de suivre l'emplacement de nombreux véhicules sur des sites web qui récoltent les noms des points d'accès Wi-Fi et leur emplacement [62].
- Le système d'un constructeur automobile a envoyé des statistiques sur la consommation de carburant, des coordonnées géographiques précises, la vitesse, la direction et la destination en clair à un serveur central [63].

Il existe de nombreux autres exemples de violations de données à partir de ces dispositifs [25,28,30,32,64,65,66,67]. Les fuites de données à partir du cloud ne sont pas nouvelles ou spécifiques aux dispositifs IoT, mais la prévalence des vulnérabilités de fuite de données dans les services hébergés dans le cloud est particulièrement problématique pour les dispositifs IoT grand public, qui sont non seulement de plus en plus omniprésents mais collectent aussi de plus en plus de données personnelles et privées.

▪ Fuites depuis et entre les appareils

Les appareils IoT de différents fabricants, exécutant de nombreuses applications logicielles différentes, peuvent tous résider sur le même réseau local. Bien que les techniques de cryptage Wi-Fi standard puissent protéger la confidentialité des transmissions de données sur le réseau local, le cryptage seul ne garantit pas la confidentialité des utilisateurs.

Dans certains cas, les dispositifs du même réseau ou de réseaux voisins peuvent être en mesure d'observer les données d'autres dispositifs. Par exemple, un dispositif peut "fuir" des données vers des dispositifs ou des utilisateurs proches (soit sur le même réseau local, soit sur le réseau Wi-Fi, soit simplement à proximité). Même avec le cryptage Wi-Fi, un dispositif peut toujours observer la présence d'autres dispositifs sur le même réseau local, et les adresses matérielles des autres dispositifs - qui peuvent souvent révéler le type de dispositif - sont aussi généralement visibles en clair. Ce niveau de visibilité pourrait, par exemple, permettre au logiciel d'un cadre photo numérique de surveiller les interactions d'un utilisateur avec d'autres appareils sur le même réseau.

Les données qui fuient d'un appareil à l'autre peuvent inclure des informations telles que le nom des personnes présentes dans un foyer, la localisation géographique précise d'un foyer, ou même les produits achetés par un consommateur. Par exemple, une étude récente a découvert qu'un thermostat laissait échapper des informations géographiques précises de la maison [17]. Dans une autre étude récente, des chercheurs ont été en mesure de déterminer le code PIN d'un guichet automatique sur la base des données accélérométriques transmises par Bluetooth à partir d'un dispositif de suivi de la condition physique [68].

5.3 Susceptibilité à l'infection par des logiciels malveillants et autres abus

Les logiciels malveillants, qui sont des logiciels malveillants installés sur un appareil d'utilisateur qui perturbent généralement les opérations, obtiennent un accès non autorisé ou lancent des attaques, peuvent infecter les appareils IoT par divers mécanismes. De même, d'autres formes d'abus peuvent se produire. En voici quelques exemples :

- Le fabricant peut ne pas sécuriser correctement la chaîne d'approvisionnement en logiciels [69] et permettre ainsi l'installation de logiciels malveillants sur le logiciel initialement livré du dispositif IoT [34], comme indiqué à la section 4.5.
- Les appareils peuvent être livrés avec un logiciel obsolète qui contient des vulnérabilités connues. Lorsqu'un utilisateur connecte l'appareil au réseau, celui-ci devient immédiatement une cible pour les attaquants. Des études antérieures ont démontré que le "temps de survie" (c'est-à-dire le temps pendant lequel un appareil est connecté au réseau avant d'être infecté) peut dans certains cas être inférieur à dix minutes [70]. [6] Si un appareil est livré avec un logiciel obsolète et ne vérifie pas immédiatement les mises à jour logicielles, il risque d'être infecté immédiatement.
- Les mécanismes de mise à jour des logiciels peuvent ne pas inclure l'authentification des chargements de logiciels pour garantir que le logiciel provient d'une source fiable. Grâce à l'ingénierie sociale, l'utilisateur peut être influencé ou incité à charger un logiciel compromis sur un dispositif IoT.
- Le logiciel peut inclure des capacités de ligne de commande ou des interfaces de programmation d'applications (API) qui peuvent être exploitées (avec ou sans la participation de l'utilisateur) pour charger un logiciel malveillant sur un dispositif IoT.
- L'appareil a des ports inutiles laissés ouverts et non sécurisés, tels que telnet. Ces ports inutiles ont été utilisés pour compromettre un appareil, par exemple en demandant à l'appareil d'accéder à une destination afin de télécharger un logiciel malveillant [71,72,73]. Les ports inutiles peuvent également être utilisés dans des attaques par amplification.
- L'appareil utilise une authentification par défaut faible, comme des noms d'utilisateur et des mots de passe communs ou faciles à deviner (par exemple, "admin", "password") [74]. En outre, l'authentification pour l'accès à distance peut ne pas avoir été sécurisée, ce qui permet à des personnes qui ne sont pas physiquement présentes dans la maison de se connecter à l'appareil et d'y installer des logiciels malveillants [13,75,76,77,78].

5.4 Possibilité d'interruption de service

Un aspect important de la sécurité des dispositifs IoT est la disponibilité des services face aux pannes et aux attaques des dispositifs. La perte potentielle de disponibilité ou de connectivité diminue non seulement la fonctionnalité des dispositifs IoT, mais peut également dégrader la sécurité des dispositifs dans certains cas, par exemple lorsqu'un dispositif IoT ne peut plus fonctionner sans cette connectivité (par exemple, un système d'alarme domestique se désactivant si la connectivité est perdue). Un dispositif IoT peut subir une interruption de service de plusieurs manières.

- **Perte de support d'une application hébergée dans le nuage.** Si l'appareil dépend de la communication avec un service en nuage, il peut ne pas fonctionner lorsqu'il perd la connectivité avec le service en nuage. Cette déconnexion peut se produire pour diverses raisons, notamment l'interruption de la connectivité Internet, des bogues dans le service logiciel en nuage, la faillite d'un vendeur ou d'un fabricant, ou la décision d'un consommateur d'interrompre un abonnement à un service.
- **Perte de connectivité au réseau. La** connectivité au sein d'un réseau domestique peut être interrompue, par exemple en raison d'un câble d'alimentation débranché, d'interférences radio avec le Wi-Fi ou d'un pare-feu décidant de restreindre l'accès.
- **Dommage de l'appareil. Un** appareil peut être physiquement endommagé, ou son logiciel peut être corrompu ou inopérant (parfois appelé "bricking").

Un appareil "bricolé", c'est-à-dire endommagé physiquement ou logiquement, peut être irrécupérable, tandis qu'un appareil qui dépend de la communication avec un service hébergé dans le nuage peut redevenir opérationnel lorsque la communication est rétablie.

Les pannes de certains services peuvent endommager les biens et mettre les utilisateurs en danger. Par exemple, un bug logiciel dans un thermostat IoT a entraîné le non-fonctionnement des systèmes de chauffage domestique et (par conséquent) le gel des tuyaux dans les maisons [51]. Le mauvais fonctionnement des systèmes de chauffage et de refroidissement peut entraîner des décès. Lorsque les dispositifs IoT sont responsables de tout, de la santé personnelle à la sécurité de la maison, les enjeux pour la sécurité des utilisateurs sont élevés.

5.5 Les problèmes de sécurité et de confidentialité des dispositifs risquent de persister

La présente section explique brièvement pourquoi les problèmes de sécurité décrits dans la section précédente sont susceptibles de persister. On pourrait s'attendre à ce qu'un grand nombre de ces appareils IoT ne reçoivent jamais de mise à jour logicielle, soit parce que le fabricant (ou une autre partie de la chaîne d'approvisionnement IoT, ou le fournisseur de services IoT) ne fournit pas de mises à jour, soit parce que les consommateurs n'appliquent pas les mises à jour déjà disponibles. Il existe de nombreux exemples de cela avec des types d'appareils similaires [79,80,81,82].

▪ De nombreux appareils IoT ne seront jamais réparés

Le déploiement de mises à jour logicielles qui corrigent les vulnérabilités de sécurité critiques est difficile en général, mais les dispositifs IoT posent des défis uniques. Tout d'abord, de nombreux vendeurs et fabricants de dispositifs ne disposent pas de systèmes ou de processus permettant de déployer des mises à jour logicielles sur des milliers de dispositifs (ou plus). Deuxièmement, il est difficile de déployer des mises à jour via le réseau sur des appareils qui fonctionnent dans les foyers des consommateurs, car les mises à jour peuvent parfois interrompre le service et avoir le potentiel de "briquer" l'appareil, si elles ne sont pas effectuées correctement. En outre, certains appareils peuvent même ne pas être en mesure d'effectuer des mises à jour logicielles [83].

Trois approches de mise à jour logicielle ont vu le jour dans le secteur de l'électronique grand public. Deux d'entre elles reposent sur l'intervention de l'utilisateur (un défaut fondamental), tandis que la troisième est automatique et ne requiert aucune action de la part de l'utilisateur. L'efficacité de chacune d'entre elles varie dans la pratique. Ces approches sont les suivantes :

- **Mises à jour logicielles initiées par l'utilisateur.** Cette approche exige que l'administrateur local de l'appareil lance manuellement la vérification et l'installation de toute mise à jour logicielle de l'appareil. On trouve un exemple de ce modèle sur le marché des passerelles domestiques ou des routeurs. Pour certains de ces appareils, l'utilisateur doit télécharger une nouvelle image logicielle sur le site Web du fabricant, puis accéder à une page Web d'administration locale de l'appareil, trouver l'interface de mise à jour logicielle et télécharger un fichier. Ce processus prend non seulement beaucoup de temps, mais il peut être décourageant pour les utilisateurs non techniques ou occasionnels pour lesquels un appareil peut encore fonctionner "suffisamment bien".

- **Vérifications automatisées des mises à jour logicielles, avec l'approbation de l'utilisateur.** Ces dispositifs vérifient périodiquement la présence de nouvelles mises à jour logicielles. Lorsqu'une mise à jour est disponible, l'appareil présente à l'utilisateur une invite qui lui demande la permission de procéder à la mise à jour. Les téléviseurs intelligents et les consoles de jeux utilisent souvent cette approche. Dans ces scénarios, l'application d'une mise à jour logicielle particulière peut prendre plusieurs minutes, voire plus, c'est pourquoi l'utilisateur a la possibilité de différer l'installation.

- **Mises à jour logicielles entièrement automatisées.** Certains appareils vérifient périodiquement si un nouveau logiciel est disponible ; s'il l'est, ils le téléchargent et l'installent sans intervention de l'utilisateur [84,85]. Dans certains cas, l'appareil peut appliquer la mise à jour à un moment particulier de la journée, par exemple tard dans la nuit ou lorsqu'il n'y a pas eu d'activité relative à l'appareil pendant un certain temps, afin de minimiser les perturbations pour l'utilisateur. Malheureusement, les mises à jour logicielles automatisées peuvent également poser des problèmes à certains utilisateurs qui ont des plafonds de données (le cas échéant), et lorsque les mises à jour elles-mêmes introduisent de nouveaux bogues [51].

Les approches courantes pour les mises à jour logicielles sont soit initiées par l'utilisateur, soit approuvées par l'utilisateur, qui ont toutes deux tendance à conduire à des taux de mise à jour relativement faibles [86]. Par conséquent, des millions de passerelles domestiques appartenant au client et entretenues par lui (COAM) ne recevront probablement jamais de mise à jour logicielle. Par exemple, certains modèles de passerelles domestiques NetGear ont été livrés avec un bogue logiciel qui a provoqué l'inondation aléatoire des serveurs DNS des FAI avec des milliers de requêtes DNS par seconde, soit plusieurs millions par jour, ou un déluge de requêtes NTP vers les serveurs NTP [87,88,89,90]. Bien que ce bogue logiciel spécifique ait été signalé depuis de nombreuses années, les opérateurs de réseau continuent néanmoins à observer ces dispositifs exécutant des logiciels plus anciens et se comportant mal sur le réseau, effectuant par inadvertance des attaques DDoS en raison de bogues logiciels.

- **Les mises à jour logicielles ne se limitent pas aux bogues**

Il convient également de garder à l'esprit que les mises à jour logicielles ne sont pas simplement destinées à corriger des bogues de sécurité ou de confidentialité. Elles peuvent également être destinées à introduire de nouvelles fonctions importantes. En outre, elles peuvent être plus généralement liées aux performances et à la sécurité, comme la prise en charge ou la correction de bogues liés à l'adressage IPv6, à la validation des extensions de sécurité DNS (DNSSEC) et au contrôle des tampons TCP (par exemple, "buffer bloat") ou à la gestion active des files d'attente (AQM).

- **Les consommateurs sont peu enclins à mettre à jour le logiciel des dispositifs IoT**

Peu d'utilisateurs finaux mettent systématiquement à jour le logiciel de leur propre chef, à moins que l'interface utilisateur graphique (IUG) de l'appareil ne le leur rappelle constamment et de manière ostensible (c'est-à-dire une fenêtre contextuelle régulière sur un PC, un compteur dans une boutique d'applications mobiles, une icône d'application rebondissante, etc. D'autres travaux récents suggèrent que les utilisateurs renoncent à appliquer les mises à jour logicielles sur les appareils fixes et mobiles pour diverses raisons, allant de la perturbation de leur cycle de travail aux coûts des données associés aux mises à jour logicielles [86].

Bien qu'aucune étude approfondie sur le comportement des utilisateurs en matière de mise à jour logicielle n'ait été entreprise pour les appareils IoT, la situation est probablement pire que pour les appareils conventionnels, ou non IoT. En plus du comportement déjà risqué des utilisateurs en matière de mises à jour logicielles, de nombreux appareils IoT ne disposent pas d'une interface graphique ou d'un autre indicateur de la disponibilité ou de la nécessité d'un nouveau logiciel. De plus, la prolifération des appareils, tant en nombre qu'en diversité, fait du suivi des mises à jour logicielles une tâche difficile pour le consommateur Internet typique.

Ainsi, pour les appareils IoT, il est préférable de supposer que la plupart des utilisateurs finaux ne prendront jamais d'initiative pour mettre à jour le logiciel de l'appareil.

5.6 Le remplacement du dispositif peut être une alternative aux mises à jour logicielles

Dans certains cas, le remplacement complet d'un appareil peut être une alternative aux mises à jour logicielles. Certains dispositifs IoT peuvent être si peu coûteux que la mise à jour du logiciel peut être peu pratique ou non rentable. Par exemple, un adaptateur de charge qui coûte 0,99 $ peut avoir une fonction IoT limitée. À ce coût unitaire, la mise à jour d'un appareil peut ne pas être économique ; il peut être plus logique de recycler l'appareil et d'en acheter un autre. Toutefois, cette approche nécessite les éléments suivants pour offrir une alternative sécurisée aux mises à jour logicielles :

- Un moyen d'identifier quand une ou plusieurs vulnérabilités accumulées dans un appareil l'ont compromis au point qu'il doit être remplacé.
- Un moyen de désactiver la communication avec le dispositif une fois qu'il a été déterminé qu'il est vulnérable. Parmi les exemples de méthodes possibles, citons la désactivation à distance de l'appareil du réseau ou le blocage de l'accès à l'appareil depuis une passerelle domestique.
- Un moyen d'informer les utilisateurs que la communication avec l'appareil a été désactivée.

Même dans ces cas, bien sûr, les utilisateurs peuvent être réticents à cesser d'utiliser un dispositif tant qu'il continue à fonctionner en partie. Cependant, tant que la capacité de communication du dispositif a été désactivée, son utilisation continue ne devrait pas présenter de faille de sécurité.

6 Un rôle possible pour la technologie des réseaux domestiques

La sécurisation par défaut des appareils par les fabricants constitue une étape importante pour améliorer la sécurité et la confidentialité de l'IoT, mais elle est loin d'être suffisante. Même les appareils IoT qui ne sont pas infectés par des logiciels malveillants peuvent toujours écouter le trafic d'autres réseaux domestiques (par exemple, via des logiciels installés par le fabricant ou des logiciels tiers), compromettant ainsi la vie privée des utilisateurs. Une maison est souvent considérée comme un environnement isolé ou doté d'un pare-feu, et de multiples dispositifs IoT non liés auront généralement un accès illimité derrière ce pare-feu. En outre, comme mentionné aux sections 3.4 et 5.1, un seul dispositif non sécurisé ou compromis dans le réseau domestique peut conduire à des attaques de type "stepping-stone", de sorte que la "défense en profondeur" [91] est essentielle.

Des études et des rapports récents ont suggéré qu'à l'avenir, un appareil de réseau domestique pourrait jouer un certain rôle dans le contrôle et la gestion du trafic que les dispositifs IoT échangent entre eux et avec le reste d'Internet [92]. Les capacités possibles d'un tel appareil réseau comprennent :

- Découverte et inventaire automatiques des appareils domestiques connectés à Internet [93].
- Mécanismes permettant de présenter à l'utilisateur des informations claires sur (1) les données que l'appareil envoie au reste de l'Internet et (2) les autres appareils de la maison avec lesquels l'appareil communique, comme cela a été fait dans le passé pour les smartphones et les navigateurs [94,95].
- Des mécanismes qui fournissent à l'utilisateur des moyens simples d'empêcher ou de désactiver la communication d'un seul appareil avec d'autres appareils IoT sur le réseau domestique, ou avec des serveurs de stockage dans le cloud, *sans altérer la fonctionnalité primaire de l'appareil.* Une étude récente a pu y parvenir avec deux exemples de dispositifs IoT, une ampoule Philips Hue et un thermostat Nest [92].

La technologie de réseau visant à améliorer la sécurité et la confidentialité pourrait finalement prendre l'une des nombreuses formes suivantes. Une passerelle de réseau domestique, qu'elle soit séparée (par exemple, un concentrateur IoT ou un routeur domestique séparé) ou intégrée à l'équipement fourni par le FAI, pourrait effectuer des mesures au sein du réseau qui aident les utilisateurs à comprendre les flux de données complexes à la fois entre les dispositifs IoT dans la maison et entre ces dispositifs et les sites et services tiers à l'extérieur de la maison. En ce sens, la technologie de réseau dans la maison qui surveille le trafic des appareils peut finalement aider à améliorer la *transparence du* comportement de ces appareils IoT.

Il existe un certain conflit entre la surveillance et la gestion du trafic IoT par un hub et la sécurité de bout en bout du trafic lui-même. Il convient de noter que même si le trafic réseau vers et depuis ces dispositifs est crypté de bout en bout, certaines caractéristiques, telles que les autres dispositifs et emplacements avec lesquels un dispositif particulier communique, seront toujours évidentes à partir de ce trafic. Une normalisation permettant une classification et une protection coopératives du trafic avec un tel concentrateur IoT permettrait au dispositif d'être une partie reconnue et authentifiée de l'écosystème, fournissant à cette gestion un contrôle à grain fin disponible pour l'initiateur du trafic sur une base d'opt-in.

En plus d'aider simplement à visualiser ces flux de trafic, une telle passerelle pourrait appliquer des paramètres *par défaut raisonnables* pour améliorer la sécurité et la confidentialité des appareils IoT connectés. Par exemple, des recherches récentes suggèrent qu'un pare-feu de réseau domestique peut empêcher certains appareils d'exfiltrer des journaux et d'autres informations vers des fournisseurs de nuages tiers sans paralyser la fonctionnalité de l'appareil lui-même [92]. Une question ouverte consiste à identifier des paramètres de pare-feu par défaut raisonnables qui pourraient être installés sur une telle passerelle pour améliorer la sécurité et la confidentialité. Étant donné qu'un tel pare-feu pour réseau domestique pourrait donner lieu à une "course à l'armement" en matière de protection de la vie privée (on pourrait par exemple imaginer qu'un fabricant d'appareils ne fournisse pas de mises à jour de sécurité à un utilisateur qui bloque les capacités de suivi de l'appareil), un aspect de la certification des appareils pour les fabricants et les vendeurs pourrait finalement consister à s'assurer que les consommateurs conservent un *choix* éclairé quant à la manière dont ces appareils communiquent entre eux et avec les sites et services tiers.

Enfin, l'interaction entre les dispositifs IoT peut nécessiter une médiation plus complexe. Par exemple, si un utilisateur ne souhaite généralement pas que certains dispositifs communiquent ou interagissent entre eux, il peut y avoir des cas d'utilisation spécifiques qui permettent la communication ou l'interaction entre les dispositifs pour des tâches spécifiques.

Prenons l'exemple d'un scénario dans lequel un utilisateur souhaiterait faire varier automatiquement l'intensité des lumières lorsqu'il regarde un film à la maison. Dans ce cas, l'application pourrait impliquer une communication médiatisée entre un dispositif de diffusion en continu (par exemple, un Roku ou une Apple TV) et les prises et interrupteurs intelligents (par exemple, un interrupteur WeMo de Belkin). D'autre part, en général, un utilisateur peut ne pas vouloir que ces dispositifs interagissent, ou même qu'ils observent le trafic de chacun. Ainsi, la passerelle réseau, associée à l'interface utilisateur appropriée, peut finalement offrir de meilleures possibilités pour ce type d'interaction médiatisée complexe.

Des rapports récents suggèrent que nombre de ces objectifs sont probablement à portée de main. Par exemple, des chercheurs ont utilisé un pare-feu de réseau domestique pour empêcher un thermostat Nest d'envoyer ses journaux d'état au nuage, sans nuire à l'appareil lui-même [92]. Toutefois, comme il est peu probable que l'utilisateur type configure des règles de pare-feu, ces fonctions de pare-feu doivent être plus faciles à utiliser et, si possible, automatisées, avant d'être considérées comme pratiques.

7 Recommandations

Cette section du rapport présente les recommandations du groupe de travail technique (TWG) du BITAG. Bien que les sections précédentes de ce rapport aient abordé le potentiel de solutions à plus long terme, tournées vers l'avenir (par exemple, le rôle de la technologie des réseaux domestiques pour atténuer l'insécurité des appareils), cette section se concentre sur les recommandations que le GTCBT estime pouvoir mettre en œuvre à court terme en utilisant la technologie existante.

7.1 Les dispositifs IoT doivent utiliser les meilleures pratiques logicielles actuelles

- **Les appareils IoT doivent être livrés avec des logiciels raisonnablement récents**

  BITAG recommande que les appareils IoT soient expédiés aux clients ou aux points de vente au détail avec un logiciel raisonnablement à jour qui ne contient pas de vulnérabilités graves et connues. Toutefois, les bogues logiciels sont en quelque sorte une "réalité" et il n'est pas rare que de nouvelles vulnérabilités soient découvertes pendant que les appareils sont en rayon. Il est donc essentiel qu'un dispositif IoT dispose d'un mécanisme permettant aux appareils de recevoir des mises à jour logicielles automatiques et sécurisées (voir point suivant).

- **Les dispositifs IoT doivent disposer d'un mécanisme de mise à jour logicielle automatisée et sécurisée**

  Les bogues logiciels doivent être réduits au minimum, mais, comme indiqué ci-dessus, ils sont inévitables. Il est donc essentiel qu'un dispositif IoT dispose d'un mécanisme de mise à jour logicielle automatique et sécurisée, comme indiqué à la section 5.5.

  BITAG recommande que les fabricants d'appareils IoT ou les fournisseurs de services IoT conçoivent donc leurs appareils et systèmes en partant du principe que de nouveaux bogues et vulnérabilités seront découverts au fil du temps. Ils devraient concevoir des systèmes et des processus pour assurer la mise à jour automatique des logiciels des appareils IoT, sans exiger ou attendre un quelconque type d'action de la part de l'utilisateur, ni même d'opt-in de sa part.

  Bien que ces mises à jour doivent être automatiques et obligatoires pour les utilisateurs finaux, si, pour une raison quelconque, le système de mise à jour doit permettre de choisir entre l'option "opt-out" et l'option "opt-in", alors, sur la base d'études sur l'interaction homme-machine, un tel système devrait être "opt-out" de sorte que les mises à jour se produisent automatiquement par défaut et sans aucune intervention de l'utilisateur, approbation de l'utilisateur ou autre action de l'utilisateur final. La possibilité pour un utilisateur de configurer la nature des mises à jour logicielles peut être importante pour certains utilisateurs finaux, comme ceux qui utilisent des appareils dans des environnements où les ressources sont limitées (par exemple, connexions par satellite ou autres endroits où les coûts des données sont élevés).

  Dans certains cas, les dispositifs de réseau domestique pourraient interagir avec les consommateurs pour émettre des alertes périodiques afin de faciliter la prise de décision en connaissance de cause (par exemple, en posant à l'utilisateur des questions qu'il peut comprendre sur la manière dont il souhaite que les dispositifs interagissent). L'intégration de ce type de fonction exige un soin extrême dans la conception, afin de garantir que ces alertes à l'utilisateur sont significatives et que le volume des mises à jour n'est pas écrasant. Ce type de fonctionnalité peut être compliqué à mettre en œuvre de manière fiable.

- **Les appareils IoT devraient utiliser une authentification forte par défaut**

  BITAG recommande que les dispositifs IoT soient sécurisés par défaut (par exemple, protégés par un mot de passe) et n'utilisent pas de noms d'utilisateur et de mots de passe courants ou facilement devinables (par exemple, "admin", "password"). Enfin, l'authentification pour l'accès à distance doit être sécurisée, car elle permet potentiellement à d'autres personnes qui ne sont pas physiquement présentes dans la maison de surveiller et de contrôler des aspects au sein de la maison (par exemple, modifier les commandes de climatisation, surveiller l'activité des utilisateurs).
  Les informations d'authentification doivent être uniques pour chaque appareil.

  Les méthodes d'authentification par défaut qui répondent à ces critères sont les suivantes :

(1) l'expédition de chaque appareil avec un mot de passe fixe par défaut, mais en demandant à l'utilisateur de le changer dans le cadre du processus d'installation (c'est-à-dire avant que l'appareil ne fonctionne) ; et (2) l'expédition de chaque appareil avec un mot de passe unique pour chaque unité et l'impression du mot de passe sur une étiquette qui est apposée sur l'appareil.

- **Les configurations des dispositifs IoT doivent être testées et renforcées.**

Certains appareils IoT permettent à un utilisateur de personnaliser le comportement de l'appareil. BITAG recommande aux fabricants de tester la sécurité de chaque appareil avec une gamme de configurations possibles, par opposition à la simple configuration par défaut. L'interface d'un appareil devrait empêcher - ou du moins décourager activement - les utilisateurs de configurer l'appareil d'une manière qui le rendrait moins sûr.

7.2 Les dispositifs IoT doivent respecter les meilleures pratiques en matière de sécurité et de cryptographie

BITAG recommande aux fabricants de dispositifs IoT de sécuriser les communications en utilisant la sécurité de la couche de transport (TLS) ou la cryptographie légère (LWC) [96,97,98]. Certains appareils peuvent effectuer un chiffrement à clé symétrique en temps quasi réel. En outre, la cryptographie légère (LWC) offre des options supplémentaires pour sécuriser le trafic à destination et en provenance de dispositifs aux ressources limitées. Si les dispositifs s'appuient sur une infrastructure à clé publique (PKI), une entité autorisée doit pouvoir révoquer les certificats lorsqu'ils sont compromis, comme le font les navigateurs Web et les systèmes d'exploitation des PC [99,100,101,102,103,104,105]. Les services en nuage peuvent renforcer l'intégrité des certificats émis par les autorités de certification en participant, par exemple, au programme Certificate Transparency [106]. Enfin, les fabricants doivent veiller à éviter les méthodes de cryptage, les protocoles et les tailles de clé présentant des faiblesses connues.

Les fournisseurs qui s'appuient sur une prise en charge hébergée dans le cloud pour les dispositifs IoT doivent configurer leurs serveurs pour suivre les meilleures pratiques, notamment en configurant l'implémentation TLS pour n'accepter que les dernières versions du protocole TLS.

- **Cryptage des communications de configuration (commande et contrôle) par défaut**

  Comme expliqué à la section 5.1, l'utilisation d'une communication non authentifiée ou en clair pour la gestion d'un dispositif présente un risque de sécurité important. BITAG recommande que toutes les communications pour la gestion des appareils se fassent par un canal authentifié et sécurisé.

- **Communications sécurisées vers et depuis les contrôleurs IoT**

  Si les dispositifs IoT utilisent un contrôleur centralisé pour faciliter la communication par Internet avec un service en nuage, BITAG recommande que ce canal de communication soit sécurisé dans les deux sens.

- **Cryptage du stockage local des données sensibles**

  BITAG recommande que toutes les données sensibles ou confidentielles (par exemple, la clé privée, la clé pré-partagée, les informations sur l'utilisateur ou l'installation) résident dans un stockage crypté.

- **Authentifier les communications, les modifications de logiciels et les demandes de données**

  BITAG recommande que les dispositifs IoT authentifient les points d'extrémité avec lesquels ils communiquent. L'authentification de la communication implique de vérifier l'identité du point d'extrémité, ce qui implique également de vérifier que le certificat utilisé par le point d'extrémité est signé par une autorité de certification à laquelle le dispositif fait confiance et qui n'a pas été révoquée.

- **Utilisez des informations d'identification uniques pour chaque appareil**

  BITAG recommande que chaque dispositif ait des informations d'identification uniques. Si un dispositif utilise la cryptographie à clé publique (par exemple, pour signer des messages, échanger une clé de session ou s'authentifier), chaque dispositif doit avoir un certificat unique et vérifiable. Si un dispositif utilise la cryptographie à clé symétrique, les paires de points d'extrémité ne devraient jamais partager la clé symétrique avec d'autres parties.

- **Utilisez des informations d'identification qui peuvent être mises à jour**

  Le BITAG recommande aux fabricants de dispositifs de prendre en charge un mécanisme sécurisé permettant de mettre à jour les informations d'identification utilisées par un dispositif. Toutefois, la mise en œuvre de cette recommandation de manière sécurisée nécessite une attention particulière, car une mise en œuvre incorrecte peut elle-même introduire un nouveau vecteur d'attaque.

- **Fermer les ports inutiles et désactiver les services inutiles**

Le BITAG recommande aux fabricants de dispositifs de fermer les ports inutiles, tels que telnet, car les ports inutiles peuvent être non sécurisés ou peuvent être compromis d'une autre manière [107]. Les dispositifs doivent fermer ou désactiver les interfaces et fonctions administratives qui ne sont pas utilisées. Ils ne doivent pas non plus être livrés avec des pilotes qu'ils n'utilisent pas.

- **Utilisez des bibliothèques qui sont activement entretenues et soutenues.**

  Bon nombre des recommandations formulées dans ce rapport exigent la mise en œuvre de canaux de communication sécurisés. Cependant, les implémentations maison des protocoles cryptographiques et des canaux de communication sécurisés peuvent elles-mêmes introduire des vulnérabilités. Le BITAG recommande aux fabricants de dispositifs, lorsqu'ils mettent en œuvre les recommandations de ce rapport, d'utiliser, dans la mesure du possible, des bibliothèques et des cadres qui bénéficient d'un soutien et d'une maintenance actifs.

7.3 Les dispositifs IoT doivent communiquer de manière restrictive plutôt que permissive.

BITAG recommande que les appareils IoT ne communiquent qu'avec des points d'extrémité de confiance. Lorsque cela est possible, les appareils ne doivent pas être joignables par défaut via des connexions entrantes. Les appareils IoT ne doivent pas s'appuyer uniquement sur le pare-feu du réseau pour restreindre la communication, car certaines communications entre appareils au sein de la maison ne traversent pas nécessairement le pare-feu.

Il convient de noter qu'une recommandation du BITAG visant à restreindre la *configuration* des communications des dispositifs IoT ne doit pas se faire au détriment d'un écosystème ouvert. Un utilisateur doit pouvoir configurer les communications entre des dispositifs IoT arbitraires, et les dispositifs qui se font confiance doivent être autorisés à communiquer. Les communications sécurisées peuvent amorcer des listes de confiance restreintes qui reflètent l'ensemble des dispositifs avec lesquels un dispositif donné s'attend à communiquer. Ces communications inter-appareils ne devraient être autorisées que par des mécanismes de confiance et des canaux de communication sécurisés.

7.4 Les dispositifs IoT devraient continuer à fonctionner si la connectivité Internet est interrompue

Le BITAG recommande qu'un dispositif IoT soit capable d'exécuter sa ou ses fonctions principales (par exemple, un interrupteur d'éclairage ou un thermostat doit continuer à fonctionner avec des commandes manuelles), même s'il n'est pas connecté à Internet. En effet, la connectivité Internet peut être interrompue pour des causes allant d'une mauvaise configuration accidentelle à une attaque intentionnelle (par exemple, une attaque par déni de service) ; la fonction du dispositif doit être robuste face à ces types de perturbations de la connectivité.

Les dispositifs IoT qui ont des implications pour la sécurité des utilisateurs devraient continuer à fonctionner en mode déconnecté pour protéger la sécurité des consommateurs. Dans ces cas, le dispositif ou le système dorsal devrait informer l'utilisateur de la panne.

Dans la mesure du possible, les fabricants d'appareils doivent faire en sorte que les utilisateurs puissent facilement désactiver ou bloquer (par exemple, à l'aide d'un pare-feu) divers trafics réseau sans entraver la fonction principale de l'appareil.

7.5 Les appareils IoT doivent continuer à fonctionner en cas de défaillance du back-end du cloud.

De nombreux services qui dépendent ou utilisent un back-end en nuage peuvent continuer à fonctionner, même dans un état dégradé ou partiellement fonctionnel, lorsque la connectivité au back-end en nuage est interrompue ou que le service lui-même tombe en panne. Par exemple, un thermostat dont les réglages peuvent être modifiés via un service en nuage devrait, dans le pire des cas, continuer à fonctionner en utilisant les derniers réglages connus ou les réglages par défaut. Une caméra de sécurité domestique hébergée dans le nuage doit être accessible depuis l'intérieur de la maison, même en cas de défaillance de la connectivité Internet.

7.6 Les dispositifs IoT doivent prendre en charge les meilleures pratiques d'adressage et de nommage

De nombreux dispositifs IoT peuvent rester déployés pendant de nombreuses années après leur installation. Par conséquent, les périphériques IoT doivent prendre en charge les meilleures pratiques relativement récentes, bien qu'actuelles, pour

l'adressage IP et l'utilisation du système de noms de domaine (DNS). La prise en charge des derniers protocoles d'adressage et de nommage garantira que ces appareils resteront fonctionnels pendant des années, qu'ils seront performants et qu'ils pourront prendre en charge d'importantes fonctionnalités de sécurité basées sur le DNS.

- **IPv6**

  BITAG recommande que les appareils IoT prennent en charge la version la plus récente du protocole Internet, IPv6.

- **DNSSEC**

  BITAG recommande que les dispositifs IoT prennent en charge l'utilisation ou la validation des extensions de sécurité DNS (DNSSEC) lorsque des noms de domaine sont utilisés. Par exemple, si un dispositif IoT communique avec un service en nuage en utilisant le domaine exemple.com, le fournisseur de nuage doit pouvoir signer le domaine et le dispositif IoT doit pouvoir valider cette signature (ou s'assurer que son résolveur DNS en amont l'a fait et l'a indiqué dans une réponse DNS).

7.7 Les dispositifs IoT devraient être livrés avec une politique de confidentialité facile à trouver et à comprendre.

BITAG recommande que les dispositifs IoT soient livrés avec une politique de confidentialité, mais cette politique doit être facile à trouver et à comprendre pour un utilisateur type.

7.8 Dévoiler les droits permettant de réduire à distance les fonctionnalités des dispositifs IoT

BITAG recommande que si la fonctionnalité d'un dispositif IoT peut être diminuée à distance par un tiers, comme par le fabricant ou le fournisseur de services IoT, cette possibilité doit être clairement indiquée à l'utilisateur au moment de l'achat.

7.9 L'industrie des dispositifs IoT devrait envisager un programme industriel de cybersécurité

BITAG recommande à l'industrie des dispositifs IoT ou à un groupe connexe d'électronique grand public d'envisager la création d'un programme soutenu par l'industrie, dans le cadre duquel une sorte de logo ou de mention "Secure IoT Device" pourrait figurer sur les emballages de vente au détail des dispositifs IoT. Un tel programme pourrait être analogue à la manière dont la Wi-Fi Alliance ou d'autres groupes valident la conformité des appareils à diverses normes et/ou meilleures pratiques.

Un ensemble de meilleures pratiques soutenues par l'industrie semble être le moyen le plus pragmatique d'équilibrer l'innovation dans l'IdO et les défis de sécurité associés à la nature fluide de la cybersécurité, et d'éviter la mentalité de liste de contrôle qui peut se produire avec les processus de certification.

7.10 La chaîne d'approvisionnement de l'IdO doit jouer son rôle dans la résolution des problèmes de sécurité et de confidentialité de l'IdO.

Dans la chaîne d'approvisionnement actuelle de l'usine au détail, il est souvent difficile de définir les rôles que chaque partie joue au fil du temps. C'est pourquoi elles sont définies ici simplement comme la "chaîne d'approvisionnement IoT". Les utilisateurs finaux des dispositifs IoT et d'autres personnes dépendent de la chaîne logistique IoT pour protéger leur sécurité et leur vie privée, et certaines ou toutes les parties de cette chaîne logistique IoT jouent un rôle essentiel tout au long du cycle de vie du produit. En plus des autres recommandations de cette section, BITAG recommande que la chaîne d'approvisionnement IoT prenne les mesures suivantes :

- Les appareils doivent être dotés d'une **politique de confidentialité** claire et compréhensible, en particulier lorsqu'un appareil est vendu en même temps qu'un service continu.

- Les appareils devraient disposer d'un **mécanisme de réinitialisation** pour les appareils IoT qui efface toute la configuration à utiliser lorsqu'un consommateur retourne ou revend l'appareil. Les fabricants de dispositifs devraient également fournir un mécanisme permettant de supprimer ou de réinitialiser toutes les données que le dispositif respectif stocke dans le cloud.

- Les fabricants doivent fournir un **système de signalement des bogues** avec des mécanismes de soumission des bogues bien définis et une politique de réponse documentée.

- Les fabricants doivent protéger la **chaîne d'approvisionnement en logiciels sécurisés** afin d'éviter l'introduction de logiciels malveillants au cours du processus de fabrication ; les vendeurs

et les fabricants doivent prendre les mesures appropriées pour sécuriser leur chaîne d'approvisionnement en logiciels.

- Les fabricants doivent **assurer le soutien d'un dispositif IoT tout au long de sa durée de vie**, depuis sa conception jusqu'à sa mise hors service, en faisant preuve de transparence sur la période pendant laquelle ils prévoient d'assurer le soutien continu d'un dispositif et sur ce que le consommateur doit attendre du fonctionnement du dispositif à la fin de sa durée de vie.

- **Les** fabricants doivent fournir des **méthodes claires permettant aux consommateurs de déterminer qui ils peuvent contacter pour obtenir de l'aide** et des **méthodes permettant de contacter les consommateurs** pour diffuser des informations sur les vulnérabilités des logiciels ou d'autres problèmes.

- Les fabricants doivent **signaler la découverte et la correction des vulnérabilités logicielles** qui représentent des menaces pour la sécurité ou la vie privée des consommateurs.

- Les fabricants doivent fournir un **processus de signalement des vulnérabilités** avec un formulaire de signalement des vulnérabilités bien défini, facile à trouver et sécurisé, ainsi qu'une politique de réponse documentée. Les fabricants devraient envisager de se conformer à la norme ISO 30111 [108], une norme pour le traitement des rapports de vulnérabilité.

8 Autres groupes s'intéressant à cette question

Bien que le BITAG ait un point de vue unique sur cette question, il convient de noter que plusieurs autres groupes se concentrent également sur divers aspects de cette question. Ces groupes sont les suivants

- Alliance pour le protocole Internet pour les objets intelligents (IPSO) [109].
- Institut des ingénieurs électriciens et électroniciens (IEEE) [110]
- Instituts nationaux des normes et de la technologie (NIST) [111]
- Groupe de travail sur l'ingénierie Internet [112]
    - LWIG (Light-Weight Implementation Guidance) [113] (en anglais)
    - 6Lo (IPv6 sur les réseaux de nœuds soumis à des contraintes de ressources) [114].
    - 6TiSCH (IPv6 sur le mode TSCH de l'IEEE 802.15.4e) [115].
    - ROLL (Routing Over Low power and Lossy networks) [116] (Routage sur les réseaux à faible puissance et à pertes)
    - CoRE (Constrained RESTful Environments) [117] (en anglais)
    - DICE (DTLS in Constrained Environments) [118] (en anglais)
    - ACE (Authentification et autorisation pour les environnements contraints) [119].
    - COSE (CBOR Object Signing and Encryption) [120] (en anglais)
    - 6lowpan IPv6 sur WPAN à faible puissance (fermé) [121] (en anglais)
- GSMA : La vie connectée [122]
- IRTF : Internet Research Task Force [123] (en anglais)
    - T2TRG : Thing-to-Thing Research Group (Groupe de recherche sur les relations entre les choses) [124]
- W3C : Worldwide Web Consortium [125]
    - WoT : Groupe d'intérêt sur le Web des objets [126]
- Commission fédérale du commerce (FTC) des États-Unis [127,128,129].
- Département du commerce des États-Unis, Administration nationale des télécommunications et de l'information (NTIA) [130, 131].
- Forum sur la gouvernance de l'Internet (FGI) [132]
- Online Trust Alliance [133]
- Comité technique mixte 1 de l'Organisation internationale de normalisation (ISO/CEI JTC1) [134] : A créé deux groupes de travail spéciaux sur la gestion et l'Internet des objets ; l'un est administré par l'ANSI.
    - Commission électrotechnique internationale [135] : Bien que la CEI ne se limite pas uniquement aux dispositifs IoT (et travaille sur toutes les technologies électriques/électroniques), elle a réalisé plusieurs documents de recherche sur l'IoT qui peuvent contenir des normes.
- InterNational Committee for Information Technology Standards (INCITS) [136] : Accrédité par l'ANSI, pour "servir de groupe consultatif technique américain central pour un effort mondial".

- Groupe de travail multipartite TRUSTe sur la protection de la vie privée dans l'IdO [137] : Vise à élaborer des normes techniques pour aider les entreprises à développer les solutions nécessaires à la protection de la vie privée des consommateurs dans l'IoT.
- Institut des ingénieurs en électricité et en électronique (IEEE) P2413 [138] : Un projet de l'IEEE concernant une norme pour un cadre architectural pour l'IoT.
- Wireless IoT Forum [139] : "N'est pas un organisme de normalisation, mais vise à fournir des exigences... aux organismes de normalisation lorsqu'il y a un manque de normes (par exemple, la connectivité sans fil à longue portée), et à favoriser le consensus lorsqu'il y a des normes concurrentes (par exemple, la découverte des appareils domestiques)."
    - Groupe "Applications" : groupe de travail qui examine les API standard.
    - Groupe Connectivité : groupe de travail évaluant l'accès radio.
    - Groupe réglementaire : groupe de travail chargé d'harmoniser les réglementations mondiales en matière d'exemption de licence et la disponibilité du spectre sous licence.
- Open Connectivity Foundation (anciennement appelée Open Interconnect Consortium) [140] : Organisation créée par Intel, Cisco et Samsung pour créer une spécification interopérable ouverte pour l'IdO. A également acquis le Forum UPnP.
- Object Management Group (OMG) [141] : Consortium international de normes technologiques à but non lucratif, effectuant un travail important sur l'IdO industriel.
    - Consortium de l'Internet industriel [142] : "... est le consortium international à but non lucratif et à adhésion ouverte... qui définit le cadre architectural et l'orientation de l'Internet industriel." Travaille à l'accélération de l'adoption des technologies WAN sans fil dédiées au marché de l'IoT. Fondé par CISCO, il comprend Accenture, Arkessa, BT Telensa et WSN.
- oneM2M [143] : Élaboration de spécifications techniques répondant au besoin d'une couche de service M2M commune pouvant être intégrée à divers matériels et logiciels.
- Société internationale d'automatisation (ISA) [144] : "Association professionnelle à but non lucratif qui établit des normes pour ceux qui appliquent l'ingénierie et la technologie pour améliorer la gestion, la sécurité et la cybersécurité des systèmes modernes d'automatisation et de contrôle." A effectué quelques recherches sur l'IdO, mais rien n'indique l'existence d'un groupe de travail.
- OASIS [145] : "Consortium à but non lucratif qui conduit le développement, la convergence et l'adoption de normes ouvertes pour la société de l'information mondiale."
    - OASIS Advanced Message Queuing Protocol (AMQP) TC : Définition d'un protocole Internet omniprésent, sécurisé, fiable et ouvert pour la gestion de la messagerie d'entreprise.
    - OASIS Message Queuing Telemetry Transport (MQTT) TC : Fournit un protocole de transport de messagerie fiable, léger, de type publication/abonnement, adapté à la communication dans des contextes M2M/IoT où une petite empreinte de code est requise et/ou la bande passante du réseau est limitée.
    - OASIS Open Building Information Exchange (oBIX) TC : Permettre aux systèmes de contrôle mécanique et électrique des bâtiments de communiquer avec les applications d'entreprise.
- Hypercat [146] : Un consortium et une norme conduisant à un IoT sécurisé et interopérable pour l'industrie et les villes.
- Alliance AllSeen [147] : A créé AllJoyn, qui est un "écosystème ouvert et collaboratif".

- Thread Group [148] : A créé le protocole Thread, qui est un protocole de mise en réseau libre de droits pour l'Internet des objets. Offre une certification des produits.

9 Références

1] James Manika et al., L'Internet des objets : Mapping the Value Beyond the Hype, McKinsey Global Institute, juin 2015, http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the- physical-world.

[2] Brian Krebs, "IoT Reality : Smart devices, Dumb defaults ", Krebs on Security, Blog, 8 février 2016, http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/.

[3] Kalev Leetaru, " How the Internet of Things will Turn your Living Room into The Future Cyber Battleground ", 6 nov. 2015, Forbes.com, http://www.forbes.com/sites/kalevleetaru/2015/11/06/how-the-internet-of-things-will-turn-your-living-room-into-the- future-cyber-battleground/ (dernière visite le 18 nov. 2016).

[4] IEEE Standards Association, IEEE 802.15 : Wireless Personal Area Networks (PANs), https://standards.ieee.org/about/get/802/802.15.html (dernière visite le 18 novembre 2016).

[5] X10, https://www.x10.com/ (dernière visite le 18 novembre 2016).

[6] Hewlett Packard, Étude de recherche sur l'Internet des objets : rapport 2015, HP Enterprise, 2015, *disponible à l'adresse suivante* . https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[7] John Pescatore, Securing the Internet of Things Survey, Sans Institute Analyst Survey, janvier 2014, *disponible à l'adresse suivante* . https://www.sans.org/reading-room/whitepapers/analyst/securing-internet-things-survey-34785.

[8] Charlie Osborne, " Internet of Things devices lack fundamental security, study finds ", 8 avril 2015, ZDNet, http://www.zdnet.com/article/internet-of-things-devices-lack-fundamental-security-study-finds/ (dernière visite le 18 novembre 2016).

[9] Ka-Ping Yee, "Aligning security and usability". IEEE Security & Privacy 2.5 (2004) : 48-55, *disponible sur* http://zesty.ca/pubs/yee-sid- ieeesp2004.pdf.

[10] Veracode, L'Internet des objets : Security Research Study, Whitepaper, 2014, *disponible à l'adresse suivante* . https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf

[11] Rebecca E. Grinter, et al, "The work to make a home network work". *ECSCW 2005*. Springer Netherlands, 2005, *disponible à l'adresse* http://www.cc.gatech.edu/~beki/c27.pdf.

[12] Yin Min Pa Pa, et al. "IoTPOT : Analysing the Rise of IoT Compromises". (2015), *disponible à l'adresse* https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

[13] Symantec, " IoT devices being increasingly used for DDoS attacks ", Symantec Security Response, 22 septembre 2016, *disponible sur :* http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks.

[14] Steve Rogerson, " IoT blamed for denial of service attacks ", IoT MTM Council, 29 avril 2015, *disponible sur* . http://www.iotm2mcouncil.org/serviceattacks.

[15] Energin Janina, " Distributed denial-of-service (DDoS attack) knocked the file-sharing site Pirate Bay offline ", 17 mai 2012, ceoworld.biz, http://ceoworld.biz/ceo/2012/05/17/distributed-denial-of-service-ddos-attack-knocked-the-file-sharing-site-pirate-bay- offline.

[16] Angela Moscaritolo, "FBI arrests six in click-fraud cyber scam that netted $14M", SC Magazine, 9 novembre 2011, http://www.scmagazine.com/fbi-arrests-six-in-click-fraud-cyber-scam-that-netted-14m/article/216399/.

[17] Sarthak Grover et Nick Feamster, The Internet of Unpatched Things, PrivacyCon 2016, https://www.ftc.gov/system/files/documents/public_comments/2015/10/00071-98118.pdf.

[18] Bruce Schneier, "The Internet of Things Is Wildly Insecure - And Often Unpatchable", Wired, 6 janvier 2014, https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html.

[19] Bruce Schneier, " Surveillance et Internet des objets ", Blog, 21 mai 2013, https://www.schneier.com/blog/archives/2013/05/the_eyes_and_ea.html.

[20] Matt Loeb, " Internet of Things Security Issues Require a Rethink on Risk Management ", Wall Street Journal, 14 octobre 2015, http://blogs.wsj.com/cio/2015/10/14/internet-of-things-security-issues-require-a-rethink-on-risk-management/.

[21] Arik Hesseldahl, " A Hacker's-Eye View of the Internet of Things ", Recode.net, 7 avril 2015, http://recode.net/2015/04/07/a- hackers-eye-view-of-the-internet-of-things/.

[22] Arik Hesseldahl, " L'Internet des objets est le nouveau terrain de jeu des hackers ", Recode.net, 29 juillet 2014, http://recode.net/2014/07/29/the-internet-of-things-is-the-hackers-new-playground/.

[23] Julie Knudson, " Security Challenges of the Internet of Things : L'absence de protocoles normalisés et les nouveaux flux de trafic de l'IoT compliquent les efforts de sécurité des administrateurs ", Enterprise Networking Planet, 13 mai 2015, http://www.enterprisenetworkingplanet.com/netsecur/security-challenges-of-the-internet-of-things.html.

[24] Reddit, Liste de discussion sur la vie privée, " J'ai acheté et retourné un ensemble de caméras de sécurité domestiques connectées en WiFi, j'ai oublié de supprimer mon compte et je peux maintenant surveiller le nouveau propriétaire ", https://www.reddit.com/r/privacy/comments/4ortwb/i_bought_and_returned_a_set_of_wifi_connected/ (dernière visite le 18 novembre 2016).

[25] Christina Cardoza, "Des pneus Princeton pour savoir si vos appareils IoT sont sûrs", SD Times, 22 janvier 2016, *disponible à l'adresse suivante* .
http://sdtimes.com/princeton-tries-to-find-out-are-your-iot-devices-safe/.

[26] Christian Dancke Tuen, "Security in Internet of Things Systems", thèse de maîtrise, Université norvégienne des sciences et de la technologie, département de télématique, juin 2015, *disponible sur* https://brage.bibsys.no/xmlui/bitstream/handle/11250/2352738/12892_FULLTEXT.pdf?sequence=1&isAllowed=y.

[27] Hewlett Packard, Étude sur la sécurité de l'Internet des objets : Smartwatches, IoT Research Series 2014,
http://go.saas.hpe.com/l/28912/2015-07-20/325lbm/28912/69038/IoT_Research_Series_Smartwatches.pdf.

[28] Kim Zetter, " Hospital Networks are Leaking Data, Leaving Critical Devices Vulnerable ", 25 juin 2014,
https://www.wired.com/2014/06/hospital-networks-leaking-data/.

[29] Mario Ballano Barcena et Candid Wueest, Insecurity in the Internet of Things, 12 mars 2015, Symantec,
https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-things-ds.pdf.

[30] Katie Natopoulos, "Somebody's watching : how a simple exploit lets strangers tap into private security cameras", 3 février 2012, The Verge,
http://www.theverge.com/2012/2/3/2767453/trendnet-ip-camera-exploit-4chan.

[31] Brian Krebs, "This is Why People Fear the Internet of Things", 8 février 2016, Krebs on Security,
https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/.

[32] Brady Dale, " Huit échecs de sécurité de l'Internet des objets : Changez les mots de passe de vos routeurs lorsque vous les installez, pour l'amour du ciel ", Observer, 16 juillet 2015, http://observer.com/2015/07/eight-internet-of-things-security-fails/.

[33] Michael Winter, "Calif. youth admits Miss Teen USA 'sextortion' plot", USA Today, 12 novembre 2013,
http://www.usatoday.com/story/news/nation/2013/11/12/miss-teen-usa-sextortion-guilty-plea/3510461/.

[34] Kevin Townsend, " Malware Found in IoT Cameras Sold by Amazon ", Security Week, 11 avril 2016,
http://www.securityweek.com/malware-found-iot-cameras-sold-amazon.

[35] Johannes Ullrich, "Coin Mining DVRs : A compromise from start to finish", Internet Storm Center, SANS ISC InfoSec Forums,
https://isc.sans.edu/forums/diary/Coin+Mining+DVRs+A+compromise+from+start+to+finish/18071/.

[36] Kim Zetter, " An Unprecedented Look at STUXNET, the World's First Digital Weapon ", WIRED, 3 nov. 2014,
https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[37] Swati Khandelwal, " IoT Botnet - 25 000 caméras CCTV Hacked to launch DDoS Attack ", The Hacker News, 28 juin 2016,
http://thehackernews.com/2016/06/cctv-camera-hacking.html.

[38] Dahua, Déclaration sur la cybersécurité, communiqué de presse, 1er octobre 2016, *disponible à l'adresse suivante* .
http://www.dahuasecurity.com/en/us/single.php?nid=274.

[39] Dahua, page principale de Dahua Support Wiki, http://www.dahuawiki.com/Main_Page (dernière visite le 18 novembre 2016).

[40] Dahua, Comment créer un système de sécurité plus sûr, http://www.dahuasecurity.com/en/us/best-practices.php (dernière visite le 18 novembre 2016).

[41] Broadband Internet Technical Advisory Group (BITAG), SNMP Reflected Amplification DDoS Attack Mitigation, août 2012, http://bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf.

[42] T. Dierks & E. Rescorla, "The Transport Layer Security (TLS) Protocol 1.2", RFC 5246, Aug. 2008, https://tools.ietf.org/html/rfc5246.

[43] E. Rescorla & N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, Jan. 2012,
https://tools.ietf.org/html/rfc6347.

[44] Aaron Ardiri, "Est-il possible de sécuriser les microcontrôleurs utilisés dans le cadre de l'IoT ?", EVO Things, Blogs/Tutoriels, 27 août 2014,
https://evothings.com/is-it-possible-to-secure-micro-controllers-used-within-iot/ ;

[45] Reinhard Seiler, Blog, Truecrypt benchmark for Raspberry Pi, 20 juillet 2012, http://blog.rseiler.at/2012/07/truecrypt-benchmark- for-raspberry-pi.html.

[46] Darlene Storm, " MEDJACK : les pirates détournent les dispositifs médicaux pour créer des portes dérobées dans les réseaux hospitaliers ", Computerworld, 8 juin 2015, http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create- backdoors-in-hospital-networks.html.

[47] Kim Zetter, " How Thieves Can Hack and Disable Your Home Alarm System ", WIRED, 23 juillet 2014,
https://www.wired.com/2014/07/hacking-home-alarms/.

[48] Marek Majkowski, " Say Cheese : a snapshot of the massive DDoS attacks coming from IoT cameras ", 11 octobre 2018, Cloudflare Blog, https://blog.cloudflare.com/say-cheese-a-snapshot-of-the-massive-ddos-attacks-coming-from-iot-cameras/ (dernière visite le 18 novembre 2016).

[49] Nest, " Historique des mises à jour logicielles du thermostat d'apprentissage Nest ", Nest Support, https://nest.com/support/article/Nest-Learning-Thermostat-software-update-history (dernière visite le 18 novembre 2016).

[50] Nest, " How do I update the software on my Nest Learning Thermostat ", Nest Support, https://nest.com/support/article/How-do-I- update-the-software-on-my-Nest-Learning-Thermostat (dernière visite le 18 novembre 2016).

[51] Nick Bilton, " Le thermostat Nest laisse les utilisateurs dans le froid ", 13 janvier 2016, NYTimes, *disponible sur* .
http://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html.

[52] Catalin Cimpanu, " Security Researcher with Implanted Pacemaker Sounds the Alarm on IoT Medical Devices ", Softpedia, 5 janvier 2016,
http://news.softpedia.com/news/security-researcher-with-implanted-pacemaker-sounds-the-alarm-on-iot-medical-devices- 498448.shtml.

[53] Russ Housley, Les mots du président de l'IAB : Déclaration de l'IAB sur la confidentialité de l'Internet, IETF Journal mars 2015,
https://www.internetsociety.org/publications/ietf-journal-march-2015/words-iab-chair-12.

[54] Jane Wakefield, " Smart LED light bulbs leak wi-fi passwords ", BBC News, 8 juillet 2014, http://www.bbc.com/news/technology- 28208905.

[55] SEC Consult, "House of Keys : Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide ", Blog, 25 nov. 2015, http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html (dernière visite le 18 nov. 2016).

[56] Erik C. Davis, "Clustering and Outlier Detection : Methods and Applications in Smart Home Networks", Undergraduate Dissertation, Operations Research and Financial Engineering. Université de Princeton. Juin 2016 .

[57] Yin Zhang & Vern Paxson, "Detecting Stepping Stones", USENIX *Security Symposium,* août 2000, https://www.cs.utexas.edu/~yzhang/papers/stepping-sec00.pdf.

[58] Robert Vamosi, "Covert Hacking of IoT Trivial Say Researchers", Mocana, 28 février 2014, https://www.mocana.com/blog/2014/02/28/covert-hacking-iot-trivial-say-researchers.

[59] Lorenzo Franceschi-Bicchierai, " Internet-Connected Fisher Price Teddy Bear Left Kids' Identities Exposed ", Motherboard, 2 février 2016, http://motherboard.vice.com/read/internet-connected-fisher-price-teddy-bear-left-kids-identities-exposed.

[60] Lorenzo Franceschi-Bicchierai, " Bugs in 'Hello Barbie' Could Have Let Hackers Spy on Children's Chats ", Motherboard, 4 déc. 2015, http://motherboard.vice.com/read/bugs-in-hello-barbie-could-have-let-hackers-spy-on-kids-chats.

[61] Lorenzo Franceschi-Bicchierai, "Hacked Toymaker VTech Admits Breach Actually Hit 6.3 Million Children," Motherboard, Dec. 1, 2015, http://motherboard.vice.com/read/hacked-toymaker-vtech-admits-breach-actually-hit-63-million-children.

[62] BBC, " Mitsubishi Outlander hybrid car alarm 'hacked' ", BBC News : Technology, 6 juin 2016, http://www.bbc.com/news/technology-36444586.

[63] Darlene Storm, "Nissan Leaf secretly leaks driver location, speed to websites", ComputerWorld, 14 juin 2011, http://www.computerworld.com/article/2470123/endpoint-security/nissan-leaf-secretly-leaks-driver-location--speed-to- websites.html.

[64] Leo Kelion, " Nissan Leaf electric cars vulnerability disclosed ", BBC News : Technology, 24 février 2016, http://www.bbc.com/news/technology-35642749.

[65] Colin Neagle, " Smart refrigerator hack exposes credentials ", NetworkWorld, 26 août 2015, http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

[66] Newswise, " Georgia Tech Warns of Threats to Cloud Data Storage, Mobile Devices in Latest 'Emerging Cyber Threats' Report ", communiqué de presse, 6 nov. 2013, http://www.newswise.com/articles/georgia-tech-warns-of-threats-to-cloud-data-storage-mobile-devices-in- latest-emerging-cyber-threats-report.

[67] Institute for Information Security & Privacy, Georgia Institute of Technology, Emerging Cyber Threats Report 2016, 2016, *disponible à l'adresse* http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf.

[68] Phys.Org, " Your smartwatch is giving away your ATM PIN ", 6 juillet 2016, http://phys.org/news/2016-07-smartwatch-atm-pin.html (dernière visite le 7 octobre 2016).

[69] Robert J. Ellison et al, "Evaluating and Mitigating Software Supply Chain Security Risks", Software Engineering Institute, Note technique, mai 2010, *disponible sur* http://www.sei.cmu.edu/reports/10tn016.pdf.

[70] Internet Storm Center, Survival Time : Summary, https://isc.sans.edu//survivaltime.html (dernière visite le 18 novembre 2016).

[71] Brian Krebs, " KrebsOnSecurity Hit with Record DDoS ", KrebsOnSecurity, 21 septembre 2016, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (dernière visite le 3 octobre 2016).

[72] Flashpoint, "Attack of Things !", Blog Post, 17 septembre 2016, https://www.flashpoint-intel.com/attack-of-things/ (dernière visite le 18 novembre 2016).

[73] Drew Fitzgerald, " Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks ", Wall Street Journal, 30 sept. 2016, http://www.wsj.com/articles/hackers-infect-army-of-cameras-dvrs-for-massive-internet-attacks-1475179428 (dernière visite le 3 oct. 2016).

[74] Federal Trade Commission, " ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk ", communiqué de presse, 23 février 2016, *disponible sur* https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges- insecure-home-routers-cloud-services-put.

[75] Network World, " KrebsOnSecurity moves to Project Shield for protection against DDoS attack censorship ", Ms. Smith Blog, 25 sept. 2016, http://www.networkworld.com/article/3123806/security/krebsonsecurity-moves-to-project-shield-for-protection-against-ddos- attack-censorship.html (dernière visite le 3 oct. 2016).

[76] Brian Krebs, " The Democratization of Censorship ", KrebsOnSecurity, 16 septembre 2016, https://krebsonsecurity.com/2016/09/the- democratization-of-censorship/ (dernière visite le 3 octobre 2016).

[77] Tim Greene, " Largest DDoS attack ever delivered by botnet of hijacked IoT devices ", Network World, 23 septembre 2016, http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html (dernière visite le 3 octobre 2016).

[78] Dan Goodin, " Record-breaking DDoS reportedly delivered by >145k hacked cameras ", ArsTechnica, 28 sept. 2016, http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/ (dernière visite le 3 oct. 2016).

[79] David Plonka & Elisa Boschi, L'Internet des anciens et des non gérés, 2016, *disponible sur* . https://down.dsg.cs.tcd.ie/iotsu/subs/IoTSU_2016_paper_25.pdf.

[80] David Plonka, Measurement and Analysis for the Internet of Things, 18 juillet 2016, *disponible à l'adresse suivante* . https://www.ietf.org/proceedings/96/slides/slides-96-maprg-8.pdf.

[81] Lucian Constantin, " Attackers hijack CCTV cameras to launch DDoS attacks ", Computerworld, 22 oct. 2015, http://www.computerworld.com/article/2996079/internet-of-things/attackers-hijack-cctv-cameras-to-launch-ddos-attacks.html.

[82] Kashmir Hill, "This guy's light bulb performed a DoS attack on his entire smart house", Fusion.net, 3 mars 2015, http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/.

[83] Tom Spring, " Insecurity : Pinpointing the Problems ", ThreatPost, 21 juillet 2016, https://threatpost.com/iot-insecurity-pinpointing- the-problems/119389/.

[84] DirectTV, Guide de l'utilisateur : Genie et récepteurs DVR HD antérieurs, pg. 107, http://www.directv.com/learn/pdf/System_Manuals/DIRECTV/DIRECTV_HDDVR_HR20-44.pdf.

[85] Roku, " Comment mettre à jour le logiciel de mon lecteur Roku ? ", https://support.roku.com/hc/en-us/articles/208755668-How-can-I- update-the-software-on-my-Roku-player- (dernière visite le 18 novembre 2016).

[86] Arunesh Mathur, et al. "They Keep Coming Back Like Zombies' : Improving Software Updating Interfaces", *USENIX Symposium on Usable Security and Privacy,* 2016, *disponible à l'adresse* https://www.usenix.org/system/files/conference/soups2016/soups2016-paper- mathur.pdf.

[87] David Plonka, Flawed Routers Flood University of Wisconsin Internet Time Server, 19 juillet 2006, http://pages.cs.wisc.edu/~plonka/netgear-sntp/.

[88] Comcast, " Some NetGear Routers Causing Flood of DNS Queries ", Comcast DNS News, 20 mai 2013, http://dns.xfinity.com/index.php/entry/some-netgear-routers-causing-flood-of-dns-queries.

[89] NetGear Community Discussion List, "Thousands of DNS Requests Per Second !?", 2 mars 2012, https://community.netgear.com/t5/General-WiFi-Routers/Thousands-of-DNS-Requests-Per-Second/td-p/414710.

[90] Benoit Panizzon, DDOS Attack by Netgear Products caused by CNAME instead of A record ?, [SWINOG] Discussion List, 27 juin 2013, http://lists.swinog.ch/public/swinog/2013-June/005863.html.

[91] National Security Agency, Defense in Depth, Whitepaper, 2010, *disponible sur* https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf.

[92] Vijay Sivaraman et al. " Network-Level Security and Privacy Control for Smart-Home IoT Devices ", *IEEE Wireless and Mobile Computing, Networking, and Communications.* 2015, https://www.researchgate.net/publication/281275810_Network- Level_Security_and_Privacy_Control_for_Smart-Home_IoT_Devices.

[93] Konstantinos Grivas & Stelios Zerefos, Inventaires domestiques augmentés, Conférence européenne sur l'intelligence ambiante, 2015.

[94] William Enck, et al. "TaintDroid : An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones," In Proc. of the USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 2010, *available at* http://appanalysis.org/tdroid10.pdf.

[95] Disconnect, Disconnect Privacy Tool, https://disconnect.me/ (dernière visite le 18 novembre 2016).

[96] Masanobu Katagi et Shiho Moriai, Lightweight Cryptography for the Internet of Things, 2011, https://www.iab.org/wp- content/IAB-uploads/2011/03/Kaftan.pdf.

[97] GitHub, " SSL and TLS Deployment Best Practices ", SSL Labs Wiki, https://github.com/ssllabs/research/wiki/SSL-and-TLS- Deployment-Best-Practices (dernière visite le 3 octobre 2016).

[98] Mozilla, " Security/Server Side TLS ", Mozilla Wiki, https://wiki.mozilla.org/Security/Server_Side_TLS (dernière visite le 18 novembre 2016).

[99] Dan Auerbach, " 2011 In Review : Ever-Clearer Vulnerabilities in Certificate Authority System ", Electronic Frontier Foundation, 27 décembre 2011, https://www.eff.org/deeplinks/2011/12/2011-review-ever-clearer-vulnerabilities-certificate-authority-system.

[100] Wikipedia, Liste des révocations, https://en.wikipedia.org/wiki/Revocation_list (dernière visite le 18 novembre 2016).

[101] Dennis Fisher, " Final Report on Diginator Hack Shows Total Compromise of CA Servers ", ThreatPost, 31 oct. 2012, https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/.

[102] Eric Mill, " Certificate Authorities are actually a Tremendous Problem ", Blog Post, 21 juin 2013, https://konklone.com/post/certificate-authorities-are-actually-a-tremendous-problem (dernière visite le 18 novembre 2016).

[103] Chester Wisniewski, " Another certificate authority issues dangerous certificates, Naked Security ", 3 nov. 2011, https://nakedsecurity.sophos.com/2011/11/03/another-certificate-authority-issues-dangerous-certficates/ (dernière visite le 18 nov. 2016).

[104] Glenn Fleishman, "The Huge Web Security Loophole That Most People Don't Know About, And How It's Being Fixed", FastCompany, *disponible sur* http://www.fastcompany.com/3042030/tech-forecast/the-huge-web-security-loophole-that-most-people-dont-know- about-and-how-its-be.

[105] Steve Roosa, " The Flawed Legal Architecture of the Certificate Authority Trust Model ", Freedom to Tinker, 15 déc. 2010, https://freedom-to-tinker.com/blog/sroosa/flawed-legal-architecture-certificate-authority-trust-model/ (dernière visite le 18 nov. 2016).

[106] Google, Certificate Transparency Project, What is Certificate Transparency, https://www.certificate-transparency.org/what-is-ct (dernière visite le 18 novembre 2016).

[107] Level 3 Threat Research Labs, "Attack of Things !", Level 3 Blog, http://blog.level3.com/security/attack-of-things/ (dernière visite le 18 novembre 2016).

[108] Organisation internationale de normalisation, ISO/IEC 30111:2013 : Technologies de l'information - Techniques de sécurité - Processus de traitement des vulnérabilités, 2013, *disponible sur* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231.

[109] IPSO Alliance, http://www.ipso-alliance.org (dernière visite le 18 novembre 2016).

[110] Institute of Electrical and Electronics Engineers (IEEE), https://www.ieee.org (dernière visite le 18 novembre 2016).

[111] Département du commerce des États-Unis, Institut national des normes et de la technologie, http://nist.gov (dernière visite le 18 novembre 2016).

[112] Internet Engineering Task Force (IETF), http://www.ietf.org (dernière visite le 18 novembre 2016).

[113] Internet Engineering Task Force (IETF), Light-Weight Implementation Guideance (lwig) https://datatracker.ietf.org/wg/lwig/ (dernière visite le 18 novembre 2016).

[114] Internet Engineering Task Force (IETF), IPv6 Over Networks of Resource-Constrained Nodes (6lo), https://datatracker.ietf.org/wg/6lo/ (dernière visite le 18 novembre 2016).

[115] Internet Engineering Task Force (IETF), IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch), https://datatracker.ietf.org/wg/6tisch/ (dernière visite le 18 novembre 2016).

[116] Internet Engineering Task Force (IETF), Routing over Low power and Lossy networks (roll), https://datatracker.ietf.org/wg/roll/ (dernière visite le 18 novembre 2016).

[117] Internet Engineering Task Force (IETF), Constrained RESTful environments (core), https://datatracker.ietf.org/wg/core/ (dernière visite le 18 novembre 2016).

[118] Internet Engineering Task Force (IETF), DTLS in Constrained Environments (dés), https://datatracker.ietf.org/wg/dice (dernière visite le 18 novembre 2016).

[119] Internet Engineering Task Force (IETF), Authentification et autorisation pour les environnements contraints (ace), https://datatracker.ietf.org/wg/ace/(dernière visite le 18 novembre 2016).

[120] Internet Engineering Task Force (IETF), CBOR Object Signing and Encryption (cose) https://datatracker.ietf.org/wg/cose/ (dernière visite le 18 novembre 2016).

[121] Internet Engineering Task Force (IETF), IPv6 over Low power WPAN (6lowpan), https://datatracker.ietf.org/wg/6lowpan (dernière visite le 18 novembre 2016).

[122] Groupe Speciale Mobile Association (GSMA), GSMA IoT Security Guidelines, http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/ (dernière visite le 18 novembre 2016).

[123] Internet Research Task Force, http://irtf.org (dernière visite le 18 novembre 2016).

[124] Internet Research Task Force, Thing-to-Thing Research Group, https://irtf.org/t2trg (dernière visite le 18 novembre 2016).

[125] World Wide Web Consortium (W3C), http://www.w3c.org (dernière visite le 18 novembre 2016).

[126] World Wide Web Consortium (W3C), groupe d'intérêt sur le Web des objets, https://www.w3.org/WoT/IG/ (dernière visite le 18 novembre 2016).

[127] Federal Trade Commission, Bureau of Consumer Protection et Office of Policy Planning, In The Matter of The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancemenet of the Internet of Things, Docket No. 160331306-6306-01, Comments of Staff, https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection- office-policy-planning-national-telecommunications/160603ntiacomment.pdf.

[128] Commission fédérale du commerce, Internet of Things : Privacy & Security in a Connected World, Staff Report, janvier 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled- internet-things-privacy/150127iotrpt.pdf.

[129] Dennis Fisher, FTC Warns of Security and Privacy Risks in IoT Devices, 3 juin 2016, https://www.onthewire.io/ftc-warns-of- security-and-privacy-risks-in-iot-devices/ (dernière visite le 18 novembre 2016).

[130] National Telecommunications & Information Administration, Internet of Things, https://www.ntia.doc.gov/category/internet- things (dernière visite le 18 novembre 2016).

[131] L'administration nationale des télécommunications et de l'information, le ministère américain du commerce, recherche Comment on Potential Policy Issues Related to Internet of Things, Communiqué de presse, 5 avril 2016, https://www.ntia.doc.gov/press- release/2016/us-department-commerce-seeks-comment-potential-policy-issues-related-internet-thi.

[132] Forum sur la gouvernance de l'Internet, Coalition dynamique sur l'Internet des objets, https://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/827-dciot-2015-output-document- 1/file.

[133] Online Trust Alliance, Internet of Things, 19 septembre 2016, https://otalliance.org/initiatives/internet-things (dernière visite le 18 novembre 2016).

[134] Organisation internationale de normalisation (ISO), Comité technique mixte ISO/CEI sur les technologies de l'information, http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?c ommid=45020 (dernière visite le 18 novembre 2016).

[135] Commission électrotechnique internationale (CEI), http://www.iec.ch/ (dernière visite le 18 novembre 2016).

[136] Comité international pour les normes de technologie de l'information, http://www.incits.org/ (dernière visite le 18 novembre 2016).

[137] TRUSTe, Privacy Risk Summit 2016, 8 juin 2016, http://www.truste.com/events/privacy-risk/.

[138] Institute of Electronic and Electrical Engineers (IEEE), P2413 - Standard for an Architectural Framework for the Internet of Things (IoT), https://standards.ieee.org/develop/project/2413.html (dernière visite le 18 novembre 2016).

[139] Wireless IoT Forum, http://www.wireless-iot.org/ (dernière visite le 18 novembre 2016).

[140] Open Connectivity Foundation, https://openconnectivity.org/ (dernière visite le 18 novembre 2016).

[141] Object Management Group, http://www.omg.org/ (dernière visite le 18 novembre 2016).

[142] Industrial Internet Consortium, http://www.iiconsortium.org/ (dernière visite le 18 novembre 2016).

[143] oneM2M, http://www.onem2m.org/ (dernière visite le 18 novembre 2016).

[144] Bill Lydon, "Internet of Things : Industrial automation industry exploring and implementing IoT", InTech Magazine, mars-avril 2014, *disponible à l'adresse* https://www.isa.org/standards-and-publications/isa-.
publications/intech-magazine/2014/mar-apr/cover-story-internet-of-things/.

[145] OASIS, OASIS Committee Categories:IoT/M2M, https://www.oasis-open.org/committees/tc_cat.php?cat=iot (dernière visite le 18 novembre 2016).

[146] HYPERCAT, http://www.hypercat.io/ (dernière visite le 18 novembre 2016).

[147] AllSeen Alliance, https://allseenalliance.org/ (dernière visite le 18 novembre 2016).

[148] Thread, http://threadgroup.org/ (dernière visite le 18 novembre 2016).

10 Contributeurs et réviseurs de documents

- Fred Baker, *CISCO*
- Steven Bauer, *MIT*
- Richard Bennett
- Don Bowman, *Sandvine*
- William Check, *NCTA*
- kc claffy, *UCSD/CAIDA*
- David Clark, *MIT*
- Shaun Cooley, *CISCO*
- Amogh Dhamdhere, *UCSD/CAIDA*
- Nick Feamster, *Université de Princeton*
- Francis Ferguson, *niveau 3*
- Joseph Lorenzo Hall, *Centre pour la démocratie et la technologie*
- Ken Ko, *ADTRAN*
- Jason Livingood, *Comcast*
- Patrick McManus, *Mozilla*
- Chris Morrow, *Google*
- Donald Smith, *CenturyLink*
- Barbara Stark, *AT&T*
- Darshak Thakore, *CableLabs*
- Matthew Tooley, *NCTA*
- Jason Weil, *Charter Communications*
- Greg White, *CableLabs*
- Todd Whitenack, *Cellcom*

David Winner, *Charter Communication*

Département américain de la sécurité intérieure

PRINCIPES STRATÉGIQUES POUR LA SÉCURISATION DE L'INTERNET DES CHOSES (IoT)

Version 1.0

15 novembre 2016

Homeland Security

La croissance des dispositifs, systèmes et services connectés en réseau, qui constituent l'internet des objets (IdO)[1], crée des opportunités et des avantages immenses pour notre société. Cependant, la sécurité de l'IdO n'a pas suivi le rythme rapide de l'innovation et du déploiement, créant des risques substantiels pour la sécurité et l'économie. Le présent document explique ces risques et fournit un ensemble de principes non contraignants et de meilleures pratiques suggérées afin de parvenir à un niveau de sécurité responsable pour les appareils et les systèmes que les entreprises conçoivent, fabriquent, possèdent et exploitent.

Croissance et prévalence de l'internet des objets

Les appareils connectés à l'internet permettent des connexions transparentes entre les personnes, les réseaux et les services physiques. Ces connexions permettent des gains d'efficacité, des utilisations inédites et des expériences personnalisées qui intéressent à la fois les fabricants et les consommateurs. Les appareils connectés au réseau sont déjà omniprésents, voire essentiels, dans de nombreux aspects de la vie quotidienne, qu'il s'agisse des trackers de fitness, des stimulateurs cardiaques, des voitures ou des systèmes de contrôle qui fournissent l'eau et l'électricité à nos foyers. Les promesses offertes par l'IdO sont presque illimitées.

Priorité à la sécurité de l'IdO

Si les avantages de l'IoT sont indéniables, la réalité est que la sécurité ne suit pas le rythme de l'innovation. Alors que nous intégrons de plus en plus de connexions réseau dans les infrastructures critiques de notre pays, des processus importants qui étaient autrefois exécutés manuellement (et bénéficiaient donc d'une certaine immunité contre les cyberactivités malveillantes) sont désormais vulnérables aux cybermenaces. Notre dépendance nationale croissante à l'égard des technologies connectées en réseau s'est accrue plus vite que les moyens de la sécuriser.

L'écosystème IoT présente des risques tels que la manipulation par des acteurs malveillants du flux d'informations en provenance et à destination des appareils connectés au réseau ou l'altération des appareils eux-mêmes, ce qui peut entraîner le vol de données sensibles et la perte de la vie privée des consommateurs, l'interruption des activités commerciales, le ralentissement des fonctionnalités de l'internet par des attaques par déni de service distribué à grande échelle et des perturbations potentielles des infrastructures critiques.

L'année dernière, lors d'une cyberattaque qui a temporairement mis hors service le réseau électrique de certaines régions d'Ukraine, le monde a pu constater les conséquences critiques que peuvent avoir les défaillances des systèmes connectés.
Parce que notre nation dépend désormais de réseaux fonctionnant correctement pour mener de nombreuses activités vitales, la sécurité de l'IdO est désormais une question de sécurité intérieure.

[1] Dans ce contexte, le terme IoT fait référence à la connexion de systèmes et de dispositifs à des fins essentiellement physiques (par exemple, détection, chauffage/refroidissement, éclairage, actionnement de moteurs, transport) à des réseaux

d'information (y compris l'internet) via des protocoles interopérables, souvent intégrés dans des systèmes embarqués.

Il est impératif que le gouvernement et l'industrie travaillent ensemble, rapidement, pour s'assurer que l'écosystème IoT repose sur une base digne de confiance et sécurisée. En 2014, le comité consultatif du président sur les télécommunications de sécurité nationale (NSTAC) a souligné la nécessité d'une action urgente.

> L'adoption de l'IdO va augmenter à la fois en vitesse et en portée, et [aura] un impact sur pratiquement tous les secteurs de notre société. Le défi de la nation est de s'assurer que l'adoption de l'IdO ne crée pas de risques excessifs. En outre, il existe une petite fenêtre - qui se referme rapidement - pour s'assurer que l'IdO est adopté d'une manière qui maximise la sécurité et minimise les risques. Si le pays n'y parvient pas, il devra en assumer les conséquences pendant des générations. [2]

Le moment est venu de s'attaquer à la sécurité de l'IdO. Ce document pose les jalons d'un engagement avec les secteurs public et privé sur ces questions essentielles. Il s'agit d'une première étape pour motiver et encadrer les conversations sur les mesures positives pour la sécurité de l'IdO parmi les développeurs, les fabricants et les fournisseurs de services de l'IdO, ainsi que les utilisateurs qui achètent et déploient les appareils, les services et les systèmes. Les principes et pratiques suggérés ci-dessous permettent de mettre l'accent sur la sécurité et de renforcer le cadre de confiance qui sous-tend l'écosystème IoT.

Aperçu des principes stratégiques

De nombreuses vulnérabilités de l'IdO pourraient être atténuées grâce à des pratiques exemplaires reconnues en matière de sécurité, mais trop de produits aujourd'hui n'intègrent même pas de mesures de sécurité de base. De nombreux facteurs contribuent à ce manque de sécurité. L'un d'entre eux est le fait qu'il n'est pas toujours évident de déterminer qui est responsable des décisions en matière de sécurité dans un monde où une entreprise peut concevoir un appareil, une autre fournir les composants logiciels, une autre exploiter le réseau dans lequel l'appareil est intégré, et une autre déployer l'appareil. Ce défi est amplifié par l'absence de normes et de standards internationaux complets et largement adoptés pour la sécurité de l'IdO. Parmi les autres facteurs qui contribuent à cette situation, citons le manque d'incitations pour les développeurs à sécuriser correctement les produits, puisqu'ils ne supportent pas nécessairement les coûts d'un manquement à cette obligation, et une sensibilisation inégale à la manière d'évaluer les caractéristiques de sécurité des options concurrentes.

Les principes suivants, énoncés dans la section suivante, offrent aux parties prenantes un moyen d'organiser leur réflexion sur la manière de relever ces défis en matière de sécurité de l'IdO :

Intégrer la sécurité dès la phase de conception

Mises à jour de sécurité avancées et gestion des vulnérabilités

S'appuyer sur des pratiques de sécurité éprouvées

[2] Rapport du National Security Telecommunications Advisory Committee au président sur l'Internet des objets, 19 novembre

2014.

Prioriser les mesures de sécurité en fonction de leur impact potentiel

Promouvoir la transparence dans l'IdO

Connectez-vous prudemment et délibérément

Comme pour tous les efforts de cybersécurité, l'atténuation des risques liés à l'IdO est une responsabilité partagée entre le gouvernement et le secteur privé, qui évolue constamment. Les entreprises et les consommateurs sont généralement responsables de leurs propres décisions concernant les caractéristiques de sécurité des produits qu'ils fabriquent ou achètent. Le rôle du gouvernement, en dehors de certains contextes réglementaires spécifiques et des activités d'application de la loi, est de fournir des outils et des ressources pour que les entreprises, les consommateurs et les autres parties prenantes puissent prendre des décisions éclairées sur la sécurité de l'IdO.

Portée, objectif et public cible

L'objectif de ces principes non contraignants est de fournir aux parties prenantes des suggestions de pratiques qui les aident à prendre en compte la sécurité lorsqu'elles développent, fabriquent, mettent en œuvre ou utilisent des dispositifs connectés au réseau. Plus précisément, ces principes sont destinés à :

1	Les **développeurs de l'IdO** doivent tenir compte de la sécurité lors de la conception et du développement d'un dispositif, d'un capteur, d'un service ou de tout autre composant de l'IdO ;
2	Les **fabricants d'IoT** pour améliorer la sécurité des appareils des consommateurs et des appareils gérés par les fournisseurs ;
3	les **fournisseurs de services,** qui mettent en œuvre des services par le biais de dispositifs IoT, à prendre en compte la sécurité des fonctions offertes par ces dispositifs IoT, ainsi que la sécurité sous-jacente de l'infrastructure permettant ces services ; et
4	Les **consommateurs au niveau industriel et commercial** (y compris le gouvernement fédéral et les propriétaires et exploitants d'infrastructures critiques) pour servir de leaders dans l'engagement des fabricants et des fournisseurs de services sur la sécurité des appareils IoT.

Les principes énoncés ci-dessous sont conçus pour améliorer la sécurité de l'IdO dans l'ensemble des activités de conception, de fabrication et de déploiement. L'adoption généralisée de ces principes stratégiques et des pratiques suggérées associées améliorerait considérablement la sécurité de l'IdO. Il n'existe toutefois pas de solution unique pour atténuer les risques liés à la sécurité de l'IdO. Toutes les pratiques énumérées ci-dessous ne seront pas également pertinentes pour la diversité des dispositifs IoT. Ces principes sont destinés à être adaptés et appliqués par le biais d'une approche fondée sur les risques qui tient compte des contextes commerciaux pertinents, ainsi que des menaces et conséquences particulières pouvant résulter d'incidents impliquant un dispositif, un système ou un service connecté au réseau.

Intégrer la sécurité dès la phase de conception

La sécurité doit être évaluée comme une partie intégrante composante de tout appareil connecté au réseau. Bien qu'il y ait des exceptions, dans de trop nombreux cas, des facteurs économiques ou une méconnaissance des risques poussent les entreprises à commercialiser des appareils sans se soucier de leur sécurité. Intégrer la sécurité dès la phase de conception permet de réduire les perturbations potentielles et d'éviter l'effort beaucoup plus difficile et coûteux consistant à tenter d'ajouter la sécurité aux produits après leur développement et leur déploiement. En se concentrant sur la sécurité en tant que caractéristique des appareils connectés au réseau, les fabricants et les fournisseurs de services ont également la possibilité de se différencier sur le marché. Les pratiques ci-dessous sont quelques-unes des façons les plus efficaces de prendre en compte la sécurité dès les premières phases de conception, de développement et de production.

Quels sont les effets potentiels de l'absence de sécurité lors de la conception ?

Le fait de ne pas concevoir et mettre en œuvre des mesures de sécurité adéquates pourrait être préjudiciable au fabricant en termes de coûts financiers, de coûts de réputation ou de coûts de rappel du produit. Bien qu'il n'y ait pas encore de jurisprudence établie concernant le contexte de l'IdO, on peut s'attendre à ce que les principes traditionnels de la responsabilité civile des produits s'appliquent.

PRATIQUES SUGGÉRÉES :

Activez la sécurité par défaut grâce à des noms d'utilisateur et des mots de passe par défaut uniques et difficiles à craquer. Les noms d'utilisateur et les mots de passe des dispositifs IoT fournis par le fabricant sont les suivants

souvent jamais modifiés par l'utilisateur et sont facilement craqués. Les botnets fonctionnent en recherchant en permanence des dispositifs IoT protégés par des noms d'utilisateur et des mots de passe connus par défaut. Les contrôles de sécurité forts devraient être quelque chose que le consommateur industriel doit délibérément désactiver plutôt que d'activer délibérément.

Construisez l'appareil en utilisant le **système d'exploitation le** plus **récent** qui soit techniquement viable et économiquement réalisable. De nombreux dispositifs IoT utilisent des systèmes d'exploitation Linux, mais il se peut qu'ils n'utilisent pas le système d'exploitation le plus récent. L'utilisation du système d'exploitation actuel garantit que les vulnérabilités connues auront été atténuées.

Utilisez du **matériel qui intègre des fonctions de sécurité** pour renforcer la protection et l'intégrité du dispositif. Par exemple, utilisez des puces informatiques qui intègrent la sécurité au niveau des transistors, incorporées dans le processeur, et qui assurent le cryptage et l'anonymat.

Concevoir en tenant compte des perturbations du système et du fonctionnement. Comprendre les conséquences qui pourraient découler de la défaillance d'un dispositif permettra aux développeurs, aux fabricants et aux fournisseurs de services de prendre des décisions plus éclairées en matière de sécurité en fonction des risques. Dans la mesure du possible, les développeurs doivent construire des dispositifs IoT pour qu'ils tombent en panne de manière sûre et sécurisée, afin que la panne n'entraîne pas de perturbation systémique plus importante.

Promouvoir les mises à jour de sécurité a
et la gestion des vulnérabilités

Même lorsque la sécurité est prise en compte dès la phase de conception, des vulnérabilités peuvent être découvertes dans les produits après leur déploiement. Ces failles peuvent être atténuées par des correctifs, des mises à jour de sécurité et des stratégies de gestion des vulnérabilités. Lors de la conception de ces stratégies, les développeurs doivent prendre en compte les implications d'une défaillance du dispositif, la durabilité du produit associé et le coût anticipé de la réparation. En l'absence de la possibilité de déployer des mises à jour de sécurité, les fabricants peuvent être confrontés à la décision de faire des rappels coûteux ou de laisser en circulation des dispositifs présentant des vulnérabilités connues.

FOCUS ON : NTIA Multi-Processus des parties prenantes sur les correctifs et les mises à jour

L'Administration nationale des télécommunications et de l'information (NTIA) a convoqué un processus multipartite concernant la "mise à niveau et le correctif de l'Internet des objets" afin de réunir les parties prenantes pour partager les différents points de vue sur la mise à niveau et le correctif de sécurité, et pour établir des objectifs plus concrets en vue d'une adoption à l'échelle de l'industrie.

PRATIQUES SUGGÉRÉES :

Envisagez des moyens de **sécuriser le dispositif par des connexions réseau ou par des moyens automatisés**. Idéalement, les correctifs seraient appliqués automatiquement et s'appuieraient sur des protections cryptographiques d'intégrité et d'authenticité pour remédier plus rapidement aux vulnérabilités.

Envisagez de **coordonner les mises à jour logicielles entre les fournisseurs tiers** pour remédier aux vulnérabilités et aux améliorations de la sécurité afin de garantir que les appareils des consommateurs disposent de l'ensemble complet des protections actuelles.

Développer des **mécanismes automatisés pour traiter les vulnérabilités**. Dans le domaine de l'ingénierie logicielle, par exemple, il existe des mécanismes permettant d'ingérer en temps réel des informations provenant de rapports sur les vulnérabilités critiques émanant des communautés de chercheurs et de pirates informatiques. Cela permet aux développeurs de prendre en compte ces vulnérabilités dans la conception du logiciel et de réagir le cas échéant.

Élaborer une politique concernant la **divulgation coordonnée des vulnérabilités**, y compris les pratiques de sécurité associées pour traiter les vulnérabilités identifiées. Une politique de divulgation coordonnée doit impliquer les développeurs, les fabricants et les fournisseurs de services, et inclure des informations concernant toute vulnérabilité signalée à une équipe de réponse aux incidents de sécurité informatique (CSIRT). L'US Computer Emergency Readiness Team (US-CERT), l'Industrial Control Systems (ICS)-CERT et d'autres CSIRT fournissent régulièrement des alertes techniques, y compris après des incidents majeurs, qui donnent des informations sur les vulnérabilités et les mesures d'atténuation.

S'appuyer sur des pratiques de sécurité reconnues

De nombreuses pratiques éprouvées utilisées dans la sécurité informatique et réseau traditionnelle peuvent être appliquées à l'IdO. Ces approches peuvent aider à identifier les vulnérabilités, à détecter les irrégularités, à répondre aux incidents potentiels et à se remettre des dommages ou des perturbations subis par les dispositifs IoT.

FOCUS ON : Cadre de gestion des risques de cybersécurité du NIST

Le National Institute of Standards and Technology (NIST) a publié un cadre pour la gestion des risques liés à la cybersécurité qui a été largement adopté par le secteur privé, intégré entre les secteurs et au sein des organisations. Le cadre est largement reconnu comme une pierre de touche complète pour la gestion des risques cybernétiques des organisations https://www.nist.gov/cyberframework. Bien qu'il ne soit pas spécifique à l'IdO, le cadre de gestion des risques constitue un point de départ pour l'examen des risques et des meilleures pratiques.

PRATIQUES SUGGÉRÉES :

Commencez par les **pratiques de base en matière de sécurité logicielle et de cybersécurité** et appliquez-les à l'écosystème IoT de manière flexible, adaptative et innovante.

Se référer aux **directives sectorielles** pertinentes, lorsqu'elles existent, comme point de départ pour envisager les pratiques de sécurité. Certaines agences fédérales traitent des pratiques de sécurité pour les secteurs uniques qu'elles réglementent. Par exemple, la National Highway Traffic Safety Administration (NHTSA) a récemment publié des orientations sur les meilleures pratiques en matière de cybersécurité pour les véhicules modernes, qui abordent certains des risques uniques posés par les véhicules autonomes ou semi-autonomes. De même, la Food and Drug Administration a publié un projet d'orientation sur la gestion post-commercialisation de la cybersécurité desdispositifsmédicaux.

Pratiquez la défense en profondeur. Les développeurs et les fabricants doivent adopter une approche globale de la sécurité qui comprend des défenses en couches contre les menaces de cybersécurité, y compris les outils de niveau utilisateur en tant que points d'entrée potentiels pour les acteurs malveillants. Cela est particulièrement utile si les mécanismes de correction ou de mise à jour ne sont pas disponibles ou insuffisants pour remédier à une vulnérabilité spécifique.

Participer à des **plates-formes de partage d'informations** pour signaler les vulnérabilités et recevoir en temps utile des informations essentielles sur les cybermenaces et les vulnérabilités actuelles des partenaires publics et privés. Le partage d'informations est un outil essentiel pour garantir que les parties prenantes sont au courant des menaces dès qu'elles se présentent3. Le National Cybersecurity and Communications Integration Center (NCCIC) du Department of Homeland Security (DHS), ainsi que les centres de partage et d'analyse d'informations (ISAC) et les organisations de partage et d'analyse d'informations (ISAO) multi-états et sectoriels, en sont des exemples.

[3] "Information Sharing", National Cybersecurity and Communications Information Center.

Prioriser les mesures de sécurité en fonction de leur impact potentiel

Les modèles de risque diffèrent considérablement dans l'écosystème IoT. Par exemple, les consommateurs industriels (tels que les propriétaires et exploitants de réacteurs nucléaires) auront des considérations différentes de celles d'un consommateur de détail. Les conséquences d'une défaillance de la sécurité chez les différents clients varieront également de manière significative.
Il est donc essentiel de se concentrer sur les conséquences potentielles d'une perturbation, d'une violation ou d'une activité malveillante sur l'ensemble des consommateurs afin de déterminer où il convient d'orienter les efforts de sécurité et qui est le mieux à même d'atténuer les conséquences importantes.

Les mesures de sécurité de l'IdO doivent-elles se concentrer sur le dispositif IdO ?

Étant donné que l'objectif de tous les processus IoT est de recueillir des informations à un point physique et de motiver une décision basée sur ces informations (avec parfois des conséquences physiques), les mesures de sécurité peuvent se concentrer sur une ou plusieurs parties du processus IoT. Comme indiqué précédemment, les risques liés à l'IdO commencent avec le dispositif spécifique, mais ne s'y limitent certainement pas. Les développeurs, les fabricants et les fournisseurs de services doivent prendre en compte les risques spécifiques à l'appareil IoT ainsi qu'au processus et au service, et décider, en fonction de l'impact relatif sur les trois, où les mesures les plus robustes doivent être appliquées.

PRATIQUES SUGGÉRÉES :

Connaître l'**utilisation et l'environnement prévus d'**un appareil, dans la mesure du possible. Cette prise de conscience aide les développeurs et les fabricants à prendre en compte les caractéristiques techniques de l'appareil IoT, la façon dont l'appareil peut fonctionner et les mesures de sécurité qui peuvent être nécessaires.

Effectuez un **exercice de** "**red-teaming"**, dans lequel les développeurs tentent activement de contourner les mesures de sécurité nécessaires au niveau des applications, du réseau, des données ou des couches physiques. L'analyse et la planification des mesures d'atténuation qui en résultent devraient permettre de hiérarchiser les décisions sur le lieu et la manière d'intégrer des mesures de sécurité supplémentaires.

Identifier et authentifier les dispositifs connectés au réseau, notamment pour les consommateurs industriels et les réseaux d'entreprise. L'application de mesures d'authentification pour les dispositifs et services connus permet au consommateur industriel de contrôler les dispositifs et services qui se trouvent dans son cadre organisationnel.

Promouvoir la transparence dans l'IdO

Dans la mesure du possible, les développeurs et les fabricants doivent connaître leur chaîne d'approvisionnement**,** à savoir s'il existe des vulnérabilités associées aux composants logiciels et matériels fournis par des fournisseurs extérieurs à leur organisation. La dépendance à l'égard des nombreuses solutions logicielles et matérielles peu coûteuses et facilement accessibles utilisées dans l'IdO peut rendre cette tâche difficile. Étant donné que les développeurs et les fabricants s'appuient sur des sources extérieures pour obtenir des solutions logicielles et matérielles peu coûteuses et facilement accessibles, ils peuvent ne pas être en mesure d'évaluer avec précision le niveau de sécurité intégré dans les composants lors du développement et du déploiement de dispositifs connectés au réseau. En outre, étant donné que de nombreux dispositifs IoT s'appuient sur des paquets open source, les développeurs et les fabricants ne sont souvent pas en mesure d'identifier les sources de ces composants.

Une sensibilisation accrue pourrait aider les fabricants et les consommateurs industriels à déterminer où et comment appliquer des mesures de sécurité ou intégrer des redondances. En fonction du profil de risque du produit en question, les développeurs, les fabricants et les prestataires de services seront mieux équipés pour atténuer les menaces et les vulnérabilités de manière appropriée et aussi rapidement que possible, que ce soit par l'application de correctifs, le rappel du produit ou la mise en garde des consommateurs.

PRATIQUES SUGGÉRÉES :
Effectuez des évaluations des risques de bout en bout qui tiennent compte des **risques** internes et des **risques liés aux fournisseurs tiers,** dans la mesure du possible. Les développeurs et les fabricants devraient inclure les vendeurs et les fournisseurs dans le processus d'évaluation des risques, ce qui créera de la transparence et leur permettra de prendre conscience des vulnérabilités potentielles des tiers et de promouvoir la confiance et la transparence. La sécurité doit être réévaluée en permanence à mesure que le composant de la chaîne d'approvisionnement est remplacé, retiré ou mis à niveau.
Envisagez de créer un **mécanisme divulgué publiquement pour utiliser les rapports de vulnérabilité**. Les programmes Bug Bounty, par exemple, s'appuient sur des méthodes de crowdsourcing pour identifier les vulnérabilités que les équipes de sécurité internes des entreprises ne peuvent pas toujours détecter.
Envisager le développement et l'utilisation d'une nomenclature **logicielle** pouvant être utilisée comme moyen d'instaurer une confiance partagée entre les vendeurs et les fabricants. Les développeurs et les fabricants devraient envisager de fournir une liste des composants matériels et logiciels connus dans l'emballage de l'appareil d'une manière qui tienne compte de la nécessité de protéger les questions de propriété intellectuelle. Cette liste peut être un outil précieux pour les autres acteurs de l'écosystème IoT, qui pourront ainsi comprendre et gérer leurs risques et corriger les vulnérabilités immédiatement après un incident.

Connectez-vous prudemment et délibérément

Les consommateurs d'IoT, en particulier dans le contexte industriel, doivent délibérément se demander si une connectivité continue est nécessaire compte tenu de l'utilisation du dispositif IoT et des risques associés à sa perturbation. Les consommateurs IoT peuvent également contribuer à contenir les menaces potentielles posées par la connectivité du réseau en se connectant avec précaution et de manière délibérée, et en mettant en balance les risques d'une violation ou d'une défaillance potentielle d'un dispositif IoT avec les coûts de la limitation de la connectivité à Internet.

Dans l'environnement en réseau actuel, il est probable que tout dispositif IoT donné puisse être perturbé au cours de son cycle de vie. Les développeurs, les fabricants et les consommateurs de dispositifs IoT doivent tenir compte de l'impact d'une perturbation sur la fonction principale du dispositif IoT et sur les opérations commerciales qui suivent la perturbation.

Chaque appareil en réseau doit-il être connecté en permanence et automatiquement à l'Internet ?

En 2015, la Federal Trade Commission a publié un guide intitulé "Start with Security : A Guide for Businesses" pour les aider à déterminer cette même question. S'il peut être pratique d'avoir un accès continu au réseau, cela peut ne pas être nécessaire pour l'objectif de l'appareil - et des systèmes ; par exemple, les réacteurs nucléaires, où une connexion continue à Internet ouvre la possibilité d'une intrusion aux conséquences potentiellement énormes.

PRATIQUES SUGGÉRÉES :

Informer les consommateurs d'appareils IdO de l'usage prévu de toute connexion réseau. Les connexions internet directes peuvent ne pas être nécessaires pour faire fonctionner les fonctions critiques d'un dispositif IoT, en particulier dans le cadre industriel. Les informations sur la nature et l'objectif des connexions peuvent éclairer les décisions des consommateurs.

Établissez des connexions intentionnelles. Dans certains cas, il est dans l'intérêt du consommateur de ne pas se connecter directement à l'Internet, mais plutôt à un réseau local qui peut regrouper et évaluer toute information critique. Par exemple, les systèmes de contrôle industriel (ICS) doivent être protégés par les principes de défense en profondeur publiés par https://ics- cert.us-cert.gov/recommended_practices.

Intégrer des contrôles pour permettre aux fabricants, aux fournisseurs de services et aux consommateurs de désactiver des connexions réseau ou des ports spécifiques lorsque cela est nécessaire ou souhaité pour permettre une **connectivité sélective**. En fonction de l'objectif de l'appareil IoT, fournir aux consommateurs des conseils et un contrôle sur la mise en œuvre finale peut être une bonne pratique.

CONCLUSION

Notre nation ne peut pas se permettre une génération de dispositifs IoT déployés avec peu de considération pour la sécurité. Les conséquences sont trop importantes compte tenu du potentiel de nuisance pour nos infrastructures critiques, notre vie privée et notre économie.

Au moment où le DHS publie ces principes, nous reconnaissons les efforts en cours de nos collègues des autres agences fédérales, ainsi que le travail des entités du secteur privé pour faire progresser les architectures et instituer des pratiques visant à assurer la sécurité de l'IdO. Ce document est une première étape pour renforcer ces efforts en articulant des principes de sécurité globaux. Mais d'autres étapes seront certainement nécessaires.

Le DHS identifie quatre lignes d'effort qui devraient être entreprises par le gouvernement et l'industrie pour renforcer la sécurité de l'IdO.

QUATRE LIGNES D'EFFORT :
Coordonner l'ensemble des départements et agences fédéraux pour s'engager auprès des parties prenantes de l'IdO et explorer conjointement les moyens d'atténuer les risques posés par l'IdO. Le DHS et ses partenaires fédéraux continueront à s'engager auprès des partenaires industriels pour déterminer les approches susceptibles d'améliorer la sécurité de l'IdO, et pour promouvoir la compréhension des tendances technologiques en évolution qui peuvent traiter les risques de l'IdO. Les efforts futurs porteront également sur la mise à jour et l'application de ces principes, à mesure que les meilleures pratiques et approches seront affinées et comprises.
Sensibiliser les parties prenantes aux risques liés à l'IdO. Il est important que les parties prenantes soient conscientes des risques liés à l'IdO afin qu'elles puissent se positionner pour y faire face. Le DHS va accélérer les initiatives de sensibilisation, d'éducation et de formation du public, en partenariat avec d'autres agences, le secteur privé et des partenaires internationaux. Le DHS, en collaboration avec d'autres agences, entreprendra également des initiatives plus directement adaptées à des secteurs particuliers et à des consommateurs individuels.
Identifier et faire progresser les incitations à l'intégration de la sécurité de l'IdO. Les décideurs, les législateurs et les parties prenantes doivent envisager des moyens de mieux encourager les efforts visant à renforcer la sécurité de l'IdO. Dans l'environnement actuel, il est trop souvent difficile de déterminer qui est responsable de la sécurité d'un produit ou d'un système donné. En outre, les coûts d'une sécurité insuffisante ne sont souvent pas supportés par ceux qui sont les mieux placés pour améliorer la sécurité. Le DHS et toutes les autres parties prenantes doivent examiner comment la responsabilité civile, la cyberassurance, la législation, la réglementation, la gestion de la certification volontaire, les initiatives de normalisation, les initiatives volontaires au niveau de l'industrie et d'autres mécanismes pourraient améliorer la sécurité tout en encourageant l'activité économique et l'innovation révolutionnaire. À l'avenir, le DHS se réunira avec ses partenaires pour discuter de ces questions essentielles et solliciter des idées et des commentaires.
Contribuer aux processus d'élaboration de normes internationales pour l'IdO. L'IdO fait partie d'un écosystème mondial, et d'autres pays et organisations internationales commencent à évaluer bon nombre de ces mêmes considérations de sécurité. Il est important que les activités liées à l'IdO ne se divisent pas en ensembles de normes ou de règles incohérentes. Alors que le DHS se

concentre de plus en plus sur les efforts liés à l'IdO, nous devons nous engager avec nos partenaires internationaux et le secteur privé pour soutenir le développement de normes internationales et veiller à ce qu'elles soient conformes à notre engagement à encourager l'innovation et à promouvoir la sécurité.

Le DHS se réjouit de ces prochaines étapes de collaboration. Ensemble, nous pouvons, et devons, relever ces défis complexes. Ce faisant, nous ferons en sorte que l'avenir de notre réseau connecté soit non seulement innovant, mais aussi sécurisé et construit pour durer.

EN ANNEXE : CONSEILS ET RESSOURCES SUPPLÉMENTAIRES

Les principes contenus dans ce document ont été élaborés sur la base des informations recueillies dans les rapports de l'industrie et lors de discussions avec le secteur privé, les associations professionnelles, les entités non gouvernementales et les partenaires fédéraux, notamment le NIST et le NTIA.

Département de la sécurité intérieure

- https://www.dhs.gov/sites/default/files/publications/draft-lces-security-comments-508.pdf
- https://www.dhs.gov/publication/security-tenets-lces
- https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

Autres entités fédérales

- Comité consultatif sur les télécommunications pour la sécurité nationale
    1. Rapport final du NSTAC sur l'Internet des objets

- NTIA
    1. Avis et demande de commentaires sur les avantages, les défis et les rôles potentiels du gouvernement dans la promotion de l'Internet des objets rôles potentiels du gouvernement pour favoriser l'avancement de l'Internet des objets
        a) Commentaires
    2. Livre vert - Cybersécurité, innovation et économie de l'internet, 2011
    3. De nouvelles perspectives pour l'Internet des objets émergent
    4. Remarques de la secrétaire adjointe adjointe Simpson lors de l'atelier " Fostering the Advancement " (favoriser l'avancement) de l'Internet des objets, 9/9/2016
        a) Annonce de l'atelier sur la promotion de l'Internet des objets
    5. Ressource/examen/catalogue de l'Internet Policy Task Force sur les avantages, les défis et les rôles potentiels du gouvernement pour favoriser l'avancement de l'Internet des objets.

- NIST
    1. Cadre de cybersécurité
    2. Programme Systèmes cyber-physiques (CPS)
        a) Projet de groupe de travail public (PWG) sur les systèmes cyber-physiques(CPS) Framework version 1.0
            - Commentaires acceptés jusqu'au2 septembre 2015

3. Programme Smart-Grid
4. Groupe de travail technique international sur le cadre desvilles intelligentes basées sur l'IdO (International Technical Working Group on IoT-Enabled Smart CityFramework)
5. Publication spéciale (SP) 800-183 du NIST, Réseau des objets, 28/07/2016.
    a) Communiqué de presse du NIST

- Commission fédérale du commerce
    1. Rapport du personnel de la FTC, "Internet of Things : Privacy & Security in a Connected World ", janvier 2015.

- Congrès des États-Unis
    1. Audience de la commission du Sénat sur le commerce, les sciences et les transports, "Le monde connecté : Examen de l'Internet desobjets".
    2. Résolution unanimement bipartisane du Sénat (S. Res. 110) appelant à une stratégie nationale pour guider le développement de l'Internet des objets.
    3. Commission de l'énergie et du commerce de la Chambre des représentants, "L'Internet des objets : Explorer la prochainefrontièretechnologique"
- Government Accounting Office
    1. Engagement du GAO avec le DHS : le GAO est actuellement engagé avec le DHS sur l'IdO, code 100435 [lettre de notification du 15 janvier 2016 disponible via ce lien].
        a) Statut/entrée dans la liste la plus récente, celle du 3 juin 2016, des missions actives du GAO liées auDHS.

Sources externes

La liste des ressources supplémentaires est fournie uniquement à titre de référence et ne constitue pas une approbation par le ministère de la Sécurité intérieure (DHS). Le DHS ne cautionne aucun produit, service ou entreprise commerciale.

- Conseil atlantique
    1. Les maisons intelligentes et l'internet des objets - http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things
- Je suis la cavalerie
    1. Cadre de cybersécurité automobile à cinq étoiles - https://iamthecavalry.org/5star
    2. Serment d'Hippocrate pour les dispositifs médicaux connectés - https://iamthecavalry.org/oath
- Alliance pour la confiance en ligne
    1. Meilleures pratiques pour les consommateurs

- Industrial Internet Consortium : http://www.iiconsortium.org/IISF.htm
- Projet ouvert de sécurité des applications Web (OWASP)

1. Projet Internet des objets
   https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
2. Guide de la sécurité de l'Internet des objets
   https://www.owasp.org/index.php/IoT_Security_Guidance

- Safecode.org meilleures pratiques industrielles pertinentes www.safecode.org
- AT&T
  1. Explorer la sécurité de l'IdO
- Symantec
  1. Architecture de référence de l'Internet des objets
     https://www.symantec.com/content/dam/symantec/docs/white-papers/iot- security-reference-architecture-fr.pdf