Une feuille de route

Vers une résilience contre les botnets

---

29 novembre 2018

Table des matières

Feuille de route

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 aux secrétaires du commerce et de 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) "[2.]

Les départements du commerce et de la sécurité intérieure ont travaillé conjointement à cet effort, publiant en mai 2018 le rapport sur le renforcement de la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées et distribuées, connu sous le nom de rapport sur les botnets.[3] Sur la base des contributions des parties prenantes de l'industrie et du gouvernement, le rapport a appelé le gouvernement fédéral à délimiter clairement les priorités d'action. Cette feuille de route initiale présente les actions qui pourraient réduire considérablement la menace des botnets et des attaques similaires, conformément aux priorités de l'administration telles qu'elles sont énoncées dans la stratégie nationale en matière de cybercriminalité. [La] feuille de route identifie cinq lignes d'effort, chacune avec un ensemble de tâches et de délais d'exécution. Dans cette version initiale, 85 tâches sont répertoriées, mais ce nombre évoluera au fil du temps, à mesure que certaines tâches seront achevées et que d'autres apparaîtront.

Comme expliqué dans le rapport Botnet, de nombreuses actions du rapport se soutiennent mutuellement par conception, même entre les objectifs. Certaines actions sont déjà en cours, d'autres dépendent de facteurs extérieurs, et un ensemble final attend un leadership et/ou un financement. Nous ne nous attendons pas à ce que toutes les actions se déroulent simultanément, en raison de considérations telles que les contraintes de ressources ou les différents niveaux de sophistication des communautés de parties prenantes concernées. Il convient également de noter que, bien que ces actions aient été identifiées dans le rapport sur les botnets, leur mise en œuvre rendra l'ensemble de l'écosystème Internet plus sûr et aura un impact bien au-delà des limites du rapport lui-même.

La feuille de route qui suit présente les tâches liées à chaque action dans le cadre de cinq lignes d'effort :

1. Internet des objets ;
2. Entreprise ;
3. Infrastructure Internet ;
4. Développement et transition technologique ; et
5. Sensibilisation et éducation.

Certaines tâches relèvent de la responsabilité directe du gouvernement fédéral, tandis que d'autres sont spécifiques au secteur privé. Certaines tâches 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 menées par l'industrie et dépendant du gouvernement fédéral donneront des résultats productifs.

---

[1] Exec. Order No. 13,800, 82 Fed. Reg. 22,391, à 22,394 (11 mai 2017), *disponible sur* . https://www.federalregister.gov/d/2017-10004.

[2] *Id.*

[3] U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats (mai 2018), *disponible sur* https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets.

[4] Nat'l Sec. Council, National Cyber Strategy of the United States of America (septembre 2018), *disponible sur* . https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Les départements du commerce et de la sécurité intérieure continuent d'accueillir l'intérêt des membres du secteur privé qui souhaitent contribuer à une action du rapport sur les botnets. De nombreuses actions de la feuille de route devraient être menées par l'industrie, le monde universitaire ou la société civile. Le cas échéant, cette feuille de route identifie les leaders du secteur privé ou les structures de gouvernance existants pour les tâches concernées. Lorsque des organismes existants mènent déjà des actions connexes ou représentent déjà des communautés clés, ils sont encouragés à prendre la direction des opérations. Le gouvernement a le pouvoir de convoquer et le fera, mais pour atteindre les résultats énoncés dans le rapport sur les botnets, l'industrie et la société civile devront s'engager dans l'ensemble de l'écosystème. Les tâches identifiées et les informations associées doivent être considérées comme non contraignantes et flexibles pour s'adapter aux changements de l'écosystème numérique au fil du temps.

Dans les cas où une ou plusieurs parties du secteur privé n'ont pas encore été identifiées comme chef de file, le gouvernement fédéral fournira un mécanisme de coordination et de communication. Le gouvernement fédéral rencontrera aussi périodiquement les parties concernées pour faciliter la collaboration et partager les résultats. Les organisations identifiées comme "contributeurs" dans les répartitions des tâches ci-dessous constituent une liste non exhaustive des efforts actuels qui contribuent aux solutions. Les organisations sont encouragées à rechercher des opportunités de collaboration et de partenariat dans la mesure du possible. Le gouvernement américain valorise l'innovation et attend du marché qu'il détermine les solutions les plus rapides aux problèmes identifiés.

En plus des dépendances fédérales, certaines actions ont un ordre temporel naturel. Par exemple, les programmes d'évaluation des actions 5.1 et 5.2 dépendent de l'établissement de bases de capacités de sécurité appropriées dans l'action 1.1, et ne peuvent donc pas commencer immédiatement. D'autres actions sont mûres pour une priorisation parce que le travail est déjà en cours, comme le profil du cadre de cybersécurité (CSF) du National Institute of Standards and Technology (NIST) 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 parce que les développements réduisent la possibilité pour les États-Unis d'influencer la direction (action 1.2).

Enfin, pour suivre les progrès accomplis, le ministère du Commerce (Commerce) et le ministère de la Sécurité intérieure (DHS) élaboreront une mise à jour de l'état d'avancement sur 365 jours à l'intention du président, qui devra être remise un an après la publication initiale de la feuille de route. Cette mise à jour fera le point sur 1) les progrès réalisés par l'ensemble de la communauté par rapport à la feuille de route ; 2) les impacts de ces activités de la feuille de route ; 3) une réévaluation de la menace d'attaques automatisées et distribuées, y compris si la menace augmente ou diminue, et toute raison connue d'un tel changement ; et 4) quelles activités devraient être prioritaires dans l'année à venir.

II. Carte routière

Les sous-sections suivantes présentent des tâches tirées des 24 actions énoncées dans le rapport sur les botnets dans le cadre de cinq *lignes d'effort* :

1. Internet des objets ;
2. Entreprise ;
3. Infrastructure Internet ;
4. Développement et transition technologique ; et
5. Sensibilisation et éducation.

Les cinq axes d'effort sont eux-mêmes subdivisés en *flux de travail* composés de *tâches*. Lorsque les tâches ont des dépendances, elles sont organisées en *séries*. Chaque description de tâche comprend un

un bref résumé et une référence à un numéro d'action du Botnet Report, identifie les chefs de tâches (s'ils sont déterminés) et les acteurs de soutien, identifie les tâches qui doivent être achevées avant de commencer ou de terminer, et propose des dates de début et de fin par trimestre de l'année civile**.** Le département du Commerce et le DHS accueillent les commentaires des parties prenantes sur tous les éléments des tâches de la feuille de route, en particulier l'identification des responsables et des partenaires contribuant aux actions identifiées, ainsi que les délais.

IoT Line of Effort : Relever le niveau de sécurité de l'IdO

Le rapport sur les botnets a reconnu l'impact des appareils connectés sur la capacité à étendre la portée et l'échelle des attaques automatisées et distribuées contre les cibles de l'écosystème. La ligne d'effort sur l'Internet des objets (IoT) se concentre sur la réduction des risques de sécurité dans l'écosystème IoT par l'établissement de normes de sécurité de base appliquées à l'ensemble du cycle de vie des appareils connectés.

Volet 1 de l'IdO : développer des marchés robustes pour des dispositifs IdO dignes de confiance

Ce domaine de travail se concentre sur le développement d'un marché solide pour les dispositifs offrant des capacités de sécurité appropriées pour trois secteurs : les consommateurs/utilisateurs domestiques, les utilisateurs industriels et le gouvernement fédéral. La tâche initiale fondamentale décrit un ensemble de capacités de sécurité de base qui sont largement applicables (idéalement, applicables aux trois secteurs) et qui peuvent être soutenues par un large éventail de systèmes d'évaluation. Une fois le noyau défini, des séries de tâches simultanées sont lancées pour chacun des trois secteurs. Chaque série de tâches définit un sur-ensemble du noyau de base adapté à ce secteur, suivi d'un ensemble d'activités de soutien conçues pour développer un marché solide pour les produits conformes.

Définir une base de référence des capacités de sécurité essentielles

Cette tâche établit un ensemble de capacités de sécurité de base nécessaires au déploiement sécurisé des dispositifs IoT, quel que soit l'environnement prévu. Les capacités de sécurité de base doivent être fournies ou facilitées par des plateformes de développement communes afin de limiter l'impact sur le délai de mise sur le marché et de permettre l'innovation. Ces capacités de base doivent également être appropriées pour les schémas d'évaluation de la conformité basés sur l'attestation et l'évaluation par une tierce partie.

Nom de la tâche : Définir la base de référence des capacités de sécurité essentielles

Numéro d'action : 1.1

Résumé des tâches : Comparer/analyser différents documents de référence pour identifier les "capacités de sécurité de base" largement acceptées et applicables qui pourraient être prises en charge par l'ensemble des systèmes d'évaluation. Au minimum, la base de référence des capacités porterait sur la sécurité des dispositifs et des données. Le NIST publiera la ligne de base consensuelle sous la forme d'un livre blanc du NIST ou d'un rapport interagences (NISTIR) pour référence et utilisation dans des tâches futures.

Contributeur(s) : NIST (responsable), propriétaires de la ligne de base, fournisseurs de kits de développement, consortiums de consommateurs, Council to Secure the Digital Economy (CSDE)[5]/Consumer Technology Association (CTA) Tâches préalables : N/A

Début prévu[6] : 1Q19 Achèvement prévu : 3Q19

[5] *Voir le* Conseil pour la sécurité de la Dig. Econ., *disponible sur* https://securingdigitaleconomy.org/

[6] Toutes les dates de début sont des estimations par année civile et sont sujettes à la détermination des ressources.

Établir un marché robuste pour les dispositifs IdO fiables destinés aux consommateurs et aux particuliers.

Les tâches suivantes sont conçues pour établir une base de capacités de sécurité largement adoptée pour les produits IoT domestiques/consommateurs, avec une grande disponibilité des produits et une forte reconnaissance des clients. Ces tâches commencent par compléter la base de référence des capacités de sécurité par des exigences spécifiques au marché de l'IdO domestique/consommateur. Pour encourager le développement et le déploiement de dispositifs conformes, un système d'attestation ou d'évaluation est créé, ainsi que des outils d'éducation et de sensibilisation qui aideront les clients à faire des choix éclairés en matière d'achats IoT.

Nom de la tâche : Élaboration d'une base de référence en matière de sécurité de l'IdO pour les consommateurs et les foyers

Numéro d'action : 1.1

Résumé des tâches : s'appuyer sur les capacités de base pour identifier la base de sécurité appropriée pour l'IdO des consommateurs et des foyers.

Contributeur(s) : Industrie de l'IdO, société civile, NIST, CSDE/CTA Tâches préalables : Publier la base de référence des capacités de sécurité fondamentales Début prévu : 2Q19

Achèvement prévu : 1Q20

Nom de la tâche : Établir ou soutenir des programmes d'évaluation pour les dispositifs IdO domestiques/consommateurs

Numéro d'action : 5.1

Résumé des tâches : établir ou soutenir des programmes d'évaluation ou d'attestation agiles pour les dispositifs IoT grand public/domestiques qui répondent à la ligne de base ci-dessus.

Contributeur(s) : Industrie, société civile, CTIA, NIST, autres parties prenantes du gouvernement américain (USG), CSDE/CTA

Tâches préalables : Développer une base de référence pour la sécurité de l'IdO pour les consommateurs et les foyers

Début prévu : En cours

Achèvement prévu : 2Q20

Nom de la tâche : Explorer l'étiquetage pour l'IdO domestique/consommateur

Numéro d'action : 5.1

Résumé des tâches : explorer l'utilité d'une approche d'étiquetage volontaire, ou d'autres options informationnelles, pour améliorer la sensibilisation des consommateurs/des appareils IoT domestiques.

Contributeur(s) : Commission fédérale du commerce (FTC), NTIA, autres partenaires fédéraux, industrie de l'IdO, détaillants, société civile, universités, CSDE/CTA.

Tâches préalables : N/A Début prévu : 4Q19 Achèvement prévu : 4Q20

Nom de la tâche : Mettre en œuvre des stratégies de sensibilisation aux dispositifs IdO fiables pour les consommateurs et les particuliers.

Numéro d'action : 5.1

Résumé des tâches : développer des outils d'information, tels que l'étiquetage ou le marquage, qui aident les consommateurs motivés à identifier les produits IoT domestiques et de consommation conformes.

Contributeur(s) : Industrie de l'IdO, détaillants, CSDE/CTA

Tâches préalables : Établir un programme d'évaluation pour les dispositifs IoT domestiques/consommateurs ; explorer l'étiquetage pour les dispositifs IoT domestiques/consommateurs.

Début prévu : 2Q20 Achèvement prévu : 2Q21

Nom de la tâche : Federal Support for Consumer/Home IoT Security Baseline & Assessment Numéro de l'action : 5.5

Résumé des tâches : accroître l'engagement du gouvernement américain auprès des communautés d'utilisateurs ciblées et de la société civile afin de promouvoir la sensibilisation et l'acceptation de la base de référence en matière de sécurité de l'IdO pour les consommateurs et les particuliers et du ou des programmes d'évaluation correspondants ; tirer parti des activités de sensibilisation existantes du DHS, telles que STOP.THINK.CONNECT.

Contributeur(s) : DHS, Commerce, FTC, société civile

Tâches préalables : Élaborer une base de référence en matière de sécurité de l'IdO pour les consommateurs et les foyers ; établir un programme d'évaluation des dispositifs IdO domestiques.

Début prévu : 2Q20

Achèvement prévu : 1Q23

Établir un marché robuste pour les dispositifs IoT industriels dignes de confiance

Les tâches suivantes sont conçues pour établir une base de capacités de sécurité largement adoptée pour les produits IoT industriels, avec une grande disponibilité des produits et une forte reconnaissance des clients. Ces tâches commencent par compléter la base de référence des capacités de sécurité par des exigences spécifiques au marché de l'IdO industriel. Pour encourager le développement et le déploiement de dispositifs conformes, un ou plusieurs systèmes d'évaluation sont créés, ainsi que des outils d'éducation et de sensibilisation pour informer les clients.

Nom de la tâche : Développer une base de référence pour la sécurité de l'IdO industriel
Numéro d'action : 1.1
Résumé des tâches : s'appuyer sur les capacités de base pour identifier la base de sécurité appropriée aux environnements industriels/SCADA.
Contributeur(s) : Industrie de l'IdO industriel, laboratoires nationaux, DHS, agences sectorielles, conseils de coordination sectorielle (par exemple, énergie, santé, transport).
Tâches préalables : Publier la base de référence des capacités de sécurité fondamentales Début prévu : 2Q19
Achèvement prévu : 4Q19

Nom de la tâche : Établir un programme d'évaluation des dispositifs industriels IoT
Numéro d'action : 5.2
Résumé des tâches : établir un ou des programmes d'évaluation rentables pour les dispositifs industriels IoT qui répondent aux exigences de base.
Contributeur(s) : Industrie de l'IdO industriel, laboratoires nationaux, DHS, agences sectorielles, conseils de coordination sectorielle (par exemple, énergie, santé, transport).
Tâches préalables : Développer une base de référence pour la sécurité de l'IoT industriel Début prévu : 4Q19
Achèvement prévu : 2Q20

Nom de la tâche : Explorer l'étiquetage ou un autre système de transparence pour les dispositifs industriels IoT.
Numéro d'action : 5.2
Résumé des tâches : travailler à l'élaboration d'une approche d'étiquetage volontaire, ou d'un autre schéma de transparence de l'information, comme option pour informer les clients des entreprises industrielles.
Contributeur(s) : Industrie de l'IdO industriel, laboratoires nationaux, DHS, agences sectorielles, conseils de coordination sectorielle (par exemple, énergie, santé, transport).
Tâches préalables : Développer une base de référence pour la sécurité de l'IoT industriel Début prévu : 4Q19
Achèvement prévu : 4Q20

Nom de la tâche : Soutenir la sensibilisation des clients aux dispositifs IoT industriels
Numéro d'action : 5.2
Résumé des tâches : créer des outils informationnels tels que des étiquettes ou des marques qui aident les clients des entreprises industrielles à identifier les produits IoT industriels conformes.
Contributeur(s) : Industrie de l'IdO industriel, détaillants, DHS par le biais du Conseil national des centres d'analyse et de partage de l'information (ISAC).
Tâches préalables : Développer une base de référence pour la sécurité de l'IdO
industriel Début prévu : 2Q20
Achèvement prévu : 4Q20

Nom de la tâche : Promouvoir l'adoption d'un régime d'évaluation par les infrastructures critiques
Numéro d'action : 5.2
Résumé des tâches : Par l'intermédiaire de l'ISAC Council, le DHS et l'industrie évalueront le(s) régime(s) de certification commerciale pour les produits IdO et TI au fur et à mesure de leur apparition pour l'applicabilité aux infrastructures essentielles.
Contributeur(s) : DHS (chef de file), industrie de l'IdO, laboratoires nationaux, DHS, agences sectorielles, conseils de coordination sectorielle (par exemple, énergie, santé, transport).
Tâches préalables : Établir un programme d'évaluation des dispositifs industriels IoT Début prévu :
3Q20
Achèvement prévu : 2Q21

Établir un marché robuste pour les dispositifs IdO fédéraux fiables.

Les tâches suivantes sont conçues pour établir une base de capacités de sécurité largement adoptée pour les produits IoT fédéraux, avec une grande disponibilité des produits et une forte reconnaissance des clients. Ces tâches commencent par compléter la base de référence des capacités de sécurité par des exigences spécifiques au marché IoT fédéral.
Afin d'encourager l'acquisition et le déploiement de dispositifs conformes, des règlements fédéraux sur les marchés publics sont établis et font référence à la ligne de base fédérale.

Nom de la tâche : Identifier les exigences fédérales en matière de sécurité de l'IdO
Numéro d'action : 2.3
Résumé des tâches : réunir les principales parties prenantes dans une série de réunions pour identifier les capacités de sécurité non essentielles qui sont communes/spécifiques aux environnements fédéraux.
Contributeur(s) : Office of Management and Budget (OMB), General Services Administration (GSA), Department of Defense (DOD), DHS, NIST, Federal Chief Information Officer (CIO) Council, Federal chief information security officers (CISOs)
Tâches préalables : Publier la base de référence des capacités de sécurité
fondamentales Début prévu : TBD
Achèvement prévu : TBD

Nom de la tâche : Spécifier la base de référence fédérale pour les capacités de sécurité de l'IdO
Numéro d'action : 2.3
Résumé des tâches : en collaboration avec l'industrie et les agences, élaborer et publier un référentiel fédéral de capacités de sécurité de l'IdO.
Contributeur(s) : NIST (responsable), DHS, Federal CIO Council, RSSI fédéraux, industrie, CSDE/CTA Tâches préalables : Identifier les exigences fédérales en matière de sécurité de l'IdO
Début prévu : 3Q19 Achèvement
prévu : 1Q20

Nom de la tâche : Établir une réglementation fédérale sur l'approvisionnement en IdO
Numéro d'action : 2.3
Résumé des tâches : établir des règles d'approvisionnement fédérales pour soutenir l'acquisition de dispositifs IoT conformes à la base de capacité de sécurité IoT fédérale.
Contributeur(s) : GSA (chef de file), OMB, Conseil fédéral des DPI, RSSI fédéraux et responsables des achats Tâches préalables : Définir la base de référence des capacités fédérales en matière de sécurité de l'IdO
Début prévu : TBD Achèvement prévu : TBD

Volet 2 de l'IdO : Adoption et durabilité de la sécurité de l'IdO

Ce domaine de travail se concentre sur le développement de l'écosystème mondial des dispositifs IdO en général. En d'autres termes, le portefeuille d'actions spécifié dans ce volet renforce la sécurité des produits de l'IdO et favorise la confiance dans le marché de l'IdO, indépendamment des trois bases de référence de sécurité spécifiques au secteur. Les tâches sont axées sur la collaboration entre les communautés de la cybersécurité et des technologies opérationnelles, ainsi que sur la défense des politiques internationales, l'harmonisation et les normes. À l'exception de l'élaboration de normes IdO pertinentes au niveau mondial, ces activités ont peu de dépendances. L'un des principaux défis consistera à hiérarchiser les activités en fonction des ressources disponibles.

Étendre la gestion des risques à l'IdO

De nombreux programmes de cybersécurité d'entreprise sont passés à des approches fondées sur les risques, telles que le cadre de cybersécurité du NIST. Les normes, les directives et les meilleures pratiques que ces organisations exploitent pour gérer les risques liés à la cybersécurité à l'aide du Cadre et des approches connexes se sont historiquement concentrées sur les technologies de l'information (TI) et les réseaux TI traditionnels. Dans cette série de tâches, les approches de gestion des risques sont étendues pour aider les organisations à mieux comprendre et gérer les risques de cybersécurité et de confidentialité associés à leurs dispositifs IoT tout au long de leur cycle de vie.

Nom de la tâche : Activer l'approche de gestion des risques pour la sécurité de l'IdO
Numéro d'action : 1.5
Résumé des tâches : publier la NISTIR 8228, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks", afin de soutenir les approches de gestion des risques pour la sécurité de l'IoT. Contributeur(s) : NIST (responsable), industrie
Tâches préalables : N/A Début prévu : En
cours Achèvement prévu : 1Q19

Nom de la tâche : Publier les meilleures pratiques pour les fabricants de dispositifs IoT
Numéro d'action : 1.5
Résumé des tâches : Identifier les meilleures pratiques qui contribuent aux résultats des clients identifiés dans le nouveau NISTIR 8228, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks" en utilisant les capacités de sécurité de base.
Contributeur(s) : NIST (responsable), TBD
Tâches préalables : Mettre en place une approche de gestion des risques pour la sécurité de l'IdO ; publier une base de référence des capacités de sécurité essentielles.
Début prévu : 2Q19 Achèvement prévu :
2Q20

Nom de la tâche : Commercialisation des technologies de mise à jour sécurisée

Numéro d'action : 1.5
Résumé des tâches : promouvoir les normes et les cadres commerciaux pour les mises à jour sécurisées. Encourager les kits de développement de l'IdO à intégrer des mécanismes de mise à jour sécurisée afin de réduire le temps de mise sur le marché des développeurs. Publier les spécifications de l'IETF (Internet Engineering Task Force) pour la mise à jour sécurisée des dispositifs IoT afin d'encourager la prise en charge des correctifs de sécurité dans le commerce.
Contributeur(s) : Participants à l'IETF, NIST, NTIA, autres Tâches
préalables : N/A
Début prévu : En cours Achèvement prévu :
2Q19

Nom de la tâche : Alignez la facilité d'utilisation et la facilité de gestion sur les capacités des clients.
Numéro d'action : 3.2
Résumé des tâches : donner la priorité à des processus de déploiement et de configuration simples et directs pour les dispositifs commercialisés auprès des particuliers et des petites entreprises.
Contributeur(s) : Consumer Technology Association (CTA), industrie IT et IoT Tâches préalables :
N/A
Début prévu : En cours Achèvement prévu : En
cours

Établir des normes IoT pertinentes à l'échelle mondiale

Le rapport sur les botnets indiquait que "le gouvernement et l'industrie des États-Unis devraient s'engager conjointement avec les développeurs de normes et de spécifications internationales volontaires dirigées par l'industrie afin d'établir des normes pertinentes au niveau mondial". Cette série de tâches encourage le gouvernement américain et l'industrie à rechercher conjointement des normes internationales compatibles avec les bases de capacités élaborées dans le cadre du chantier précédent.

Nom de la tâche : Établir des normes IoT pertinentes à l'échelle mondiale
Numéro d'action : 1.2
Résumé des tâches : Le gouvernement et l'industrie des États-Unis devraient, par le biais de processus de discussion inclusifs, identifier conjointement un ensemble de lieux clés pour l'élaboration de normes internationales volontaires en matière de sécurité de l'IdO et lancer une activité de normalisation. Les participants peuvent introduire la base de référence des capacités de sécurité fondamentales en tant que contribution une fois la base de référence achevée.
Contributeur(s) : NIST, NTIA, DHS, IICSWG, industrie de
l'IdO Tâches préalables : N/A
Début prévu : En cours
Achèvement prévu : 4Q19

Nom de la tâche : Identifier les mesures incitatives pour l'adoption des normes de sécurité par l'IdO
Numéro d'action : 2.3
Résumé des tâches : identifier les mesures incitatives existantes et nécessaires pour l'adoption par le secteur privé de normes et de bases de sécurité de l'IdO, qui peuvent être adoptées par le gouvernement américain.
Contributeur(s) : industrie de l'IdO, DHS, Commerce, FTC, agences sectorielles, conseils de coordination sectorielle
Tâches préalables : Établir des normes IoT pertinentes au niveau mondial Début
prévu : TBD
Achèvement prévu : TBD

Ligne d'effort de l'entreprise

La ligne d'effort Entreprise se concentre sur les actions qui peuvent être prises au niveau de la gestion de l'entreprise pour réduire le risque global pour l'entreprise et l'écosystème des botnets et des attaques automatisées et distribuées.

L'Enterprise Line of Effort comporte quatre axes de travail complémentaires :

- Profils CSF pour l'atténuation et la protection
- Migration vers des architectures de réseau d'entreprise avancées
- Adoption par le gouvernement fédéral des meilleures pratiques d'entreprise
- Technologie opérationnelle

Enterprise Workstream 1 : Profils CSF pour l'atténuation et la protection

Le cadre de cybersécurité du NIST est devenu un outil essentiel pour les entreprises et les agences qui utilisent une approche basée sur les risques pour obtenir des résultats de sécurité appropriés. Cette série de tâches établit des profils CSF consensuels de l'industrie pour atténuer les menaces de déni de service distribué (DDoS) et combattre les botnets. Une fois les profils établis par l'industrie, le gouvernement fédéral adapte ces profils à l'environnement fédéral.

Nom de la tâche : Développer un profil CSF pour l'atténuation des DDoS

Numéro d'action : 2.2
Résumé des tâches : travailler avec l'industrie pour développer un profil CSF consensuel pour l'atténuation des DDoS.
Contributeur(s) : Cybersecurity Coalition (chef de file),[7] industrie de l'écosystème numérique, NIST, NTIA, DHS, société civile.
Tâches préalables : N/A Début prévu : En
cours Achèvement prévu : 1Q19

Nom de la tâche : Publier le profil CSF fédéral pour l'atténuation des DDoS

Numéro d'action : 2.3
Résumé des tâches : publier le profil CSF fédéral pour l'atténuation des DDoS en tant que publication spéciale du NIST. Contributeur(s) : NIST (responsable), DHS, agences fédérales, parties prenantes de l'écosystème numérique, société civile Tâches préalables : Développer un profil CSF pour l'atténuation des DDoS.
Début prévu : 2Q19 Achèvement prévu :
3Q19

Nom de la tâche : Développer un profil CSF pour l'atténuation de la menace des botnets

Numéro d'action : 2.2
Résumé de la tâche : élaborer des profils CSF consensuels de l'industrie pour l'atténuation de la menace des botnets.
Contributeur(s) : Cybersecurity Coalition (chef de file), parties prenantes de l'écosystème numérique, NIST, NTIA, DHS, société civile.
Tâches préalables : N/A Début
prévu : En cours Achèvement
prévu : 2Q19

[7] *Voir* Cybersecurity Coalition, *disponible à l'adresse* https://www.cybersecuritycoalition.org/.

Nom de la tâche : Publier le profil CSF fédéral pour l'atténuation de la menace des botnets
Numéro d'action : 2.3
Résumé des tâches : publier le profil CSF fédéral pour l'atténuation des menaces de botnet en tant que publication spéciale du NIST.
Contributeur(s) : NIST (responsable), DHS, agences fédérales, parties prenantes de l'écosystème numérique, société civile Tâches préalables : Développer un profil CSF pour l'atténuation de la menace des botnets.
Début prévu : 2Q19 Achèvement prévu :
3Q19

Nom de la tâche : Sensibiliser les entreprises à l'atténuation des DDoS
Numéro d'action : 3.3
Résumé des tâches : établir des campagnes de partenariat et des activités d'engagement stratégique pour améliorer les connaissances des utilisateurs et des entreprises sur les menaces distribuées automatisées et les meilleures pratiques de sécurité.
Contributeur(s) : Cybersecurity Coalition, NTIA, DHS, NIST, société civile Tâches
préalables : N/A
Début prévu : En cours Achèvement prévu :
TBD

Axe de travail 2 : Faire progresser les architectures de réseau d'entreprise

Les entreprises doivent 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. Dans ce domaine de travail, une série d'activités simultanées identifie les meilleures pratiques actuelles et explore les technologies émergentes pour les architectures de réseau d'entreprise.

Nom de la tâche : Améliorer et faire évoluer les meilleures pratiques en matière de gestion du trafic du réseau d'entreprise.
Numéro d'action : 3.1
Résumé des tâches : améliorer et faire évoluer les politiques constructives et les meilleures pratiques en matière de gestion du trafic réseau des entreprises dans les secteurs ciblés de l'écosystème, en gardant à l'esprit les exigences des petites entreprises. Faire évoluer les meilleures pratiques à mesure que les technologies et les architectures progressent, et combler les lacunes des meilleures pratiques pour les nouveaux acteurs et les nouveaux venus.
Contributeur(s) : CSDE /CTA (chef de file), groupes de coordination de l'industrie, opérateurs de réseaux d'entreprise, groupes d'opérateurs de réseaux (NOG), ingénieurs de réseaux, NIST, NTIA, DHS, DOD, fournisseurs de services Internet, fournisseurs d'infrastructures, entreprises de l'écosystème numérique mondial, société civile
Tâches préalables : N/A.
Début prévu : En cours. Achèvement
prévu : 2Q2019

Nom de la tâche : Promouvoir des architectures de réseau d'entreprise qui atténuent les risques de menaces automatisées et distribuées.
Numéro d'action : 3.3
Résumé des tâches : promouvoir la mise en œuvre et l'adoption d'architectures de réseau d'entreprise avancées qui atténuent le risque de menaces automatisées et distribuées. Identifier où les lacunes dans l'adoption par les entreprises prolifèrent, et entreprendre des efforts pour comprendre les obstacles du marché et des politiques à l'intégration et au déploiement.
Contributeur(s) : CSDE, organismes de coordination de l'industrie, ingénieurs et opérateurs de réseaux d'entreprise, NOGs, NTIA, NIST, DHS, Committee on National Security Systems (CNSS), universités, société civile.

Tâches préalables : Améliorer et faire évoluer les meilleures pratiques en matière de gestion du trafic réseau Début prévu : 2Q2019
Achèvement prévu : TBD

Nom de la tâche : Accélérer la disponibilité nationale des services Internet IPv6
Numéro d'action : 3.4
Résumé des tâches : le gouvernement travaille avec les parties prenantes pour soutenir la transition complète vers IPv6 par les fournisseurs de services Internet (FSI) en identifiant les leçons apprises de l'industrie et d'autres pays, en identifiant à la fois les obstacles à la transition et les incitations potentielles.
Contributeur(s) : NTIA (chef de file), registres Internet régionaux (RIR), FAI, industrie informatique et IoT
Tâches préalables : N/A
Début prévu : 4Q19 Achèvement
prévu : 2Q20

Nom de la tâche : Accélérer la transition vers les réseaux d'entreprise IPv6
Numéro d'action : 3.4
Résumé des tâches : démontrer l'impact et l'aspect pratique du déploiement de l'informatique d'entreprise uniquement en IPv6. Contributeur(s) : NIST (responsable), industrie
Tâches préalables : N/A Début
prévu : TBD Achèvement prévu :
TBD

Nom de la tâche : Établir des exigences pour le réseau de confiance zéro (ZTN)
Numéro d'action : 3.3
Résumé des tâches : Le groupe de travail sur les réseaux de confiance zéro du Federal CIO Council élaborera les exigences initiales pour le déploiement par les agences des réseaux de confiance zéro (ZTN). Grâce à ces exigences, les ministères et les organismes seront en mesure d'intégrer ces caractéristiques au fur et à mesure de l'émergence de technologies adaptées.
Contributeur(s) : Groupe de travail sur les réseaux à confiance zéro du Federal CIO Council (responsable)[8]
Tâches préalables : N/A Début prévu : En
cours Achèvement prévu : 4Q18

Nom de la tâche : Évaluer la faisabilité actuelle de la ZTN
Numéro d'action : 3.3
Résumé des tâches : Le National Cybersecurity Center of Excellence (NCCoE) et les collaborateurs de l'industrie réaliseront une étude de faisabilité pour les exigences ZTN identifiées par le groupe de travail ZTN du CIO Council en utilisant des technologies commerciales et émergentes.
Contributeur(s) : NIST (responsable), DHS, Conseil des DSI Groupe de travail sur les réseaux de confiance zéro
Tâches préalables : Établir des exigences pour un réseau de confiance zéro
Début prévu : En cours Achèvement prévu :
4Q19

Nom de la tâche : Identifier les meilleures pratiques pour la gestion du réseau IoT
Numéro d'action : 1.5

[8] *Voir* About the Council, CIO Council, *disponible à l'adresse* https://www.cio.gov/about/.

Résumé des tâches : à l'aide des résultats du projet NCCoE Mitigating IoT-Based DDoS et de l'étude de faisabilité ZTN, le NIST identifiera les meilleures pratiques actuelles pour la gestion des réseaux d'entreprise lorsque les environnements comprennent des dispositifs IoT.

Contributeur(s) : NIST (responsable), DHS, écosystème numérique, industrie et société civile Tâches préalables : Évaluer la faisabilité actuelle du ZTN ; atténuer les DDoS basés sur l'IdO Début prévu : 3Q19

Achèvement prévu : 2Q20

Volet 3 : Adoption par le gouvernement fédéral des meilleures pratiques d'entreprise

Les parties prenantes ont indiqué que l'adoption par le gouvernement fédéral de pratiques de "bon voisinage" fournirait une base à l'échelle de l'écosystème 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 éventuellement nommer et faire honte aux mauvais acteurs) démontreraient la détermination du gouvernement fédéral et encourageraient les autres parties à prendre des mesures bénéfiques. Dans cette série de tâches, le gouvernement fédéral réalise des activités pour s'assurer que ces meilleures pratiques sont correctement reflétées dans les politiques, les normes, les directives et la surveillance des agences fédérales.

Nom de la tâche : Adoption par le gouvernement fédéral des profils CSF fédéraux pour les menaces automatisées et distribuées

Numéro d'action : 2.3
Résumé des tâches : l'OMB publie des directives à l'intention des agences, y compris les délais d'adoption et de rapport, concernant l'adoption des profils CSF fédéraux pour les menaces distribuées automatisées. Le NIST crée ou identifie des outils de mesure pour quantifier les progrès.
Contributeur(s) : OMB e-Gov (chef de file), NIST, DHS, autres agences du gouvernement américain.
Tâches préalables : Profil CSF fédéral pour l'atténuation des DDoS ; Profil CSF fédéral pour la prévention et l'atténuation des botnets.
Début prévu : En cours Achèvement prévu :
2Q20

Nom de la tâche : Mettre en œuvre le filtrage entrée/sortie dans tous les réseaux des agences fédérales américaines

Numéro d'action : 2.3
Résumé des tâches : Les agences fédérales veillent à ce que les réseaux d'agences et les services d'information de réseau fournis commercialement prennent des mesures actives pour empêcher le trafic avec des adresses de source de réseau usurpées.
Contributeur(s) : DHS (chef de file), GSA, OMB, autres agences fédérales, prestataires de services sous contrat fédéral
Tâches préalables : N/A Début
prévu : En cours Achèvement
prévu : 3Q19

Nom de la tâche : Élaborer des directives fédérales de sécurité pour les réflecteurs

Numéro d'action : 2.3
Résumé des tâches : compléter les directives existantes du NIST pour l'exploitation des serveurs et des résolveurs DNS par une publication spéciale du NIST établissant des directives générales pour l'exploitation du protocole NTP (Network Time Protocol) et d'autres ressources largement déployées basées sur le protocole UDP (User Datagram Protocol).
Contributeur(s) : NIST (responsable),
DHS Tâches préalables : N/A Début
prévu : En cours

Achèvement prévu : 2Q19

Nom de la tâche : Mettre en œuvre les directives de sécurité fédérales pour les réflecteurs
Numéro d'action : 2.3
Résumé des tâches : rendre obligatoire la mise en œuvre des directives du NIST pour les ressources réfléchissantes par toutes les agences fédérales.
Contributeur(s) : DHS (co-responsable), OMB (co-responsable), NIST
Tâches préalables : Élaborer des directives de sécurité fédérales pour les réflecteurs
Début prévu : 2Q19
Achèvement prévu : 2Q20

Nom de la tâche : Suivi et remédiation des ressources vulnérables des agences fédérales
Numéro d'action : 2.3
Résumé des tâches : dresser la liste des agences fédérales ayant des ressources de réflexion qui ne sont pas conformes aux directives du NIST et suivre les progrès.
Contributeur(s) : DHS (chef de file), OMB, départements et agences américains
Tâches préalables : Adoption des profils CSF fédéraux pour les menaces automatisées et distribuées
Début prévu : 2Q20
Achèvement prévu : En cours

Enterprise Workstream 4 : Technologie opérationnelle

Une série de tâches sont précisées ci-dessous afin de combler les lacunes de compréhension entre les communautés de la cybersécurité et des technologies opérationnelles (TO). Les experts en cybersécurité n'ont souvent qu'une connaissance limitée des limites et des contraintes imposées par les préoccupations propres aux technologies opérationnelles (par exemple, la sécurité), tandis que la communauté des technologies opérationnelles n'a qu'une connaissance limitée des risques et des capacités en matière de cybersécurité.

Nom de la tâche : Les communautés de la cybersécurité et des technologies de l'information collaborent pour améliorer la compréhension des défis de la cybersécurité des technologies de l'information.
Numéro d'action : 4.5
Résumé des tâches : la communauté de la cybersécurité collabore avec la communauté de l'OT pour améliorer la compréhension des défis de la cybersécurité.
Contributeur(s) : DHS (chef de file), agences sectorielles, laboratoires nationaux, conseils de coordination sectorielle
Tâches préalables : N/A
Début prévu : 2Q19 Achèvement prévu :
3Q21

Nom de la tâche : Développer le partage d'informations OT-Cybersécurité
Numéro d'action : 4.5
Résumé des tâches : étendre les engagements fédéraux actuels qui favorisent le partage d'informations entre les communautés de l'OT et de la cybersécurité.
Contributeur(s) : DHS (chef de file), agences sectorielles, laboratoires nationaux, conseils de coordination sectorielle
Tâches préalables : N/A
Début prévu : 2Q19 Achèvement prévu :
3Q21

Nom de la tâche : Promouvoir l'adoption par l'OT des technologies de sécurité informatique
Numéro d'action : 4.5

Résumé des tâches : étendre les engagements fédéraux actuels qui favorisent l'adoption par l'OT des technologies de sécurité informatique.
Contributeur(s) : NIST (responsable), DHS, agences sectorielles, conseils de coordination sectorielle Tâches préalables : N/A
Début prévu : En cours Achèvement prévu :
3Q21

Ligne d'effort de l'infrastructure

La ligne d'effort "Infrastructure" se concentre sur les actions qui nécessiteront une coordination entre la grande diversité des acteurs de l'écosystème numérique, ou qui ont une incidence sur les capacités fonctionnelles essentielles de l'infrastructure numérique mondiale.

La ligne d'effort "Infrastructure" comporte quatre axes de travail complémentaires :

- Amélioration de la sécurité du routage
- Le partage de l'information dans la pratique
- Protocoles de partage de l'information
- Recherche et développement

Volet infrastructure 1 : Améliorations de la sécurité du routage

L'Internet a été conçu pour faciliter les communications résilientes entre les points finaux, et a accordé moins d'attention aux services de sécurité de base. En conséquence, l'état de la sécurité du routage sur l'Internet est bien en deçà de ce qui peut être réalisé avec les outils et pratiques courants et plus récents. Cette série de tâches fait progresser le déploiement de technologies anti-spoofing de longue date et de technologies plus récentes pour se protéger contre les détournements et les fuites de routes.

Nom de la tâche : Supprimer les obstacles juridiques et politiques à l'adoption de l'infrastructure à clé publique pour les ressources (ICPR)
Numéro d'action : 2.3
Résumé des tâches : établir une stratégie juridique consensuelle afin d'éliminer les obstacles à l'adoption du RPKI, notamment la délivrance de certificats RPKI pour les détenteurs d'adresses anciennes, les questions de responsabilité et les obstacles aux modèles de déploiement alternatifs.
Contributeur(s) : Universités, ingénieurs Internet, NIST, NTIA, DOD, registres Internet régionaux et locaux.
Tâches préalables : N/A Début
prévu : 2Q19 Achèvement prévu :
1Q20

Nom de la tâche : Les agences fédérales adoptent le RPKI
Numéro d'action : 2.3
Résumé des tâches : Les détenteurs d'adresses et les fournisseurs de services fédéraux créent des autorisations d'origine de route (ROA) pour les ressources d'adresses et appliquent les ROA aux décisions de routage Internet afin de limiter les détournements de route.
Contributeur(s) : DHS (chef de file), OMB, DOD, agences fédérales
Tâches préalables : Supprimer les obstacles juridiques et politiques à l'adoption du RPKI
Début prévu : 1Q20
Achèvement prévu : 1Q21

Nom de la tâche : Augmenter l'évolutivité et la robustesse des mécanismes anti-spoofing
Numéro d'action : 2.3
Résumé des tâches : le gouvernement et l'industrie poursuivent leurs recherches afin de rendre l'anti-spoofing plus évolutif et robuste, et disponible à tous les niveaux de l'Internet.
Contributeur(s) : DHS (chef de file), incubateurs technologiques fédéraux, NIST, ingénieurs Internet, universités
Tâches préalables : N/A
Début prévu : En cours Achèvement prévu :
4Q19

Nom de la tâche : Étendre l'adoption, la sensibilisation et l'application des mécanismes de lutte contre la spoliation.
Numéro d'action : 2.3
Résumé des tâches : promouvoir l'adoption et étendre la mise en œuvre de mécanismes anti-spoofing, le cas échéant, dans l'ensemble de l'infrastructure Internet.
Contributeur(s) : Propriétaires et exploitants d'infrastructures Internet, société civile, NIST, NTIA, DHS
Tâches préalables : Augmenter l'évolutivité et la robustesse des mécanismes anti-spoofing Début prévu : 4Q19
Achèvement prévu : 4Q20

Nom de la tâche : Établir un observatoire et un tableau de bord des normes mutuellement acceptées pour la sécurité du routage (MANRS) pour les mesures de sécurité du routage.
Numéro d'action : 2.5
Résumé des tâches : développer des mesures et un site web pour évaluer la sécurité et la résilience du système de routage Internet au fil du temps.
Contributeur(s) : Internet Society, RIRs Tâches
préalables : N/A
Début prévu : En cours
Achèvement prévu : 4Q18

Nom de la tâche : Développer des exigences de sécurité pour les services Internet
Numéro d'action : 3.3
Résumé des tâches : Publier SP 800-189, "Secure Inter-Domain Traffic Exchange : BGP Robustness and DDoS Mitigation".
Contributeur(s) : NIST
(responsable) Tâches préalables :
N/A Début prévu : En cours
Achèvement prévu : 2Q19

Nom de la tâche : Explorer l'évolution des menaces et les solutions émergentes autour de la sécurité du routage.
Numéro d'action : 3.3
Résumé des tâches : engager les parties prenantes et les acteurs de l'infrastructure Internet à comprendre les avantages et les limites des solutions de sécurité de routage existantes et émergentes, en capturant les préoccupations des parties prenantes et les atténuations potentielles.
Contributeur(s) : NTIA, propriétaires et opérateurs d'infrastructures Internet, société civile, NIST, DHS
Tâches préalables : N/A
Début prévu : 3Q19 Achèvement
prévu : 3Q20

Infrastructure Workstream 2 : Partage de l'information dans la pratique

Les grands fournisseurs de réseaux partagent actuellement les techniques de gestion des réseaux et les tactiques défensives qui sont efficaces contre certaines menaces. Les services répressifs dépendent des informations du secteur privé pour lancer des enquêtes. Cette série de tâches vise à étendre le partage d'informations aux petits ISP et aux fournisseurs de réseaux étrangers, et à faire en sorte que les services répressifs soient alertés le plus tôt possible, tout en respectant les directives et réglementations en matière de protection de la vie privée.

Nom de la tâche : Accroître l'accès des petits FAI aux informations sur les menaces partagées par l'industrie
Numéro d'action : 2.1
Résumé des tâches : étendre le partage d'informations au niveau national pour améliorer la participation des petits ISP. Contributeur(s) : Fournisseurs d'infrastructure, DHS par le biais de l'ISAC Communications.
Tâches préalables : N/A Début prévu : TBD
Achèvement prévu : TBD

Nom de la tâche : Développer le partage des informations sur les menaces à l'échelle mondiale et régionale
Numéro d'action : 2.1
Résumé des tâches : améliorer les mécanismes de partage de l'information pour faciliter un partage mondial et régional élargi.
Contributeur(s) : Équipes mondiales de réponse aux incidents de sécurité informatique (CSIRT), DHS, NOG, ISAC, fournisseurs d'infrastructures.
Tâches préalables : N/A Début
prévu : 1Q19 Achèvement prévu :
TBD

Nom de la tâche : Élargir les accords de partage de l'information
Numéro d'action : 2.1
Résumé des tâches : Le gouvernement américain tire parti des ISAC, des partenariats NOG, du Forum des équipes de réponse aux incidents et de sécurité (FIRST), et travaille avec des pairs internationaux pour étendre les accords de partage d'informations.
Contributeur(s) : DHS, NOGs, ISAC Council, ISACs, FIRST, partenariats avec les forces de l'ordre, cybercentres/centres de fusion
Tâches préalables : N/A Début
prévu : TBD Achèvement prévu :
TBD

Nom de la tâche : Partager des informations opportunes et exploitables avec les forces de l'ordre
Numéro d'action : 4.1
Résumé des tâches : fournir des informations encore plus opportunes et exploitables pour faciliter, soutenir et accélérer les actions de répression, y compris celles qui concernent les réseaux de zombies distribués dans le monde entier.
Contributeur(s) : Ministère de la Justice (DOJ)/Federal Bureau of Investigations (FBI), FTC, ISACs, DHS, NOGs, CSIRTs mondiaux, grandes entreprises et fournisseurs d'infrastructure.
Tâches préalables : N/A Début
prévu : TBD Achèvement prévu :
TBD

Nom de la tâche : Améliorer le partage des informations du gouvernement américain avec l'industrie
Numéro d'action : 4.1
Résumé des tâches : améliorer l'opportunité et la pertinence des informations partagées par le gouvernement américain avec l'industrie.
Contributeur(s) : USG Cyber Centers, DHS, agences sectorielles, ISAC/organisations de partage et d'analyse de l'information (ISAO)
Tâches préalables : N/A Début prévu : TBD
Achèvement prévu : TBD

Nom de la tâche : Améliorer l'exactitude des ressources de données critiques pour la sécurité
Numéro d'action : 4.1
Résumé des tâches : les bases de données WHOIS, qui comprennent les informations d'enregistrement des ressources de nommage et de numérotation de l'Internet (par exemple, les adresses IP et les noms de domaine), sont améliorées afin de faciliter l'attribution des mauvais acteurs. Des mécanismes sont mis au point pour préserver la rapidité d'accès aux informations WHOIS () tout en respectant les règles de protection de la vie privée (par exemple, le règlement général de l'UE sur la protection des données [RGPD]) et en soutenant le travail d'enquête sur les botnets.
Contributeur(s) : Bureaux d'enregistrement de noms de domaine, NTIA, Internet Corporation for Assigned Names and Numbers (ICANN), RIR, forces de l'ordre, universités et société civile.
Tâches préalables : N/A Début prévu :
En cours Achèvement prévu : En
cours

Infrastructure Workstream 3 : Protocoles de partage de l'information

Cet ensemble de tâches se concentre sur la normalisation des protocoles de partage d'informations afin d'augmenter la vitesse et de permettre une réponse automatisée. L'amélioration de l'utilité des protocoles de partage de l'information complète les tâches du processus de partage de l'information en augmentant la valeur de l'information qui est partagée.

Nom de la tâche : Soutenir l'automatisation du partage de l'information
Numéro d'action : 2.1
Résumé des tâches : Améliorer les protocoles de partage de l'information afin d'augmenter la vitesse et de soutenir la réponse automatisée.
Contributeur(s) : DHS, ISAO, industrie, société civile, consortiums Tâches préalables :
N/A
Début prévu : TBD Achèvement prévu : TBD

Nom de la tâche : Soutenir la réponse collaborative aux incidents
Point d'action : 4.4
Résumé des tâches : l'IETF finalise le protocole DOTS (DDoS Open Threat Signaling). Les entreprises ayant des stratégies d'atténuation des DDoS multipartites mettent en œuvre et déploient DOTS pour faciliter une action coordonnée.
Contributeur(s) : IETF, entreprises de l'écosystème numérique, société
civile Tâches préalables : N/A
Début prévu : En cours
Achèvement prévu : TBD

Nom de la tâche : Améliorer les protocoles de partage de l'information pour faciliter le partage de l'information à l'échelle mondiale

Numéro d'action : 2.4
Résumé des tâches : le gouvernement et l'industrie des États-Unis examineront et amélioreront les protocoles d'échange d'informations, tels que STIX (Structured Threat Information Expression) et TAXII (Trusted Automated Exchange of Indicator Information), afin de faciliter l'échange mondial d'informations concernant les menaces automatisées.
Contributeur(s) : DHS (chef de file), ISAO, centres de recherche et de développement financés par le gouvernement fédéral (FFRDC), industrie.
Tâches préalables : N/A Début prévu : TBD
Achèvement prévu : TBD

Nom de la tâche : Établir des normes internationales pour faciliter le partage de l'information

Numéro d'action : 2.4
Résumé des tâches : l'industrie, avec le soutien du gouvernement américain, établira des normes internationales pour le partage des informations afin de faciliter la coordination mondiale.
Contributeur(s) : Industrie (chef de file), DHS, ISAC/ISAO, société civile Tâches
préalables : N/A
Début prévu : TBD Achèvement
prévu : TBD

Infrastructure Workstream 4 : Recherche et développement

Nom de la tâche : Incorporation des meilleures pratiques en matière d'infrastructure dans le cadre de cybersécurité du NIST

Numéro d'action : 3.3
Résumé des tâches : évaluer en permanence les progrès des meilleures pratiques et technologies de sécurité en vue de leur inclusion dans le cadre de cybersécurité du NIST.
Contributeur(s) : NIST (chef de file), fournisseurs d'infrastructure
Tâches préalables : N/A
Début prévu : TBD Achèvement prévu : TBD

Nom de la tâche : Perturber l'écosystème des attaquants par la transparence et la traçabilité

Numéro d'action : 4.4
Résumé de la tâche : L'écosystème des menaces automatisées et distribuées favorise l'attaquant. Cette tâche développe des méthodes pour perturber les écosystèmes qui sont traditionnellement exploités pour lancer des botnets, comme la communauté des joueurs, et augmenter le risque pour les attaquants par la transparence et la responsabilité. L'industrie et les pouvoirs publics plaident conjointement au sein des forums multipartites pertinents pour une mise en œuvre plus large des mesures qui perturbent les outils et les incitations des attaquants.
Contributeur(s) : ICANN, RIRs, NTIA, Application de la loi, FTC Tâches
préalables : N/A
Début prévu : TBD Achèvement
prévu : TBD

Ligne d'effort pour le développement et la transition technologique

La ligne d'effort "Développement et transition technologiques" comporte trois axes de travail complémentaires :

- Mise en place d'un marché des logiciels sécurisé
- Coordination internationale
- Recherche et développement

Volet 1 du développement et de la transition technologiques : Établir un marché des logiciels sécurisés

Cette série de tâches permet d'établir un marché solide et durable pour les systèmes et les applications développés grâce à des pratiques de développement de logiciels sécurisés. Les tâches consistent à établir des lignes directrices largement acceptées pour le développement de logiciels sécurisés, à accroître l'efficacité des outils de développement de logiciels sécurisés afin d'augmenter le retour sur investissement, et à présenter ces progrès dans des forums technologiques parrainés par le gouvernement.

Nom de la tâche : Établir des directives pour le cycle de vie du développement de logiciels sécurisés
Numéro d'action : 1.3
Résumé des tâches : en collaboration avec l'industrie, le NIST définit des directives relatives au cycle de vie du développement de logiciels sécurisés qui seront publiées dans une publication spéciale du NIST.
Contributeur(s) : NIST (chef de file), DHS, industrie Tâches
préalables : N/A
Début prévu : En cours
Achèvement prévu : 2Q20

Nom de la tâche : Développer des directives pour la transparence des composants logiciels
Numéro d'action : 1.3
Résumé de la tâche : explorer comment les fabricants et les fournisseurs peuvent communiquer des informations utiles et exploitables sur les composants logiciels tiers dans les logiciels modernes et les appareils IoT, et comment ces données peuvent être utilisées par les entreprises pour favoriser de meilleures décisions et pratiques en matière de sécurité.
Contributeur(s) : NTIA (chef de file), secteurs des infrastructures critiques, parties prenantes de l'écosystème numérique Tâches préalables : N/A
Début prévu : En cours Achèvement prévu :
2Q19

Nom de la tâche : Combler les lacunes des outils de développement logiciel
Numéro d'action : 1.3
Résumé des tâches : Le programme de recherche et développement en matière de réseaux et de technologies de l'information (NITRD) favorisera le financement de la recherche ciblée et les activités de transition technologique en collaboration pour les outils de développement de logiciels nécessaires à l'adoption efficace et efficiente du cycle de vie de développement de logiciels sécurisés (SSDLC).
Contributeur(s) : NITRD (responsable)
Tâches préalables : N/A Début prévu : En
cours Achèvement prévu : 1Q23

Nom de la tâche : Améliorer les chaînes d'outils de développement de logiciels

Numéro d'action : 1.3
Résumé des tâches : Accélérer le développement et l'adoption de techniques de développement de logiciels efficaces et efficientes en gérant une compétition ouverte pour les chaînes d'outils de développement de logiciels.
Contributeur(s) : NIST (responsable), DHS
Tâches préalables : N/A Début prévu : En cours
Achèvement prévu : 1Q22

Nom de la tâche : Présenter les progrès des pratiques de codage sécurisé et partager les informations sur les risques de sécurité

Numéro d'action : 5.3
Résumé des tâches : présenter les avancées en matière de pratiques et d'outils de codage sécurisés développés par le monde universitaire et les chercheurs en sécurité et partager des informations sur les risques de sécurité lors de la conférence annuelle PrivacyCon.
Contributeur(s) : CFT (principal) Tâches
préalables : N/A Début prévu : 3Q19
Achèvement prévu : En cours

Nom de la tâche : Les agences exigent un développement sécurisé pour les logiciels disponibles sur le marché du gouvernement (GOTS)

Numéro d'action : 2.3
Résumé des tâches : Les réglementations fédérales en matière d'approvisionnement sont établies pour les contrats de développement de logiciels GOTS qui encouragent ou rendent obligatoire l'application du SSDLC. Contributeur(s) : GSA, OMB, DOD, autres départements et agences des États-Unis.
Tâches préalables : Définir la base de référence des capacités de sécurité
fondamentales Début prévu : TBD
Achèvement prévu : TBD

Nom de la tâche : Les agences achètent des logiciels commerciaux développés en toute sécurité (COTS).

Numéro d'action : 2.3
Résumé des tâches : Des règlements fédéraux sont établis pour l'acquisition de logiciels COTS qui préfèrent ou exigent un développement utilisant le SSDLC.
Contributeur(s) : GSA (chef de file), OMB, DHS (programme de diagnostic et d'atténuation continus), DOD, autres départements et agences des États-Unis.
Tâches préalables : Définir la base de référence des capacités de sécurité
fondamentales Début prévu : TBD
Achèvement prévu : TBD

Nom de la tâche : Développer les meilleures pratiques pour les logiciels en fin de vie

Numéro d'action : 1.5
Résumé des tâches : développer une gamme de processus de fin de vie pour les logiciels et les dispositifs morts et orphelins qui équilibrent les exigences des clients et des entreprises.
Contributeur(s) : CTA, NTIA, autres participants gouvernementaux et industriels Tâches
préalables : N/A
Début prévu : En cours
Achèvement prévu : 4Q19

Développement et transition technologiques Axe de travail 2 : Coordination internationale

Nom de la tâche : Améliorer la coordination existante entre le gouvernement américain et les normes internationales
Numéro d'action : 4.2
Résumé des tâches : S'appuyer sur les travaux du Groupe de travail interagences sur la normalisation de la cybersécurité internationale (IICSWG) pour améliorer encore la coordination du gouvernement américain dans son engagement auprès des organismes internationaux de normalisation. Identifier des stratégies pour la promotion de l'élaboration de normes par l'industrie au sein de ces organismes.
Contributeur(s) : NIST (responsable), agences membres de l'IICSWG Tâches
préalables : N/A
Début prévu : En cours Achèvement prévu : En
cours

Nom de la tâche : Optimiser la coordination des normes entre l'industrie et le GUS
Numéro d'action : 4.2
Résumé des tâches : établir un cadre et une stratégie pour poursuivre la coordination entre les entités industrielles américaines et les agences fédérales qui participent à l'élaboration des normes internationales.
Contributeur(s) : NIST, NTIA, État, IICSWG, industrie, CSDE, associations commerciales.
Tâches préalables : N/A Début prévu : En cours
Achèvement prévu : En cours

Nom de la tâche : Promouvoir l'adoption internationale des meilleures pratiques par le biais d'un engagement international bilatéral et multilatéral
Numéro d'action : 4.2
Résumé des tâches : promouvoir l'adoption des meilleures pratiques reconnues au niveau international par le biais d'un engagement bilatéral, multilatéral et multipartite, en tirant parti de l'expertise des agences du gouvernement américain.
Contributeur(s) : État, NTIA, NIST, industrie, société civile Tâches
préalables : N/A
Début prévu : En cours
Achèvement prévu : TBD

Nom de la tâche : Promouvoir la sensibilisation et l'adoption d'outils, de protocoles et de meilleures pratiques spécifiques à l'échelle mondiale.
Numéro d'action : 3.3
Résumé des tâches : promouvoir la mise en œuvre et l'adoption d'outils, de protocoles et de meilleures pratiques établis qui traitent des cyberrisques automatisés à l'échelle. Élaborer des guides de mise en œuvre faciles à comprendre et travailler avec les parties prenantes du monde entier. Développer la capacité à mesurer l'impact de cette mise en œuvre.
Contributeur(s) : Global Cyber Alliance, organismes de coordination de l'industrie, NTIA, NIST, DHS
Tâches préalables : N/A
Début prévu : En cours Achèvement
prévu : En cours

Nom de la tâche : Promouvoir les meilleures pratiques pour le DNS au niveau international
Numéro d'action : 4.2
Résumé des tâches : promouvoir les meilleures pratiques et les outils pertinents pour le DNS par le biais des positions américaines dans les forums multipartites, tels que l'ICANN, l'IETF et le Forum sur la gouvernance de l'Internet.

Contributeur(s) : NTIA (chef de file), participants multilatéraux du gouvernement et du secteur privé Tâches préalables : N/A
Début prévu : En cours Achèvement
prévu : En cours

Développement et transition technologiques Axe de travail 3 : Recherche et développement

La croissance rapide de la capacité DDoS offerte par les botnets basés sur l'IdO met en péril l'efficacité des techniques actuelles d'atténuation des DDoS. La recherche et le développement de techniques qui offrent une atténuation plus proche de la source - ou qui exploitent les nouvelles analyses de données, l'apprentissage automatique ou l'intelligence artificielle - sont nécessaires de toute urgence pour devancer les acteurs malveillants. Des activités de recherche menées par l'industrie sont nécessaires pour développer et déployer des technologies innovantes. En tant que principale source de financement de la recherche fondamentale en matière de cybersécurité, le gouvernement fédéral devrait soutenir cette action par des financements ciblés et des activités de collaboration en matière de transition technologique.

Nom de la tâche : Accélérer la recherche et le développement financés par le gouvernement fédéral pour atténuer les menaces distribuées.

Numéro d'action : 1.4
Résumé des tâches : promouvoir le financement de la recherche ciblée et les activités de transition technologique en collaboration pour les technologies qui atténuent les menaces distribuées automatisées.
Contributeur(s) : NITRD (responsable), DHS, départements et agences des États-Unis
Tâches préalables : N/A
Début prévu : En cours Achèvement prévu : En
cours

Nom de la tâche : Accélérer le développement et le déploiement de technologies innovantes pour la prévention et l'atténuation des menaces distribuées.
Numéro d'action : 1.4
Résumé des tâches : L'industrie, le monde universitaire et le gouvernement devraient accélérer le développement et le déploiement de technologies innovantes pour la prévention et l'atténuation des menaces distribuées. Contributeur(s) : Acteurs de l'écosystème dans un environnement concurrentiel
Tâches préalables : N/A Début prévu :
En cours Achèvement prévu : En
cours

Nom de la tâche : Accroître la responsabilité en matière de gestion du trafic
Numéro d'action : 2.5
Résumé des tâches : examiner dans quelle mesure les accords de système inter-autonome, d'échange de trafic et de transit peuvent améliorer la responsabilité de la gestion du trafic.
Contributeur(s) : NOGs, incubateurs technologiques fédéraux, DHS, société civile, université
Tâches préalables : N/A
Début prévu : TBD Achèvement
prévu : TBD

Nom de la tâche : Accélérer la R&D de l'industrie pour atténuer les menaces distribuées
Numéro d'action : 1.4
Résumé des tâches : Accélérer le développement et le déploiement de technologies innovantes pour la prévention et l'atténuation des menaces distribuées.
Contributeur(s) : Consortiums et laboratoires industriels, universités

Tâches préalables : N/A Début prévu : TBD
Achèvement prévu : TBD

Nom de la tâche : Priorité à la transition technologique
Numéro d'action : 2.5
Résumé des tâches : mettre l'accent sur les stratégies de transition technologique en tant qu'élément clé des plans de recherche pour les nouveaux outils et pratiques de gestion du trafic réseau.
Contributeur(s) : Coalition TBD de l'industrie, du gouvernement et de la société civile Tâches
préalables : N/A
Début prévu : TBD Achèvement prévu : TBD

Nom de la tâche : Promouvoir les meilleures pratiques émergentes
Numéro d'action : 1.4
Résumé des tâches : amplifier les efforts de recherche et de transition technologique à mesure que les technologies arrivent à maturité et que les meilleures pratiques émergent.
Contributeur(s) : Société civile TBD Tâches
préalables : N/A Début prévu : En cours
Achèvement prévu : En cours

Sensibilisation et éducation Ligne d'effort

La ligne d'effort "Sensibilisation et éducation" comporte deux axes de travail complémentaires :

- Promouvoir la confiance des consommateurs
- Former la main-d'œuvre

Sensibilisation et éducation Axe de travail 1 : Promouvoir la confiance des consommateurs

Le manque de confiance des consommateurs dans la sécurité des dispositifs IdO peut freiner l'adoption de l'IdO. Cette série de tâches se concentre sur le renforcement de la confiance des consommateurs pour leur permettre d'identifier les produits qui répondent à leurs besoins, qui respectent les déclarations de sécurité des vendeurs et qui offrent une réelle protection en appliquant les technologies de cybersécurité disponibles dans le commerce.

Nom de la tâche : Promouvoir un déploiement approprié des produits
Numéro d'action : 4.3
Résumé des tâches : informer les consommateurs sur les différentes lignes de base et les programmes d'évaluation qui montreront que les produits déployés utilisent une sécurité appropriée.
Contributeur(s) : Agences sectorielles, société civile, groupes de consommateurs, FTC, DHS, NTIA, CTA Tâches
préalables : Établir un programme d'évaluation pour les dispositifs IdO domestiques ; établir un programme d'évaluation pour les dispositifs IdO industriels ; spécifier la base des capacités de sécurité IdO.
Début prévu : 1Q20 Achèvement prévu :
3Q23

Nom de la tâche : Dissuader les pratiques commerciales illégales
Numéro d'action : 4.3

Résumé des tâches : arrêter et dissuader les pratiques commerciales illégales des fournisseurs d'IdO et d'informatique par des mesures d'exécution.
Contributeur(s) : FTC (chef de file)
Tâches préalables : N/A Début prévu :
En cours Achèvement prévu : En
cours

Nom de la tâche : Atténuation des attaques DDoS basées sur l'IdO
Numéro d'action : 1.5
Résumé des tâches : démontrer l'impact et l'aspect pratique de la combinaison des descriptions d'utilisation du fabricant (MUD), de la signalisation des menaces, des mises à jour sécurisées et de la cyberhygiène de base pour protéger les dispositifs IoT et atténuer l'impact des dispositifs IoT compromis.
Contributeur(s) : NIST (chef de file), société civile, ingénieurs Internet
Tâches préalables : N/A
Début prévu : En cours Achèvement
prévu : En cours

Sensibilisation et éducation Axe de travail 2 : Former la main-d'œuvre

Avec la mise en ligne d'une gamme complète de produits et de services, les menaces de cybersécurité apparaissent dans de nouvelles catégories de produits. Les concepteurs de produits sont profondément imprégnés des risques traditionnels associés à leurs produits, mais ils ignorent souvent les nouveaux risques qui peuvent être introduits lorsque les produits sont connectés au réseau. Cette série de tâches se concentre sur l'éducation de la main-d'œuvre existante et émergente, quelle que soit la discipline d'ingénierie, sur la cybersécurité de base.

Nom de la tâche : Préparer le personnel de programmation
Numéro d'action : 1.3
Résumé des tâches : intégrer les principes de conception sécurisée et les outils de soutien dans les cours de programmation tout au long du cursus.
Contributeur(s) : Milieu universitaire, communauté de développement de logiciels sécurisés, prestataires de formation et de certification, organismes d'accréditation, gouvernement.
Tâches préalables : N/A Début prévu : En
cours Achèvement prévu : 2Q20

Nom de la tâche : Préparer le personnel d'ingénierie
Numéro d'action : 5.4
Résumé des tâches : intégrer les principes de cybersécurité dans les programmes d'études de toutes les disciplines de l'ingénierie.
Contributeur(s) : Milieu universitaire, gouvernements fédéral et des États Tâches
préalables : N/A
Début prévu : En cours Achèvement prévu :
2Q20

Nom de la tâche : Aligner le programme d'études sur les besoins de la main-d'œuvre
Numéro d'action : 5.3

Résumé des tâches : continuer à promouvoir le cadre de l'Initiative nationale pour l'éducation à la cybersécurité (NICE) comme outil de référence pour l'élaboration du contenu des cours, notamment en ce qui concerne le développement de logiciels.
Contributeur(s) : NIST (responsable), universités, organismes d'accréditation, sociétés professionnelles, prestataires de services de certification.

Tâches préalables : N/A Début
prévu : En cours Achèvement
prévu : 4Q18

Nom de la tâche : Mettre en place un programme éducatif sur la cybersécurité pour les ingénieurs
Numéro d'action : 5.4
Résumé des tâches : faire de la cybersécurité une exigence fondamentale dans toutes les disciplines de l'ingénierie, et créer ou exploiter les formations en ligne existantes en matière de cybersécurité pour les ingénieurs.
Contributeur(s) : NIST, communauté de l'enseignement de la cybersécurité, programmes d'accréditation
Tâches préalables : N/A
Début prévu : En cours Achèvement prévu :
1Q21

III. Les prochaines étapes

Les départements du commerce et de la sécurité intérieure travailleront avec d'autres agences gouvernementales américaines et le secteur privé pour coordonner et suivre les activités de la feuille de route. Le DHS assurera la coordination entre les agences sectorielles et avec les organisations chargées des infrastructures critiques. Le département du commerce coordonnera les normes et les activités techniques par l'intermédiaire du NIST, et assurera la coordination entre le gouvernement et l'économie numérique par l'intermédiaire de la NTIA.

Nous fournirons également des mises à jour périodiques, notamment :

- Rencontrer et communiquer régulièrement avec les parties prenantes du secteur privé qui mènent des initiatives clés afin de partager les informations et les progrès.
- Convoquer les parties prenantes à mi-parcours (environ six mois après la publication de la feuille de route), dans le cadre d'un atelier ou d'une autre session, pour discuter des progrès réalisés dans la mise en œuvre de la feuille de route.
- Fournir au président un rapport d'étape de 365 jours sur la mise en œuvre, à remettre un an après la publication de la feuille de route finale, comme indiqué dans le rapport sur les botnets. Ce rapport fera le point sur les progrès réalisés par l'ensemble de la communauté, réévaluera la menace dans la mesure du possible et abordera les principales activités de l'année à venir.

Comme indiqué dans le rapport sur les botnets et dans la section II du présent document, le problème des attaques automatisées et distribuées ne peut être résolu par une seule entité et nécessitera une action, une coordination et une exploitation de l'innovation dans l'ensemble du gouvernement et du secteur privé (y compris l'industrie, les universités et la société civile). Les ministères se réjouissent de travailler avec le secteur privé et d'autres entités gouvernementales au cours de l'année à venir et au-delà pour améliorer la sécurité de l'écosystème Intern