NISTIR 8192

Renforcer la résilience de l'Internet et de la Écosystème de communication

Compte rendu d'un atelier du NIST

Tim Polk

Cette publication est disponible gratuitement auprès de :
https://doi.org/10.6028/NIST.IR.8192

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8192

Renforcer la résilience de l'Internet et de la Écosystème de communication

Compte rendu d'un atelier du NIST

Tim Polk
Division de la cybersécurité appliquée
Laboratoire de technologie de l'information

Cette publication est disponible gratuitement auprès de :
https://doi.org/10.6028/NIST.IR.8192

Septembre 2017

Département du commerce des États-Unis
Wilbur L. Ross, Jr, Secrétaire

Institut national des normes et de la technologie
Kent Rochford, directeur par intérim du NIST et sous-secrétaire au commerce pour les normes et la technologie

Rapport interne du National Institute of Standards and Technology 8192
33 pages (septembre 2017)

Cette publication est disponible gratuitement auprès de : https://doi.org/10.6028/NIST.IR.8192

Les commentaires sur ce sujet peuvent être soumis jusqu'au 5 février 2018 à :

Institut national des normes et de la technologie
Attn : Division de la cybersécurité appliquée, Laboratoire de technologie de l'information 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Courriel : distributed.threats@nist.gov

Voir la section 5 du présent document pour plus de détails.

Rapports sur la technologie des systèmes informatiques

Le laboratoire de technologie de l'information (ITL) du National Institute of Standards and Technology (NIST) promeut l'économie et le bien-être public des États-Unis en fournissant des services techniques et des services d'assistance technique le leadership pour l'infrastructure de mesure et de normalisation de la nation. L'ITL développe des tests, des essais des méthodes, des données de référence, des mises en œuvre de la preuve de concept et des analyses techniques pour faire avancer le projet de la le développement et l'utilisation productive des technologies de l'information. Les responsabilités de l'ITL comprennent l'élaboration de normes et de lignes directrices en matière de gestion, d'administration, de technique et de physique, pour la sécurité et la confidentialité rentables des informations autres que celles liées à la sécurité nationale dans les systèmes fédéraux de gestion de l'information les systèmes d'information.

Résumé

Ces actes documentent la conférence des 11 et 12 juillet 2017 intitulée "Renforcer la résilience de l'Internet et de l'industrie des télécommunications".
Atelier "Écosystème de communication" dirigé par le National Institute of Standards and Technologie. Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", les secrétaires au commerce et à la sécurité intérieure doivent "conjointement mener un processus ouvert et transparent pour identifier et promouvoir l'action des parties prenantes appropriées pour améliorer la résilience de l'écosystème de l'internet et des communications et pour encourager collaboration dans le but de réduire considérablement les menaces perpétrées par les systèmes automatisés et les systèmes d'information les attaques distribuées (par exemple, les botnets)". L'atelier a été conçu pour permettre aux parties prenantes d'explorer une gamme de solutions actuelles et émergentes pour faire face aux menaces automatisées et distribuées dans un environnement ouvert et transparente. L'atelier a attiré 150 participants de diverses parties prenantes et a été menée selon les règles de Chatham House.

Mots clés

Botnet ; menace distribuée ; attaque par déni de service distribué (DDoS) ; Internet des objets ; résilience ; racine de confiance ; mise à jour sécurisée

Remerciements

Bien que l'Institut national des normes et de la technologie (NIST) ait convoqué cet atelier, il n'en est rien. Ce succès est dû aux contributions perspicaces offertes par les 150 participants de l'industrie, le monde universitaire, les organismes de normalisation, les organisations non gouvernementales et les agences gouvernementales. Nous apprécions tout particulièrement les contributions des présidents et des panélistes de notre panel ; leur réflexion. Les discussions stimulantes ont été essentielles au succès des séances en petits groupes qui ont suivi.

Enfin, ce rapport d'atelier n'aurait pas été possible sans l'extraordinaire soutien que nous avons reçu de la part de la Commission européenne reçu du National Cybersecurity Center of Excellence (NCCoE) du NIST et de The MITRE. Corporation, l'opérateur du NCCoE. Le NCCoE est une collaboration entre le secteur public et le secteur privé pour accélérer l'adoption généralisée d'outils et de technologies intégrés de cybersécurité, et est coparrainé par l'État du Maryland et le comté de Montgomery, Md. Le NCCoE et MITRE a mis à disposition des experts en la matière pour recueillir les contributions de nos participants et a effectué une analyse détaillée après l'atelier, identifiant les principaux domaines d'intérêt et préoccupation. Les experts en la matière qui ont soutenu ce processus étaient :

- Brian Abe (NCCoE)
- Drew Allensworth (NCCoE)
- Brittany Biondo (Mitre)
- David Dandar (Mitre)
- Lura Danley (Mitre)
- Zachary Furness (NCCoE)
- Diane Khula (Mitre)
- Susan Prince (NCCoE)
- Julie Steinke (NCCoE)
- Caroline Tan (NCCoE)
- Aaron Temin (NCCoE)
- Teresa Thomas (NCCoE)
- Mary Yang (NCCoE)

Résumé exécutif

Executive Order 13800, " Renforcement de la cybersécurité des réseaux fédéraux et des systèmes critiques "Infrastructure" a été publié le 11 mai 2017. Dans la section 2 (d), le décret exige que la Commission européenne les secrétaires au commerce et à la sécurité intérieure doivent "diriger conjointement un programme ouvert et transparent" pour identifier et promouvoir l'action des parties prenantes appropriées afin d'améliorer la résilience de l'économie européenne l'écosystème de l'internet et des communications et d'encourager la collaboration dans le but de réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées (par exemple, les botnets)." L'ordre exécutif ordonne aux départements de publier un rapport préliminaire en janvier 2018 et soumettre le rapport final au président au plus tard le 11 mai 2018.[1]

Ces actes documentent la conférence des 11 et 12 juillet 2017 intitulée "Renforcer la résilience de l'Internet et de l'industrie des télécommunications". Atelier "Écosystème de communication" dirigé par le National Institute of Standards and Technologie. L'atelier faisait partie d'un ensemble de travaux menés simultanément par différents groupes de travail de la Commission européenne les composantes des ministères afin d'impliquer les parties prenantes et d'identifier les actions appropriées. Le site L'atelier a attiré 150 participants issus de diverses communautés de parties prenantes et s'est déroulé dans les conditions suivantes selon les règles de Chatham House.
Six thèmes primordiaux sont apparus au cours des discussions de l'atelier :

1. La nature globale du problème : la majorité des appareils compromis qui constituentl es botnets sont géographiquement situés en dehors des États-Unis. Une action coordonnée avec partenaires internationaux seront nécessaires pour augmenter la résilience de l'écosystème contre ces menaces.
2. La disponibilité d'outils efficaces : Les outils, processus et pratiques nécessaires pour améliorer de manière significative la résilience de l'écosystème sont largement disponibles, et régulièrement appliquées dans certains secteurs du marché, mais généralement sous-utilisées.
3. L'importance de la sécurisation des produits tout au long de leur cycle de vie : Les appareils qui sont vulnérables au moment du déploiement, manque de moyens pour corriger les vulnérabilités après leur découverte, ou restent en service après la fin de l'assistance technique du fournisseur, ce qui permet d'assembler des réseaux de zombies et des réseaux distribués menaces bien trop faciles.
4. L'impact des lacunes en matière d'éducation et de sensibilisation : Les lacunes en matière de connaissances dans les foyers et les entreprises les clients, les développeurs de produits et les opérateurs d'infrastructures entravent le déploiement de la des outils, des processus et des pratiques qui rendraient l'écosystème plus résilient. Sur le site en particulier, des mécanismes conviviaux permettant d'identifier des choix plus sûrs, par analogie à le programme Energy Star ou l'indice de choc des véhicules sont nécessaires pour informer les acheteurs décisions.
5. Conflits entre les incitations du marché et les objectifs de résilience : Les incitations du marché perçues ne s'aligne pas sur l'objectif de "réduire considérablement les menaces perpétrées par les systèmes automatisés et les systèmes d'information" les attaques distribuées". Les incitations du marché motivent les développeurs et les vendeurs de produits à minimiser les coûts et les délais de mise sur le marché, plutôt que d'intégrer la sécurité ou de proposer une sécurité efficace. des mises à jour.

[1] Le texte intégral du décret est disponible à l'adresse https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

6. La nécessité d'une action intersectorielle coordonnée : Aucune communauté de parties prenantes n'est Il n'est pas possible de s'attaquer au problème de manière isolée. Les contributions de tous les secteurs seront nécessaire pour augmenter de manière significative la résilience de l'écosystème contre les réseaux de zombies et les virus les menaces distribuées automatisées.

L'atelier a permis de recueillir des informations essentielles qui, avec les commentaires du public reçus en réponse à l'appel à propositions, ont permis d'améliorer la qualité des services offerts.
Demande de commentaires de la National Telecommunication and Information Administration et une Le rapport du Comité consultatif sur les télécommunications pour la sécurité nationale informera le Conseil des ministres de l'Union européenne l'élaboration du projet de rapport. Les implications pour le rapport de janvier 2018 sont les suivantes :

- Les actions proposées dans le rapport aborderont chacun des thèmes primordiaux tirés de les participants à l'atelier.
- Le rapport recommandera une ou plusieurs actions proposées pour chacune des parties prenantes groupes (c'est-à-dire les fournisseurs d'infrastructure, les développeurs de produits, les entreprises, les utilisateurs privés), le monde universitaire et le gouvernement).
- Les parties prenantes non gouvernementales s'attendent à ce que le gouvernement fédéral montre l'exemple et promouvoir les actions des autres parties prenantes par des mesures incitatives plutôt que par la réglementation.
- De nombreuses actions auront des dépendances avec des actions attribuées à d'autres parties prenantes, donc les mécanismes de collaboration devront également être identifiés dans le rapport.
- Les recommandations comprendront probablement des actions immédiates visant à accroître la sensibilisation et à le déploiement des technologies actuellement disponibles, les actions à moyen terme pour créer un marché incitations (notamment pour garantir le cycle de vie complet des produits) et promouvoir la coopération international la coordination et la collaboration, ainsi que des actions à long terme pour développer de nouvelles technologies.

Les autres contributions publiques sur ce sujet sont les bienvenues et peuvent être envoyées à l'adresse suivante distributed.threats@nist.gov. Les contributions soumises avant le 15 octobre 2017 seront prises en compte pour inclusion dans le rapport préliminaire, qui sera partagé avec la communauté le ou avant le 5 janvier 2018.

Les contributions et commentaires du public sur le rapport préliminaire seront acceptés jusqu'en février. 5, 2018. Après la clôture de la période de commentaires, un atelier public sera organisé en février pour discuter de la résolution prévue des commentaires. Sur la base des commentaires du public et des discussions tenues lors du deuxième atelier, les départements complèteront le rapport pour le soumettre au président. au plus tard le 11 mai 2018.

Table des matières

Liste des annexes

Liste des figures

1. Introduction

Executive Order 13800, " Renforcement de la cybersécurité des réseaux fédéraux et des systèmes critiques "Infrastructure" a été publié le 11 mai 2017. Dans la section 2 (d), le décret exige que la Commission européenne les secrétaires au commerce et à la sécurité intérieure doivent "diriger conjointement un programme ouvert et transparent" pour identifier et promouvoir l'action des parties prenantes appropriées afin d'améliorer la résilience de l'économie européenne l'écosystème de l'internet et des communications et d'encourager la collaboration dans le but de réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées (par exemple, les botnets)." L'ordre exécutif ordonne aux départements de publier un rapport préliminaire en janvier 2018 et soumettre le rapport final au président au plus tard le 11 mai 2018.[2]

Ces actes décrivent la conférence des 11 et 12 juillet 2017 intitulée " Renforcer la résilience de l'Internet et de l'industrie ".Atelier "Écosystème de communication" dirigé par le National Institute of Standards and Technology (NIST) comme première étape de ce processus. L'atelier s'est déroulé dans le cadre de Règles de Chatham House. Les participants ont été encouragés à partager les opinions et les informations présentés à l'atelier, mais il leur a été demandé de s'abstenir d'identifier les orateurs ou leurs l'affiliation. Conformément aux règles, le présent rapport n'associe pas les questions soulevées dans le cadre de l'enquête de l'Union européenne atelier avec des organisations ou des secteurs industriels.

L'atelier a complété plusieurs volets de travail menés simultanément par différentes composantes des ministères pour engager les parties prenantes et identifier les actions appropriées, y compris une demande pour les commentaires publiés par l'Administration nationale des télécommunications et de l'information (National Telecommunications and Information Administration) (NTIA)[3] et du département de la sécurité intérieure (DHS) pour la sécurité nationale et la protection de l'environnement Conseil consultatif des télécommunications (NSTAC). [4]

Le compte rendu se compose de cinq éléments principaux : cette introduction, un bref rappel de l'histoire de l'Union européenne et de son histoire. le processus employé pour organiser l'atelier et élaborer le compte rendu ; un atelier résumé mettant en évidence les thèmes communs de l'atelier ; impacts anticipés par la les informations obtenues des participants à l'atelier sur le projet public du rapport qui Commerce et le DHS publieront en janvier 2018 ; et les possibilités d'un engagement continu sur les questions suivantes ce sujet.

[2] Le texte intégral du décret est disponible à l'adresse https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

[3] La National Telecommunications and Information Administration (NTIA) a publié la "Request for Comments on Promouvoir l'action des parties prenantes contre les botnets et autres menaces automatisées" le 8 juin. Informations supplémentaires, notamment les commentaires publics reçus par la NTIA sont disponibles à l'adresse suivante : https://www.ntia.doc.gov/federal-register-notice/2017/rfc-. promouvoir l'action des parties prenantes contre les réseaux de robots et autres menaces automatisées.

[4] Pour de plus amples informations sur le NSTAC, veuillez consulter le site https://www.dhs.gov/national-security-telecommunications-advisory-. comité.

2. Planification, exécution et analyse des ateliers

Planification de l'atelier

Immédiatement après l'émission de l'E.O. 13800, et parallèlement à ces efforts, le NIST a commencé à planifier un atelier public, en collaboration avec nos partenaires de la NTIA et du DHS, en tant qu'une étape initiale vers l'engagement des parties prenantes dans l'élaboration du rapport. L'atelier était conçu pour permettre aux parties prenantes d'explorer de manière ouverte et transparente une série de questions actuelles et futures les solutions émergentes visant à renforcer la résilience de l'écosystème de l'internet et des communications (la écosystème) contre les menaces automatisées et distribuées. L'atelier a été annoncé le 6 juin 2017 avec seulement cinq semaines d'avance pour s'assurer que les contributions puissent être reflétées dans le rapport de Janvier projet public. Malgré le délai, l'atelier a rapidement enregistré une inscription complète de 150 personnes participants représentant diverses communautés de parties prenantes. L'équipe de planification de l'atelier apprécie tout particulièrement les nombreux aménagements réalisés par nos panélistes, nos orateurs et notre personnel les facilitateurs à participer étant donné le court délai et les perturbations inattendues des voyages aériens. [5]

Aperçu de l'atelier

L'ordre du jour était structuré comme une série de panels modérés et de sessions en petits groupes explorant les thèmes suivants contributions potentielles des cinq principales communautés de parties prenantes : infrastructure de communication les fournisseurs, les développeurs de produits, les clients, les chercheurs et les gouvernements. En plus d'offrir les groupes de discussion avaient pour but de stimuler la discussion en petits groupes. sessions. Les animateurs des groupes de discussion ont été chargés d'orienter la discussion vers l'identification d'un large éventail d'objectifs de développement durable une gamme d'options pour une communauté spécifique de parties prenantes (par exemple, les fournisseurs d'infrastructures, les fabricants de produits, etc. développeurs, ou propriétaires de réseaux) pour améliorer la résilience de l'écosystème face à l'automatisation menaces distribuées. Il a été demandé aux animateurs de reporter la discussion sur les options spécifiques à d'autres pays à la session appropriée, mais la discussion mettant en évidence les dépendances entre les actions possibles des différentes communautés de parties prenantes ont été encouragées. Les facilitateurs étaient que les participants aux groupes de discussion ne sont pas tenus de parvenir à un consensus sur un point particulier ou établir un ordre ou un ordre de priorité de ces options.

Analyse et préparation de la procédure

Le National Cybersecurity Center of Excellence (NCCoE) du NIST a fourni des informations sur la cybersécurité d'experts en la matière (PME) pour servir de scribes aux séances en petits groupes et a effectué la première évaluation de l'impact de l'événement l'analyse technique des contributions collectées. Environ 787 contributions ont été classées dans les catégories suivantes dix catégories principales ; 313 contributions ont également été classées dans l'une des cinq catégories suivantes catégories mineures orthogonales.

[5] Voir https://www.washingtonpost.com/news/dr-gridlock/wp/2017/07/10/hazmat-incident-at-air-traffic-control-center-delays-vols-autour-de-la-région-de-washington/?utm_term=.d009260f400e.

Les principales catégories étaient les suivantes :

- Sensibilisation
- Les défis de l'entreprise
- Développement et cycle de vie des produits
- Complexité de l'écosystème
- Rôle du consommateur
- Gouvernance
- Partage de l'information, collaboration et confidentialité
- Données
- Métriques
- Technologies fondamentales et émergentes

Les scribes ont classé les sujets de discussion soulevés lors de leurs sessions en petits groupes selon les critères suivants catégories, et des pourcentages agrégés ont été élaborés. La répartition des 787 contributions est représentée dans la figure 1, ci-dessous. Près de la moitié des contributions ont été qualifiées d'entreprises des défis ou des problèmes de gouvernance.

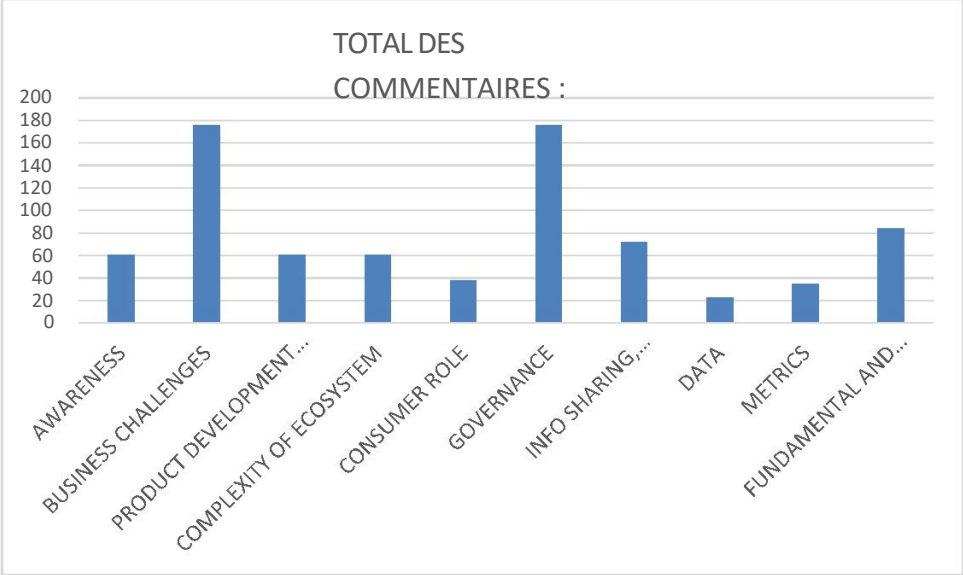

Figure 1. Distribution des contributions telles que caractérisées par les scribes

Les catégories mineures étaient :

- Adversaires
- Communication
- Cybersécurité
- Leçons et meilleures pratiques
- Normes

Les scribes ont classé les sujets de discussion soulevés lors de leurs sessions en petits groupes selon les critères suivants des catégories mineures, et des pourcentages agrégés ont été élaborés. La répartition des 313 est illustré dans la figure 2 ci-dessous. Plus de la moitié des commentaires attribués aux contributions mineures les catégories suivantes ont été jugées comme des questions de cybersécurité, avec les leçons apprises, la communication et les questions de sécurité. Les normes de l'Union européenne ont recueilli l'essentiel des commentaires restants.

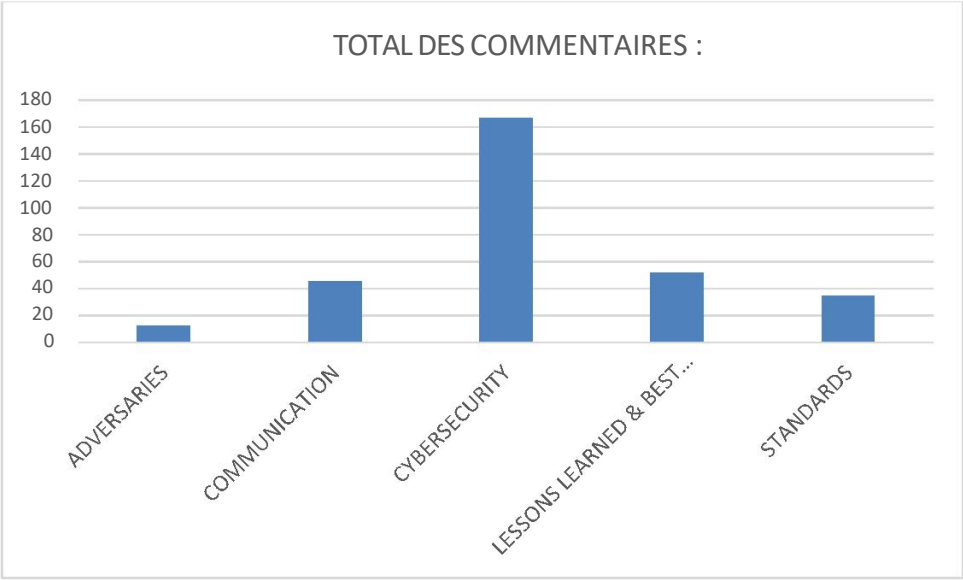

Figure 2. Caractérisation des contributions selon les domaines thématiques mineurs

Les experts du NIST ont basé cette procédure sur les notes brutes fournies par le NCCoE.
les scribes, les listes à puces des points saillants préparées par les scribes, et l'analyse fournie par le NCCoE, en tant que ainsi que les notes personnelles des PME du NIST.

3. Résumé de l'atelier

Cette section résume les questions soulevées par les présentateurs et les participants à l'atelier au cours de l'atelier au cours de l'atelier et est présenté en deux sous-sections.

- La première sous-section présente six thèmes primordiaux qui ont émergé des discussions. Ces thèmes s'appliquent à de multiples secteurs et ont été soulevés par différents participants lors des réunions suivantes à de multiples occasions. Bien que le consensus n'ait pas été jugé et ne doive pas être présumé, quelques s'est prononcé contre ces concepts.

- La deuxième sous-section offre des informations sectorielles (c'est-à-dire spécifiques à une communauté de parties prenantes) questions et observations. Dans certains cas, il s'agit d'une vue plus détaillée de la situation de l'entreprise mais dans d'autres, les concepts sont simplement uniques à ce secteur. Le site les observations sectorielles sont organisées par panel d'ateliers.

Bien que l'atelier ait porté sur l'ensemble des menaces distribuées automatisées, il convient de noter que a noté que la conversation portait souvent sur l'Internet des objets. Il était clair que le Mirai a été une priorité pour de nombreux participants et a fourni un contexte commun pour les discussions sur les questions suivantes la sécurisation du cycle de vie des produits, l'éducation et la sensibilisation, et bien d'autres sujets. Le contexte de l'IdO est seulement réitéré dans les résumés qui suivent lorsque les questions ou les observations étaient spécifiques à l'UE IoT (par opposition à un cadrage illustratif.)

Comme indiqué précédemment, l'atelier a été mené selon les règles de Chatham House, et les animateurs ont été invités à se concentrer sur la mise en évidence des options d'action plutôt que sur l'obtention d'un consensus ou d'un accord. obtenir des mesures objectives de soutien. Ce résumé utilise les expressions "plusieurs participants", "un certain nombre de participants" et "de nombreux participants" pour indiquer notre évaluation subjective de la situation des niveaux croissants de soutien ou d'intérêt au-delà de la ligne de base normale.

Thèmes primordiaux

Six thèmes primordiaux ont été rencontrés tout au long des discussions de l'atelier6 :

1. La nature globale du problème ;
2. La disponibilité d'outils efficaces ;
3. L'importance de la sécurisation des produits tout au long de leur cycle de vie ;
4. L'impact des lacunes en matière d'éducation et de sensibilisation ;
5. Conflits entre les incitations du marché et les objectifs de résilience ; et
6. La nécessité d'une action intersectorielle coordonnée.

Les participants à l'atelier ont noté à plusieurs reprises que les botnets et les menaces distribuées sont un problème mondial. Bien qu'il y ait des exceptions, la majorité des appareils compromis qui constituent les botnets sont les suivants situés géographiquement en dehors des États-Unis. Actions visant à renforcer la sécurité des appareils vendues aux États-Unis, ou qui protègent contre les menaces provenant des télécommunications domestiques

[6] Il convient de noter que les participants à l'atelier n'ont pas convenu de ces thèmes ni établi de priorité. Par conséquent, l'ordre des six thèmes est le suivant non significatif.

de la circulation, ne peut traiter qu'une partie du problème. Action coordonnée avec les partenaires internationaux sera nécessaire pour accroître la résilience de l'écosystème face à ces menaces. Bien que la resolution exigera une approche globale, il y a eu un large consensus sur le fait que les États-Unis pourraient et doit montrer la voie dans la lutte contre ces menaces, en montrant l'exemple et en promouvant l'égalité des chances des normes de comportement appropriées.

Un large consensus s'est également dégagé sur les possibilités d'action immédiate. Pour citer un intervenant a déclaré : "Nous ne partons pas d'une feuille blanche". En appliquant une série de mesures bien Grâce à des outils, des processus et des pratiques connus et efficaces, nous pouvons améliorer de manière significative la résilience de l'industrie de la pêche de l'écosystème. Ces outils ont prouvé leur valeur dans le domaine de l'informatique personnelle. Cependant, ces technologies et processus ne sont pas inclus dans les pratiques communes pour les produits le développement et le déploiement dans de nombreux autres secteurs. Un ensemble (ou plusieurs ensembles) de normes minimales ou doit être établi, même si ce n'est peut-être pas de manière formelle, afin de garantir que les meilleures pratiques sont appliquées dans tous les secteurs.

Traiter l'ensemble du cycle de vie du produit/réseau avec ces outils, processus et pratiques était un autre thème dominant. L'importance d'intégrer la sécurité dès le début, plutôt que d'en faire une priorité plutôt que de le boulonner plus tard, était une croyance largement partagée. Beaucoup trop de produits sont livrés avec des vulnérabilités connues ; ces produits peuvent être détectés, attaqués et compromis dans les délais suivants quelques minutes après le déploiement. Des mécanismes de mise à jour sécurisés sont nécessaires pour remédier aux vulnérabilités découverts pendant la durée de vie normale du produit. Des processus clairs et efficaces pour traiter les problèmes de fin de de vie sont également nécessaires, car les vulnérabilités des produits obsolètes ne peuvent être traitées, ce qui garantit que les adversaires disposent d'un point de départ fiable lorsqu'ils pénètrent dans une entreprise ou établissent une botnet.

Les participants ont noté un problème systémique d'éducation et de sensibilisation. Près de 6 % des Les recommandations/commentaires formulés lors des séances de travail de l'atelier ont mis l'accent sur l'importance des éléments suivants l'éducation et la sensibilisation. De nombreux participants ont cité la sécurité des transports, où le port de la ceinture de sécurité et l'éducation à la sécurité sont des éléments essentiels. Les résultats des crash-tests ont conduit à de meilleurs résultats, comme une réussite en matière d'éducation et de sensibilisation. D'autres ont cité le même secteur comme un exemple à suivre, avec de longs délais d'exécution avant la généralisation de l'utilisation de l'Internet l'acceptation des ceintures de sécurité et d'autres améliorations technologiques. Energy Star a également fait l'objet de discussions répétées, avec des mesures simples pour les consommateurs. Un organisme indépendant pour tester et certifier les caractéristiques liées à la sécurité et offrir un système de notation plus accessible, a été fréquemment citée comme une étape importante vers l'identification par les consommateurs de produits dotés de solides caractéristiques de sécurité.

Les incitations du marché perçues ne sont pas en phase avec nos objectifs de sécurité et de résilience, selon de nombreux participants à l'atelier. Les développeurs et les vendeurs de produits minimisent 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. Une grande partie de la discussion a porté sur les techniques visant à créer des incitations au marché, telles que la certification indépendante des produits, mais certaines estimaient qu'une intervention plus active du gouvernement (par exemple, une réglementation) serait éventuellement nécessaire pour surmonter les défaillances du marché. Cependant, les participants ont noté que la conformité réglementaire peut également être à en contradiction avec nos objectifs de sécurité et de résilience. [7]

[7] Par exemple, un certain nombre de participants ont cité une réticence historique du secteur des soins de santé à appliquer des correctifs aux dispositifs médicaux afin d'éviter le renouvellement de la certification par la Food and Drug Administration. Notez que les directives actuelles de la FDA traitent de cette question, en autorisant des correctifs sans exiger une nouvelle certification dans certains cas. Voir "Gestion post-commercialisation de la cybersécurité dans le secteur médical".

Un autre thème est l'incapacité d'un secteur particulier à avoir un impact sur la résilience de l'écosystème. de manière isolée. Les fournisseurs d'infrastructures peuvent améliorer l'efficacité des mécanismes anti-DDoS, mais ils peuvent toujours être surmontés par un plus grand nombre de dispositifs. Les fabricants de dispositifs peuvent améliorer la qualité de leurs produits, mais nous ne disposons pas de la technologie nécessaire pour construire des produits parfaits. Ainsi, certains appareils seront toujours vulnérables à la compromission. De même, les propriétaires d'entreprises peuvent augmenter leurs investissements en matière de sécurité mais certains de leurs systèmes seront vulnérables, et les adversaires disposent de tout l'Internet pour lancer des attaques contre l'entreprise. Les chercheurs peuvent développer de meilleures technologies, mais les améliorations de la sécurité ne sont réalisées que si les fournisseurs incluent ces les technologies dans les produits, les clients achètent ces produits et les déploient de manière appropriée. Des contributions de tous les secteurs seront nécessaires pour augmenter de manière significative la résilience de l'UE contre les botnets et les menaces distribuées automatisées.

Résumés par secteur

Cette section passe en revue les questions et les observations de l'atelier du point de vue de chacun des groupes suivants communauté des parties prenantes à tour de rôle. Dans certains cas, il s'agit d'une vision plus détaillée ou plus nuancée de la situation les thèmes généraux, mais dans d'autres, les concepts sont simplement uniques à ce secteur.

Infrastructure

Le secteur des fournisseurs d'infrastructures a fait l'objet du premier panel de l'atelier et des éléments suivants session en petits groupes. Le panel s'est concentré sur l'état actuel de l'infrastructure, les tendances, et l'état actuel de l'industrie et des approches prometteuses pour atténuer les menaces distribuées automatisées telles que les DDoS, avec un accent particulier sur les botnets et l'IoT.

Plusieurs participants ont fait remarquer que l'infrastructure de l'Internet est beaucoup plus résiliente aujourd'hui, et que résiste presque quotidiennement à des attaques par déni de service distribué (DDoS) d'une ampleur inimaginable auparavant. Ce site démontre à la fois l'efficacité des outils actuels et la nature de la course aux armements des DDoS protection.

Les participants ont explicitement identifié un certain nombre d'outils et de techniques pour la protection contre les DDoS, à savoir énumérés ci-dessous avec une brève discussion sur leurs points forts et leurs limites. (L'ordre de présentation n'a pas signification.)

- Filtrage entrée/sortie : De nombreux participants ont fait référence à l'Internet Engineering Task Force (IETF) Best Current Practice (BCP) 38, "Network Ingress Filtering", et BCP 84, "Ingress Filtering for Multi-Homed Networks". Historiquement, les attaques DDoS se sont appuyées sur l'usurpation d'adresse réseau, lorsque des systèmes compromis revendiquent des adresses sources qui ne sont pas n'existent pas sur le réseau local, afin de cacher l'emplacement des ressources des attaquants. [8] Par le trafic le filtrage aux frontières de l'entreprise et le rejet du trafic qui est clairement illégitime, il est possible de limiter l'efficacité et la portée de ces attaques.

Appareils",
https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[8] Certaines attaques DDoS récentes, comme celle de Mirai, ont revendiqué des adresses sources légitimes.

Le BCP 38 et le BCP 84 ont été publiés en 2000 et 2004, respectivement, mais leur adoption et leur mise en œuvre n'ont pas eu lieu. Le déploiement a été lent et inégal. Alors que le niveau de soutien actuel a fait l'objet d'un débat lors de la conférence de l'atelier, le déploiement omniprésent du filtrage du trafic a reçu un large soutien pour les réseaux de périphérie. Une brève discussion a eu lieu sur les limites du filtrage dans le cadre de l'initiative de l'Union européenne pour la protection de l'environnement dorsale de l'internet, où le routage asymétrique (où le trafic entre deux points terminaux suit des chemins séparés dans chaque direction) complique la différenciation du trafic légitime de celui avec des adresses réseau usurpées.

- Services de protection DDoS hors site : Les FAI offrent une protection DDoS hors site pour les clients, où le trafic est rerouté et filtré avant d'être acheminé vers le site de l'entreprise réseau du client. Les services de protection contre les dénis de service distribué (DDoS) nécessitent le provisionnement d'importantes ressources supplémentaires des ressources (en termes de systèmes spécialisés et de bande passante supplémentaire) pour absorber et traiter les données de l'enquête le trafic supplémentaire prévu. Ces services se sont avérés efficaces dans de nombreux cas, mais les prestataires de services sont continuellement obligés d'augmenter le niveau des ressources supplémentaires au fur et à mesure que les botnets s'agrandissent et la bande passante totale des attaques augmente.

  L'efficacité de ces services est limitée en partie par la sensibilisation des clients. DDoS les services de protection nécessitent la mise à disposition de ressources supplémentaires importantes (en termes de systèmes spécialisés et bande passante supplémentaire), ils ne figurent donc pas dans le réseau de base les offres de services. Les clients peuvent ne pas être conscients des risques présentés par les attaques DDoS jusqu'à ce qu'ils deviennent des victimes, ou que ces services soient même disponibles. Même lorsqu'une l'entreprise a la connaissance et la volonté de se procurer des services anti-DDoS, l'architecture des modifications peuvent être nécessaires pour optimiser le niveau de sécurité atteint.

  (Note : Les communications entre les clients et les fournisseurs de services présentent une autre défi à l'efficacité des services de protection contre les attaques DDoS hors site. Voir Temps réel signalisation, ci-dessous).

- Protection DDoS sur site : Les attaques DDoS sont conçues pour cibler le site de l'entreprise les ressources critiques, telles que les applications clés ou le pare-feu de l'entreprise, la protection locale peuvent être plus efficaces. Ces services "sur site" sont désormais disponibles en tant que services de gestion de l'information complément aux services traditionnels de protection DDoS des fournisseurs de services (hors site) proposés par les FAI. Comme indiqué ci-dessus, la sensibilisation des clients aux risques et aux technologies disponibles est essentielle nécessaire comme préalable à l'amélioration de la résilience grâce à ces technologies.

- Signalisation en temps réel : Comme indiqué ci-dessus, les communications avec les services de protection contre les DDoS et les pendant les attaques peut être problématique. Plusieurs participants ont mis en avant l'Internet Le groupe de travail DDoS Open Threat Signaling (DOTS) de l'Engineering Task Force a été créé en tant que groupe de travail sur les menaces ouvertes source prometteuse de solutions dans un avenir proche. Le DOTS développe actuellement une suite des normes pour la signalisation en temps réel de la télémétrie liée aux DDoS et le traitement des menaces sur des liens qui peuvent être encombrés par des attaques de trafic.

Les participants ont également souligné un certain nombre de défis spécifiques aux approches basées sur les infrastructures pour améliorer la résilience de l'écosystème.

- Coordination mondiale : L'Internet est une infrastructure mondiale, tout comme la menace. Les approches fondées sur les infrastructures exigent une coopération et une coordination étroites. Participants

a indiqué que la coopération entre les pairs nationaux est devenue assez solide, mais la
La communication et la coopération internationales ont été inégales. Des efforts sont
déployés pour établir des normes et codifier les pratiques, mais ces efforts sont à la traîne du problème.
Les participants ont noté que près de cinquante entreprises ont accepté les normes mutuellement convenues pour la sécurité du routage (MANRS), et cet accord pourrait être considéré comme un modèle de effort spécifique aux botnets. D'autres ont cité le code de conduite anti-bot des États-Unis pour l'Internet fournisseurs de services (ABC pour les ISP) élaborés par la Federal Communications Conseil de la Commission sur la sécurité, la fiabilité et l'interopérabilité des communications ("CSRIC"). [9]

- Complexité : Les problèmes d'infrastructure sont exacerbés par la complexité croissante de l'infrastructure. Internet - pas seulement l'avènement de l'IoT, mais aussi l'expansion de l'infrastructure multi-tenant. Les normes et les pratiques qui sont largement appliquées aux PC et aux serveurs n'ont pas été appliqué uniformément à l'espace IoT, avec des conséquences malheureuses, et les petits FAI ne n'ont pas la capacité de mettre en œuvre les mêmes normes et pratiques que les grands ISP. Même lorsqu'une entreprise a la connaissance et le désir de se procurer des services anti-DDoS, des modifications architecturales peuvent être nécessaires pour optimiser le niveau de sécurité atteint.

- Métriques : Il n'existe pas de paramètres utilisables pour caractériser les attaques et documenter leur gravité. Un participant a fait remarquer que le Federal Bureau of Investigation avait mis au point un système de 75 cadre d'attributs pour décrire les attaques distribuées, mais que compléter cette description ont pris tellement de temps que les attaques étaient souvent terminées. Les métriques utilisables et largement reconnues sont nécessaire pour faciliter la coordination et la coopération.

- Interdépendances : Les participants ont noté un certain nombre de dépendances avec d'autres secteurs. Faible Les attributs de sécurité des dispositifs périphériques, et en particulier des dispositifs IoT, font qu'il est extrêmement difficile d'assurer la sécurité de ces dispositifs difficile pour l'infrastructure de se protéger contre ces attaques.
- Éducation et sensibilisation : Il est urgent d'éduquer et de sensibiliser les clients, lorsque les FAI contactent les entreprises pour les alerter des problèmes, mais les entreprises sont souvent mal équipées de comprendre le problème ou de s'acquitter de leurs propres responsabilités. Ils assument généralement que leur fournisseur d'accès "allait s'occuper de ça", quoi que ça puisse être.

- L'éducation et la sensibilisation du personnel opérationnel ont également été jugées problématiques. Sur le site en particulier, certains ont estimé qu'un faible déploiement du filtrage BCP 38 chez les FAI étrangers, les petits les FAI nationaux et les routeurs BGP maintenus par les entreprises était en grande partie le résultat de lacunes dans les compétences au sein de ces organisations.

Fabricant du produit

La deuxième table ronde et la séance en petits groupes ont permis d'explorer les efforts actuels et les possibilités futures en matière de

[9] Conseil pour la fiabilité et l'interopérabilité de la sécurité des communications (CSRIC) III, Code de conduite anti-bot (ABC) des États-Unis pour l'utilisation de l'Internet. Fournisseurs d'accès à Internet (FAI), Rapport final, GT 7 (mars 2012),

http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

les fabricants de composants de réseau et de dispositifs (y compris les fournisseurs de solutions IoT) pour répondre à la les causes profondes des récents botnets (accès illimité au réseau, mots de passe codés en dur et bogues logiciels). La discussion a porté sur des produits développés tant pour les entreprises que pour les particuliers.

Il existe deux caractérisations générales du problème du développement de produits. La plus
La caractér caractér caractér caractér caractérisation prévalence a indiqué que le nombre de vulnérabilités dans les produits doit être considérablement réduit pour qu'il soit plus difficile de compromettre des dispositifs en masse et de lancer des attaques de grande envergure.

D'un autre côté, les produits ne seront jamais parfaits, aussi certains participants ont-ils estimé que nous devions se concentrer sur les technologies qui limitent les dommages causés par les dispositifs compromis. Les deux ne sont pas en conflit, et la plupart semblent penser que les deux voies doivent être poursuivies.

Pour ce qui est de rendre plus difficile la compromission des systèmes, de nombreux participants ont souligné que cela était un problème lié au cycle de vie des produits. Il est crucial, selon eux, de gérer la vulnérabilité des depuis l'expédition initiale du produit, en passant par son utilisation, jusqu'à sa fin de vie.

Un certain nombre de techniques qui réduire la vulnérabilité des produits ont été discutés :

- Afin de réduire la vulnérabilité des produits lors de leur déploiement initial, les participants ont propose l'application accrue d'un certain nombre d'outils et de meilleures pratiques complémentaires. Pour exemple, les processus de développement sécurisés par la conception sont plus susceptibles d'aboutir à des défaillances qui sont généralement sécurisés et évitent les mots de passe administratifs codés en dur et les d'autres écueils courants. Les chaînes d'outils de développement de logiciels sensibles à la sécurité peuvent éliminer les erreurs de codage courantes, telles que la plupart des débordements de mémoire tampon.
- Même lorsqu'ils sont développés à l'aide de méthodologies de conception sécurisée et de méthodes axées sur la sécurité les chaînes d'outils, les vulnérabilités dans les logiciels sont susceptibles d'être détectées, ce qui se poursuit pendant des mois ou des années après le premier déploiement du produit. Les logiciels malveillants ciblant ces vulnérabilités sont souvent largement disponibles quelques jours ou se maines après leur détection. Pour gérer la vulnérabilité de ces de nombreux participants ont affirmé qu'une mise à jour sûre et, de préférence, automatique, était necessaire absolument indispensable. En outre, ils ont affirmé que les fabricants devraient s'engager à la correction des failles de sécurité pendant une période minimale après le déploiement.
- Les racines de la confiance sont une technologie complémentaire qui a été citée par de nombreux participants. En fournissant un ensemble de fonctions de base et hautement fiables, nous pouvons augmenter l'assurance que le logiciel et le micrologiciel sont inchangés ou n'ont été modifiés que par une mise à jour sécurisée mécanismes. Le module de plateforme de confiance (TPM) est un exemple largement répandu, mais...peut être trop coûteux pour les appareils peu coûteux. De nouveaux efforts, tels que le Trusted Computing (TCG), le Device Identity Composition Engine (DICE) peut étendre le champ d'application de la norme DICE les produits qui intègrent ces technologies en fournissant une base pour l'identité des dispositifs et la protection des données vérifier que les mises à jour logicielles ont été installées. Les appareils ont besoin d'une identité délivrée par le fabricant afin qu'il y ait un moyen de savoir de quel type d'appareil il s'agit et quelle est sa configuration, les logiciels et les correctifs sont destinés à l'appareil. Le projet de publication NIST SP 800-193 du 30 mai 2017 décrit les racines de la confiance pour la protection, la détection et la récupération qui pourraient être appliquées dans l'espace IoT en tant que blocs de construction pour récupérer des appareils à distance. Personnes sont peu susceptibles de gérer individuellement les dispositifs IoT, d'où la nécessité d'une récupération automatisée.

Dans de tels cas, les mises à jour ne sont plus diffusées (ou peut-être ne l'ont-elles jamais été), de sorte qu'il n'est plus possible de les utiliser.
les vulnérabilités persistent indéfiniment. Ceci a des parallèles avec les logiciels sans licence, où les mises à jour de sécurité ne sont généralement pas disponibles.
Les participants ont salué la décision de Microsoft de mettre à jour Windows XP afin d'atténuer les effets du WannaCry, malgré l'arrêt de la prise en charge trois ans auparavant, mais a estimé qu'il s'agissait d'une un cas exceptionnel. Les participants ont considéré que les propositions antérieures de solutions générales à la fin de vie problèmes, comme la diffusion de logiciels pour des produits non pris en charge dans le cadre de l'open source communauté, comme peu pratique.

Les participants ont noté que les techniques ci-dessus sont largement connues et bien comprises. Elles sont appliquée largement dans certains secteurs (par exemple, les systèmes d'exploitation), mais presque jamais dans d'autres (par exemple, la l'internet des objets). Un certain nombre d'obstacles et de causes profondes ont été suggérés, notamment :

- Éducation et sensibilisation des consommateurs : Les fabricants de produits sont motivés par les ventes, et les consommateurs n'ont pas le recul nécessaire pour donner la priorité à la sécurité ou la capacité à identifier les produits présentant une plus grande assurance. Les consommateurs peuvent ne pas être naturellement motives de choisir de tels produits, étant donné que les produits compromis continuent souvent à être performants leur fonction donnée tout en participant à des attaques distribuées. L'éducation des consommateurs devrait se concentrer sur les implications potentielles en matière de sécurité et de performances plutôt que sur les botnets la prévention - les utilisateurs ne se soucient peut-être pas de savoir si leur nanny cam attaque une grande banque, mais ils s'en soucient sur les étrangers qui envahissent la vie privée de leur famille.

  Une fois motivés, les consommateurs auront encore besoin d'aide pour sélectionner les produits qui sont susceptibles de présentent moins de vulnérabilités tout au long du cycle de vie du déploiement. Aucun mécanisme satisfaisant pour transmettre aux consommateurs des informations sur la sécurité des produits existe aujourd'hui Energy Star pour l'efficacité énergétique et le National Highway Traffic Safety Les notes de sécurité 5 étoiles de la NHTSA pour la sécurité des véhicules ont été citées comme suit des exemples importants et réussis.

- Éducation et sensibilisation des développeurs de produits : L'espace entre les technologies de l'information et les lignes de produits s'estompent, l'éducation des développeurs de produits en matière de sécurité est devenue une urgence besoin. Les concepteurs d'appareils électroménagers savent comment conserver les aliments à une température sûre température, nettoyer des tissus ou griller du pain. Au fur et à mesure que ces produits font partie de la nous demandons à ces concepteurs d'intégrer de nouvelles exigences en matière de sécurité qui leur sont étrangères. En particulier, l'industrie doit reconnaître que la mise à jour sécurisée les mécanismes sont nécessaires pour "tout".
- Inadéquation avec les incitations du marché : De nombreux développeurs de produits ont peur que l'investissement en matière de sécurité rendront leurs produits plus chers et retarderont le déploiement de l'innovation de nouvelles fonctionnalités qui permettent de gagner des parts de marché. Les grands fournisseurs ont un système de développement plus robuste mais les startups et les petites entreprises s'appuient souvent sur des processus moins matures.
- Responsabilité peu claire : Une discussion a également eu lieu concernant la responsabilité – qui devrait être responsable de la sécurité des produits ? Les propriétaires ? Les vendeurs ? Pour les utilisateurs privés et les petites entreprises, il semble peu pratique de les tenir pour responsables si leur DVR domestique ou leur la caméra de sécurité de leur magasin est compromise et ajoutée à un botnet.

Pour les utilisateurs industriels, nous pouvons peut-être avoir des attentes plus élevées, mais à mesure que les dispositifs IoT se multiplient il peut y avoir des limites là aussi. Dans les deux environnements, les protocoles tels que le description de l'usage du fabricant (MUD, voir la segmentation du réseau virtuel ci-dessous) peut contribuer à transférer une partie de la responsabilité aux fabricants de manière évolutive.

Le second point de vue est que les produits ne seront jamais parfaits et que les incitations ne sont tout simplement pas suffisantes se concentrer sur la sécurité. Cela renforce l'idée que la mise à jour sécurisée est un élément fondamental de la sécurité mais nous devons également trouver des moyens de limiter les dommages causés par les dispositifs compromis. Plusieurs directions à suivre ont été proposées, notamment

- Segmentation des réseaux virtuels : Historiquement, les systèmes connectés à l'Internet ont bénéficié une connectivité totale au niveau des couches réseau et transport. [10] Les besoins des utilisateurs humains sont imprévisible, de sorte qu'il serait impossible de gérer le trafic en le limitant de manière significative. La sécurité les implications d'une connectivité totale sont importantes : tout dispositif sur Internet peut être utilisé pour lancer une attaque sur n'importe quel autre appareil ; une fois compromis, l'appareil devient un outil de lancement pour les mouvements latéraux à l'intérieur de l'entreprise et les attaques sur d'autres sites Internet les appareils connectés. Avec l'émergence de l'Internet des objets (IoT), les communications besoins de nombreux appareils deviennent plus prévisibles et les implications en matière de sécurité d'un système complet de gestion de la sécurité sont plus importantes connectivité inacceptable. Par exemple, un thermostat IoT peut avoir besoin de communiquer...avec le site web du fabricant pour les mises à jour mais n'a probablement pas besoin de communiquer avec une bourse de valeurs.

  La norme MUD actuellement en cours d'élaboration au sein de l'IETF offre une voie potentielle. avant. Lorsque des périphériques rejoignent le réseau, ils demandent une adresse IP par le biais de la fonction Dynamic Protocole de configuration des hôtes (DHCP). Lorsqu'il utilise MUD, l'appareil indique également comment d'obtenir en toute sécurité une description des exigences de communication de l'appareil auprès dufabricant. Les fournisseurs d'équipement de réseautique tirent parti du fichier MUD et de leurs systèmes de gestion de réseau existants.
  la possibilité d'appliquer le filtrage des paquets sur une base individuelle. S'il est compromis, l'attaquantne pourrait pas utiliser le thermostat IoT pour se déplacer latéralement dans la cafetière ou attaquer la bourse.
- La signalisation des menaces offre une autre approche pour limiter l'accès au reseau Troisièmement. Les services de tiers identifient les systèmes ou domaines hôtes qui présentent une menace relative pour le système d'information écosystème (ou un secteur de l'industrie). Cette information est transmise aux abonnés les réseaux d'entreprise, qui établissent des filtres de route appropriés et rejettent les données potentiellement dangereuses trafic nuisible. Bien que MUD soit conçu pour prendre en charge des dispositifs avec des caractéristiques bien définies, il n'y a pas d'autre solution de communication, la signalisation des menaces renforce la sécurité des données personnelles des dispositifs informatiques ayant des besoins de communication déterminés par l'utilisateur (et imprévisibles).

Clients : Entreprises, particuliers et administrations

La troisième table ronde et la séance de travail ont permis d'examiner comment les clients, en particulier dans les entreprises, peuvent les deux se protègent contre les attaques distribuées - y compris les DDoS, les attaques sur les systèmes critiques et les attaques contre la sécurité.

[10] Par la suite, les administrateurs réseau ont pu limiter l'accès par des règles de pare-feu s'appliquant à toute l'entreprise. généralement aucune limitation au sein de l'entreprise.

et la fraude - et éviter de faire partie du problème. Les participants ont été invités à mettre en évidence les capacités et les limites des meilleures pratiques actuelles et des technologies émergentes, et considérer le potentiel de collaboration intersectorielle.

De nombreux participants ont réparti les clients en trois grandes catégories : les utilisateurs privés, les entreprises et les particuliers gouvernement. Dans certaines discussions, les entreprises ont été différenciées en fonction de leur taille - soit en tant que grandes entreprises, soit en tant que petites entreprises par rapport aux petites et moyennes entreprises (PME), ou les start-ups par rapport aux entreprises établies. Les participants avaient des attentes très différentes pour les différentes catégories de clients en termes de la sensibilisation, les meilleures pratiques, l'applicabilité des technologies et la collaboration.

Les participants ont identifié un certain nombre de meilleures pratiques actuelles et émergentes :

- Comme indiqué précédemment, de nombreux participants ont identifié une mise à jour sécurisée pour tous les appareils en réseau, incluant à la fois un mécanisme de mise à jour approprié et un engagement du fournisseur à fournir comme la meilleure pratique actuelle la plus importante. Les détails d'une le mécanisme de mise à jour dépendait du client visé. Par exemple, les participants a suggéré que les utilisateurs domestiques ne bénéficieraient d'une mise à jour sécurisée que si le mécanisme était automatique et sans surveillance. Les grandes entreprises exigeraient un niveau de contrôle plus élevé grâce à des outils de gestion centralisés. Les besoins et les attentes des PME pourraient varier en fonction de l'architecture et de l'expertise du réseau.

- Le partage d'informations en temps réel a été identifié comme une meilleure pratique actuelle pour le gouvernement et les grandes entreprises. Le partage de l'information, tant au sein de l'entreprise qu'à travers le écosystème, permettra aux entreprises de mieux protéger les ressources. Les participants ont observé que les acteurs malveillants sont meilleurs que nous dans ce domaine.

  Cependant, les informations doivent être partagées sous une forme exploitable, plutôt que sous forme non formatée texte. Il existe de multiples solutions actuellement disponibles pour la cybersécurité Générale le partage d'informations. En particulier, les participants ont identifié le système de menaces structurées. Information eXpression (STIX™) et Trusted Automated eXchange of Indicator (échange automatique d'indicateurs de confiance). Information (TAXII™) comme meilleure pratique actuelle. La signalisation des menaces DDoS Open (DOTS), actuellement en cours d'élaboration au sein de l'IETF, fournira une solution spécifique aux DDoS. solution.

- des architectures de réseau qui limitent les flux de trafic afin de restreindre les vecteurs d'attaque potentiels et de réduire les coûts. Les attaques contraignantes qui peuvent être lancées à partir de systèmes compromis ont également été abordées. Les technologies émergentes qui établissent des réseaux segmentés virtuels, comme le MUD (voir Fabricant de produits, ci-dessus) permettrait de fournir des informations exploitables pour les réseaux domestiques et d'entreprise de manière évolutive. Pour les anciens appareils, le reseau l'équipement pourrait tirer parti de la " signalisation des menaces " (par exemple, le partage d'informations pour identifier les menaces locales) systèmes compromis et systèmes ou domaines externes suspects) et limiter le traffic de manière appropriée.

Étant donné que la plupart des technologies nécessaires sont largement comprises, des discussions importantes ont eu lieu consacré aux obstacles perçus et aux moteurs potentiels de l'adoption.

- L'impact actuel et potentiel de la cyberassurance a été largement débattu. Expérience d'autres secteurs démontre que l'assurance peut favoriser l'adoption de technologies. Par exemple, les réductions d'assurance automobile pour les freins antiblocage et les coussins gonflables sont encouragés les consommateurs doivent donner la priorité à ces caractéristiques. L'assurance des bâtiments exige souvent que la fumée détecteurs et peuvent accorder des réductions pour les gicleurs ou d'autres mesures actives. Cependant, Les offres d'assurance cybernétique sont souvent incohérentes et il a été jugé qu'elles n'avaient que peu d'impact sur l'environnement impact à ce jour sur le déploiement des technologies de cybersécurité.
- Certains participants ont suggéré que des données actuarielles supplémentaires seront nécessaires pour positiver avoir un impact sur le marché. Une fois que les données sont disponibles pour imposer des exigences uniformes et offrir des rabais pour des options avantageuses, la cyberassurance pourrait influencer positivement les entreprises propriétaires.
- L'éducation et la sensibilisation sont un problème systémique, en particulier pour les PME et les utilisateurs à domicile. Sur en moyenne, on s'attendait à ce que les pouvoirs publics et les grandes entreprises aient une connaissance importante de la question et une connaissance relativement approfondie des exigences en matière de sécurité pour soutenir la sélection des produits et la mise en œuvre des meilleures pratiques. D'autre part, le vivier national de cybersécurité les experts ne sont pas assez nombreux pour imposer ces attentes aux PME, et les utilisateurs privés ne peuvent pas être tenus pour responsables qui devraient devenir des experts en cybersécurité.

  Alors qu'ils sont noyés sous les informations, les clients n'ont aucun moyen de différencier l'huile de serpent de l'huile d'olive des technologies efficaces. Par exemple, un participant a reçu 32 e-mails pour des produits qui a déclaré se protéger contre WannaCry le lendemain du lancement de cette attaque. Peu de les clients auraient la possibilité d'évaluer leurs réclamations, de sorte que la plupart ne prennent aucune mesure.

  Pour faciliter la prise de décisions productives en matière d'achat et de déploiement, les clients ont besoin de des données accessibles. Les participants ont souligné l'importance de la certification des produits et a débattu de l'impact des différents régimes de certification. La cote de sécurité 5 étoiles de la NHTSA et la carte de pointage ENERGY STAR du DOE ont été cités comme exemples de certification d'emballage les données sous une forme accessible. Les participants fondent de grands espoirs sur les initiatives en cours à Underwriters' Laboratories et Consumer Reports, bien que les critères de ces efforts soient les suivants n'était pas clair. Projets de démonstration du NCCoE et leurs guides de pratique associés offrent une autre option prometteuse.

- Les participants ont adopté une série de points de vue concernant les possibilités d'un système strictement volontaire l'adoption. Bien que tous les participants aient exprimé une préférence pour les mesures volontaires, il y a eu des échanges de vues entre les participants la crainte que la lenteur de l'adoption ne contraigne le gouvernement à intervenir, notamment dans les secteurs qui sont déjà réglementés. La perspective d'une réglementation au niveau de l'État était particulièrement préoccupante concernant les participants. La possibilité de 50 règlements légèrement différents serait contre-productive, compliquant l'offre de produits et de services. Toutefois, l'imposition d'exigences accrues aux entités gouvernementales elles-mêmes, pour montrer l'exemple et créer un marché initial, a été fréquemment recommandée.
- La clarté des règlements (s'ils sont imposés) a été jugée essentielle pour éviter les imprévus conséquences. Lorsqu'ils sont forcés de déduire, les obstacles réglementaires sont souvent imaginés comme des contraintes...ou empêcher la mise en œuvre de mécanismes de sécurité appropriés.

- Les participants ont également exprimé des inquiétudes quant au coût. Sans incitations gouvernementales, les coûts pour renforcer la cybersécurité doivent être répercutés sur les consommateurs. Dans un contexte économique mondial l'imposition d'exigences au niveau national peut entraver la compétitivité de l'entreprise les entreprises à l'étranger.

En résumé, les participants s'accordent à dire que des changements culturels seront nécessaires avant que les utilisateurs à domicile et les entreprises américaines maximisent leur contribution à la résilience de l'écosystème.

Recherche et université

La deuxième journée de l'atelier a débuté par le panel sur les orientations de la recherche, dont le thème était le suivant également abordé dans le cadre de la seule séance de discussion du deuxième jour, plus tard dans la matinée. L'objectif des discussions était d'identifier et d'explorer les lacunes en matière de résilience des réseaux, et mettre en évidence les possibilités de combler ces lacunes.

Les participants ont identifié un large éventail d'orientations de recherche qui pourraient avoir un impact positif sur la résilience de l'écosystème, notamment :

- Métrique et classification : Méthodes de métrique et de classification pour l'automatisation les menaces distribuées pourraient améliorer la priorisation des ressources pour les efforts d'atténuation et le droit les mesures d'exécution.

- Modélisation des botnets/DDoS : Modèles robustes pour les botnets et autres menaces automatisées qui englobant la détection, le transfert de données et l'application de la loi, pourrait permettre de mettre en place un système plus complet et des réponses coordonnées.

- Comportement des acteurs malveillants : Les changements dans le comportement des acteurs DDoS auront un impact négatif sur la l'efficacité de nombreuses techniques actuelles. Ces changements comprennent la nationalisation de l'État mafias et organisations cybercriminelles ; le passage des "ressources volées" aux "ressources criminelles" infrastructure" ; et le passage d'un trafic piloté par l'utilisateur à des systèmes automatisés/IoT. Recherche est nécessaire pour prévoir l'impact de ces changements sur les technologies anti-DDoS actuelles.

- Questions sociotechniques : La résilience, comme de nombreux aspects de la cybersécurité, a des implications sociales et techniques et ne peuvent être traitées par la seule technologie. Les participants ont souligné l'importance des approches de recherche qui tiennent compte des aspects humains, sociaux et organisationnels, facteurs économiques et techniques, et leur impact sur le déploiement et l'exploitation d'une des infrastructures résilientes. Les interfaces homme-machine (voir ci-dessous) ont fait l'objet d'une attention particulière. Des recherches sont également nécessaires pour comprendre comment concevoir des organisations plus résilientes face à une cyberattaque et plus efficaces dans leur reprise après incident ou sinistre processus.

- Interfaces homme-machine : Compte tenu de nos défis de main-d'œuvre en matière de cybersécurité, Il est urgent d'améliorer les interfaces homme-machine. La relation entre les technologies opérationnelles (par exemple, les composants SCADA) et leurs opérateurs était de un intérêt particulier. L'automatisation offre potentiellement de nombreux avantages en matière de sécurité, mais les opérateurs auront besoin d'une plus grande transparence des algorithmes avant d'accorder leur confiance décisions de la machine.

Les utilisateurs à domicile représentent un autre défi pour l'interface machine. L'ingénierie au service du comportement de l'utilisateur, plutôt que de supposer des changements improbables, peut accroître l'efficacité des technologies actuelles.

- Apprentissage automatique/intelligence artificielle (IA) : Les techniques d'apprentissage automatique et d'IA peuvent offrent de nouvelles voies pour la détection précoce et l'adaptation aux stress, y compris ceux qui sont distribués. menaces. Recherches supplémentaires sur la prise de décision par des machines, la modélisation de scénarios hypothétiques, et l'utilisation de big data (provenant de capteurs de réseaux et de systèmes) pour établir des lignes de base normales pourrait potentiellement contribuer à la résilience de l'écosystème.
- Attribution : L'attribution des incidents de sécurité informatique est problématique, et l'on peut dire que plus difficile pour les botnets et les menaces distribuées. L'identification de l'acteur malveillant et du les systèmes compromis contribueraient positivement à l'atténuation des effets des attaques, et permettre des actions de répression qui pourraient dissuader les acteurs ultérieurs.
- Preuve de l'efficacité : Comme pour d'autres aspects de la sécurité informatique, les preuves de l'efficacité des outils et des systèmes de gestion de la sécurité sont essentielles.

- Remédiation : Après avoir détecté une compromission, les utilisateurs sont souvent confrontés à des options peu appétissantes : essayer de nettoyer le système ; ou jeter l'appareil. Le nettoyage du système est souvent peu fiables ; les processus de remédiation peuvent être complexes, et les menaces persistantes avancées (APT) sont conçus pour survivre à la remédiation. La mise au rebut des dispositifs est coûteuse et peu pratique dans la plupart des scénarios. Une recherche qui rend l'assainissement plus simple et plus fiable pour les utilisateurs permettrait de clarifier ces choix et d'accroître la résilience après une compromission détectée.

- L'architecture des réseaux pour la résilience : La conception des réseaux peut avoir un impact sur la résilience, et limiter options pour les mécanismes anti-DDoS. Recherche sur la conception des réseaux afin de maximiser la résilience et la préservation des options est nécessaire.

- Une grande partie de la recherche récente sur la résilience des réseaux s'est concentrée sur l'amélioration de la visibilité des reseaux les réseaux de périphérie, mais il existe des possibilités d'exploiter les nouveaux capteurs et de faire d'Internet "plus intelligents" dans leur cœur. Pour permettre la mise en place de ces architectures de nouvelle génération, des recherches sont nécessaires pour qui identifie les types de capteurs, l'endroit où les placer, les informations à recueillir et les données à transmettre partagé, et avec qui.

Les participants ont également relevé plusieurs obstacles aux efforts axés sur la recherche visant à améliorer la résilience de l'économie. du réseau, notamment :

- Éducation et sensibilisation : La physique, la chimie et d'autres domaines scientifiques sont présentés beaucoup plus tôt dans le système éducatif des États-Unis que l'informatique en général et que la cybersécurité en particulier. Une exposition tardive au domaine limite l'intérêt, car de nombreux étudiants ont identifié un domaine d'étude avant d'entrer à l'université. Attirer davantage les meilleurs et les plus brillants aurait probablement un effet d'entraînement sur l'ensemble de la propriété intellectuelle.
- Manque de ressources monétaires : Les budgets de recherche diminuent dans les secteurs public et privé les secteurs privés. La National Science Foundation finance une partie importante des projets de l'UE la recherche fondamentale et appliquée dans ce domaine, mais le montant total des fonds disponibles est insuffisant pour financer tous les efforts de recherche prometteurs.

Gouvernement et politique publique

Le deuxième panel de la deuxième journée s'est penché sur les options des gouvernements et des politiques publiques pour améliorer la résilience de l'économie de l'écosystème. Le sujet a également été abordé, ainsi que les orientations de la recherche, dans le cadre de l'initiative la séance de discussion du deuxième jour aura lieu plus tard dans la matinée.

Comme pour les autres secteurs, les participants ont noté que de nombreuses activités en cours au sein du gouvernement et de l'industrie de l'énergie sont en cours.
politiques publiques sont déjà en cours pour améliorer la résilience de l'écosystème, notamment :

- Mesures d'application de la loi : Les organismes chargés de l'application de la loi, à tous les niveaux, poursuivent plus de les crimes liés à la cybersécurité, y compris ceux impliquant des menaces distribuées automatisées. Sur le site en particulier, les participants ont fait remarquer que le Federal Bureau of Investigation a retiré une certain nombre de botnets très médiatisés ces dernières années. Ces succès constituent une base pour les affaires futures et créer une mesure de dissuasion.

- Application de la réglementation : Les organismes de réglementation élaborent et appliquent des politiques pour la cybersécurité dans leur champ d'application traditionnel. Par exemple, la Food and Drug L'administration a établi des lignes directrices pour les dispositifs médicaux qui découplent les fonctions de base de l'appareil les mises à jour de sécurité des régimes de certification de produits existants, et le Federal Trade Commission européenne (FTC) a pris des mesures dans de nombreuses affaires liées à la confidentialité et à la sécurité. IoT ont fait l'objet de certaines de ces mesures d'exécution.
- Initiatives politiques : Les questions de confidentialité et de sécurité des données pour les dispositifs IoT ont fait l'objet d'une attention particulière des initiatives politiques dans plusieurs ministères et agences. La série d'ateliers sur l'IdO de la FTC en se concentrant sur des dispositifs IoT spécifiques (par exemple, les drones, les téléviseurs intelligents) et le rapport public de la FTC sur l'état de l'art et le concours "IoT Home Inspector Challenge" ont été deux exemples marquants d'une longue série d'initiatives liste des activités.
- Éducation et sensibilisation : Le gouvernement fédéral s'efforce de combler les lacunes en matière d'éducation à l'échelle nationale grâce à l'initiative nationale pour l'éducation à la cybersécurité (NICE), qui comprend de nombreuses agences gouvernementales. Les agences de régulation sont indépendantes la poursuite d'activités éducatives complémentaires, telles que la publication d'orientations et de blogues qui s'adressent à leurs parties prenantes.

- Coordination et collaboration internationales : D'autres gouvernements réagissent également menaces distribuées automatisées pour l'écosystème, et font appel à leurs partenaires traditionnels partenaires et alliés pour coordonner et échanger des informations.

Comme dans d'autres secteurs, ces efforts sont importants, mais il faut en faire davantage pour atténuer l'évolution de la situation menace. Les participants ont identifié plusieurs vecteurs différents permettant au gouvernement d'avoir un impact sur la résilience des entreprises le réseau, notamment :

- Approvisionnement : Tout en reconnaissant que le pouvoir d'achat du gouvernement fédéral n'est plus la force dominante du marché des technologies de l'information, les participants ont encourage le gouvernement à utiliser le pouvoir de la bourse de concert avec des moyens techniques bien specifies comme une étape vers des objectifs clés et pour diriger le secteur privé. Par exemple, en exigeant des fournisseurs qu'ils prennent en charge les mises à jour de sécurité automatisées, le gouvernement pourrait augmenter

la résilience des composantes de l'écosystème appartenant au gouvernement fédéral et gérées par lui, et élargir la gamme d'options disponibles pour les entités du secteur privé axées sur la sécurité.

- Recherche fondamentale : Les participants ont noté que le gouvernement fédéral reste le principal source de financement de la recherche fondamentale dans la plupart des disciplines scientifiques. L'industrie est se concentrent, à juste titre, sur les dernières étapes de la R&D. Le gouvernement fédéral doit donc s'assurer que le financement est à la fois suffisant et bien orienté.

- Coopération et coordination internationales : Comme indiqué précédemment, l'écosystème est mondial, et la lutte efficace contre les menaces distribuées nécessitera une coopération entre et la coordination avec les fournisseurs de services, les fabricants et les entreprises utilisatrices non américaines. Dans certains cas, ces entités sont étroitement liées aux États-nations. Le gouvernement fédéral est particulièrement bien placé pour promouvoir et faciliter la coopération et la coordination avec ces pays entités.

- Application de la loi : Les efforts déployés par les services de répression pour démanteler les réseaux de zombies et atténuer les effets de ces derniers. Les menaces ont reçu un large soutien de la part des participants. Un soutien prudent à la révision et à la révision des politiques qui entravent les poursuites a été exprimée, avec la réserve que les revisions doit trouver un équilibre entre les préoccupations relatives à l'application de la loi et les droits à la vie privée et à la propriété.

- Créer des incitations au marché : Plusieurs participants ont indiqué que le projet de document Communiquer la capacité de mise à jour de la sécurité des dispositifs IoT afin d'améliorer la transparence pour Consommateurs, élaborés dans le cadre du processus multipartite de la NTIA sur l'internet des objets. La mise à niveau de la sécurité et l'application de correctifs, comme un exemple qui pourrait créer des incitations commerciales pour les mises à niveau de sécurité. [11]

- Réglementation et incitations du marché : Les participants préfèrent les incitations du marché à la réglementation Générale initiatives réglementaires, mais ont exprimé un certain pessimisme compte tenu des échecs passés du marché. Les participants ont noté que de nouvelles réglementations axées sur la cybersécurité dans des secteurs actuellement réglementés pourraient être appropriés et avoir un impact positif s'ils sont soigneusement étudiés. Médical les dispositifs médicaux ont été mis en avant comme l'un de ces secteurs industriels, et les récentes déclarations de la FDA concernant le rapiéçage ont été cités comme un exemple de réglementation réfléchie et équilibrée. Les réglementations pourraient également avoir un impact positif en clarifiant les responsabilités et les obligations de rendre des comptes à différentes étapes du cycle de vie du produit ou du processus de réponse aux incidents.

  - Il a été suggéré de suivre un modèle tel que celui utilisé par le Comité international de la Croix-Rouge. Union des télécommunications - Secteur radio (UIT-R) pour la gestion du spectre radioélectrique au niveau international pourrait être une bonne approche pour établir comment coopérer en le cyberespace au niveau international.

[11] Pour le projet de document, voir https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-_jul_14_2017_-_ntia_multistakeholder_process.pdf. Pour en savoir plus sur l'effort IoT dirigé par la NTIA, voir https://www.ntia.doc.gov/category/internet-.choses.

- Éducation et sensibilisation : Il existe déjà de nombreuses directives en matière de cybersécurité défensive disponibles et qui sont soit inconnus, soit ignorés. Il faudrait peut-être mettre davantage l'accent sur pour obtenir une mise en œuvre plus généralisée des protections de base.

    - Si nous comptons sur les consommateurs pour gérer la cybersécurité, nous devons à la fois faciliter les choses et fournir davantage d'informations, beaucoup plus tôt qu'actuellement, sur des modèles pour aider les gens à comprendre la cybersécurité.

- Rationalisation de l'assainissement : Le gouvernement peut peut-être faire davantage pour faciliter l'assainissement après une violation. Les citoyens peuvent-ils obtenir de l'aide pour se remettre d'une violation, par exemple en faisant Il est plus facile d'informer les personnes et les organisations de la création de nouveaux comptes et de l'ouverture d'anciens comptes les comptes sont nuls.

- Établir des directives : Les participants ont suggéré que le gouvernement fédéral en général, et le NIST en particulier, pourrait aider l'industrie par des directives supplémentaires pour soutenir action volontaire. Un certain nombre de participants ont cité le processus que le NIST a utilisé pour élaborer la cadre pour l'amélioration de la cybersécurité des infrastructures critiques (Cybersecurity Framework) comme un modèle de construction de consensus vers des orientations utiles et acceptées. Les participants ont explicitement suggéré d'étendre le cadre de cybersécurité afin d'aborder les points suivants IoT. [12]

- Donner l'exemple : Les participants ont noté que relativement peu de dispositifs dans les récents botnets étaient situés aux États-Unis, validant ainsi les approches de sécurité nationale. Cette histoire à succès est en grande partie négligée et n'est pas reproduite. Créer des incitations pour ceux qui ne sont pas aux États-Unis à prendre les mesures de sécurité, nous devons prouver notre succès et en faire la publicité au niveau international, en partageant notre solution. Grâce à ce succès, nous, en tant que communauté, avons pu convaincre les bonnes personnes les gens à agir et à prendre des décisions en matière de dépenses de cybersécurité.

- Encourager les actions non commerciales : Du point de vue des FAI, il y a des coûts associés avec certaines tâches qui augmentent la résilience du réseau mais qui ne bénéficient pas directement soit le client, soit le FAI. (La mise en quarantaine et la notification des clients ont été citées comme un moyen de réduire les risques de contamination exemple). Le gouvernement pourrait encourager ces actions non marchandes en fournissant des fonds ou en permettant aux entreprises de récupérer leurs coûts.

[12] L'extension du CSF à l'IdO nécessiterait très probablement l'élaboration d'un profil du secteur de l'IdO, à l'instar des efforts déployés par le CSRIC IV pour le secteur de l'IdO. secteur des communications. Voir CSRIC IV, Cybersecurity Risk Management and Best Practices, Final Report, WG 4 (Mar. 2015),

https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

4. Conclusions et implications

L'Executive Order 13800 a demandé aux départements du commerce et de la sécurité intérieure de soumettre un rapport au Président qui "identifiera et encouragera l'action des autorités compétentes". parties prenantes pour améliorer la résilience de l'écosystème de l'internet et des communications et pour encourager la collaboration dans le but de réduire considérablement les menaces perpétrées par les systèmes automatisés et les attaques distribuées (par exemple, les botnets)".

L'atelier a fourni des informations essentielles qui, avec la demande de commentaires de la NTIA et le document le rapport du NSTAC sera pris en compte dans l'élaboration du projet de rapport. Implications pour la conférence de Janvier le rapport comprend :

- Les actions proposées dans le rapport aborderont chacun des thèmes primordiaux tirés de les participants à l'atelier.

- Le rapport recommandera une ou plusieurs actions proposées pour chacune des parties prenantes groupes (c'est-à-dire les fournisseurs d'infrastructure, les développeurs de produits, les entreprises, les utilisateurs privés), le monde universitaire et le gouvernement).

- Les parties prenantes non gouvernementales s'attendent à ce que le gouvernement fédéral montre l'exemple et promouvoir les actions des autres parties prenantes par des mesures incitatives plutôt que par la réglementation.

- De nombreuses actions auront des dépendances avec des actions attribuées à d'autres parties prenantes, donc les mécanismes de collaboration devront également être identifiés dans le rapport.

- Les recommandations comprendront probablement des actions immédiates visant à accroître la sensibilisation et à le déploiement des technologies actuellement disponibles, les actions à moyen terme pour créer un marché incitations (notamment pour garantir le cycle de vie complet des produits) et promouvoir la coopération international la coordination et la collaboration, ainsi que des actions à long terme pour développer de nouvelles technologies.

5. Prochaines étapes et possibilités d'engagement

Parallèlement à la publication de ce rapport, la NTIA publiera un résumé des déclarations soumis en réponse à la demande de commentaires de juin 2017. [13] Ministère du commerce et de la patrie Le service de sécurité commencera à élaborer le rapport en se fondant sur les commentaires du public fournis à l'adresse suivante date, en incorporant les contributions supplémentaires reçues. En parallèle, le NSTAC poursuivra les travaux suivants son rapport pour publication le 31 octobre 2017.

Les autres contributions publiques sur ce sujet sont les bienvenues et peuvent être envoyées à l'adresse suivante distributed.threats@nist.gov. Les commentaires soumis au plus tard le 15 octobre 2017 seront pris en considération pour l'inclusion dans le rapport préliminaire, qui sera partagé avec la communauté au plus tard à la date suivante le 5 janvier 2018.

Les contributions et commentaires du public sur le rapport préliminaire seront acceptés jusqu'en février. 5, 2018. Après la clôture de la période de commentaires, un atelier public sera organisé en février pour discuter de la résolution prévue des commentaires. Sur la base des commentaires du public et des discussions tenues lors de l'atelier, les départements complèteront le rapport pour le soumettre au Président le ou le avant le 11 mai 2018.

[13] Voir https://www.ntia.doc.gov/federal-register-notice/2017/report-responses-ntia-s-request-commentaires-promouvoir-l'action-des-parties-prenantes

A. Ordre du

Les pages suivantes présentent l'ordre du jour public de l'atelier tel qu'il a été affiché avant l'atelier.

Il y a eu deux changements d'ordre du jour "le jour même" : Carlos Morales de Arbor Networks a participé à le premier panel (Infrastructure des communications) au nom d'Arabella Harrington ; et Craig Hyps de Cisco a participé au deuxième panel (Produits) à la place d'Eric Wenger.

Renforcer la résilience de l'écosystème de l'internet et des communications

Centre d'excellence national de cybersécurité du NIST, Rockville MD

11 et 12 juillet 2017

Objectif de l'atelier : L'objectif de cet atelier est d'explorer une série de questions actuelles et émergentes liées à l'environnement des solutions pour améliorer la résilience de l'Internet contre les menaces distribuées automatisées, telles que les suivantes les botnets. Le déploiement de ces solutions dépendra de la capacité et de la volonté des différentes parties à prendre des mesures. En fonction de la solution spécifique, des actions peuvent être requises par les fournisseurs d'infrastructure, les fabricants de dispositifs, les propriétaires de systèmes et de réseaux, la communauté des chercheurs, les pouvoirs publics, et/ou les développeurs de normes. En explorant l'espace des solutions avec un large éventail de participants, le NIST espère identifier des pistes prometteuses pour toutes les parties afin de renforcer la résilience de l'internet.

Résultats de l'atelier : Le NIST produira un document sur le déroulement de l'atelier qui résumera la session. Les discussions, les résultats et les opportunités pour les prochaines étapes. Les résultats de cet atelier seront les suivants servent également de contribution aux activités de mise en œuvre liées à l'Executive Order 13800, *Strengthening the Cybersécurité des réseaux fédéraux et des infrastructures critiques*.

Agenda

Mardi 11 juillet 2017

7:30	**Enregistrement du Registrant**
8:30	**Bienvenue et aperçu de l'atelier**
8:45	**Préparer le terrain** *Cette séance plénière résumera l'espace problématique (par exemple, l'écosystème des botnets), identifiera les parties prenantes (développeurs de normes/protocoles, fournisseurs d'infrastructures, consommateurs, les fabricants, les régulateurs) dans l'atténuation des botnets, et examiner les approches et les résultats passés.*
9:30	**Ari Schwartz, Venable** **Le point de vue du fournisseur d'infrastructure : Normes actuelles et émergentes, meilleures pratiques, et technologies (panel 1)** *Cette session plénière explorera les efforts actuels et les opportunités futures pour améliorer le la résilience de l'infrastructure (par exemple, l'Internet). Ce panel discutera de l'état actuel, les tendances et les approches actuelles et prometteuses pour atténuer les menaces distribuées automatisées comme les DDOS, avec un accent particulier sur les botnets et l'IoT.* **Russ Housley, Vigil Security (modérateur)** **Richard Barnes, Cisco** **Arabella Hallawell, Arbor Networks** **Danny McPherson, VeriSign** **Brian Rexroad, AT&T**

10:15	**Pause**
10:30	**Session 1 en petits groupes (assignés)**
12:00	**Déjeuner**
1:00	**Développement de produits (Panel 2)** *Cette séance plénière examinera les efforts actuels et les possibilités futures en matière de réseaux. les fabricants de composants et de dispositifs (y compris les fournisseurs de solutions IoT) pour s'attaquer aux racines du problème les causes des botnets récents (accès illimité au réseau, mots de passe codés en dur et bogues logiciel). La portée de la session comprend l'utilisation en entreprise et à domicile.* **Yolonda Smith, Pwnie Express (modérateur)** **Anura S. Fernando, Laboratoire des assureurs (Underwriters Laboratory)** **Jeff Greene, Symantec** **Rob Spiger, Microsoft** **Eric Wenger, Cisco**
1:45	**Session 2 en petits groupes (assignés)**
3:00	**Pause**
3:15	**Le point de vue du client : Approches actuelles (Panel 3)** *Cette session plénière examinera comment les utilisateurs d'Internet, en particulier dans les entreprises, peuvent de se protéger et d'éviter de faire partie du problème. Les panélistes commenceront par une vue d'ensemble des défis auxquels une entreprise peut être confrontée en raison d'attaques distribuées, notamment DDoS, applications web et fraude. La discussion mettra en évidence les capacités et les limites des meilleures pratiques actuelles et des technologies émergentes, ainsi que le potentiel de l'intégration intersectorielle collaboration.* **Nadya Bartol, Boston Consulting Group (modérateur)** **Steve Curren, HHS Office of the Assistant Secretary for Preparedness and Response (Bureau du secrétaire adjoint pour la préparation et la réponse)** **Matt Eggers, Chambre de commerce américaine** **Bradley Nix, directeur adjoint de l'US-CERT au NCCIC, DHS** **Spencer Wilcox, Exelon**
4:00	**Session 3 en petits groupes (assignés)**
5:00	**Ajournement Jour 1**

12 juillet 2017

7:30	**Enregistrement du Registrant**
8:30	**Bienvenue et remarques d'ouverture**
8:45	**Orientations de la recherche** *Ce panel identifiera et explorera les lacunes dans les approches visant à atténuer les réseaux de zombies, et mettre en évidence les possibilités de combler ces lacunes.* **Pat Muoio, Cybertech Consulting (modérateur)** **David Dagon, Ga Tech** **Keith Marzullo, Univ. de MD** **Phil Reitinger, Global Cyber Alliance**
9:30	**Le rôle du gouvernement** *Cette session plénière examinera les efforts actuels et les possibilités futures des gouvernements pour améliorer la résilience de l'infrastructure, ce qui peut inclure des mesures politiques et réglementaires. les approches, les incitations et les facteurs de motivation du marché, les impacts économiques et les relations internationales considérations.* **Grace Koh, NEC (modérateur)** **Andi Arias, FTC** **Tom Grasso, FBI** **John Nicholson, ambassade du Royaume-Uni** **Malikah (Mikki) Smith, HHS/ONC**
10:15	**Pause**
10:30	**Groupes de discussion sur la recherche et le rôle du gouvernement**
11:15	**Pause**
11:30	**Résumé des séances de travail de la première journée**
12:00	**Discussion ouverte**
12:30	**Clôture et prochaines étapes (DOC/DHS)**
12:45	**Ajournement**