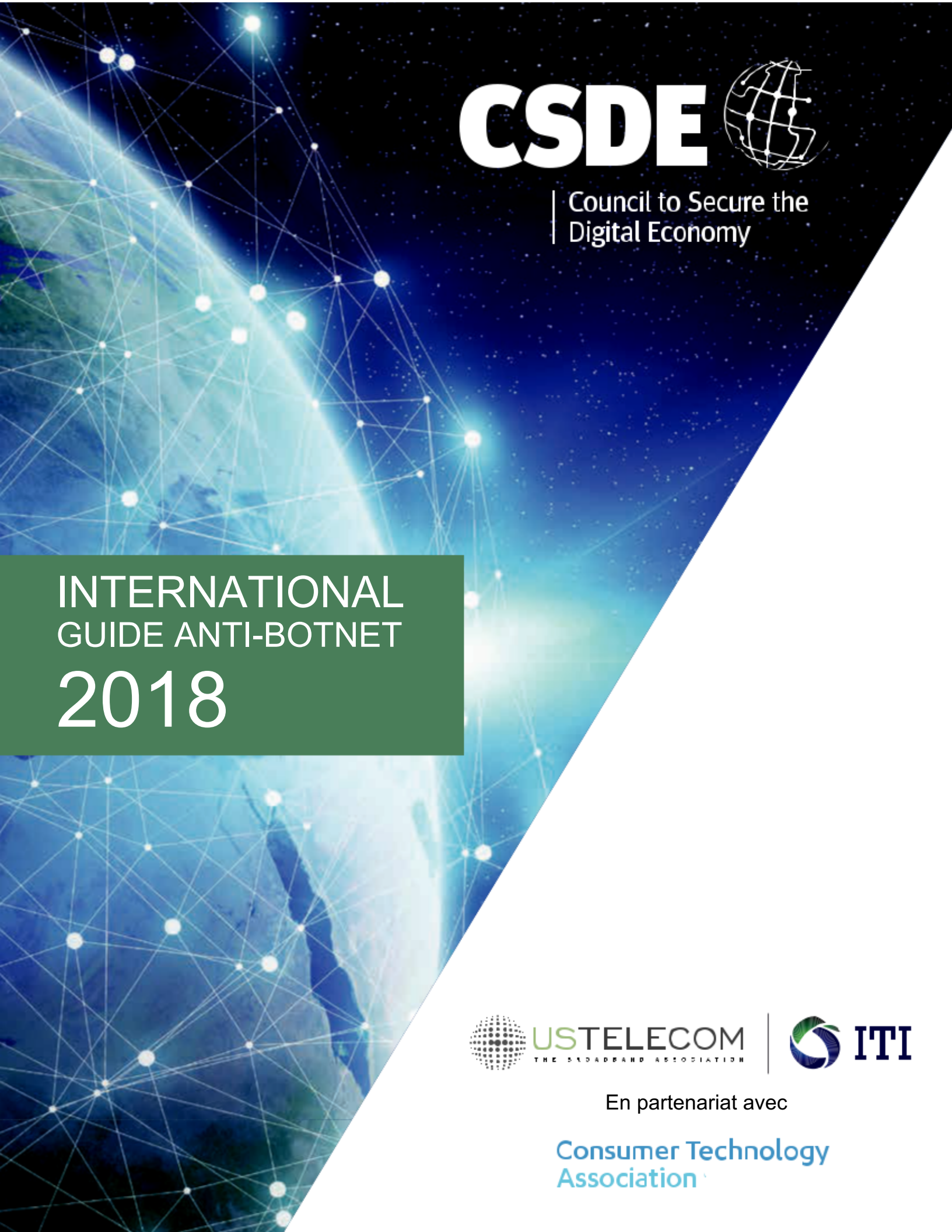

CSDE

Council to Secure the Digital Economy

INTERNATIONAL GUIDE ANTI-BOTNET 2018

USTELECOM THE BROADBAND ASSOCIATION | ITI

En partenariat avec

Consumer Technology Association

AVIS

Le Guide international anti-botnet a été élaboré pour faciliter l'atténuation des botnets et autres menaces automatisées et distribuées par le biais d'une participation volontaire et d'une collaboration entre les différentes parties prenantes de l'écosystème mondial de l'Internet et des communications. Le Guide fournit des informations et des encouragements aux parties prenantes des technologies de l'information et de la communication (TIC) sur les mesures positives à mettre en œuvre pour atteindre cet objectif, comme elles le jugent approprié, en fonction de leur situation individuelle et de leurs relations mutuelles.

Le guide met en évidence des pratiques volontaires efficaces pour chaque segment du secteur des TIC, allant de "de base" à "avancées". Les leaders de l'industrie qui ont élaboré ce guide reconnaissent qu'aucune combinaison de mesures ne peut garantir l'élimination de toutes les menaces et de tous les risques, mais ils estiment que ces pratiques, tant de base qu'avancées, constituent un cadre de référence précieux pour les parties prenantes des TIC, qui peuvent ainsi identifier et choisir leurs propres pratiques pour atténuer les menaces d'attaques automatisées et distribuées. Le Guide reconnaît que les différents acteurs des TIC sont confrontés à des défis, des considérations et des priorités différents lorsqu'ils mettent en œuvre des mesures de sécurité. Par conséquent, les pratiques identifiées dans ce Guide, et le Guide dans son ensemble, sont des outils que les acteurs des TIC devraient mettre en œuvre en fonction de leur situation ; il ne s'agit pas d'exigences ou de mandats, ni d'obligations de quelque nature que ce soit.

Bon nombre des pratiques et technologies abordées dans le présent document sont déjà utilisées par les grandes entreprises pour protéger leurs réseaux et systèmes, qu'il s'agisse de confier l'inspection approfondie des paquets (IAP) à des fournisseurs de services réseau ou d'interdire l'utilisation d'appareils ne disposant pas de mesures de sécurité intégrées suffisantes. Cependant, la mise en œuvre de ces capacités dans l'espace grand public a des implications politiques plus larges. Par exemple :

- Des capacités avancées telles que l'IAP du trafic IP, bien qu'utiles dans certains contextes, pourraient avoir des répercussions importantes sur la vie privée des individus si elles étaient déployées sur les réseaux publics.
- S'il est exigé par les gouvernements pour atteindre d'autres objectifs politiques, le filtrage du trafic des réseaux publics sur la base des adresses IP et d'autres moyens peut également avoir des répercussions sur la libre circulation de l'information.
- Les entreprises disposent de personnel informatique qualifié qui négocie des exigences détaillées avec leurs fournisseurs et intègre des analyses coûts-avantages dans la prise de décision. Une telle dynamique n'existe pas dans l'espace des consommateurs, où l'analyse coûts-avantages peut différer considérablement de celle d'une entreprise à grande échelle. Pour les consommateurs, les questions de coût et de protection des consommateurs devront être évaluées selon une échelle de gestion des risques différente.
- Les appareils dont on estime que les capacités de sécurité sont insuffisantes ne peuvent pas simplement être interdits de vente dans un pays donné sur une base ad hoc sans tenir compte des implications en matière de commerce international et des autres réglementations locales.

Contenu

01 Résumé exécutif

Les membres du Council to Secure the Digital Economy (CSDE) et de la Consumer Technology Association (CTA)™ couvrent l'ensemble de l'écosystème mondial complexe de l'Internet et des communications, fournissant des infrastructures, des logiciels et des appareils qui profitent à une partie importante des consommateurs, des petites entreprises, des grandes entreprises privées, des gouvernements et des organisations à but non lucratif du monde entier - collectivement, l'économie numérique mondiale.

Les entreprises qui ont contribué à ce guide ont été parmi les premières à adopter des pratiques volontaires pour sécuriser l'écosystème contre les cybermenaces. Dans le même temps, le secteur technologique a bénéficié de pratiques de conception sécurisée, de services de sécurité gérés et d'une assistance tout au long du cycle de vie fournis par des fournisseurs mondiaux de matériel, de logiciels, de dispositifs et de systèmes, ainsi que de services connexes. Pourtant, les défis sont nombreux pour les fournisseurs d'infrastructures, les développeurs de logiciels, les fabricants de dispositifs et de systèmes, les installateurs de systèmes et les entreprises de tous types.

Le Guide international de lutte contre les botnets du CSDE, élaboré en étroite collaboration avec le CTA, s'appuie sur les diverses perspectives, pratiques et expériences mondiales de ces parties prenantes pour s'attaquer à un défi persistant et croissant pour l'économie numérique mondiale : les botnets et autres menaces automatisées et distribuées.

Activer la responsabilité partagée pour sécuriser l'économie numérique mondiale. L'économie numérique a été un moteur de la croissance commerciale et de l'amélioration de la qualité de vie dans le monde entier.

Mais aucune partie prenante, que ce soit dans le secteur public ou privé, ne contrôle ce système. Au contraire, gérer en toute sécurité les possibilités offertes par cette croissance est le défi et la responsabilité de chaque partie prenante de la communauté des technologies de l'information et des communications (TIC).

Ces dernières années, cependant, les botnets sont devenus particulièrement et de plus en plus dommageables et coûteux pour l'économie numérique. Les botnets sont de vastes réseaux d'ordinateurs et d'appareils compromis, connectés à Internet, que des acteurs malveillants peuvent commander pour commettre des attaques par déni de service distribué (DDoS), propager des ransomwares, des attaques de phishing et des campagnes de désinformation amplifiant les médias sociaux inauthentiques, ainsi que d'autres actes malveillants. [1] Malheureusement, le nombre de personnes, d'entreprises et d'appareils connectés augmente, tout comme le potentiel de ces attaques malveillantes. Aujourd'hui, le potentiel destructeur des botnets a augmenté de manière exponentielle, car ils attaquent et exploitent les milliards d'appareils de l'Internet des objets (IoT), dont le nombre devrait atteindre 20 milliards d'appareils connectés d'ici 2020. Avec cette surface d'attaque substantielle et croissante, ce n'est pas une coïncidence si le coût mondial des cybercrimes devrait atteindre des billions de dollars. Les botnets sont le moteur à l'échelle industrielle de ces pertes.

En fait, la menace des botnets est plus grave aujourd'hui qu'à n'importe quel moment de l'histoire. Des attaques énormes et très médiatisées contre de grandes organisations ont été récemment documentées, tandis qu'un courant sous-jacent d'attaques plus petites et moins médiatisées a entraîné des dommages continus mais inconnus. Ces évolutions entraînent des coûts directs et tangibles - se chiffrant en milliards de dollars - pour l'économie numérique. Le site

Les coûts immatériels sont tout aussi préjudiciables, car ces menaces sapent la confiance fondamentale dans l'économie numérique.

Ce guide vise à inverser ces tendances. Bien que les auteurs de ce guide soutiennent fermement le rôle important que jouent les gouvernements dans la mise en place d'un écosystème diversifié, l'imposition d'exigences réglementaires prescriptives et axées sur la conformité entravera l'innovation en matière de sécurité qui est essentielle pour le succès de l'entreprise.
est essentielle pour garder une longueur d'avance sur les menaces sophistiquées d'aujourd'hui. En outre, les efforts politiques antérieurs étaient fondés sur des solutions utopiques à ces menaces, reposant sur l'idée que les fournisseurs de services internet (FSI) peuvent simplement fermer tous les réseaux de zombies ou que les fabricants peuvent rendre tous les appareils universellement sûrs. Au contraire, des solutions dynamiques et flexibles, fondées sur des normes consensuelles volontaires, guidées par les demandes du marché et mises en œuvre par les parties prenantes de l'économie numérique mondiale, constituent la meilleure réponse à ces défis systémiques en constante évolution.

Pour permettre de telles solutions et encourager le partage des responsabilités entre toutes les parties prenantes, le présent guide définit un ensemble de pratiques de base que les différentes parties prenantes devraient mettre en œuvre ; en outre, il met en évidence des capacités avancées supplémentaires qui sont actuellement disponibles mais sous-utilisées. La mise en œuvre généralisée des pratiques de sécurité présentées dans ce guide réduira considérablement les réseaux de zombies et contribuera à sécuriser l'économie numérique mondiale. Le Guide propose des solutions concrètes, actuellement disponibles, à un défi mondial qui ne peut être relevé par une seule partie prenante, un seul pays ou par un mandat gouvernemental. Le Guide est le fruit d'une collaboration permanente avec des entreprises de plusieurs secteurs et pays pour réduire considérablement la menace des botnets, et d'une analyse de l'évolution rapide des menaces et des vulnérabilités mondiales, ainsi que des adversaires de plus en plus capables et déterminés.

Le guide se fonde sur les principes de sécurité fondamentaux suivants, qu'il cherche à promouvoir de manière positive :

- La sécurité exige des solutions dynamiques et flexibles, portées par les puissantes forces du marché mondial et aussi agiles et adaptables que les cybermenaces à atténuer, plutôt que des mécanismes de conformité réglementaire qui diffèrent selon la juridiction locale ou nationale.
- La sécurité est une responsabilité partagée entre toutes les parties prenantes de l'écosystème de l'internet et des communications. Les parties prenantes du gouvernement et de l'industrie devraient promouvoir des solutions qui augmentent les responsabilités de tous les acteurs, plutôt que de chercher des solutions faciles entre certains composants ou parties prenantes sélectionnés.
- La sécurité repose sur un travail d'équipe et un partenariat mutuellement bénéfiques entre les gouvernements, les fournisseurs, les prestataires, les chercheurs, les entreprises et les consommateurs, grâce à une action collective contre les mauvais acteurs et à des récompenses pour les contributions des acteurs responsables.

  Ces principes sont le fondement de la nouvelle approche de l'atténuation des botnets que les circonstances exigent.

Le guide international anti-botnet : Résumé des pratiques et des capacités. En raison de la complexité et de la diversité du "système de systèmes" que constituent l'Internet et l'écosystème de communication associé, il est impossible de fournir un ensemble de directives qui s'appliquent uniformément à toutes les parties prenantes. Le guide regroupe ces divers composants sur la base de cinq types constitutifs de parties prenantes fournisseurs, prestataires et utilisateurs : (1) l'infrastructure, (2) le développement de logiciels, (3) les appareils et systèmes d'appareils, (4) l'installation de systèmes pour les particuliers et les petites entreprises, et (5) les entreprises. Pour chacune de ces composantes, le guide présente les pratiques de base que toutes ces parties prenantes devraient aspirer à respecter, ainsi que les capacités avancées qui sont actuellement disponibles - bien que sous-utilisées - sur le marché. Ces pratiques et capacités, résumées brièvement ci-dessous, constituent le cœur de ce guide.

1. Infrastructure. Dans le cadre de ce guide, le terme "infrastructure" fait référence à tous les systèmes qui permettent la connectivité et l'opérabilité - non seulement aux installations physiques des fournisseurs de services Internet, de dorsale, de cloud, d'hébergement web, de livraison de contenu, de système de nom de domaine et d'autres services, mais aussi aux réseaux définis par logiciel et aux autres systèmes qui reflètent l'évolution de l'Internet, des choses tangibles au concept numérique. Nous recommandons des pratiques de base et des capacités avancées pour l'infrastructure afin d'inclure :
   - Détecter le trafic malveillant et les vulnérabilités
   - Atténuer les menaces distribuées
   - Coordination avec les clients et les pairs
   - Saisie et retrait de domaines d'adresses

2. Développement de logiciels. [2] Le logiciel est un élément de plus en plus omniprésent de tous les autres composants de l'écosystème. Il existe une grande variété de processus de développement complexes et d'interdépendances qui favorisent l'innovation et l'amélioration des logiciels. Nous recommandons que les logiciels soient généralement constitués de pratiques de base et de capacités avancées pour inclure :
   - Pratiques de développement "Secure-by-Design
   - Gestion de la vulnérabilité de la sécurité
   - Transparence des processus de développement sécurisés

3. Dispositifs et systèmes de dispositifs. [3] Un dispositif connecté individuel (ou "dispositif d'extrémité") peut lui-même être constitué de plusieurs composants, notamment des modules matériels, des puces, des logiciels, des capteurs ou d'autres composants opérationnels. Au-delà de l'appareil individuel lui-même, il existe de multiples couches supplémentaires de connectivité qui constituent un nouveau marché très dynamique, notamment pour l'innovation en matière de sécurité. Pour les "objets" de l'IoT, ainsi que les applications et les services qui les accompagnent, nous recommandons des pratiques de base et des capacités avancées :
   - Pratiques de développement "Secure-by-Design
   - Les racines de la confiance
   - Gestion du cycle de vie des produits, y compris de leur fin de vie
   - Utilisation de la chaîne d'outils axée sur la sécurité

4. Installation de systèmes pour les foyers et les petites entreprises. [4] Les foyers et les petites entreprises bénéficient d'appareils connectés dans plusieurs catégories. Ces systèmes peuvent être installés par des propriétaires de maisons et d'entreprises bricoleurs, ou par des professionnels : intégrateurs, entrepreneurs d'alarme et autres. En nous inspirant fortement de The Connected Home Security System[5], nous recommandons des pratiques de base et des capacités avancées à inclure :
   - Authentification et gestion des justificatifs
   - Configuration du réseau
   - Gestion du matériel réseau
   - Entretien de la sécurité

5. Les entreprises. [6] En tant que principaux propriétaires et utilisateurs d'appareils et de systèmes en réseau, y compris un nombre en augmentation exponentielle de systèmes de dispositifs IoT, les entreprises de tous types - gouvernement, secteur privé, universitaire, à but non lucratif - ont un rôle essentiel à jouer dans la sécurisation de l'écosystème numérique. Pour les entreprises, nous recommandons des pratiques de base et des capacités avancées à inclure :
   - Mises à jour sécurisées
   - Partage d'informations en temps réel
   - Des architectures de réseau qui gèrent les flux de trafic en toute sécurité
   - Résistance accrue aux attaques DDoS
   - Gestion des identités et des accès
   - Atténuer les problèmes liés aux produits anciens et piratés

Prochaines étapes et mise en œuvre. La publication de ce guide n'est qu'une première étape. Ensuite, nous allons engager stratégiquement un large éventail de parties prenantes, y compris les gouvernements de pays partageant les mêmes idées, afin de promouvoir les pratiques de base et les capacités avancées du Guide. En outre, nous mettrons à jour, publierons et promouvrons une nouvelle version du guide chaque année.

L'économie numérique a été un moteur de croissance commerciale et d'amélioration de la qualité de vie dans le monde entier, créant des emplois et des opportunités sur tous les continents. Elle représente peut-être déjà 20 % de la valeur économique mondiale.

02 | Introduction

Les membres du Council to Secure the Digital Economy (CSDE)[7] et de la Consumer Technology Association8 (CTA)™ couvrent l'intégralité de l'écosystème mondial complexe de l'internet et des communications. Ces organisations comptent parmi leurs membres des entreprises qui fournissent les systèmes humains et techniques qui créent, gèrent et installent les capacités de connectivité, les logiciels et les appareils qui profitent à une partie importante des consommateurs, des petites entreprises, des grandes entreprises privées, des gouvernements et des organisations à but non lucratif du monde - collectivement, l'économie numérique mondiale. Le Guide international de lutte contre les botnets du CSDE, élaboré en étroite collaboration avec le CTA, s'appuie sur les diverses perspectives internationales de ces parties prenantes, ainsi que sur leurs pratiques influentes et leurs actions dans le monde réel, pour relever un défi persistant et croissant pour cette économie numérique : les botnets et autres menaces automatisées et distribuées. [9]

Aperçu du défi. L'économie numérique a été un moteur de croissance commerciale et d'amélioration de la qualité de vie dans le monde entier, créant des emplois et des opportunités sur tous les continents. Selon certaines estimations, elle représenterait déjà 20 % de la valeur économique mondiale. [10] Bien que le PIB ne puisse à lui seul rendre compte de l'ensemble des contributions de l'économie numérique à la valeur économique mondiale - toute valeur fournie numériquement n'implique pas une transaction commerciale - le Wall Street Journal rapporte que l'économie numérique valait 11 500 milliards de dollars en 2016 et pourrait atteindre 23 000 milliards de dollars, soit près d'un quart du PIB mondial, d'ici 2025.[11] La croissance de l'économie numérique est alimentée en permanence par l'adoption par les entreprises et les consommateurs de technologies nouvelles et émergentes. La croissance de l'économie numérique est alimentée en permanence par l'adoption de technologies nouvelles et émergentes par les entreprises et les consommateurs.

Ces dernières années, cependant, les réseaux de zombies sont devenus particulièrement et de plus en plus nuisibles et coûteux pour l'économie numérique. Ils sont capables de propager des logiciels malveillants[13], de mener des attaques par déni de service[14] et de diffuser artificiellement de la désinformation corrosive sur les médias sociaux15. [15] Un seul botnet peut désormais comprendre plus de 30 millions de points d'extrémité "zombies" et permettre aux acteurs malveillants de réaliser des profits à six chiffres par mois. [16] Il n'y a jamais eu autant de systèmes vulnérables qu'aujourd'hui, simplement en raison de la croissance considérable et par ailleurs prometteuse de l'économie numérique elle-même - notamment en ce qui concerne le déploiement rapide de milliards d'appareils de l'Internet des objets (IdO), dont on estime qu'ils atteindront 20 milliards d'appareils connectés d'ici 2020.[17] Les avantages de cette économie connectée révolutionnent pour le bien des entreprises et des activités des consommateurs, et les entreprises qui ont développé ce guide innovent de nouvelles mesures de sécurité au fur et à mesure du déploiement des appareils. Néanmoins, des appareils non sécurisés continuent d'affluer sur le marché sans que les systèmes en place soient conçus pour les sécuriser. [18] De plus, il est désormais possible pour des acteurs malveillants relativement peu qualifiés de louer un puissant botnet qu'ils utiliseront pour des activités néfastes à grande échelle. [19]

Ces évolutions infligent des coûts directs et tangibles à l'économie numérique. Par exemple, depuis 2017, les logiciels malveillants se sont répandus en Europe, en Asie et sur le continent américain, causant plus de 10 milliards de dollars de dommages. [20] On estime qu'au cours des cinq prochaines années, les cybercrimes seuls coûteront globalement aux entreprises un total cumulé de 8 000 milliards de dollars (en amendes, pertes d'activité, coûts de remédiation, etc.) [21]

> **"La lutte contre les botnets nécessite une collaboration transfrontalière et multidisciplinaire, des approches techniques innovantes et le déploiement généralisé de mesures d'atténuation qui respectent les principes fondamentaux de l'Internet."**
>
> **- LA SOCIÉTÉ DE L'INTERNET**

Les coûts immatériels sont tout aussi préjudiciables, car ces menaces sapent la confiance fondamentale dans l'économie numérique.

Posture et objectifs stratégiques. Notre objectif est d'inverser ces tendances. Si nous reconnaissons et soutenons le rôle important de rassembleur que les gouvernements peuvent jouer en aidant à canaliser les activités des divers acteurs de l'écosystème, nous pensons également que les exigences réglementaires fondées sur la conformité entravent en fait l'innovation en matière de sécurité qui est nécessaire pour rester en tête des menaces sophistiquées d'aujourd'hui. En d'autres termes, non seulement les exigences réglementaires prescriptives sont rarement efficaces, mais elles sont en fait généralement contre-productives par rapport à l'objectif de sécurité. [22] Les solutions dynamiques et flexibles qui s'appuient sur des normes consensuelles volontaires, qui répondent aux demandes du marché et qui sont mises en œuvre par les parties prenantes de l'économie numérique mondiale constituent la meilleure réponse aux défis systémiques en constante évolution, tels que les botnets malveillants, qui menacent tous les acteurs de cet écosystème complexe.

C'est pourquoi le présent guide vise à donner aux participants responsables de l'économie numérique les moyens d'assurer son avenir et d'en exploiter tout le potentiel. Nous pensons qu'une collaboration active et une action collective seront commercialement bénéfiques pour toutes les parties prenantes, grandes et petites, sur le long terme. À cette fin, le présent guide peut être utilisé pour accroître la résilience de l'écosystème de l'internet et des communications et renforcer l'intégrité transactionnelle de l'infrastructure numérique sous-jacente. Le guide invite toutes les parties prenantes de ce marché numérique mondial à mettre en œuvre un ensemble d'outils, de pratiques et de processus de base ; il met également en évidence des capacités avancées supplémentaires qui sont actuellement disponibles, mais peut-être encore sous-utilisées. La mise en œuvre généralisée des pratiques de sécurité présentées dans ce guide réduira considérablement les réseaux de zombies et contribuera à sécuriser l'économie numérique mondiale.

Méthodologie et prochaines étapes. Les entreprises qui ont contribué à la rédaction de ce Guide ont entrepris un examen complet des pratiques et des documents qui présentent les technologies et les outils connus pour être efficaces dans la lutte contre les attaques automatisées et distribuées telles que les réseaux de zombies ; elles ont également effectué des recherches dans les rapports des gouvernements et des organismes internationaux et ont consulté des experts extérieurs et des sources de l'industrie, du monde universitaire et de la société civile. [23] Mais pour être clair, la publication de ce guide n'est qu'une première étape. Ensuite, nous engagerons stratégiquement un large éventail de parties prenantes, y compris les gouvernements de pays partageant les mêmes idées, afin de promouvoir les pratiques de base et les capacités avancées du Guide. En outre, nous mettrons à jour, publierons et promouvrons une nouvelle version du Guide chaque année.

03 Botnets : Lutte contre les menaces automatisées et distribuées dans un écosystème Internet diversifié

La catégorie la plus importante de menaces automatisées et distribuées pour l'écosystème mondial de l'internet et des communications est celle des réseaux de zombies, c'est-à-dire de vastes réseaux d'ordinateurs et d'appareils connectés à l'internet qui communiquent avec des serveurs dotés de capacités de commande et de contrôle.

Les réseaux de zombies se propagent dans le monde entier grâce à des logiciels malveillants qui analysent l'internet à la recherche de réseaux, d'ordinateurs et d'autres appareils connectés non sécurisés. Lorsqu'un botnet a compromis un nombre suffisant de dispositifs, les criminels et autres acteurs malveillants peuvent les commander pour commettre une grande variété d'actes néfastes tels que des attaques par déni de service distribué (DDoS), la propagation de ransomware, des attaques de phishing et des opérations de désinformation qui amplifient artificiellement des messages inauthentiques sur les médias sociaux. [24]

La menace des réseaux de zombies est plus grave aujourd'hui qu'à tout autre moment de l'histoire. Au début des années 2000, les criminels utilisaient principalement les botnets pour des attaques par déni de service (DoS) rudimentaires qui inondaient et submergeaient les sites Web et les activités de réseau ciblés avec un trafic Internet artificiel. Au fil du temps, cependant, leurs capacités se sont accrues. En infectant un grand nombre d'appareils avec des logiciels malveillants, les pirates ont découvert qu'ils étaient en mesure de mener des activités malveillantes à une échelle beaucoup plus grande. En 2007, on a découvert qu'un botnet appelé "Storm Worm" avait rassemblé dans ses rangs près de 50 millions d'ordinateurs, qu'il utilisait pour commettre des crimes tels que la fraude boursière et l'usurpation d'identité. En 2009, on a découvert qu'un botnet envoyait chaque jour un nombre incroyable de 74 milliards de spams. [25] Et en 2011-2013, un attaquant a utilisé des botnets pour mener une campagne d'attaques DDoS contre des banques nord-américaines, en envoyant des vagues de trafic Internet vers leurs sites Web à partir de nœuds de botnet du monde entier. [26]

Aujourd'hui, les criminels utilisent de grands botnets pour toutes sortes de cybercrimes, du minage de crypto-monnaies aux attaques DDoS, comme l'attaque historique du botnet Mirai de 2016 contre le fournisseur de DNS Dyn. Le logiciel malveillant du botnet Mirai de 2016 s'est propagé à l'aide d'une liste d'identifiants de connexion par défaut pour accéder à près de 400 000 appareils d'extrémité, tels que des caméras vidéo de vidéosurveillance et des enregistreurs vidéo numériques, sans que les propriétaires ne remarquent ou n'internalisent aucune des conséquences économiques de l'infection de leurs appareils. L'attaque, dont le volume de trafic induit par les botnets était quatre fois supérieur à celui des attaques précédentes contre les grandes banques, a temporairement désactivé l'accès des utilisateurs aux principaux services et plateformes en ligne, causant de graves problèmes aux nombreux utilisateurs qui dépendaient des services en ligne d'entreprises telles que Airbnb, Amazon.com, BBC, CNN et Netflix, pour n'en citer que quelques-unes28. [28]

Si la majorité des réseaux de zombies n'atteignent pas l'ampleur de Mirai29, de nombreuses attaques de réseaux de zombies de moindre envergure sont capables de fermer des sites web et des services, de diffuser des rançongiciels et de diffuser de la désinformation sur les médias sociaux. Malheureusement, les attaques de moindre envergure sont devenues beaucoup plus accessibles aux criminels qui n'ont pas les connaissances techniques nécessaires pour construire leurs propres réseaux de zombies. Les marchés en ligne que l'on trouve sur le dark web permettent aux pirates novices d'acheter les boîtes à outils nécessaires à la conception de botnets uniques répondant à leurs besoins individuels - ce que l'on appelle "Malware as a Service" (MaaS). Si le client criminel ne souhaite pas développer ou acheter un botnet, il peut en louer un pour seulement 0,66 dollar par jour. [30] Et le criminel peut simplement acheter la fonction - par exemple, une attaque DDoS - pour aussi peu que 20 dollars31.

marché innovant. Peu après les attaques Mirai, par exemple, le créateur du botnet a publié le code source de Mirai en ligne et, depuis, de nombreux autres pirates en herbe ont créé des variantes du code original de Mirai.

Les acteurs malveillants trouvent constamment de nouvelles utilisations pour les botnets. Par exemple, les pirates ont utilisé les botnets pour tenter de relancer le tristement célèbre ransomware WannaCry, qui a mis hors d'état de nuire plus de 200 000 systèmes informatiques dans plus de 150 pays, obligeant les banques, les hôpitaux, les universités et d'autres institutions à fermer leurs portes ou à payer une rançon aux criminels. [32] L'épidémie de WannaCry a reculé lorsqu'un chercheur en sécurité a réalisé que le logiciel malveillant interrogeait un domaine non enregistré. L'enregistrement du domaine a eu l'effet d'un "coupe-circuit" qui a éteint le botnet33. [33] Les pirates ont a utilisé des "imitateurs du botnet Mirai" pour attaquer ce domaine sans relâche dans le but de ramener à la vie le ransomware temporairement vaincu. [34] Entre-temps, un ransomware encore plus sophistiqué que WannaCry - Petya - est apparu pour faire des ravages dans le monde entier, et les logiciels malveillants basés sur Petya (appelés NotPetya) ont déjà coûté plus de 10 milliards de dollars en dommages. [35]

Les capacités des botnets malveillants menacent de saper la confiance fondamentale dans l'économie numérique.

Malheureusement, à mesure que le nombre de personnes, d'entreprises et d'appareils connectés augmente, le potentiel, la puissance et les profits des grandes malveillances s'accroissent également. attaques. Comme indiqué plus haut, le nombre total d'appareils connectés utilisés dans le monde se compte en milliards, et ce n'est pas un hasard si le coût mondial des cybercrimes devrait se chiffrer en billions. Les botnets sont le moteur de ce problème à l'échelle industrielle. Outre les pertes économiques évidentes, les capacités des botnets malveillants menacent de saper la confiance fondamentale dans l'économie numérique. Ce résultat défie toute quantification, mais son impact négatif peut avoir un effet débilitant, tout comme les préoccupations liées à la pollution menacent notre confiance dans l'air que nous respirons et l'eau que nous buvons.

Le défi fondamental que représente la lutte contre les botnets dans l'écosystème mondial de l'internet, extrêmement diversifié, complexe et interdépendant, réside dans le fait que la nature essentielle de l'internet est non hiérarchique et hyperconnectée. Aucune partie prenante - gouvernement ou secteur privé - ne contrôle ce système, et pourtant nous comptons sur lui pour nous connecter tous. La lutte contre les botnets malveillants est le défi classique de la "tragédie des biens communs" : si tout le monde a un intérêt dans les biens communs de l'internet et y est inéluctablement connecté, mais que personne ne les contrôle, alors qui est responsable du nettoyage des botnets malveillants qui menacent les fonctions de base dont tout le monde dépend ?

La réponse est que toutes les parties prenantes doivent prendre leurs responsabilités, et pas seulement dans un but altruiste de nettoyage du patrimoine commun. Chaque entité de l'écosystème a intérêt à réduire le nombre de botnets malveillants. Les botnets sont utilisés pour attaquer l'internet sur lequel reposent toutes les offres de TIC, et le fait d'être impliqué dans une attaque de botnet nuit aux entreprises concernées, soit par un impact direct sur l'exécution, soit par une atteinte à la réputation.

Efforts précédents pour relever ce défi à l'échelle de l'écosystème

Les entreprises responsables de ce guide ont été parmi les premières à adopter des pratiques volontaires pour protéger l'écosystème contre les botnets. Par exemple, en 2012, les leaders du secteur des communications aux États-Unis ont élaboré le Code de conduite anti-botnet pour les fournisseurs d'accès à Internet, prenant des mesures significatives pour éradiquer les botnets par l'éducation, la détection, la notification, la remédiation et la collaboration. Parallèlement, le secteur technologique a bénéficié de pratiques de conception sécurisée, de services de sécurité gérés et d'une assistance tout au long du cycle de vie fournis par des fournisseurs mondiaux de matériel, de logiciels, de dispositifs et de systèmes, ainsi que de services connexes.

Pourtant, les défis sont nombreux dans l'ensemble de l'écosystème :

- De nombreux FAI et autres fournisseurs d'infrastructures dotés de capacités avancées poussent continuellement le marché vers un état de sécurité accrue afin d'atténuer la menace des botnets. À mesure que la taille et la complexité des botnets augmentent, les entreprises qui exploitent des réseaux d'infrastructure ont ajouté des capacités de réseau pour protéger les clients contre des attaques de plus en plus importantes. Cependant, toutes les parties prenantes peuvent faire davantage pour fonctionner efficacement dans l'écosystème - et les petits fournisseurs ont souvent besoin de conseils et de ressources pour se mettre au niveau de la ligne de base.
- Les logiciels font partie intégrante de tous les processus commerciaux et gouvernementaux mondiaux. Les divers acteurs de l'économie numérique s'appuient de plus en plus sur des logiciels sécurisés. Cette dépendance a incité les mauvais acteurs à développer des exploits de plus en plus sophistiqués. En réponse, les entreprises responsables ont développé des pratiques sécurisées pour le développement de logiciels et ont fixé des objectifs de sécurité de base.

  pour chaque étape du cycle de vie du produit. Ce sont des pratiques que les petits développeurs peuvent imiter.
- Les innovations stupéfiantes en matière de développement, de déploiement et d'utilisation des systèmes d'appareils connectés constituent une arme à double tranchant, car elles introduisent dans le monde des milliards de nouveaux appareils compatibles avec Internet et autant de nouveaux points d'entrée à exploiter par les cybercriminels. Comme indiqué plus haut, nombre de ces appareils n'ont tout simplement pas été conçus ou déployés dans un souci de sécurité - et ils ne sont pas déployés dans des systèmes capables d'atténuer leurs vulnérabilités individuelles.
- Les ordinateurs et les appareils connectés d'un foyer ou d'une entreprise doivent être sécurisés tout au long du cycle de vie de l'appareil - et peut-être surtout, dès l'installation et la configuration initiales de l'appareil. Cependant, une installation et une configuration correctes sont encore trop rares et, par conséquent, les produits n'atteignent souvent pas leurs meilleures performances de sécurité disponibles.
- Les entreprises de tous types - dans les secteurs public et privé - sont à la fois les victimes et les propagateurs hôtes des botnets et autres menaces automatisées et distribuées. Ces entreprises ont beaucoup à gagner en adoptant des solutions de sécurité comme celles qui sont de plus en plus disponibles sur le marché.

UN SEUL BOTNET PEUVENT DÉSORMAIS INCLURE

PLUS QUE

30

MILLION

DES POINTS D'EXTRÉMITÉ "ZOMBIES" ET PERMETTENT AUX ACTEURS MALVEILLANTS DE RÉALISER DES PROFITS À SIX CHIFFRES PAR MOIS.

> **La sécurité exige des solutions dynamiques et flexibles qui sont guidées par les puissantes forces du marché mondial et qui sont aussi souples et adaptables que les cybermenaces qu'il faut atténuer.**

Dans ce contexte, l'erreur commune des efforts politiques passés a été de se concentrer sur un ou deux composants de l'écosystème, ce qui équivaut à essayer d'abattre une forêt d'arbres malades en coupant simplement les branches les plus proches. Le plus souvent, le résultat sera une forêt encore pleine d'arbres malades. De même, l'atténuation des réseaux de zombies nécessite une approche plus réfléchie et plus globale. Les différentes parties de cet écosystème complexe doivent, pour leur bien individuel et collectif, approfondir et affiner leur compréhension de leurs propres responsabilités et de la manière dont elles complètent celles des autres. Et dans les cas où les lignes sont actuellement floues ou inconnues, les parties prenantes doivent travailler ensemble pour les clarifier. En l'absence d'un tel travail, les stratégies de lutte contre les botnets retomberont dans l'erreur des solutions politiques utopiques axées sur un ou deux éléments seulement...
du puzzle - par exemple, que les fournisseurs d'accès à Internet devraient simplement fermer tous les botnets, que des milliards d'appareils devraient être universellement sécurisés ou que les consommateurs devraient devenir des utilisateurs omniscients de la technologie.

Ces solutions simplistes ont échoué jusqu'à présent et il est peu probable qu'elles soient plus efficaces à l'avenir. Au lieu de cela, ce système complexe composé de milliards de composants humains et automatisés sur les marchés des consommateurs et des entreprises du secteur privé, dans les universités, la société civile et les gouvernements du monde entier, doit mettre en œuvre des méthodes d'atténuation à tous les niveaux pour renforcer sa sécurité. C'est ce que vise à faire ce Guide international anti-botnet.

Qu'est-ce qui est différent maintenant ?

Ce guide propose des solutions concrètes, actuellement disponibles, à un défi du marché actuel qui ne peut être relevé par une ou plusieurs exigences gouvernementales ou par un seul pays. Nous travaillons avec des entreprises internationales de différents secteurs pour réduire considérablement la menace des botnets. Nous avons élaboré ce guide à partir de l'analyse de l'évolution rapide des menaces mondiales, des vulnérabilités de l'écosystème et des adversaires de plus en plus capables et déterminés, en gardant à l'esprit les principes directeurs consensuels suivants :

- La sécurité exige des solutions dynamiques et flexibles, portées par les puissantes forces du marché mondial et aussi agiles et adaptables que les cybermenaces à atténuer, plutôt que des mécanismes de conformité réglementaire qui diffèrent selon la juridiction locale ou nationale.
- La sécurité est une responsabilité partagée entre toutes les parties prenantes de l'écosystème de l'internet et des communications. Les gouvernements et les acteurs du secteur devraient promouvoir des solutions qui accroissent les responsabilités de tous les acteurs, plutôt que de chercher des solutions faciles entre certains composants ou acteurs choisis.
- La sécurité repose sur un travail d'équipe et un partenariat mutuellement bénéfiques entre les gouvernements, les fournisseurs, les prestataires, les chercheurs, les entreprises et les consommateurs, construits sur un cadre qui prend des mesures collectives contre les mauvais acteurs et récompense les contributions des acteurs responsables.

04 Vue d'ensemble de l'Internet mondial et Écosystème de communication

Comme indiqué plus haut, l'économie numérique repose sur - et a été rendue possible par - un écosystème mondial complexe d'Internet et de communications, composé de nombreux systèmes, chacun d'entre eux étant très complexe en soi et très interdépendant de tous les autres. Et tous ces différents composants constituent une partie de la vulnérabilité de l'écosystème - et de sa résilience - aux menaces posées par les botnets et autres attaques automatisées et distribuées.

L'économie numérique représentait 11 500 milliards de dollars en 2016 et pourrait atteindre 23 000 milliards de dollars, soit près d'un quart du PIB mondial, d'ici 2025.

En raison de la complexité et de la diversité du "système de systèmes" que constituent l'internet et l'écosystème de communication associé, il est impossible de fournir un ensemble d'orientations qui s'appliquent uniformément à toutes les parties prenantes. Divers rapports éminents du gouvernement et du secteur privé ont

ont défini et décrit l'écosystème de l'internet et des communications à l'aide de taxonomies similaires mais différentes, adaptées aux buts et objectifs de chaque forum. [36] Plutôt que de servir de visions concurrentes de la manière dont l'écosystème devrait être compris, ces définitions se complètent et se renforcent mutuellement.

Le présent guide ne fait pas exception. Nous regroupons les composantes de l'écosystème de manière à faciliter l'identification et la mise en œuvre des mesures de lutte contre le changement climatique.

pratiques de botnet parmi les groupes de parties prenantes qui le composent. Plus précisément, le guide s'articule autour des cinq types de prestataires, fournisseurs et utilisateurs suivants :

1. Infrastructure
2. Développement de logiciels
3. Dispositifs et systèmes de dispositifs
4. Installation de systèmes pour les particuliers et les petites entreprises
5. Entreprises

Il est certain que tout effort de définition de cet écosystème complexe comporte un certain risque de sous-inclusion, qu'il soit réel ou perçu. Par exemple, l'expérience peut révéler qu'aucune des cinq catégories énumérées ci-dessus ne peut raisonnablement prendre en compte certaines plates-formes omniprésentes (par exemple, les grandes plates-formes de médias sociaux) qui impliquent une combinaison de catégories. C'est pourquoi cette taxonomie doit être considérée avec souplesse, en sachant que les frontières entre les systèmes continueront d'évoluer.

05 Pratiques et capacités des composants de l'écosystème

A. INFRASTRUCTURE

Aux fins du présent guide, le terme "infrastructure" désigne tous les systèmes qui permettent la connectivité et l'opérabilité - non seulement les installations physiques des fournisseurs de services internet, de dorsale, de cloud, d'hébergement web, de diffusion de contenu, de système de nom de domaine et d'autres services, mais aussi les réseaux définis par logiciel et les autres systèmes qui reflètent l'évolution de l'internet, des choses tangibles au concept numérique. Nous recommandons des pratiques de base et des capacités avancées pour diverses infrastructures dans l'écosystème moderne de l'internet et des communications.

Types d'infrastructures

Fournisseurs de services Internet

Un fournisseur d'accès à Internet (FAI) est une organisation qui fournit aux clients un moyen d'accéder à Internet en utilisant des technologies telles que le câble, la ligne d'abonné numérique (DSL), l'accès commuté et le sans fil. Les FAI sont connectés les uns aux autres par des points d'accès au réseau, des installations de réseau public situées sur la dorsale Internet. Les FAI utilisent ces vastes systèmes de composants dorsaux interconnectés pour transférer des informations sur de longues distances en quelques secondes. Les FAI peuvent fournir des services autres que l'accès à l'internet, notamment l'hébergement de sites web, l'enregistrement de noms de domaine, l'hébergement virtuel, des progiciels et des comptes de courrier électronique. De nombreux FAI proposent des services destinés à réduire les réseaux de zombies, notamment des solutions de sécurité gérées dans le cadre desquelles le fournisseur joue un rôle actif dans l'atténuation des menaces pour les clients. La plupart des FAI à large bande fournissent un antivirus dans le cadre de leur offre, et beaucoup avertissent les clients infectés sans frais supplémentaires.

Fournisseurs de dorsale Internet

La dorsale de l'internet est un ensemble de vastes réseaux informatiques connectés qui sont généralement hébergés par des points d'accès aux réseaux commerciaux, gouvernementaux, universitaires et autres. Ces organisations contrôlent généralement de grands réseaux à haut débit et des lignes principales en fibre optique, qui sont essentiellement un assortiment de câbles en fibre optique regroupés afin d'augmenter la capacité. Elles permettent des débits de données plus rapides et une plus grande largeur de bande sur de longues distances, et sont à l'abri des interférences électromagnétiques. Les fournisseurs de dorsales fournissent aux FAI un accès à l'internet et connectent les FAI entre eux, ce qui permet aux FAI d'offrir aux clients un accès à l'internet à haut débit. Les plus grands fournisseurs de dorsales sont appelés fournisseurs de "niveau 1". Ces fournisseurs ne sont pas limités à un pays ou à une région et disposent de vastes réseaux qui relient des pays du monde entier. Certains fournisseurs de backbone de niveau 1 sont eux-mêmes des ISP et, en raison de leur taille, ces organisations vendent leurs services à des ISP plus petits.

Fournisseurs de DNS

Le système de noms de domaine (DNS) est essentiellement un carnet d'adresses de noms de domaine associés à des adresses IP copiées et stockées sur des millions de serveurs dans le monde. Lorsqu'un utilisateur souhaite visiter un site web et tape le nom de domaine dans la barre de recherche, l'ordinateur envoie cette information à un serveur DNS. Ce serveur (également appelé "résolveur") est généralement géré par le fournisseur d'accès Internet de l'utilisateur. Le résolveur fait ensuite correspondre le nom de domaine à une adresse IP et renvoie l'adresse IP correspondante au navigateur de l'utilisateur qui ouvre alors une connexion avec le serveur web.

Les fournisseurs de DNS sont des organisations qui offrent ces services de résolution DNS. Ils fournissent les fonctions DNS les plus courantes telles que la traduction de domaine, la recherche de domaine et la redirection DNS. Les fournisseurs de DNS mettent aussi régulièrement à jour leurs serveurs de noms afin de fournir les informations les plus récentes.

Réseaux de diffusion de contenu

Un réseau de diffusion (ou de distribution) de contenu (CDN) est un réseau géographiquement dispersé de centres de données et de serveurs proxy. Le terme CDN est utilisé pour décrire de nombreux types différents de services de diffusion de contenu tels que : les téléchargements de logiciels, l'accélération du contenu web et mobile, et le streaming vidéo. Les fournisseurs de CDN peuvent également s'intéresser à d'autres secteurs comme la cybersécurité avec la protection contre les attaques DDoS et les pare-feu d'applications Web (WAF). Les CDN ont été conçus pour résoudre un problème connu sous le nom de latence, c'est-à-dire le délai qui se produit entre le moment où un utilisateur demande une page web et le moment où son contenu apparaît à l'écran. La durée de ce délai dépend généralement de la distance entre l'utilisateur final et le serveur d'hébergement. Pour raccourcir cette durée, les CDN réduisent cette distance physique et améliorent la vitesse et les performances de rendu du site en stockant une version en cache de son contenu en plusieurs endroits, appelés points de présence ou PoP ; chaque PoP connecte les utilisateurs finaux situés à proximité aux serveurs de cache responsables de la livraison du contenu. En stockant le contenu d'un site web en plusieurs endroits à la fois, une entreprise peut fournir une couverture supérieure aux utilisateurs finaux éloignés.

Fournisseurs de cloud et d'hébergement

Certaines pratiques de base ont déjà prouvé qu'elles réduisaient l'impact des attaques menées par les botnets, telles que les attaques DDoS, et devraient être mises en œuvre dans l'ensemble de l'écosystème.

Les services d'hébergement Internet permettent aux clients de rendre le contenu accessible sur Internet aux personnes et aux organisations du monde entier. Ces dernières années, l'adoption accrue des services d'hébergement en nuage, qui utilisent des serveurs distants hébergés en ligne au lieu d'un serveur local ou d'un appareil personnel, a permis aux clients d'accéder à des solutions d'hébergement évolutives et plus sûres. Les logiciels, l'infrastructure et les plates-formes hébergés dans le nuage sont accessibles sur la base d'un abonnement et permettent aux clients d'accomplir les tâches suivantes une grande variété de fonctions informatiques. Les réseaux en nuage étant décentralisés, ils peuvent généralement résister à l'interruption de nombreux composants du réseau. Cette caractéristique architecturale rend le nuage plus résistant aux botnets hautement distribués et offre des capacités d'atténuation supplémentaires. En substance, les services en nuage offrent une couche de sécurité supplémentaire en dehors de l'infrastructure fournie par un FAI. Cette couche de protection devient de plus en plus utile à mesure que l'ampleur des attaques de botnets augmente. Étant donné que le nuage se situe en amont de la cible d'une attaque de botnets, par rapport aux FAI, les services en nuage offrent une protection supplémentaire.

il peut atténuer le problème plus près de la source de l'attaque. Les services de sécurité en nuage complètent et ne diminuent pas le rôle des FAI dans l'atténuation des botnets.

Pratiques de base et capacités avancées pour l'infrastructure

Les membres du CSDE prennent des mesures essentielles pour accroître la résilience de leurs propres réseaux, des réseaux de leurs clients et de l'écosystème mondial contre les botnets. Les experts du gouvernement et de l'industrie ont constaté qu'en raison de la complexité de l'écosystème, aucun outil unique ne sera toujours efficace pour atténuer les menaces[37], ce qui signifie que l'industrie doit conserver suffisamment de souplesse pour s'adapter aux menaces émergentes et aux nouvelles technologies et nouveaux outils. Cependant, il a déjà été prouvé que certaines pratiques de base réduisaient l'impact des attaques menées par les botnets, telles que les attaques DDoS, et qu'elles devraient être mises en œuvre dans l'ensemble de l'écosystème. [38] Nous identifions ci-dessous les pratiques de base ainsi que les capacités plus avancées que les leaders industriels utilisent pour sécuriser l'écosystème contre les menaces distribuées.

1. DÉTECTER LE TRAFIC MALVEILLANT ET LES VULNÉRABILITÉS

La première étape de l'atténuation des menaces distribuées telles que les réseaux de zombies consiste à identifier les actifs qui doivent être défendus contre les attaques et les vulnérabilités potentielles (c'est-à-dire les surfaces d'attaque) qui exposent potentiellement ces actifs. En outre, les entreprises doivent se tenir informées des derniers exploits (c'est-à-dire des vecteurs d'attaque) pour chaque vulnérabilité identifiée.

Les fournisseurs peuvent tirer parti des flux de données et des mécanismes de partage d'informations de tiers de confiance, tant au sein de leur secteur qu'entre secteurs. En outre, dans de nombreux pays, les mécanismes gouvernementaux de partage de l'information permettent d'échanger des informations entre le secteur public et le secteur privé à la vitesse de la machine. [39]

Résumé des pratiques de détection de base : Les fournisseurs vérifient les types de logiciels malveillants connus dans des bases de données régulièrement mises à jour. Une entreprise responsable peut contribuer aux efforts de détection en partageant en temps utile les informations sur les nouveaux logiciels malveillants avec les fournisseurs de sécurité et les chercheurs.

Résumé des capacités de détection avancées : Les entreprises ayant accès à des ressources plus importantes peuvent disposer d'une équipe dédiée de chercheurs en sécurité capables d'analyser l'heuristique et les comportements anormaux pour détecter les logiciels malveillants. Les conclusions de ces chercheurs peuvent être partagées avec d'autres parties prenantes.

a) Analyse de la signature

Lorsque les experts en sécurité rencontrent un logiciel malveillant, ils recherchent un modèle ou une "signature" unique (par exemple, une partie du code du logiciel malveillant et du code d'exploitation). L'analyse basée sur les signatures peut ensuite être utilisée par toute personne ayant accès à une base de données actualisée de signatures de logiciels malveillants, de sorte que la menace peut être identifiée indépendamment de l'endroit où elle est rencontrée. Ce type d'analyse est courant dans les logiciels antivirus et les systèmes de détection des intrusions, et peut être utilisé pour détecter la plupart des menaces malveillantes sur un réseau. Bien que l'analyse des signatures soit couramment utilisée, des acteurs malveillants plus sophistiqués peuvent limiter l'utilité de cette technique en modifiant les spécificités des logiciels malveillants à chaque fois qu'ils se propagent. Comme un véritable virus, les logiciels malveillants peuvent s'adapter et évoluer lorsqu'ils passent d'un hôte à l'autre. Une limite plus évidente de l'analyse des signatures est qu'elle nécessite une connaissance préalable des logiciels malveillants, ce qui signifie que l'efficacité de l'analyse des signatures dépend de mises à jour opportunes et du partage des informations dans l'ensemble de l'écosystème. Idéalement, l'analyse de signatures devrait être combinée à d'autres types d'analyse, comme l'analyse heuristique ou comportementale abordée ci-dessous, afin de surmonter les limites inhérentes à cette technique.

Pratiques de base : Les fournisseurs doivent s'assurer que leurs bases de données de signatures sont à jour et ils doivent contribuer au partage d'informations sur les logiciels malveillants.

Capacités avancées : Les fournisseurs peuvent combiner l'analyse des signatures avec l'analyse de l'heuristique du code (décrite ci-dessous) et des comportements du trafic réseau (également décrits ci-dessous) pour obtenir de meilleurs résultats.

b) Analyse heuristique

L'analyse heuristique détecte les logiciels malveillants en examinant le code à la recherche de signes connus de problèmes. Il n'est pas nécessaire que le code corresponde exactement à un logiciel malveillant connu pour être signalé comme potentiellement malveillant. L'analyse heuristique recherche de nombreux indices différents pour déterminer si un code est suspect. Dans l'analyse heuristique statique, le code potentiellement malveillant est comparé au code des logiciels malveillants dans une base de données et s'il y a suffisamment de similitudes, le code est signalé. Bien que la possibilité de faux positifs existe, l'analyse heuristique est bien plus efficace que l'analyse des signatures pour combattre les menaces inconnues et évolutives. Parfois, afin de déconstruire le code en toute sécurité, les scientifiques stockent le code suspect qu'ils pensent être un logiciel malveillant dans une machine virtuelle appelée "sandbox", ce qui l'empêche de se propager à d'autres hôtes. Cette méthode est connue sous le nom d'analyse heuristique dynamique. [42]

Capacités avancées : Les fournisseurs peuvent détecter des menaces précédemment inconnues en utilisant une combinaison d'analyses heuristiques statiques et dynamiques. Les fournisseurs disposant d'équipes de chercheurs peuvent analyser le code suspect à l'intérieur d'un bac à sable afin de déterminer des stratégies d'atténuation efficaces, qui peuvent être partagées avec d'autres parties prenantes de l'écosystème.

c) Analyse comportementale

Alors que l'analyse des signatures et l'analyse heuristique se concentrent toutes deux sur le code des logiciels malveillants, l'analyse comportementale se concentre sur les "symptômes" de l'infection par les logiciels malveillants. Lorsque le trafic réseau indique un comportement inattendu, il se peut que l'origine de ce changement de comportement ne soit pas évidente au premier abord. Cependant, il existe des indicateurs connus qu'un logiciel peut être malveillant, par exemple lorsqu'il tente de obtenir des privilèges élevés ou interagir de manière anormale avec d'autres logiciels ou fichiers sur un système. L'analyse comportementale est souvent comparée à la profession médicale : un médecin peut souvent dire qu'une personne est malade avant même de savoir exactement quel est le problème. L'analyse comportementale complète d'autres types d'analyse en découvrant des menaces inconnues qui n'ont pas encore été identifiées et n'ont donc pas de signatures connues. [43]

Capacités avancées : Les fournisseurs peuvent utiliser des algorithmes pour détecter les schémas de trafic anormaux et s'appuyer sur les connaissances institutionnelles ou, si nécessaire, engager des experts en sécurité externes pour diagnostiquer les causes sous-jacentes du trafic anormal.

d) Échantillonnage de paquets

Pour donner un sens aux énormes quantités de données qui circulent sur un réseau, de nombreux grands fournisseurs utilisent une technique appelée échantillonnage de paquets. Cette technique consiste à développer des vues riches du flux de trafic à partir d'échantillons de trafic réseau capturés par les routeurs. En réduisant la quantité de données à inspecter, l'échantillonnage de paquets permet aux opérateurs de grands réseaux d'analyser le trafic, même si la taille et la vitesse des réseaux modernes augmentent.

Pratiques de base : Les fournisseurs devraient au moins échantillonner des paquets de manière pseudo-aléatoire†, en donnant aux paquets une chance d'être sélectionnés pour l'inspection. Cet échantillonnage peut être effectué sur une base neutre en termes de contenu.

Capacités avancées : Les fournisseurs peuvent utiliser des techniques d'échantillonnage plus complexes qui pondèrent les probabilités et s'adaptent de manière réactive aux changements de trafic. Ils peuvent rechercher des contenus spécifiques associés à des menaces de logiciels malveillants.

e) Honeypots et leurres au niveau des données

En plus des solutions au niveau du réseau décrites ci-dessus, les fournisseurs peuvent utiliser des leurres au niveau des données, tels que les pots de miel, pour "appâter" les attaquants. Un pot de miel est généralement constitué de données ou d'un système au sein d'un réseau qui semble avoir de la valeur pour les acteurs malveillants, qui sont ensuite bloqués ou surveillés lorsqu'ils tentent d'y accéder. Il convient de noter que les pots de miel et autres leurres peuvent être déployés par des tiers, et que les fournisseurs peuvent travailler avec ces entités pour découvrir des activités criminelles potentielles ou d'autres cyberattaques. En raison de leur utilité dans la découverte d'activités criminelles, les pots de miel sont utilisés dans les opérations d'infiltration des forces de l'ordre.

Pratiques de base : Les fournisseurs peuvent déployer un pot de miel à faible interaction, dont les fonctionnalités et les capacités de collecte d'informations sont limitées, mais qui présente un faible risque car aucune intrusion réelle n'a lieu. Le pot de miel simule une intrusion réussie pour tromper les attaquants et recueillir des informations sur eux.

Capacités avancées : Les fournisseurs peuvent en apprendre davantage sur les attaquants en déployant un pot de miel à forte interaction. Dans ce scénario, un attaquant interagit avec le système réel du fournisseur plutôt qu'avec une imitation, ce qui expose souvent des vecteurs d'attaque inconnus auparavant. En raison de l'exposition accrue aux attaques, les pots de miel à forte interaction sont intrinsèquement plus risqués, mais aussi plus révélateurs des méthodes des attaquants.

† Les nombres ou processus "pseudo-aléatoires" présentent des caractéristiques imprévisibles similaires à celles des nombres ou processus véritablement aléatoires, mais ne sont pas réellement aléatoires ou imprévisibles d'un point de vue mathématique. Dans les systèmes ne permettant pas de générer un véritable caractère aléatoire, le caractère pseudo-aléatoire est utilisé.

2. ATTÉNUER LES MENACES DISTRIBUÉES

Compte tenu de la détection du trafic malveillant et des menaces potentielles, les fournisseurs d'infrastructures peuvent également appliquer diverses méthodes d'atténuation, décrites ci-dessous, pour relever ces défis.

Résumé des pratiques d'atténuation de base : Les fournisseurs doivent utiliser le filtrage à l'entrée, c'est-à-dire appliquer un filtre qui peut limiter le débit du trafic entrant. Les fournisseurs devraient également faire un effort raisonnable pour façonner le trafic sur leurs réseaux et utiliser le blackholing et le sinkholing comme outils de gestion du réseau.

Résumé des capacités avancées d'atténuation : Les entreprises ayant accès à des ressources plus importantes peuvent utiliser le filtrage de sortie en plus du filtrage d'entrée, limitant ainsi le débit du trafic sortant et entrant. Elles peuvent utiliser des listes de contrôle d'accès (ACL) pour réduire les vecteurs d'attaque. Les entreprises peuvent prendre des mesures pour minimiser les interruptions de service lors de la mise en forme du trafic, par exemple en déployant des trous noirs sélectifs. Elles peuvent utiliser des technologies telles que BGP flowspec pour augmenter les options de gestion du trafic. Elles peuvent travailler en partenariat avec le gouvernement et l'industrie pour démanteler les botnets malveillants. Ils peuvent également proposer des services commerciaux tels que l'épuration du trafic et la protection DDoS.

a) Filtrage

L'une des complications de la lutte contre les réseaux de zombies réside dans le fait que les acteurs malveillants utilisent l'usurpation d'adresse IP pour faire croire que le mauvais trafic provient d'un autre endroit que son lieu d'origine réel. [44]

En filtrant le mauvais trafic à son entrée dans le réseau du fournisseur, ce dernier peut réduire l'efficacité de l'usurpation d'identité et donc rendre les attaques DDoS plus difficiles à réaliser.

En filtrant le mauvais trafic à son entrée sur le réseau du fournisseur (c'est-à-dire le filtrage à l'entrée, BCP38 et BCP84)[45], les fournisseurs peuvent réduire l'efficacité de l'usurpation d'identité et donc rendre les attaques DDoS plus difficiles à réaliser. En raison des avantages facilement observables de cette pratique, l'Internet Engineering Task Force (IETF) a reconnu le filtrage à l'entrée comme une meilleure pratique. [46] Il convient de noter que le filtrage à l'entrée fonctionne mieux aux points d'entrée du réseau, comme les locaux des clients, alors qu'il est beaucoup plus difficile aux points d'échange du réseau.

En outre, si les fournisseurs sont souvent bien placés pour filtrer le trafic malveillant, des techniques telles que le BCP38 devraient être employées par toute entité qui exploite son propre espace d'adressage IP, y compris les entreprises. Les fournisseurs tels que car les FAI attribuent de nombreuses adresses IP à leurs clients qui, à leur tour, peuvent exploiter leurs propres capacités de filtrage et doivent également respecter le PCA38.

De plus, en déployant des filtres à la périphérie de leurs réseaux, les fournisseurs peuvent surveiller le trafic sortant ou sortant de leur coin de l'écosystème et réduire les dommages causés aux autres parties. Le filtrage à la sortie ne remplace pas le filtrage à l'entrée, mais constitue plutôt une solution complémentaire. Une combinaison de filtrage à l'entrée et à la sortie est le meilleur moyen pour les fournisseurs d'accroître la résilience. 47

Enfin, dans un environnement réseau, les ACL sont utilisées pour identifier les flux de trafic en fonction de paramètres tels que la source et la destination, le protocole IP, les ports, le type Ether et d'autres caractéristiques. Un exemple courant est que le trafic d'une interface de sécurité inférieure ne peut pas accéder à une interface de sécurité supérieure. 48 Dans certains contextes, les ACL peuvent être configurées pour tenir compte des privilèges d'accès des utilisateurs individuels afin de limiter davantage les vecteurs d'attaque par lesquels les logiciels malveillants peuvent infiltrer un réseau.

Pratiques de base : Les fournisseurs devraient filtrer le trafic entrant (filtrage à l'entrée) aux points d'entrée du réseau afin de réduire la quantité de trafic malveillant qui entre dans leurs réseaux. Le filtre doit être capable de limiter le débit du trafic entrant en cas d'attaque qui pourrait submerger les ressources du réseau.

Capacités avancées : Idéalement, les fournisseurs devraient filtrer le trafic sortant (filtrage de sortie) en plus du trafic entrant, et ils devraient être en mesure de limiter le débit du trafic, qu'il soit sortant ou entrant. Cette solution hybride offre une plus grande protection et fait des fournisseurs des voisins responsables vis-à-vis des autres membres de l'écosystème.

En outre, les fournisseurs peuvent utiliser les ACL pour réduire les vecteurs d'attaque.

b) Mise en forme du trafic

Lorsque du trafic potentiellement malveillant est identifié, les fournisseurs peuvent gérer le trafic en toute sécurité, soit en utilisant des techniques qui aboutissent généralement à l'abandon du trafic, soit en retardant le trafic lorsque le débit de données est anormalement élevé. Ces deux techniques peuvent être utiles dans des circonstances spécifiques et peuvent faire partie d'une stratégie globale de gestion du trafic. [49]

Pratiques de base : Les fournisseurs doivent faire un effort raisonnable pour façonner le trafic sur leurs réseaux. Au minimum, les fournisseurs devraient être en mesure de déployer un "trou noir" qui empêche le trafic d'atteindre une cible. Des efforts doivent être faits pour réduire les perturbations des services légitimes en redirigeant le trafic ou en le laissant tomber uniquement dans des régions géographiques définies.

Capacités avancées : Les fournisseurs disposant de plus de ressources peuvent façonner le trafic sans causer autant de perturbations au trafic légitime. Par exemple, les centres commerciaux d'épuration peuvent nettoyer le trafic en filtrant les éléments malveillants et en envoyant le trafic légitime à sa destination. Les petits fournisseurs peuvent former des partenariats avec les grands fournisseurs pour offrir ces services à leurs clients.

c) Blackholing

Le blackholing est une technique qui supprime tout le trafic destiné à une destination en ligne spécifique. Une version courante de cette technique est le remotely triggered destination based blackholing (RTDBH), dans lequel les réseaux en amont, qui sont généralement les plus proches de la source de l'attaque, suppriment le trafic malveillant avant qu'il n'atteigne une victime potentielle.

Bien que le blackholing soit efficace pour empêcher le trafic malveillant d'atteindre sa destination, un inconvénient évident est que le trafic légitime ne peut pas non plus atteindre la destination, ce qui peut être le but explicite des acteurs malveillants. Pour minimiser ce problème, les fournisseurs peuvent utiliser une technique connue sous le nom de blackholing sélectif, qui supprime le trafic provenant de régions géographiques choisies (comme un pays ou un continent) tout en permettant au trafic provenant d'autres régions d'atteindre sa destination.

Pratiques de base : Les fournisseurs devraient avoir recours au blackholing pour protéger leurs réseaux. Même si, idéalement, les fournisseurs devraient minimiser les perturbations du trafic légitime, ils devraient au moins déployer le RTDBH de base dans les cas où des outils plus granulaires ne sont pas disponibles ou ne fonctionneraient pas aussi bien.

Capacités avancées : Les fournisseurs peuvent améliorer l'efficacité du blackholing en tirant parti de partenariats avec d'autres fournisseurs, tant pour les capteurs que pour les points de présence de filtrage. En outre, les fournisseurs peuvent déployer des trous noirs sélectifs qui minimisent les perturbations du trafic légitime en ciblant une région géographique spécifique.

d) Sinkholing

Le sinkholing est une technique par laquelle le trafic à l'intérieur d'une plage d'IP particulière est envoyé vers un serveur désigné (le "sinkhole"), tandis que le trafic à l'extérieur de cette plage d'IP se poursuit normalement. Le but du sinkholing est de capturer les botnets à des fins de recherche et d'atténuation. Le sinkholing est souvent réalisé par le biais du routage stratégique ou d'autres méthodes de routage, qui piègent les logiciels malveillants qui composent un botnet dans le sinkhole, où ils peuvent être étudiés par les forces de l'ordre et les chercheurs. Lorsque les logiciels malveillants pris dans un gouffre tentent de communiquer avec les serveurs de commande et de contrôle, les experts en sécurité peuvent suivre les adresses IP des machines auxquelles les logiciels malveillants transmettent des informations, ce qui leur permet de mieux comprendre les activités criminelles. Les fournisseurs peuvent également couper complètement les communications entre le logiciel malveillant et les serveurs de commande et de contrôle. Les failles sont essentielles au démantèlement à grande échelle des réseaux de zombies, qui utilisent des centaines de milliers de systèmes connectés à l'internet dans plusieurs pays du monde.

Pratiques de base : Les fournisseurs doivent utiliser le sinkholing comme outil de gestion du réseau pour rediriger le trafic malveillant entrant et recueillir des informations sur les menaces pesant sur le réseau du fournisseur à des fins d'analyse ou de partage d'informations.

Capacités avancées : Les leaders du secteur peuvent utiliser les sinkholes pour perturber et recueillir des renseignements sur les menaces à l'échelle de l'écosystème en partenariat avec d'autres fournisseurs et les forces de l'ordre. Les fournisseurs peuvent également aider les opérations internationales d'application de la loi en coordonnant efficacement les autorités et les parties prenantes dans de nombreuses juridictions.

e) Gommage

Les solutions d'épuration sont généralement mises en œuvre par des centres d'épuration spécialisés, qui analysent le trafic réseau et le débarrassent du trafic malveillant, notamment des attaques DDoS. Comme le filtrage est gourmand en ressources par rapport à d'autres solutions, plusieurs grands fournisseurs proposent le filtrage comme un service commercial. En redirigeant le trafic vers les centres au lieu de l'abandonner, l'épuration permet au trafic légitime d'atteindre sa destination avec un taux de réussite élevé. Cela fait du scrubbing une alternative préférable au blackholing et au sinkholing pour de nombreuses entreprises.

Capacités avancées : Les centres d'épuration peuvent ajouter une couche importante de protection aux défenses d'un fournisseur ou d'un client en filtrant de nombreux types d'attaques, sans se limiter aux attaques par inondation volumétrique. Par exemple, les centres peuvent intégrer une technologie qui protège contre les attaques basées sur le protocole SSL (liaisons cryptées).

f) BGP flowpec

La spécification de flux (flowspec) du protocole BGP (Border Gateway Protocol) est une technologie dynamique qui permet aux fournisseurs de déployer rapidement une variété d'options d'atténuation différentes, permettant ainsi aux experts de prendre des décisions en fonction de la situation. Contrairement aux routeurs qui ne prennent en charge que le blackholing, les routeurs flowspec permettent des options supplémentaires telles que le sinkholing du trafic afin qu'il puisse être étudié par des experts ou, alternativement, la mise en forme du trafic et son acheminement à un rythme défini. [51]

Capacités avancées : Les fournisseurs peuvent utiliser BGP flowspec pour élaborer des instructions personnalisées à l'intention des routeurs frontaliers, au lieu des solutions traditionnelles à taille unique. Grâce à BGP flowspec, les routeurs peuvent recevoir l'instruction d'abandonner le trafic, de le réacheminer ou d'en limiter le débit, sous réserve d'une validation appropriée de l'auteur du flux.

3. COORDONNER AVEC LES CLIENTS ET LES PAIRS

Pour remédier aux réseaux de zombies ou à d'autres menaces distribuées, les fournisseurs peuvent être amenés à informer leurs clients ou leurs pairs d'un développement afin de s'assurer de leur coopération. De toute évidence, l'efficacité des notifications aux utilisateurs dépend largement de ces derniers. Une étude commandée par le M3AAWG a révélé que les appels téléphoniques et le courrier postal sont les moyens les plus efficaces d'entrer en contact avec les utilisateurs. [52] Les autres méthodes disponibles, qui peuvent et doivent être utilisées, comprennent le courrier électronique et les avis sur les pages web. Une autre méthode pour contacter les utilisateurs est le "walled garden" - cette approche limite l'accès des utilisateurs aux services en ligne jusqu'à ce qu'ils prennent des mesures spécifiques déterminées par leur fournisseur. Dans certains pays, les approches de ce dernier type soulèvent des problèmes juridiques ou de politique publique. [53] Les pairs peuvent être notifiés avec plusieurs des mêmes méthodes que les clients. Les notifications seront plus efficaces s'il existe une relation établie. Il est utile pour les fournisseurs de se familiariser avec les acteurs clés de leur secteur d'activité afin de ne pas avoir à faire les présentations pour la première fois en cas d'urgence.

Pratiques de base : Les fournisseurs doivent avertir les clients ou les pairs qui violent la politique d'utilisation acceptable ou se livrent à des activités néfastes. Si le trafic d'un client ou d'un pair est bloqué, il faut fournir à la fois (1) un message texte ou téléphonique et (2) un avis par courriel/page Web du compte de l'utilisateur. Le client ou l'homologue doit recevoir des instructions claires sur la manière de contacter le fournisseur via des canaux de communication qui ne sont pas bloqués.

Capacités avancées : Les fournisseurs disposant d'un personnel formé et de ressources dédiées peuvent réduire considérablement le taux de faux positifs, de sorte que les clients subissent rarement une interruption lorsqu'ils utilisent les services de manière légitime.

4. SAISIE ET RETRAIT D'UN DOMAINE D'ADRESSE

Les forces de l'ordre disposent d'outils spécifiques qui ont été utilisés ces dernières années pour atténuer les effets des botnets malveillants et des acteurs criminels avec un certain succès. Lorsqu'il existe de bonnes preuves qu'un réseau criminel utilise des domaines particuliers pour mener à bien ses objectifs néfastes (par exemple, des attaques de botnets), un fournisseur peut travailler en coopération avec les forces de l'ordre - et généralement sur leurs instructions - pour supprimer les domaines, conformément aux lois en vigueur. Une action répressive qui entraîne des conséquences concrètes pour les acteurs malveillants est la seule solution qui s'attaque à la cause des réseaux de zombies et des attaques DDoS, plutôt qu'aux symptômes. Ce type d'action est gourmand en ressources et nécessite souvent une analyse médico-légale approfondie. Domaine à grande échelle

Les saisies peuvent également nécessiter des efforts coordonnés au niveau international. [54] Par exemple, en 2016, les fournisseurs ont collaboré avec des responsables gouvernementaux de plus de 30 pays pour démanteler le botnet Avalanche et prendre le contrôle de plus de 800 000 domaines dispersés dans l'écosystème mondial de l'internet et des communications. [55]

Pratiques de base : Les fournisseurs doivent tenir une liste facile à trouver des points de contact pour les forces de l'ordre et les chercheurs en sécurité. Les fournisseurs doivent également avoir une politique bien définie décrivant comment ils peuvent et ne peuvent pas soutenir les efforts des forces de l'ordre.

Capacités avancées : En général, les leaders du secteur disposent de plus de procédures et de technologies pour soutenir les forces de l'ordre. Ils auront également défini des politiques et des positions juridiques sur des tactiques spécifiques d'application de la loi. Ils peuvent procéder à une évaluation globale des risques pour tenir compte des exigences juridiques mondiales. En plus de coopérer avec les forces de l'ordre, les fournisseurs peuvent disposer de processus de collaboration avec les concurrents lors d'événements exceptionnels.

B. DÉVELOPPEMENT DE LOGICIELS

Les logiciels sont un élément de plus en plus omniprésent de tous les autres composants de l'écosystème abordé dans ce guide. Comme nous l'avons vu tout au long de ce guide, il existe une grande variété de processus de développement complexes et d'interdépendances qui favorisent l'innovation et l'amélioration des logiciels dans les principaux utilisateurs systémiques de logiciels mis en évidence dans ce guide : l'infrastructure, les dispositifs et systèmes de dispositifs, les installateurs de systèmes et les entreprises. Par conséquent, cette section n'a pas pour but de présenter les diverses pratiques de sécurité de base et les capacités avancées qui sont pertinentes pour le développement de logiciels spécialisés dans chaque partie de l'écosystème. Elle vise plutôt à souligner l'importance vitale d'un logiciel sécurisé dans toutes les parties de cet écosystème. Lorsqu'il n'est pas abordé spécifiquement ailleurs dans ce guide, le développement de logiciels devrait généralement comporter les pratiques suivantes.

Pratiques de base et capacités avancées pour les logiciels :

1. PRATIQUES DE DÉVELOPPEMENT "SECURE-BY-DESIGN

Les logiciels et les applications sont de plus en plus intégrés dans nos processus et produits commerciaux et d'infrastructure afin d'en améliorer l'efficacité. Mais cela en fait une cible de choix pour les pirates informatiques. L'économie mondiale, les infrastructures critiques et les opérations gouvernementales sont de plus en plus dépendantes des logiciels.

Les organisations qui suivent les meilleures pratiques font de la sécurité un élément de qualité, en appliquant une série de pratiques de développement sécurisé, notamment la formation des développeurs, l'analyse statique de la sécurité des applications, la modélisation des menaces, les tests dynamiques de sécurité des applications et les tests de pénétration manuels tout au long du cycle de développement sur la base de la gestion des risques. Des ressources destinées à aider les développeurs à adopter ces meilleures pratiques sont accessibles au public. Par exemple, SAFECode (le Software Assurance Forum for Excellence in Code), une organisation de premier plan qui se consacre à la promotion de l'assurance logicielle, publie des ressources de formation au développement de logiciels sécurisés mises gratuitement à la disposition du public, notamment les Fundamental Practices for Secure Software Development. [56]

Pratiques de base : Le développement sécurisé par conception doit inclure au minimum les éléments suivants :

- Chiffrement fort des données au repos et en transit : Le cryptage inhibe la visibilité des données en cas de vol ou d'accès inapproprié. Que les données soient au repos (c'est-à-dire stockées) ou en transit, le chiffrement est un outil essentiel pour protéger les informations. Bien qu'il existe différentes options de cryptage adaptées aux besoins d'organisations et de produits spécifiques, le cryptage doit généralement utiliser un algorithme fort qui ne peut pas être cassé facilement dans le contexte de son utilisation particulière. La puissance d'un algorithme peut varier selon le contexte, en fonction de facteurs tels que le type d'attaque en cause et la nécessité de faire fonctionner correctement certains types de services. Par exemple, un chiffrement fort peut empêcher la plupart des pare-feu et autres services d'inspection des paquets de sécurité de fonctionner.
- Sécurité par défaut : Les paramètres de configuration par défaut des logiciels devraient mettre l'accent sur la sécurité. Les paramètres devraient devoir être délibérément modifiés pour que le logiciel abaisse ses défenses afin de permettre plus d'options. Ce principe réduit considérablement les vecteurs d'attaque que les acteurs malveillants peuvent exploiter.
- Patchabilité et conception pour la mise à jour : Les logiciels doivent être conçus en prévoyant que des correctifs et des mises à jour seront nécessaires pour se protéger contre les attaques en constante évolution et de plus en plus sophistiquées des acteurs malveillants. Les correctifs et les mises à jour doivent pouvoir être livrés avec une intervention manuelle minimale, de manière raisonnablement rapide et sécurisée, aux systèmes sur lesquels le logiciel est installé.
- Principe du moindre privilège : En limitant l'accès des utilisateurs et des applications aux seuls privilèges essentiels nécessaires à l'exécution des tâches nécessaires, les développeurs de logiciels peuvent réduire la surface d'attaque d'un produit. L'application du principe du moindre privilège lors de la phase de conception réduit les chances qu'un acteur malveillant ou un service compromis obtienne un accès administratif et le contrôle d'un système.
- Analyse de la composition du logiciel : L'objectif de cette analyse est de créer un inventaire des composants open source et autres composants tiers présents dans le produit. Ce faisant, les développeurs de logiciels peuvent rester conscients des composants qu'ils n'ont pas développés eux-mêmes en cas de problème, même s'ils ne peuvent pas garantir la sécurité des composants tiers et open source. Le fait de disposer d'un inventaire des composants utilisés dans les produits et les applications peut également aider les organisations de développement à suivre et à identifier les vulnérabilités connues associées.
- Sensibilisation et éducation à la sécurité des logiciels : La sensibilisation doit s'étendre à tout le personnel qui fait partie du processus de développement des logiciels, y compris les développeurs, les chefs de produit et autres. Des possibilités d'éducation ou des exercices de formation rentables devraient être mis à disposition.

Capacités avancées : Les pratiques de pointe en matière de sécurité par la conception comprennent les éléments suivants :

- Test dynamique de sécurité des applications (DAST) : Cette technologie avancée utilise les tests de pénétration (une attaque simulée) pour découvrir les vulnérabilités pendant l'exécution d'une application. Ce type de test peut être particulièrement utile dans le contexte de l'IdO. Toutefois, il nécessite des options de configuration gérables et la possibilité d'embaucher des spécialistes hautement qualifiés.

- Test statique de sécurité des applications (SAST) : Grâce à cette technologie avancée, les développeurs peuvent analyser le code source ou les binaires et identifier les vulnérabilités. Elle est limitée aux langues et aux plateformes prises en charge. Pour de nombreux produits dans l'espace IoT, cela pourrait ne pas être une option. Toutefois, un examen minutieux du code par les pairs des composants particulièrement sensibles peut être utilisé pour renforcer la sécurité.
- Modélisation des menaces et analyse des risques pour l'architecture : Les entreprises qui travaillent avec des gouvernements ou dont les opérations sont très sensibles peuvent engager des équipes d'experts pour déterminer comment des acteurs malveillants créeraient ou exploiteraient hypothétiquement les vulnérabilités d'un système pour parvenir à des fins néfastes. Un modèle de menace peut prendre en compte de nombreux types de risques, y compris ceux impliquant des attaques automatisées et distribuées.
- Chaînes d'outils axées sur la sécurité : Les développeurs peuvent utiliser des chaînes d'outils axées sur la sécurité pour créer de nouveaux logiciels. Une chaîne d'outils est un ensemble d'outils logiciels ou matériels qui facilitent le développement de logiciels. Lorsque les chaînes d'outils donnent la priorité à la sécurité, les erreurs de codage sont moins fréquentes et les fournisseurs peuvent appliquer des contrôles de qualité. Les entreprises peuvent intégrer les nouvelles vulnérabilités et les leçons apprises dans les outils de développement.
- Sécuriser les composants tiers et open source : Les entreprises leaders s'assureront que les composants tiers et les bibliothèques open source utilisés sont exempts de vulnérabilités connues.
- En outre, les entreprises peuvent fournir une attestation aux clients sur les éléments du processus de développement de logiciels sécurisés et demander une certification d'alignement sur les normes internationales.

2. GESTION DE LA VULNÉRABILITÉ DE LA SÉCURITÉ

Les entreprises du monde entier ont des politiques différentes en ce qui concerne le moment et la durée de mise à disposition des correctifs de sécurité aux clients après la commercialisation d'un produit, afin de remédier aux vulnérabilités récemment découvertes. Si les grands fabricants de produits ont tendance à publier plus régulièrement des correctifs pour leurs produits, les petits fabricants sont généralement moins susceptibles de consacrer des ressources suffisantes au développement et à la mise à disposition de correctifs de sécurité. [57]

Pratiques de base : Les fournisseurs doivent donner la priorité aux vulnérabilités critiques dans les applications essentielles à la mission.

Capacités avancées : Les fournisseurs plus avancés peuvent corriger presque toutes les vulnérabilités connues, en particulier celles qui ont été classées par ordre de priorité lors de l'évaluation des risques. Ils sont en mesure de fournir une assurance de sécurité aux personnes qui achètent des logiciels auprès de leur entreprise ou qui interagissent avec elle par le biais d'applications.

3. TRANSPARENCE DES PROCESSUS DE DÉVELOPPEMENT SÉCURISÉS

Chacune des pratiques ci-dessus joue un rôle important dans le développement de logiciels et de matériels sécurisés. Les organisations de développement de logiciels et le secteur privé ont lancé le développement d'évaluations des processus de développement sécurisé basées sur le marché. [58] Cependant, un cadre élaboré en partenariat entre le gouvernement et les parties prenantes de l'industrie pourrait aider à normaliser la terminologie et les processus, renforçant ainsi la confiance du marché. en partenariat avec SAFECode et d'autres parties prenantes pour élaborer une publication spéciale sur la sécurité les processus et pratiques de développement de logiciels

Le NIST est actuellement

La NTIA convoque un processus multilatéral pour explorer comment les organisations peuvent communiquer des informations sur les composants logiciels tiers et offrir une plus grande transparence. [59]

Pratiques de base : Fournir une attestation de la posture de sécurité aux entreprises qui achètent des logiciels.

Capacités avancées : Fournir une assurance de sécurité à ceux qui achètent des logiciels à l'entreprise et interagissent avec l'entreprise par le biais d'applications.

C. DISPOSITIFS ET SYSTÈMES DE DISPOSITIFS

Un dispositif connecté individuel (ou "dispositif d'extrémité") peut lui-même être constitué de plusieurs composants, notamment des modules matériels, des puces, des logiciels, des capteurs ou d'autres composants d'exploitation. Des centaines de milliers d'entreprises et des millions de développeurs contribuent potentiellement aux milliards d'appareils individuels déployés dans le monde. Au-delà de l'appareil individuel lui-même, il existe de multiples couches supplémentaires de connectivité qui constituent un nouveau marché très dynamique - y compris pour l'innovation en matière de sécurité. Pour faire simple, les appareils connectés ne sont plus simplement des appareils individuels. En gardant cette complexité à l'esprit, ce guide traite des systèmes de dispositifs : l'union d'un dispositif d'extrémité connecté - c'est-à-dire une "chose" dans l'internet des objets - et de ses éléments de support associés ailleurs sur l'internet, y compris les applications et les services en nuage. [60]

Pratiques de base et capacités avancées pour les dispositifs et les systèmes de dispositifs

1. PRATIQUES DE DÉVELOPPEMENT "SECURE-BY-DESIGN

La sécurité est meilleure et plus efficace si elle fait partie du processus de développement précoce et si elle est incluse comme un facteur clé tout au long de ce processus. Certaines catégories de meilleures pratiques sont désormais communément acceptées comme des outils nécessaires pour garantir que le produit final présente les caractéristiques essentielles de confidentialité, d'intégrité et de disponibilité. [61] Les botnets tirent parti des faiblesses de la mise en œuvre des dispositifs et des systèmes. Il est donc tout à fait approprié d'inclure la planification de la sécurité dès le début et à tous les stades du développement du produit pour éviter ces faiblesses.

a) Processus de cycle de vie du développement sécurisé

Pratiques de base : Un processus de cycle de développement sécurisé (SDL) doit être mis en place. Dans le processus SDL, chaque phase de développement comporte des activités de sécurité qui peuvent être effectuées manuellement ou automatiquement. [62]

Capacités avancées : Après avoir établi un processus de cycle de vie de développement sécurisé, l'entreprise avancée mesure et développe les capacités du processus. La mesure des capacités du SDL fait partie du projet BSIMM (Building Security In - Maturity Model63) ; les documents du BSIMM sont en source ouverte et peuvent constituer une ressource pour cet effort.

b) Éléments d'une conception sûre

Cette section énumère les pratiques qui se situent au niveau du développeur dans la conception du produit.

(1) Moyens de protection des données au repos et en transit

Cette catégorie concerne principalement la protection des données stockées sur le dispositif et le chiffrement des communications de données. La mise en œuvre de ces protections peut impliquer des décisions concernant, par exemple, des éléments matériels sécurisés, un processus de démarrage sécurisé, etc : Racines de la confiance.

Pratiques de base : Les communications de données doivent être cryptées. Les données sensibles doivent être stockées de manière cryptée. Indépendamment des protocoles utilisés, si l'authentification est disponible, elle doit être utilisée. En général, les mécanismes de sécurité disponibles dans le système utilisé doivent être employés. Les techniques cryptographiques utilisées doivent éviter les méthodes obsolètes.

Capacités avancées : Les dernières versions des protocoles et des mécanismes de sécurité doivent être utilisées. La mémoire sécurisée peut être utilisée au lieu du cryptage pour les informations stockées. Il convient d'utiliser des méthodes de cryptage conformes à la norme NIST FIPS 140-2 ou ISO/IEC 24759. [64]

(2) Moyens de restreindre l'accès non autorisé

Pratiques de base : Les produits IoT nécessitent généralement des services administratifs locaux ou distants. Pendant le développement et la fabrication du produit, il peut y avoir des exigences pour d'autres types d'accès de bas niveau à la mémoire, au processeur, aux périphériques ou au flux de contrôle qui ne sont pas nécessaires ou disponibles pour l'utilisateur final de l'appareil. Ces capacités supplémentaires doivent être soigneusement protégées.

Les mesures typiques à ce niveau sont les suivantes : Des identifiants "admin" uniques par appareil ou l'obligation de changer les mots de passe au premier démarrage ; des techniques de limitation du débit pour empêcher l'identification par force brute des mots de passe ; la sécurisation ou la désactivation des ports et services de niveau développeur avant l'expédition du produit ; la suppression des services d'administration locaux et distants inutilisés ou non sécurisés tels que telnet.

Capacités avancées : Le contrôle d'accès des utilisateurs par authentification multi-facteurs doit être pris en charge.

En outre, les développeurs de dispositifs d'extrémité et de routeurs doivent prendre en compte les normes nouvelles et émergentes qui aident spécifiquement à prévenir l'accès non autorisé et l'utilisation par les botnets. Par exemple, le descripteur d'utilisation du fabricant (recommandation proposée) ou "MUD "[65] de l'IETF peut convenir à de nombreux cas d'utilisation. MUD est "une norme de logiciel intégré définie par l'IETF qui permet aux fabricants de dispositifs IoT d'annoncer les spécifications des dispositifs, y compris les schémas de communication prévus pour leur dispositif lorsqu'il se connecte au réseau".[66] Lorsque le dispositif et le routeur adhèrent aux exigences MUD, le routeur dispose d'un mécanisme pour limiter un dispositif aux fins prévues par le fabricant. Les activités en dehors de ces objectifs, comme la participation à une attaque DDoS massive, peuvent être identifiées et bloquées par le routeur local. D'autres normes telles que l'IEEE 802.1AR67 et l'architecture DICE (Device Identifier Composition Engine)[68] peuvent améliorer la sécurité du dispositif IoT et de ses composants MUD.

(3) Utilisation de l'obfuscation

Pratiques de base : Les fabricants de dispositifs ne doivent pas compter uniquement sur l'utilisation de l'obscurcissement pour sécuriser les secrets (par exemple, les clés des dispositifs, les données sensibles), mais l'obscurcissement peut être utilisé pour augmenter la difficulté d'un attaquant à localiser le secret. Néanmoins, le secret doit être protégé par d'autres moyens tels que le contrôle d'accès et le cryptage.

Capacités avancées : Mise en œuvre de la ligne de base également.

(4) Validation de l'entrée de l'utilisateur et codage de la sortie du système

Pratiques de base : Toute entrée reçue de l'extérieur du système doit être gérée de manière à ce qu'un adversaire extérieur ne puisse pas tirer parti de conséquences involontaires. L'entrée doit être validée pour la longueur, le type de caractère et les valeurs ou plages acceptables ; voir aussi liste blanche.

le filtrage. La sortie d'un sous-système vers un autre ou vers un autre site doit également être filtrée ; voir "canonisation des caractères".

Capacités avancées : Mise en œuvre de la ligne de base également.

(5) Cryptographie adaptée aux besoins du produit.

Pratiques de base : Des méthodes cryptographiques sont nécessaires pour assurer l'intégrité et la confidentialité des données, l'authentification des droits et la non-répudiation des demandes. Ces méthodes cryptographiques doivent être choisies en fonction du risque évalué, mais doivent utiliser des méthodes et des algorithmes ouverts et évalués par des pairs. Dans la mesure du possible, les méthodes cryptographiques sont actualisables.

Capacités avancées : Cryptographie forte, éprouvée et actualisable utilisant des méthodes et des algorithmes ouverts et évalués par les pairs. Veillez à ce que la cryptographie ait la capacité de prendre en charge des longueurs de clés résistantes post-quantiques pour le cryptage symétrique.

2. RACINES DE LA CONFIANCE

Divers types d'attaques reposent sur l'imitation d'une autre entité. Par exemple, une source de confiance pour les nouveaux logiciels d'un appareil est généralement le fabricant du matériel d'origine. L'installation d'un logiciel corrompu par un logiciel malveillant est évidemment à éviter. D'où la question de savoir comment faire la différence.

La solution consiste à mettre en place un système de confiance. Une chaîne de confiance est un enchaînement d'éléments matériels et logiciels dans lequel chaque élément est validé au fur et à mesure qu'il est ajouté à la chaîne. Au début de la chaîne se trouve une racine de confiance, qui est fournie par une entité faisant autorité. La validation est effectuée de manière cryptographique, à l'aide de signatures numériques. Comme le premier élément renvoie à une autorité de confiance, chaque élément validé cryptographiquement par la chaîne peut également être fiable.

Lorsque le système reçoit une mise à jour logicielle signée, il peut vérifier la signature numérique. Comme le système lui-même est ancré dans la confiance de l'entité d'origine faisant autorité, une fois la mise à jour logicielle validée, on peut faire confiance au logiciel.

a) Sécurité fondée sur le matériel

Pratiques de base : Examinez comment la sécurité liée au matériel s'intègre dans les cycles de développement sécurisé des produits actuels et futurs.

Capacités avancées : La sécurité à base de matériel est utilisée lorsque cela est techniquement possible.

3. GESTION DU CYCLE DE VIE DES PRODUITS, Y COMPRIS LA FIN DE VIE

La gestion du cycle de vie des produits fait référence à la gestion active d'un produit, de sa conception à sa fin de vie, en passant par sa fabrication et son support. La gestion de la fin de vie fait référence à une politique définie sur ce qui doit être fait lorsque le produit a atteint un point final défini dans son cycle de vie, y compris la fin d'une période de support définie, la fin d'une fonctionnalité, la fin d'une période calendaire, etc.

Pratiques de base : Les fabricants de dispositifs peuvent informer le consommateur de la politique de soutien à la sécurité et de la manière dont le dispositif est soutenu par des mises à jour pendant et après la période de soutien. Dans la mesure du possible, le dispositif doit prendre en charge la gestion des actifs du réseau en permettant d'identifier et d'auditer le dispositif de manière logique et physique et avec un contrôle d'accès approprié.

Après la période d'assistance, les consommateurs doivent avoir la possibilité de mettre l'appareil hors service et être informés de la manière de le faire. La mise hors service doit permettre au consommateur de rétablir les paramètres d'usine du produit et de supprimer toute information d'identification personnelle (IIP). Cette capacité couvre une variété de scénarios tels que la vente, l'abandon ou le recyclage du produit, y compris la vente d'une propriété sur laquelle sont installés des dispositifs IoT.

Les fournisseurs doivent créer une politique et un processus de vulnérabilité de sécurité pour identifier, atténuer et, le cas échéant, divulguer les vulnérabilités de sécurité connues dans leurs produits.

Capacités avancées : Un plan pour des mises à jour sécurisées avec une protection anti-retour et un contrôle d'accès approprié tout au long d'une période de support de sécurité définie, lorsque cela est techniquement possible. [69]

4. UTILISATION DE LA CHAÎNE D'OUTILS AXÉE SUR LA SÉCURITÉ

Les chaînes d'outils axées sur la sécurité sont des ensembles de logiciels ou de matériels qui permettent non seulement le développement, la production et la gestion de produits, mais qui ont également été conçus pour renforcer la sécurité du produit final.

Pratiques de base : Il convient d'utiliser des outils capables de vérifier si l'implémentation suit les directives de codage sécurisé et de rechercher un sous-ensemble de vulnérabilités et d'expositions communes (CVE) connues dans le logiciel libre.

Capacités avancées : Des outils tels que le fuzzing, l'exécution symbolique, le sandboxing, l'analyse statique et dynamique et les langages à mémoire sécurisée sont utilisés pour trouver et atténuer les vulnérabilités.

D. INSTALLATION DE SYSTÈMES DOMESTIQUES ET DE PETITES ENTREPRISES

Les foyers et les petites entreprises bénéficient d'appareils connectés dans plusieurs catégories. Les systèmes de chauffage, de ventilation et de climatisation (CVC) sont connectés pour des fonctions intelligentes et un accès à distance par l'occupant. Les systèmes de sécurité comprennent des caméras, des serrures et des systèmes d'alarme qui peuvent tous être gérés via l'internet. Les systèmes de divertissement bénéficient de commandes centrales qui permettent de gérer facilement des configurations audio et vidéo complexes. Il existe une très grande diversité de fabricants et de systèmes dans ces catégories. Ces systèmes peuvent être installés par des propriétaires de maisons ou d'entreprises qui se débrouillent seuls, ou par des professionnels : intégrateurs, installateurs d'alarmes, etc.

Dans l'idéal, chaque appareil et système entrant dans une maison, un bureau, un magasin, un environnement médical ou industriel sera sécurisé par les meilleures pratiques tout au long du cycle de vie de l'appareil. Ce cycle de vie comprend l'installation et la configuration de l'appareil. Une bonne installation permet d'obtenir la "meilleure sécurité disponible" du produit fabriqué. Cette section présente les pratiques de base et les capacités avancées permettant d'obtenir la meilleure sécurité possible pour les types de dispositifs les plus courants.

Le matériel ci-dessous s'inspire largement de The Connected Home Security System. [70]

Pratiques de base et capacités avancées pour l'installation de systèmes domestiques et de petites entreprises

1. AUTHENTIFICATION ET GESTION DES JUSTIFICATIFS D'IDENTITÉ

Les installations peuvent bénéficier des systèmes de gestion des mots de passe, qui sont un stockage crypté des mots de passe. Grâce à ces systèmes, les utilisateurs n'ont plus à se souvenir des mots de passe, à les gérer et à les placer dans un endroit sûr.

Pratiques de base : Si un mot de passe n'est pas unique pour le dispositif, l'installateur doit le changer pour un mot de passe fort. (Voir [1], "Mots de passe"). Des mots de passe différents doivent être utilisés pour tous les dispositifs et systèmes. L'installation doit utiliser un système de gestion des mots de passe de confiance.

Capacités avancées : Le contrôle d'accès des utilisateurs par authentification multi-facteurs est utilisé.

2. LA CONFIGURATION DU RÉSEAU

La configuration du réseau fait référence à la disposition physique et logique, aux connexions et aux paramètres des composants du réseau.

a) Généralités

Pratiques de base : Les systèmes (ordinateurs de bureau, ordinateurs portables, etc.) doivent avoir des outils antivirus et anti-malware à jour installés et en fonctionnement. Aucun système avec des privilèges administratifs ne doit être en cours d'exécution, sauf si cela est spécifiquement requis.

b) Configuration du pare-feu, du point d'accès et du routeur

Pratiques de base : L'UPnP doit être désactivé du côté WAN (côté Internet), à moins qu'il ne soit nécessaire à des fins légitimes (p. ex., jeux en mode poste à poste). Un espace DHCP adéquat doit être alloué pour l'utilisation prévue, mais sans dépasser l'utilisation prévue. Un pare-feu doit être activé et seuls les ports nécessaires doivent être débloqués. Le transfert de port doit être désactivé, sauf pour des applications spécifiques où il est nécessaire.

Capacités avancées : Les réseaux doivent être surveillés, les applications doivent utiliser des valeurs de port non standard et le transfert de port ne doit être activé que de manière sélective pour des applications spécifiques, en conjonction avec les protections du pare-feu. Bien qu'un attaquant sophistiqué puisse le contourner, le filtrage des adresses MAC doit toujours être utilisé.

c) Structure physique et logique

Pratiques de base : L'accès au réseau doit être limité depuis l'extérieur de la structure physique du site client en termes d'alimentation sans fil et de placement du câblage physique. Les segments doivent être séparés en fonction de leur objectif et utiliser des réseaux physiques ou logiques distincts, en utilisant des options telles que des canaux radio, des câblages, des points d'accès ou des passerelles distincts.

Capacités avancées : Les segments doivent en outre être séparés à des fins différentes à l'aide de VLAN ou de VPN. Un outil d'analyse des ports peut être utilisé pour surveiller le réseau privé.

3. GESTION DU MATÉRIEL DU RÉSEAU

La gestion du matériel de réseau désigne le processus continu consistant à maintenir les périphériques de réseau correctement identifiés et configurés.

a) Modems et routeurs, dispositifs de gestion de réseau

Pratiques de base : Les dispositifs de mise en réseau doivent disposer d'un processus ou d'un moyen permettant de mettre régulièrement à jour le micrologiciel.

Capacités avancées : Pour les systèmes modem/routeur/AP fournis par le fournisseur d'accès, un routeur/AP séparé peut être ajouté pour gérer le trafic du réseau local et permettre un contrôle local des mises à jour logicielles.

b) Protocoles de réseau

Les protocoles de réseau sont les langages multiniveaux utilisés par les dispositifs pour communiquer sur les réseaux, tels que TCP, UDP, IP, RTP, etc.

Pratiques de base : Les protocoles obsolètes ne doivent pas être utilisés. En particulier, n'utilisez pas ou n'autorisez pas la négociation de SSL (toute version) ou de TLS 1.0 ou 1.1.

Capacités avancées : Configurez les protocoles les plus récents, le cas échéant.

c) Liens sans fil

Les liaisons sans fil sont des connexions réseau par radio entre des dispositifs. Ces liaisons peuvent être unidirectionnelles, bidirectionnelles ou utiliser une topologie de réseau entre plusieurs dispositifs.

(1) Bluetooth

Pratiques de base : Les fonctions de sécurité disponibles doivent être activées. Les options "Non-discoverable" doivent être utilisées lorsqu'elles sont disponibles. Aucune information sensible ne doit être exposée dans les signaux des balises Bluetooth à faible énergie (BLE).

(2) NFC

Pratiques de base : Les lecteurs NFC ne doivent pas être situés ou montés de manière à permettre un "reniflage" facile ou une manipulation aisée.

(3) Wi-Fi

Pratiques de base : Outre les pratiques de configuration du réseau de base mentionnées dans d'autres sections, il convient d'utiliser des options de cryptage Wi-Fi à jour, telles que WPA2-Personal avec AES (de préférence) ou WPA2-Personal avec TKIP. Le WPS doit être désactivé. N'utilisez pas de SSID par défaut ou de diffusion.

Une option "réseau invité" est disponible sur de nombreux points d'accès ; elle doit être activée et mise à disposition pour les utilisateurs à haut risque tels que les visiteurs ou les résidents/travailleurs temporaires. Si elle est disponible, la protection de la trame de gestion 802.11aw doit être activée. Assurez-vous que l'accès à la configuration du point d'accès est protégé par un mot de passe fort, conformément aux meilleures pratiques décrites ailleurs dans ce document. Activez le filtrage des ports, le cas échéant. Choisissez un point d'accès/routeur dont le micrologiciel peut être mis à jour.

(4) Z-WAVE

Pratiques de base : La sécurité de base implique des identifiants uniques pour la maison, des fonctions administratives protégées par mot de passe et l'utilisation de dispositifs compatibles AES-128 lorsqu'ils sont disponibles.

Capacités avancées : Pour renforcer la sécurité, la puissance RF peut répondre aux exigences de distance et il est possible d'utiliser exclusivement des dispositifs compatibles AES-128.

(5) Zigbee

Pratiques de base : Le seul appareil connecté à l'Internet devrait être la passerelle ZigBee et un pare-feu devrait la protéger.

Capacités avancées : Le trafic Internet peut être filtré lorsqu'il entre et sort du réseau ZigBee par adresse (source et destination) et numéro de port. Des fonctions de sécurité 802.15.4 facultatives peuvent être activées au niveau 802.15.4 et au niveau du réseau et de l'application, le cas échéant.

(6) Contrôle d'accès aux dispositifs à distance

Cette catégorie comprend tous les types de contrôle d'accès à distance des fonctions normales d'un appareil, telles que la vidéo des caméras de sécurité, le contrôle de la température du système de chauffage, de ventilation et de climatisation, les sous-systèmes de véhicules tels que le démarrage à distance ou le déverrouillage des portes, etc.

Pratiques de base : Les alertes en cas de défaillance ou d'altération du dispositif doivent être activées lorsqu'elles sont disponibles. Tout accès à distance doit se faire derrière un pare-feu à IP restreint, n'autorisant que les adresses IP et les sous-réseaux figurant sur une liste blanche à accéder au dispositif, quel que soit le port. Si l'accès à distance depuis l'extérieur du pare-feu est une fonction requise, il faut utiliser des VPN et des ports Internet non standard pour l'accès à distance.

4. MAINTENANCE DE LA SÉCURITÉ

Pratiques de base : Dans la mesure du possible, les tentatives d'intrusion sur le réseau ou d'autres tentatives sur l'installation doivent être suivies et examinées en vue d'une action. Les tentatives d'intrusion doivent être mises en corrélation afin d'identifier les personnes ou les cibles les plus souvent attaquées au sein du réseau. La configuration du réseau doit être documentée, les dispositifs connectés doivent être énumérés et un plan de maintenance de la sécurité doit être clairement défini.

E. ENTREPRISES

En tant que principaux propriétaires et utilisateurs d'appareils et de systèmes en réseau, y compris un nombre en augmentation exponentielle de systèmes de dispositifs IoT, les entreprises de tous types - gouvernement, secteur privé, universitaires, à but non lucratif - ont un rôle essentiel à jouer dans la sécurisation de l'écosystème numérique. [71] Si les entreprises sont souvent victimes d'attaques automatisées et distribuées ainsi que de tentatives d'exfiltration de données, leurs vastes systèmes peuvent également être détournés pour accroître l'impact des attaques DDoS et autres attaques distribuées sur d'autres. Par conséquent, les entreprises font collectivement partie des acteurs importants qui partagent la responsabilité de sécuriser adéquatement leurs réseaux et systèmes afin de contribuer à sécuriser l'écosystème numérique au sens large.

Les millions d'entreprises du secteur privé et du secteur public dans le monde diffèrent considérablement en termes de connaissances et de compétences techniques, d'accès aux ressources et d'incitations à adopter des pratiques de sécurité de base. Les grandes entreprises, par exemple, disposent souvent d'un directeur de l'information et d'un directeur de la sécurité de l'information, chacun étant chargé en partie de sécuriser les systèmes et appareils en réseau de l'organisation, y compris les systèmes IdO. Les petites entreprises n'ont pas forcément les ressources nécessaires pour disposer d'un personnel dédié à l'informatique et à la sécurité de l'information et s'appuient plutôt sur des solutions prêtes à l'emploi.

Les organisations développent et proposent de plus en plus d'outils pour aider les entreprises, petites et grandes, à sécuriser leurs réseaux et systèmes. L'effort de la Coalition pour la cybersécurité visant à développer et à faire progresser les profils de prévention et d'atténuation des DDoS et des botnets dans le cadre du Cybersecurity Framework[72] est peut-être le plus pertinent pour le Guide anti-botnet. Il s'agit d'aider les entreprises et autres organisations à traiter et à atténuer les DDoS et autres attaques automatisées et distribuées.

Les entreprises de toutes tailles peuvent également prendre leurs propres mesures proactives pour atténuer les risques liés à l'écosystème, par exemple en mettant en œuvre des techniques appropriées de gestion des identités et des accès et en cessant d'utiliser des produits et des logiciels anciens et piratés qui ne sont pas mis à jour, entre autres choses. De telles mesures peuvent aider les entreprises à protéger les données sensibles et la propriété intellectuelle sur leurs réseaux, tout en contribuant à protéger l'écosystème dans son ensemble en réduisant la surface d'attaque pour les attaques DDoS et autres attaques distribuées.

Bien entendu, les fournisseurs et prestataires qui ont élaboré ce guide sont eux-mêmes de grandes entreprises mondiales. En outre, nous fournissons des solutions haut de gamme pour sécuriser les réseaux d'entreprise et atténuer les attaques DDoS et autres menaces automatisées et distribuées. Le côté "offre" de ce marché est solide et en pleine croissance ; la poursuite du développement du côté "demande" de ce marché en termes d'entreprises de toutes tailles qui demandent et négocient ces services apportera encore plus d'innovation, de sophistication et de rentabilité à ces services.

Pratiques de base et capacités avancées pour les entreprises

1. MISES À JOUR SÉCURISÉES

Si les fabricants de produits sont responsables de la création de mises à jour sécurisées, ces dernières ne s'installent généralement pas d'elles-mêmes sans l'autorisation ou une autre action de l'utilisateur. Le niveau de contrôle dont les organisations peuvent avoir besoin sur les mises à jour varie considérablement en fonction du type de client. Une grande entreprise ou une agence gouvernementale disposant d'un personnel qualifié, par exemple, peut raisonnablement déterminer quels types de mises à jour de sécurité sont appropriés et quand les mettre en œuvre. D'un autre côté, les utilisateurs domestiques réguliers peuvent bénéficier davantage des mises à jour automatiques. [73]

Pratiques de base : Les entreprises doivent installer les mises à jour dès qu'elles sont disponibles. En général, les mises à jour automatiques sont préférables.

Capacités avancées : Les entreprises disposant d'un personnel technique qualifié peuvent prendre des décisions éclairées sur la mise en œuvre des mises à jour de sécurité.

> **Les entreprises sont collectivement parmi les acteurs importants qui partager la responsabilité de l'adéquation sécuriser leurs réseaux et systèmes afin d'aider à sécuriser les écosystème numérique.**

2. PARTAGE DE L'INFORMATION EN TEMPS RÉEL

Les entreprises disposant de grands réseaux ou de réseaux très sensibles (par exemple, les grandes entreprises et les agences gouvernementales) peuvent partager des informations critiques sur les menaces avec d'autres parties prenantes et participants de l'écosystème concernés. Ces efforts se sont considérablement améliorés ces dernières années et constituent un grand pas en avant dans la lutte contre la menace des botnets et autres menaces automatisées et distribuées. [74]

. **Pratiques de base :** Les entreprises doivent être prêtes à recevoir des informations sur les cybermenaces fournies par des activités de partage d'informations et à y réagir de manière réactive et responsable, même si elles ne sont pas encore engagées à partager activement ces informations. Il peut s'agir, par exemple, d'informations provenant d'activités de partage d'informations du gouvernement et des forces de l'ordre, de diverses CERT, de groupes industriels, de fournisseurs de réseaux, d'adresses RFC2142, de mises à jour et d'alertes provenant de fournisseurs et d'autres sources.

Les entreprises doivent s'abonner à plusieurs flux ou services de renseignements sur les menaces pour les utiliser en conjonction avec les efforts de corrélation et d'automatisation de la gestion des informations et des événements de sécurité (SIEM). Les entreprises doivent avoir des processus en place pour partager les informations sur les menaces obtenues en interne ou en externe avec les actionnaires internes, de manière opportune et exploitable. Les entreprises doivent rester en contact avec les communautés de partage et connaître les processus et les mesures de protection permettant de signaler/partager correctement les incidents de cybersécurité dans leur région et leur secteur. Les entreprises doivent procéder à un partage permanent des renseignements internes sur les menaces. Les indicateurs de compromission (IOC) et les menaces notables doivent être partagés régulièrement.

Capacités avancées : Les entreprises avancées doivent s'engager à renforcer la communauté de partage de l'information sur les cybermenaces par le partage responsable et opportun d'informations désensibilisées sur les cybermenaces avec les diverses communautés de partage appropriées (gouvernement, industrie, etc.). Les entreprises avancées doivent s'assurer qu'elles disposent de capacités suffisantes pour détecter, analyser et saisir les informations sur les cybermenaces dans des formats propices aux activités de partage. Les entreprises avancées doivent participer activement à la gouvernance et au renforcement des communautés de partage d'informations sur les cybermenaces adaptées à leur région et à leur secteur. Les entreprises avancées doivent chercher à améliorer en permanence leurs capacités de détection, d'analyse, de réponse et de partage.

3. DES ARCHITECTURES DE RÉSEAU QUI GÈRENT DE MANIÈRE SÉCURISÉE LES FLUX DE TRAFIC

Les entreprises peuvent exercer un contrôle sur la conception de leurs architectures réseau pour limiter le flux de trafic malveillant lors d'une attaque DDoS menée à l'aide de botnets ou d'autres moyens. [75] Une architecture réseau conçue avec la sécurité comme objectif explicite peut compléter d'autres mesures de précaution, comme les services anti-DDoS proposés par les fournisseurs d'infrastructure et d'autres participants de l'écosystème. Les interfaces de programmation d'applications (API) gèrent les connexions entre les applications, les dispositifs et les systèmes de données dorsaux. De manière générale, les API permettent aux entreprises d'ouvrir leurs données et leurs fonctionnalités dorsales pour les réutiliser dans de nouveaux services applicatifs. Le déploiement de la sécurité au niveau du périmètre, par le biais d'une passerelle API, peut aider les entreprises à stopper les menaces avant qu'elles ne pénètrent dans l'entreprise, ce qui leur permet de donner accès aux données de l'entreprise aux développeurs d'applications tout en maintenant une sécurité forte.

Pratiques de base : Les entreprises devraient obtenir une défense intranet contre les DDoS en utilisant les capacités et les services fournis par les fournisseurs de services réseau. Les entreprises doivent normaliser l'architecture d'interconnexion entre l'Internet et l'intranet, la politique et les processus opérationnels, les paramètres de configuration de l'accès et du contrôle des flux de paquets. Les entreprises doivent mettre en place un régime qui garantit que cette architecture est correctement déployée et exploitée. En outre, les entreprises doivent inspecter tous les flux de données et les courriers électroniques entrants et sortants et bloquer les paquets ou les courriers électroniques contenant des logiciels malveillants ; bloquer le trafic réseau non autorisé vers l'intranet ; et utiliser une architecture DMZ et des pratiques opérationnelles standard.

Capacités avancées : Les entreprises avancées peuvent identifier les comportements observables qui indiquent des flux de réseaux de zombies, tels que les flux C&C de réseaux de zombies, les DNS fastflux et l'accès à des URL suspectes. Les entreprises avancées peuvent bloquer automatiquement les flux de réseaux de zombies et remédier aux sources de ces flux ; supprimer les liens URL accessibles par Internet dans les courriers électroniques entrants ; partager et recevoir des informations utilisées pour identifier les acteurs des réseaux de zombies ; et empêcher les actions DNS inappropriées à la fois par le demandeur et le serveur DNS.

Pour augmenter la résilience contre les attaques distribuées, les entreprises avancées peuvent utiliser des passerelles d'interface de programmation d'applications. Les interfaces de programmation d'applications (API) gèrent les connexions entre les applications, les dispositifs et les systèmes de données dorsaux. Le déploiement de la sécurité dans une architecture centralisée par le biais d'une passerelle API peut aider les entreprises à fournir aux développeurs d'applications un accès aux données de l'entreprise tout en maintenant une sécurité forte.

4. AMÉLIORATION DE LA RÉSILIENCE AU DDOS

Même si les efforts de sensibilisation et d'éducation des clients sont couronnés de succès, de nombreux clients n'auront pas l'expertise technique nécessaire pour sécuriser leurs propres réseaux. Plutôt que d'ignorer

En raison de la menace que peuvent représenter les botnets et autres attaques distribuées, les entreprises devraient acheter une protection commerciale contre les attaques DDoS adaptée à leur profil de risque. [76] Les services commerciaux peuvent inclure une protection hors site ou une combinaison de protection hors site et sur site qui sécurise plus solidement l'entreprise contre les attaques distribuées. Lorsque les clients achètent des produits et services commerciaux, ils réduisent considérablement la menace des botnets et autres attaques distribuées.

Les membres du CSDE fournissent certaines des solutions commerciales DDoS les plus haut de gamme du marché. Les exemples incluent les passerelles domestiques avec sécurité intégrée, les services Anycast et une variété de services de sécurité gérés. Les services Anycast augmentent la résilience aux attaques DDoS en fournissant plusieurs routes pour la livraison de contenu et en équilibrant les charges de travail sur plusieurs éléments de réseau, qui peuvent être répartis dans le monde entier. Si une attaque DDoS compromet certaines parties d'un réseau, le trafic est automatiquement réacheminé vers une autre partie. Les services de sécurité gérés comprennent des services commerciaux de scrubbing. [77] Les autres services commerciaux comprennent les pare-feu basés sur le réseau, les systèmes de gestion des appareils mobiles, l'analyse des menaces et la détection des événements, la connectivité VPN sécurisée au cloud, la sécurité du web et des applications, et la sécurité du courrier électronique.

Les fournisseurs peuvent proposer des solutions de filtrage adaptées aux besoins et aux profils de risque uniques de leurs clients. Idéalement, ces solutions intégreront des défenses sur site et hors site. Les services commerciaux peuvent permettre de bloquer le trafic malveillant plus près de la source de l'attaque, créant ainsi une couche de sécurité supplémentaire pour les clients.

Pratiques de base : Les entreprises doivent disposer d'un soutien de réserve/de secours capable de répondre efficacement aux incidents de cybersécurité et de maintenir un niveau raisonnable de sécurité.
de sécurité. Les entreprises doivent choisir des fournisseurs commerciaux dont les produits et services comportent des capacités de sécurité appropriées (par exemple, des fournisseurs d'accès Internet et des fournisseurs de services d'hébergement en nuage qui ont des capacités de protection contre les attaques DDoS, des logiciels avec des capacités de mise à jour automatique, etc.) Les entreprises doivent disposer de plans documentés et testés pour la réponse aux incidents, y compris la réponse aux attaques DDoS et aux botnets. Les entreprises doivent choisir des fournisseurs commerciaux capables de fournir des services de protection contre les attaques DDoS ou des services par défaut.
sur la réponse. Les entreprises doivent régulièrement réévaluer l'efficacité des fournisseurs commerciaux.

Capacités avancées : Les entreprises avancées doivent adopter une approche multicouche de la protection contre les attaques DDoS et les réseaux de zombies qui comprend des capacités sur site et hors site bien supportées. Les entreprises avancées devraient accroître de manière proactive l'expertise technique de leur personnel, déterminer les lacunes dans cette expertise et y remédier par une formation appropriée, un soutien retenu/de contingence et du personnel supplémentaire. Les entreprises avancées doivent considérer les services commerciaux et les logiciels qui offrent des capacités avancées telles que l'apprentissage automatique et l'analyse des modèles pour permettre des résultats de meilleure qualité. Les entreprises avancées doivent chercher à améliorer continuellement leurs capacités en réévaluant régulièrement les capacités disponibles sur le marché.

5. GESTION DES IDENTITÉS ET DES ACCÈS

Les identités constituent le point de contrôle unifié des applications, des dispositifs, des données et des utilisateurs. Les outils de gestion des identités et des accès authentifient les individus et les services et régissent les actions qu'ils sont autorisés à entreprendre. L'un des domaines les plus importants du risque informatique concerne les utilisateurs privilégiés, tels que les administrateurs informatiques, les RSSI et d'autres personnes ayant un accès étendu aux systèmes. Qu'elles soient involontaires ou malveillantes, les actions inappropriées des utilisateurs privilégiés peuvent avoir des effets désastreux sur les opérations informatiques et sur la sécurité et la confidentialité globales des actifs et des informations de l'organisation. Les systèmes doivent être configurés de manière à ce que les administrateurs n'effectuent que les actions essentielles à leur rôle - ce qui permet un "accès moins privilégié" pour réduire les risques. L'analyse des menaces peut donner un aperçu de l'activité et permettre de prévenir ou de signaler tout élément inhabituel indiquant un risque pour la sécurité. [78]

Une évolution récente qui mérite d'être soulignée est l'utilisation de clés de sécurité physiques au lieu de mots de passe ou de codes à usage unique. Depuis le début de l'année 2017, lorsque Google a commencé à demander à tous ses employés - plus de 85 000 au total - d'utiliser des clés de sécurité physiques, pas un seul compte lié au travail d'un employé n'a été hameçonné. [79]

Lorsque les clients achètent les produits et services commerciaux, ils diminuent considérablement la menace des botnets et autres les attaques distribuées.

Pratiques de base : Les pratiques de gestion des identités et des accès des organisations devraient au moins inclure les éléments suivants :

- Authentification (y compris l'authentification multifactorielle et l'authentification fondée sur le risque) - moment de l'opération d'accès qui permet de s'assurer que le sujet est bien le vrai sujet et non un usurpateur ;
- Autorisation - moment de l'opération d'accès qui détermine, compte tenu de l'état actuel, si l'accès doit être accordé ;
- Gouvernance de l'accès - un processus visant à aider les chefs d'entreprise à définir et à affiner les politiques de détermination des accès appropriés ;
- Comptabilité - processus d'enregistrement des données relatives à l'activité des utilisateurs individuels qui accèdent aux ressources du système afin d'analyser les tendances et d'identifier les comportements suspects ;
- Provisioning/Orchestration - un ensemble d'opérations qui se produisent au moment du changement facilitant le processus de rejoindre/déplacer/quitter et la coordination des événements de changement entre les ressources connectées disparates ; et.
- Référentiel d'identité - un magasin persistant pour maintenir l'état actuel et les valeurs d'attributs des profils des sujets.

Les entreprises devraient également adopter la pratique de l'offboarding, qui consiste à retirer en temps utile l'identité de l'annuaire de l'entreprise et à révoquer l'identité et les accès associés, dans les limites de l'espace disponible.

24 heures pour les accès privilégiés et les accès aux ressources du nuage.

Pour améliorer l'authentification, les entreprises devraient utiliser des phrases de passe plus fortes et plus faciles à mémoriser au lieu de mots de passe basés sur des règles syntaxiques, effectuer des vérifications dans un dictionnaire de mots de passe et utiliser un compteur de force de mot de passe. En outre, les entreprises devraient recourir à l'authentification à deux ou plusieurs facteurs (2FA/MFA) pour les accès privilégiés, par exemple les administrateurs système. Les organisations devraient utiliser un ser vice d'authentification centralisé pour les applications Web et SaaS avec l'authentification unique qui exige une authentification à deux facteurs (2FA) pour les appareils qui n'ont pas été préalablement vérifiés et approuvés. En outre, les entreprises devraient utiliser des jetons FIDO U2F pour déjouer les attaques de phishing ou prendre d'autres précautions raisonnables pour réduire le risque posé par les attaques de phishing.

Les entreprises doivent adhérer au principe de l'accès le moins privilégié - demande d'accès basée sur les rôles via le contrôle d'accès basé sur les rôles (RBAC) et/ou les approbations, détection et correction des accès hors processus, aberrants, dormants et violant la séparation des tâches (SoD), et gouvernance des accès via la revalidation périodique des accès (besoins professionnels continus ou CBN).

Les entreprises devraient procéder à la surveillance et à l'audit des utilisateurs privilégiés et à la gestion sécurisée des événements informationnels (SIEM). Elles devraient également disposer d'un coffre-fort pour les identifiants de services ou d'applications - les identifiants ne devraient pas être stockés en clair dans les fichiers de configuration.

Capacités avancées : Les entreprises avancées peuvent avoir des méthodes plus sophistiquées de gestion des identités et des accès :

- Les méthodes d'authentification continue tirent parti de la surveillance comportementale et biométrique tout au long d'une session utilisateur pour déterminer si la session a été compromise.
- L'authentification basée sur le risque permet aux entreprises de mieux comprendre le contexte autour de l'identité, par exemple grâce aux données de géolocalisation ou au comportement d'achat. Un système peut reconnaître l'identité, déterminer que l'authentification traditionnelle est inutile et autoriser l'accès. À l'inverse, si le système détecte des anomalies, comme le fait de se connecter depuis un pays étranger au milieu de la nuit après avoir eu quelques mots de passe ratés, il s'agit alors d'une opération à très haut risque et l'accès sera refusé en l'absence d'étapes d'authentification supplémentaires.
- Les solutions de gestion des accès privilégiés offrent la visibilité, la surveillance et le contrôle nécessaires pour les utilisateurs et les comptes qui détiennent les "clés du royaume". Il est essentiel que les administrateurs soient autorisés à effectuer uniquement les actions essentielles à leur rôle - ce qui permet un "accès moins privilégié" pour réduire les risques. Cette visibilité donne un aperçu de l'activité et permet de prévenir ou de signaler tout élément inhabituel indiquant un risque pour la sécurité.
- L'authentification adaptative utilise 2FA/MFA, avec un calcul des risques plus complet et plus sophistiqué, au-delà de l'empreinte digitale de l'appareil, en intégrant des facteurs tels que l'intranet ou l'internet, l'accès simultané depuis plusieurs lieux ou géographies, la connexion à des heures très irrégulières, etc.
- La gouvernance des identités en boucle fermée intègre la surveillance et l'analyse de l'activité des utilisateurs sur les serveurs et dans les applications internes avec des outils de gestion des accès, par exemple, révoquer l'accès d'un utilisateur privilégié s'il est détecté qu'il accède à des données protégées sur le serveur ou dans les applications internes de manière non autorisée.
- Une gouvernance des accès plus intelligente peut être réalisée grâce à l'analytique et à l'IA, par exemple en détectant et en révoquant les accès dormants - des accès qui n'ont pas été utilisés par leurs propriétaires pendant une période prolongée, ce qui signale des défaillances potentielles dans la gouvernance des accès ou l'offboarding.
- La détection et la protection contre le piratage peuvent être améliorées par l'intégration de la gestion des accès à privilèges et de l'analyse du comportement des utilisateurs et des entités (UEBA)

AUX ETATS-UNIS, PRESQUE

1 sur 5

ORDINATEURS PERSONNELS EXÉCUTER DES LOGICIELS PIRATÉS alors que

EN CHINE, LE POURCENTAGE D'ORDINATEURS PERSONNELS ÉQUIPÉS DE LOGICIELS PIRATÉS **DÉPASSE SOUVENT**

70%

6. ATTÉNUER LES PROBLÈMES LIÉS AUX PRODUITS PÉRIMÉS ET PIRATÉS

Les entreprises doivent cesser d'utiliser les anciens produits pour lesquels le support du fabricant est terminé. [80] Un problème étroitement lié du point de vue du support technique est celui des logiciels piratés. Aux États-Unis, près d'un ordinateur personnel sur cinq utilise des logiciels piratés, alors qu'en Chine, le pourcentage d'ordinateurs personnels équipés de logiciels piratés dépasse souvent 70 %. [81] Bien entendu, les fabricants ne corrigent généralement pas les logiciels piratés, ce qui signifie qu'ils restent vulnérables aux exploits connus. [82] Les entreprises devraient éviter les logiciels piratés et réduire le nombre total de vulnérabilités dans l'écosystème mondial de l'internet et des communications.

Pratiques de base : Les entreprises doivent remplacer les produits légitimes supportés avant que le support du fabricant n'expire. Les entreprises doivent toujours éviter les produits piratés. Ces produits sont illégaux dans la plupart des pays et contribuent largement aux failles de sécurité dans l'ensemble de l'écosystème. [83]

Capacités avancées : Les entreprises avancées peuvent disposer des derniers produits pris en charge avec les fonctions et les capacités de sécurité les plus récentes.

6 Prochaines étapes et conclusion

La publication de la version 1.0 de ce guide constitue la première étape d'une campagne stratégique sans précédent menée par l'industrie contre les botnets et autres menaces automatisées et distribuées. Le CSDE, USTelecom, l'ITI et le CTA invitent les parties prenantes à mettre en œuvre les pratiques recommandées afin de relever les défis communs et d'inverser la tendance contre les mauvais acteurs.

Comme indiqué dans l'introduction du guide, l'économie numérique a été un moteur de croissance commerciale et d'amélioration de la qualité de vie dans le monde entier. Aucune partie prenante unique - dans le secteur public ou privé - ne contrôle ce système, de sorte que la gestion sécurisée des opportunités présentées par cette croissance est la responsabilité impérative de chaque partie prenante de la communauté des TIC.

À cette fin, nous présentons ces pratiques de base et ces capacités avancées à l'attention de toutes les parties prenantes. Il s'agit de solutions dynamiques et flexibles, fondées sur des normes consensuelles volontaires et animées par les puissantes forces du marché, qui peuvent être mises en œuvre par les parties prenantes dans l'ensemble de l'économie numérique mondiale. C'est la meilleure réponse aux défis systémiques de cybersécurité auxquels nous sommes confrontés.

Avec cet impératif à l'esprit, nous prévoyons de mettre à jour, de publier et de promouvoir une nouvelle version de ce guide sur une base annuelle, reflétant les derniers développements et les percées technologiques qui aideront nos entreprises et d'autres entreprises à travers le monde à apporter des améliorations de sécurité observables et mesurables - non seulement au sein de leurs propres réseaux et systèmes, mais aussi dans l'ensemble de l'écosystème.

Dans l'immédiat, notre prochaine étape dans les mois à venir sera de promouvoir ce guide auprès d'un large éventail de parties prenantes nationales et internationales de l'écosystème de l'internet et des communications, qui sont bien placées pour promouvoir les pratiques recommandées et poursuivre un engagement constructif. La responsabilité partagée assumée par ces diverses parties prenantes est la clé pour assurer l'avenir de notre économie numérique.

07 Organisations contributrices

A propos du CSDE

Le Conseil pour la sécurisation de l'économie numérique (CSDE) rassemble des entreprises du secteur des technologies de l'information et de la communication (TIC) pour lutter contre les cybermenaces émergentes et de plus en plus sophistiquées par des actions de collaboration. Parmi les partenaires fondateurs figurent Akamai, AT&T, CA Technologies, CenturyLink, Cisco, Ericsson, IBM, Intel, NTT, Oracle, Samsung, SAP, Telefonica et Verizon. CSDE est coordonné par USTelecom et l'Information Technology Industry Council (ITI).

À propos de USTelecom

USTelecom est la principale association professionnelle représentant les prestataires de services et les fournisseurs de l'industrie des télécommunications. La diversité de ses membres va des grandes sociétés de communication cotées en bourse aux petites entreprises et aux coopératives - toutes fournissant des services de communication avancés aux marchés urbains et ruraux.

À propos de l'ITI

Le Conseil de l'industrie des technologies de l'information (ITI) est la voix mondiale du secteur des technologies. En tant que principale organisation de défense et d'élaboration de politiques pour les principales sociétés d'innovation du monde, ITI gère les relations entre les décideurs politiques, les entreprises et les organisations non gouvernementales, en proposant des solutions créatives qui font progresser le développement et l'utilisation des technologies dans le monde.

À propos de la Consumer Technology Association

La Consumer Technology Association (CTA)™ est l'association professionnelle représentant l'industrie américaine des technologies grand public, qui représente 377 milliards de dollars et soutient plus de 15 millions d'emplois aux États-Unis. Plus de

2 200 entreprises - 80 % sont des petites entreprises et des start-ups, les autres comptent parmi les marques les plus connues au monde - bénéficient des avantages de l'adhésion au CTA, notamment la défense des politiques, les études de marché, l'enseignement technique, la promotion de l'industrie, l'élaboration de normes et l'encouragement des relations commerciales et stratégiques. Le CTA possède et produit également le CES® - le lieu de rassemblement mondial de tous ceux qui prospèrent dans le domaine des technologies grand public. Les bénéfices du CES sont réinvestis dans les services industriels du CTA.

08 Notes de fin

1 Les acteurs malveillants sont aussi communément appelés "hackers", bien que tous les hackers ne soient pas malveillants. En règle générale, ce document utilise ces termes de manière interchangeable, en partant du principe que le contexte indiquera si l'individu référencé est un acteur malveillant ou non. Il convient également de noter que ce document se concentre sur les acteurs malveillants, de sorte que, d'une manière générale, le terme "hacker" dans ce document désigne un acteur malveillant.

2 Il n'est pas pratique de définir simultanément les exigences de tous les types de logiciels de l'écosystème IoT. Les appareils et systèmes d'appareils, les entreprises et les infrastructures ont des exigences spécifiques. Cette section s'applique aux domaines non couverts ailleurs dans le guide.

3 Un dispositif connecté individuel (ou "dispositif d'extrémité") peut lui-même être constitué de plusieurs composants, notamment des modules matériels, des puces, des logiciels, des capteurs ou d'autres composants d'exploitation. Des centaines de milliers d'entreprises et des millions de développeurs contribuent au développement des milliards d'appareils déployés dans le monde. Au-delà du dispositif individuel lui-même, il existe de multiples couches supplémentaires de connectivité qui constituent un nouveau marché très dynamique, y compris pour l'innovation en matière de sécurité. Pour faire simple, les appareils connectés ne sont plus simplement des appareils individuels. Compte tenu de cette complexité, ce guide traite des systèmes de dispositifs : l'union d'un dispositif d'extrémité connecté - une "chose" dans l'IdO - et de ses éléments de support associés ailleurs sur l'internet, y compris les applications et les services en nuage.

4 Les systèmes de chauffage, de ventilation et de climatisation (CVC) sont connectés pour des fonctions intelligentes et un accès à distance par l'occupant. Les systèmes de sécurité comprennent des caméras, des serrures et des systèmes d'alarme gérés via l'internet. Les systèmes de divertissement bénéficient de commandes centrales permettant de gérer facilement des configurations audio et vidéo complexes. Il existe une très grande diversité de fabricants et de systèmes dans ces catégories. Ces systèmes peuvent être installés par des propriétaires de maisons ou d'entreprises bricoleurs, ou par des professionnels : intégrateurs, installateurs d'alarmes, etc. Idéalement, chaque système de dispositifs entrant dans une maison, un bureau, un magasin, un environnement médical ou industriel sera sécurisé par les meilleures pratiques tout au long du cycle de vie du dispositif - y compris l'installation et la configuration du dispositif qui permet d'obtenir la "meilleure sécurité disponible" du produit fabriqué.

5 Consumer Tech. Ass'n, The Connected Home Security System, https:// cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx (dernière visite le 10 octobre 2018).

6 En tant que principaux propriétaires et utilisateurs d'appareils et de systèmes en réseau, y compris un nombre exponentiellement croissant de systèmes de dispositifs IoT, les entreprises de .
Tous les types d'entreprises - gouvernementales, privées, universitaires et à but non lucratif - ont un rôle essentiel à jouer dans la sécurisation de l'écosystème numérique. Si les entreprises sont souvent la cible d'attaques automatisées et distribuées ainsi que de tentatives d'exfiltration de données, leurs vastes systèmes peuvent également être détournés pour accroître l'impact des attaques DDoS et autres attaques distribuées sur d'autres. Par conséquent, les entreprises font partie des parties prenantes qui partagent la responsabilité de sécuriser adéquatement leurs réseaux et systèmes afin de contribuer à sécuriser l'écosystème numérique au sens large. Les millions d'entreprises du secteur privé et du secteur public dans le monde diffèrent considérablement en termes de connaissances et de compétences techniques, d'accès aux ressources et de motivation à adopter des pratiques de sécurité de base. Les entreprises de toutes tailles peuvent prendre leurs propres mesures proactives pour atténuer les risques liés à l'écosystème. Ces mesures peuvent aider les entreprises à protéger les données sensibles et la propriété intellectuelle sur leurs réseaux tout en contribuant à protéger l'écosystème dans son ensemble en réduisant la surface d'attaque des réseaux de zombies. Les fournisseurs et prestataires qui ont élaboré ce guide sont de grandes entreprises mondiales, et nous fournissons également des solutions haut de gamme pour sécuriser les réseaux d'entreprise et atténuer les attaques DDoS et autres menaces automatisées et distribuées. L'offre de ce marché est robuste et en pleine croissance, et le développement de la demande de ce marché se poursuit.
le fait que des entreprises de toutes tailles demandent et négocient ces services permettra de renforcer l'innovation, la sophistication et la rentabilité de ces services.

7 Descriptions de CSDE, ITI et USTelecom infra p. 41.

8 Description du CTA, infra p. 41.

9 Par souci de concision, les "botnets et autres menaces automatisées et distribuées" sont désignés ci-après par le terme "botnets".

10 Andrew Sheehy, GDP Cannot Explain The Digital Economy, Forbes (6 juin 2016), https://www.forbes.com/sites/andrewsheehy/2016/06/06/gdp-cannot-explain-the-digital-economy/#47c4db1218db.

11 Irving Wladawsky-Berger, GDP Doesn't Work in a Digital Economy, The Wall Street Journal (3 nov. 2017) https://blogs.wsj.com/cio/2017/11/03/ gdp-doesnt-work-in-a-digital-economy.

12 Paul Tentena, Artificial Intelligence to Double Digital Economy to 23 Trillion by 2025, East African Business Week (30 mai 2018),

12 http://www. busiweek.com/artificial-intelligence-to-double-digital-economy-to-23-trillion-by-2025.

13 Voir, par exemple, Catalin Cimpanu, Sly Malware Author Hides Cryptomining Botnet Behind Ever-shifting Proxy Service, ZDNet (13 septembre 2018), https:// www.zdnet.com/article/sly-malware-author-hides-cryptomining-botnet-behind-ever-shifting-proxy-service (" [L]es réseaux axés sur les opérations de minage de crypto-monnaies ont été l'une des formes les plus actives d'infections par logiciels malveillants en 2018. "

14 Sam Thielman et Chris Johnston, Major Cyber Attack Disrupts Internet Service Across Europe and US, The Guardian, (21 oct. 2016), https://www. theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service.

15 Michael Newberg, As Many as 48 Million Twitter Accounts Aren't People, Says Study, CNBC (10 mars 2017), https://www.cnbc.com/2017/03/10/ nearly-48-million-twitter-accounts-could-be-bots-says-study.html.

16 JP Buntinx, Top 4 Largest Botnets to Date, Null TX (7 janvier 2017), https:// nulltx.com/top-4-largest-botnets-to-date.

17 Daniel Newman, The Top 8 IoT Trends for 2018, Forbes (19 déc. 2017), https://www.forbes.com/sites/danielnewman/2017/12/19/the-top-8-iot-trends-for-2018/#2523096867f7 (citant HIS Markit IoT Trend Watch 2018, disponible sur https://ihsmarkit.com/industry/telecommunications.html) ; voir

18 également Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016 (7 février 2017), https://www.gartner.com/en/ newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

18 Jan-Peter Kleinhans, Internet of Insecure Things : Can Securit y Assessment Cure Market Failures ?", Stiftung Neue Verantwor tung (déc. 2017), https://www.stiftung-nv.de/sites/default/files/internet _of_ insecure_things.pdf.

19 Bill Connor, Ransomware-As-A-Service : Le prochain grand cyber
Threat ?", Forbes (17 mars 2017), https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#14a38e5b4123.

20 Andy Greenberg, The White House Blames Russia for NoPetya, the 'Most Costly Cyber Attack in History', Wired (15 février 2018) https://www.wired.com/ story/white-house-russia-notpetya-attribution ; Damien Sharkov, Russia Accused of 1.2 Billion NoPetya Cyberattack, Newsweek (15 février 2018) https://www.newsweek.com/russia-accused-massive-12-billion-cyber-attack-807867 ; CBS News, What Can We Learn from the Most Devastating Cyber Attack in History ? (22 août 2018), https://www.cbsnews.com/news/ lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation (dicussing how NotPetya malware caused over $10 billion in damage).

21 Alex Zaharov-Reutt, Cybercriminalité, les violations de données vont coûter cher aux entreprises
US $8 Trillion Thru 2022, ITWire (25 avril 2017), https://www.itwire.com/ security/77782-$8-trillion-business-cost-from-cybercrime-and-data-breaches-thru-2022.html.

22 Commc'n Sec., Groupe de travail 4 du Conseil de la fiabilité et de l'interopérabilité IV, Rapport final sur la gestion des risques de cybersécurité et les meilleures pratiques 4 (mars 2015), disponible à l'adresse https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (reconnaissant " les avantages d'une approche non réglementaire par rapport à un régime de conformité prescriptif et statique ").

23 Voir supra notes 1-22 et infra notes 24-83.

24 Daniel Palmer, Researchers Discover Huge Crypto Scam Botnet on Twitter, Coindesk (7 août 2018), https://www.coindesk.com/researchers-discover-huge-crypto-scam-botnet-on-twitter ("Des chercheurs ont découvert un énorme botnet qui imite des comptes légitimes sur Twitter pour diffuser une escroquerie de "don" de crypto-monnaies.").

25 Tobias Knecht, A Brief History of Bots and How They've Shaped the Internet Today, Abusix (23 août 2017), https://www.abusix.com/blog/a-brief-history-of-bots-and-how-theyve-shaped-the-internet-today.

26 Dustin Volz et Jim Finkle, U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam, Reuters (mars 2016), https://www.reuters.com/article/ us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.

27 Lee Matthews, World's Biggest Mirai Botnet Is Being Rented Out for DDoS Attacks, Forbes (29 novembre 2016), https://www.forbes.com/sites/ leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out-for-ddos-attacks/#6bdec4cb58ad.

28 Comparez Elie Bursztein, Inside the Infamous Mirai IoT Botnet : A Retrospective Analysis, Cloudflare (14 déc. 2017), https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis ("l'assaut Mirai était de loin le plus important, atteignant 623 Gbps") avec Sean Gallagher, Federal Grand Jury Indicts 7 Iranians for "Campaign of Cyber Attacks", Ars Technica (Mar. 24, 2016) ("À leur apogée, les attaques DDoS ont atteint 140 gigabits par seconde").

29 À noter qu'en mars 2018, le record de volume de trafic du botnet Mirai a été pulvérisé par des attaquants ciblant GitHub avec une attaque DDoS atteignant 1,35 Terrabytes par seconde (bps). Voir Lily Hay Newman, GitHub Survived the Biggest DDoS Attack Ever Recorded, Wired (1er mars 2018) https://www.wired. com/story/github-ddos-memcached. Notamment, l'attaque n'a pas utilisé de botnet. Au lieu de cela, les attaquants ont usurpé des requêtes adressées à des serveurs "memcached" vulnérables utilisés pour accélérer les sites web, inondant les victimes d'environ 1,5 million d'euros.
50 fois le volume normal du trafic internet. ("Memcached" fait référence aux systèmes de mise en cache en mémoire distribuée, qui sont souvent utilisés pour augmenter la vitesse des sites web en "mettant en cache" les données dans la mémoire vive plutôt que de s'appuyer sur des sources de données externes). Comme les serveurs memcached répondent à tout le monde - y compris aux acteurs malveillants - ils ne devraient pas être exposés à l'internet public. Cependant, environ 100 000 de ces serveurs sont exposés et vulnérables ; beaucoup d'entre eux appartiennent à de petites entreprises et organisations disposant de ressources de sécurité limitées. Voir Liam Tung, New World Record DDoS Attack Hits (en anglais)
1,7Tbps Days after Landmark GitHub Outage, ZDNet (6 mars 2018), https:// www.zdnet.com/article/new-world-record-ddos-attack-hits-1-7tbps-days-after-landmark-github-outage. Les attaques par inondation de ce type qui exploitent les vulnérabilités des serveurs sont de plus en plus populaires parmi les mauvais acteurs. Quelques jours seulement après que GitHub a survécu à "la plus grande attaque DDoS jamais enregistrée", le record a de nouveau été battu : Un client d'Arbor Networks a été visé par une attaque similaire qui a atteint 1,7 Tbps.

30 Cyren, Cyren Cyber Threat Report 8 (janv. 2017), http://www.vcwsecurity.com/wp-content/uploads/2017/01/Cyren_2017Q1_Botnet_Threat_Report.pdf.

31 Denis Makrushin, The Cost of Launching a DDoS Attack, Kaspersky (23 mars 2017), https://securelist.com/the-cost-of-launching-a-ddos-attack/77784.

32 Alfred Ng, WannaCry Ransomware Loses Its Kill Switch, So Watch Out, CNET (15 mai 2017), https://www.cnet.com/news/wannacry-ransomware-patched-updated-virus-kill-switch.

33 Ellen Nakashima, l'armée russe est derrière la cyberattaque "NotPetya". en Ukraine, la CIA conclut, Washington Post (12 janvier 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.bc4ce7d72018.

34 Andy Greenberg, Hackers Are Trying to Reignite WannaCry with Nonstop Botnet Attacks, Wired (19 mai 2017), https://www.wired.com/2017/05/ wannacry-ransomware-ddos-attack.

35 CBS News, Que pouvons-nous apprendre de la cyberattaque la plus dévastatrice de l'histoire ? (22 août 2018), https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation.

36 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 (22 mai 2018), disponible sur https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf ; Commc'n Sec, Groupe de travail 4 du Conseil de fiabilité et d'interopérabilité IV, Rapport final sur la gestion des risques de cybersécurité et les meilleures pratiques (mars 2015), disponible à l'adresse https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf ; ENISA, Botnet Measurement, Detection, Disinfection and Defence (7 mars 2011), https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence ; Int'l Telecomm.Union, ITU Botnet Mitigation Toolkit (janv. 2008), https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf.

37 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 10 (22 mai 2018), disponible sur https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

38 Tim Polk, Enhancing Resilience of the Internet and Communications Ecosystem, Nat'l Inst. of Standards and Tech. 7-9 (sept. 2017) (discutant des outils et techniques de protection contre les DDoS, notamment le filtrage ingress/egress ; la protection contre les DDoS sur site et hors site), disponible à l'adresse https://doi.

org/10.6028/NIST.IR.8192. Voir également, Ctr. for Democracy and Tech, Comments to the NTIA on Promoting Stakeholder Action Against Botnets and Other Automated Threats 2 (12 février 2018) (en accord avec le projet de rapport de la NTIA selon lequel " les techniques courantes d'atténuation des botnets comprennent le filtrage d'entrée et de sortie, le reroutage et la mise en forme du trafic Internet, et l'isolement des dispositifs ou d'autres entités "), disponible à l'adresse https://cdt.org/files/2018/02/CDT-NTIA-Botnet-Comments-Feb-2018.pdf ; Commc'n Sec, Groupe de travail 4 du Conseil de fiabilité et d'interopérabilité IV, Rapport final sur la gestion des risques de cybersécurité et les meilleures pratiques (mars 2015), disponible à l'adresse https://transition.fcc.gov/pshs/ advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

39 Voir, .e.g., États-Unis, DHS Automated Indicator Sharing (AIS) System, https://www.us-cert.gov/ais (dernier accès le 17 octobre 2018) ; Royaume-Uni, Cyber Security Information Sharing Partnership (CiSP), https://www.ncsc.gov.uk/cisp (dernier accès le 17 octobre 2018) ; Japon, Cyber Clean Center, https:// www.telecom-isac.jp/ccc/en_index.html (dernier accès le 17 octobre 2018) ; Nouvelle-Zélande, CORTEX, https://www.gcsb.govt.nz/our-work/information-assurance/cortex-faqs (dernier accès le 17 octobre 2018).

40 Voir David Strom, What Is Polymorphic Malware and Why Should I Care ? (16 octobre 2015), https://securityintelligence.com/what-is-polymorphic-malware-and-why-should-i-care.

41 Verizon, 2012 Data Breach Investigations Report 71 (2012), https:// www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf.

42 Voir Stephen Sladaritz, About Heuristics, SANS Institute 4 (23 mars 2002), disponible à l'adresse https://www.sans.org/reading-room/whitepapers/malicious/ about-heuristics-141 (qui compare les deux différents types d'analyse heuristique) ; voir également John Aycock, Computer Viruses and Malware 74 (2006) (qui explique que la seule différence entre l'heuristique statique et l'heuristique dynamique est "la façon dont les données sont recueillies" et qu'autrement les données sont identiques).

43 Voir, par exemple, Cisco, Cisco Cognitive Threat Analytics v1 (février 2016), https:// dcloud-cms.cisco.com/demo_news/cisco-cognitive-threat-analytics-v1.

44 Nat'l Inst. of Standards and Tech. Advanced DDoS Mitigation Techniques (18 oct. 2017) (" Depuis plus de dix ans, l'industrie avait développé des spécifications de techniques et des conseils de déploiement pour les techniques de filtrage au niveau IP afin de bloquer le trafic réseau avec des adresses sources usurpées "), disponible sur https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques.

45 P. Ferguson & D. Senie, Network Ingress Filtering : Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing, Internet Engineering Task Force (IETF) Network Working Group (mai 2000), disponible sur https://tools.ietf.org/html/bcp38 ; F. Baker & P. Savola, Ingress Filtering for Multihomed Networks, Internet Engineering Task Force (IETF) Network Working Group (mars 2004), disponible sur https://tools.ietf.org/html/bcp84.

46 Id.

47 Voir généralement, par exemple, Chris Benton, Egress Filtering FAQ, SANS Institute (19 avril 2006), disponible à l'adresse https://www.sans.org/readingroom/whitepapers/ firewalls/egress-filtering-faq-1059.

48 Voir Cisco, Access Control Lists (dernière mise à jour le 17 juillet 2018), https://www. cisco.com/c/fr/us/td/docs/security/asa/asa99/asdm79/firewall/asdm-79-firewall-config/access-acls. html.

49 Voir Cisco, Policing and Shaping Overview (dernière mise à jour le 23 novembre 2017), https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/ guide/fqos_c/qcfpolsh.html.

50 Voir généralement, par exemple, Guy Bruneau, DNS Sinkhole, SANS Institute (7 août 2010), https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523.

51 Voir Cisco, Implementing BGP Flowspec (dernière mise à jour le 31 janvier 2018), https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/ asr9k_r5-2/routing/configuration/guide/b_routing_cg52xasr9k/b_routing_ cg52xasr9k_chapter_011.html.

52 Voir Georgia Tech Researchers, DNS Changer Remediation Study, présentation à la 27e réunion générale du M3AAWG, San Francisco, CA (février). 19, 2013), disponible à l'adresse https://www.m3aawg.org/sites/default/files/ document/GeorgiaTech_DNSChanger_Study-2013-02-19.pdf (dernier accès le 17 octobre 2018) ; voir également Commc'n Sector Coordinating Council, Botnet Whitepaper 24-25 (17 juillet 2017) (énumérant les multiples façons dont les fournisseurs d'infrastructures peuvent avertir les utilisateurs, notamment par courriel, appel téléphonique, courrier postal, SMS, notification par navigateur web, walled garden et autres méthodes telles que les médias sociaux), disponible à l'adresse https://docs.wixstatic.com/ ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

53 Voir Ctr. for Democracy and Tech, Comments to the NIST Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malwares (14 nov. 2011) (exprimant son inquiétude quant à la pratique consistant à "couper ou à interférer de toute autre manière avec la connexion Internet d'un client" pour l'obliger à remédier à un botnet), disponible sur https://www.nist.gov/sites/default/files/ documents/itl/CDT-Comments-on-BotNet-FRN-11-14-11.pdf ; Elec. Frontier Found, Comments to the NIST Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malwares 5 (4 nov. 2011) (expliquant comment les parties non infectées pourraient voir leur accès Internet affecté par la quarantaine), disponible à l'adresse https://www.nist.gov/sites/default/files/documents/itl/EFF-Comments-to-BotNet-RFI_11-4-11.pdf.

54 Voir Commc'n Sector Coordinating Council, Botnet Whitepaper 21 (17 juillet 2017), ("Aucune technique n'est plus efficace que les actions de répression qui conduisent à l'arrestation des auteurs. C'est la seule solution qui s'attaque à la cause profonde du problème, et pas seulement à un symptôme... [E]xécuter le démantèlement d'un botnet nécessite une importante analyse médico-légale en amont et une coordination minutieuse entre de nombreuses parties prenantes, souvent au-delà des frontières internationales..... La plupart des réseaux de zombies sont de nature internationale, ce qui exige une coopération entre les nations, qui demande beaucoup de ressources et de temps"), disponible à l'adresse https://docs. wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

55 Voir Robert Wainright et Frank J. Cilluffo, Responding to Cyber Crime at Scale : A Case Study, Europol & the George Washington Univ. Ctr. for Cyber and Homeland Sec. (mars 2017), disponible sur https://cchs.gwu.edu/sites/g/ files/zaxdzs2371/f/Responding%20to%20Cybercrime%20at%20Scale%20 FINAL.pdf.

56 Voir SAFECode, Pratiques fondamentales pour le développement de logiciels sécurisés. (2018), https://safecode.org/wp-content/uploads/2018/03/SAFECode_ Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

57 Arora et al, Carnegie Mellon University, An Empirical Analysis of Software Vendors' Patching Behavior : Impact of Vulnerability Disclosure (janvier 2006) (analyse des incitations des grands vendeurs par rapport aux autres vendeurs), disponible à l'adresse https://www.heinz.cmu.edu/~rtelang/disclosure_jan_06.pdf.

58 Voir SAFECode, Principles for Software Assurance Assessment (2015), disponible à l'adresse https://safecode.org/publication/SAFECode_Principles_for_ Software_Assurance_Assessment.pdf ; CA Tech, Veracode, https://www. veracode.com/verified (dernier accès le 18 juin 2018).

59 Nat'l Inst. of Standards and Tech, NTIA Software Component Transparency, https://www.ntia.doc.gov/SoftwareTransparency (dernière consultation le 6 novembre 2018).

60 Cette section sur les appareils et les systèmes s'inspire de Consumer Tech. Ass'n, Securing Connected Devices for Consumers in the Home - A Manufacturer's Guide (CTA-CEB33), https://members.cta.tech/ctaPublicationDetails/?id=c12ebabe-84cd-e811-b96f-0003ff52809d (dernière consultation le 15 octobre 2018).

61 La planification précoce des exigences et, finalement, la certification sont essentielles à ce processus. Par exemple, la CTIA gère un programme de certification pour les dispositifs IoT, en établissant des exigences industrielles pour la sécurité des dispositifs sur les réseaux sans fil et en fournissant un programme de certification. Les détails du programme, y compris les exigences et la manière de certifier un appareil, sont disponibles ici : https://www.ctia.org/about-ctia/programs/certification-resources.

62 Voir Microsoft, What is the Security Development Lifecycle, https://www.microsoft.com/en-us/sdl/default.aspx (dernière consultation le 19 octobre 2018).

63 Voir BSIMM, https://bsimm.com (dernière consultation le 6 novembre 2018).

64 Pour plus de normes internationales, voir le NIST (Nat'l Inst. of Standards and Tech), Cryptographic Module Validation Program, https://csrc.nist.gov/projects/ cryptographic-module-validation-program/standards. En outre, le NIST dispose d'un projet de résumé des normes internationales : Nat'l Inst. of Standards and Tech, Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT), https://csrc.nist.gov/publications/detail/ nistir/8200/draft (dernier accès le 10 octobre 2018).

65 Pour la proposition de recommandation actuelle, voir IETF, Manufacturer Usage Description Specification, https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud (dernier accès le 19 octobre 2018).

66 Cisco, What is Manufacturer Usage Description ? (MUD), https://developer.cisco.com/docs/mud/#!what-is-mud (dernière consultation le 19 octobre 2018).

67 IEEE, 802.1AR : Identité des dispositifs sécurisés, https://1.ieee802.org/security/802-1ar/ (dernière consultation le 19 octobre 2018).

68 Trusted Computing Group, Device Identifier Composition Engine (DICE) Architectures, https://trustedcomputinggroup.org/work-groups/dice-architectures (dernière consultation le 19 octobre 2018).

69 Pour une discussion sur les mises à jour, voir Nat'l Inst. of Standards and Tech, Stakeholder-Drafted Documents on IoT Security, https://www.ntia.doc.gov/ IoTSecurity (dernier accès le 10 octobre 2018).

70 Consumer Tech. Ass'n, The Connected Home Security System, https:// cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx (dernière visite le 10 octobre 2018).

71 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 12-15 (22 mai 2018), disponible sur https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

72 Cybersecurity Coalition, DDoS Threat Mitigation Profile, https://www.cybersecuritycoalition.org/ddos-framework (dernière consultation le 14 novembre 2018), et Cybersecurity Coalition, Botnet Threat Mitigation Profile, https://www.cybersecuritycoalition.org/botnet-framework (dernière consultation le 14 novembre 2018).

73 Voir Commc'n Sec., Reliability and Interoperability Council II Working Group 8, Final Report on ISP Network Protection 16 (recommandant, entre autres, que les utilisateurs "[c]onfigurent [l']ordinateur pour télécharger

74 automatiquement les mises à jour critiques du système d'exploitation et des applications installées"). (Nov. 2011), disponible à l'adresse https://www.atis.org/01_legal/docs/CSRICII/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

74 Tim Polk, Enhancing Resilience of the Internet and Communications Ecosystem, Nat'l Inst. of Standards and Tech. 13 (sept. 2017) (citant les opinions des participants à l'atelier du NIST Enhancing Resilience of the Internet and Communications Ecosystem des 11 et 12 juillet 2017), disponible à l'adresse https://doi.org/10.6028/NIST.IR.8192.

75 Scott Bowen, Akamai, Defense By Design : How To Dampen DDoS Attacks With A Resilient Network, Forbes (14 septembre 2017) https://www.forbes.com/ sites/akamai/2017/09/14/defense-by-design-how-to-dampen-ddos-attacks-with-a-resilient-network/#79144da56f8a.

76 Voir, par exemple , AT&T, Distributed Denial of Service (DDoS) Defense (2014), disponible à l'adresse https://www.business.att.com/content/productbrochures/ ddos_prodbrief.pdf ; Verizon, DDoS Shield Solutions Brief (2016), disponible à l'adresse http://www.verizonenterprise.com/resources/ddos_shield_solutions_brief_en_xg.pdf ; CenturyLink, DDoS Mitigation (2014), disponible à l'adresse http:// www.centurylink.com/asset/business/enterprise/brochure/ddos-mitigation. pdf ; Telefonica, Anti-DDoS, https://www.cloud.telefonica.com/en/open-cloud/products/security/anti-ddos (dernière visite le 14 mai 2018) ; NTT, DDoS Protection Service, https://www.ntt.com/en/services/network/gin/transit/ ddos.html (dernière visite le 14 mai 2018).

77 Voir l'analyse supra, partie 5.A.2(e) (qui explique la fonction des centres de filtrage dans l'atténuation des réseaux de zombies).

78 Nat'l Inst. of Standards and Tech., Digital Identity Guidelines (juin 2017), disponible sur https://doi.org/10.6028/NIST.SP.800-63-3.

79 Brian Krebs, Google : Security Keys Neutralized Employee Phishing, Krebs on Security (23 juillet 2018) https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing.

80 Voir Microsoft, Windows XP Support has ended, https://support.microsoft.com/fr/us/help/14223/windows-xp-end-of-support (dernière visite le 15 mai 2018).

81 Voir BSA The Software Alliance, Seizing Opportunity Through License Conformité : BSA Global Software Survey 6-7 (2016), http://www.bsa.org/~/ media/Files/StudiesDownload/BSA_GSS_US.pdf.

82 Id. à 4 (discutant de la "forte corrélation" entre les logiciels malveillants et les logiciels sans licence).

83 Université nationale de Singapour, Cybersecurity Risks from Non-Genuine Software, The Link Between Pirated Software Sources and Cybercrime Attacks in Asia Pacific 6 (1er nov. 2017), https://news.microsoft.com/ uploads/2017/10/Whitepaper-Cybersecurity-Risks-from-Non-Genuine-Software.pdf ("[D]ans de nombreuses régions du monde, l'utilisation de logiciels piratés/contrefaits/non authentiques contribue fortement à la croissance des cyber-risques et est responsable d'importants préjudices économiques et de pertes de productivité. Elle est également à l'origine d'une augmentation des attaques cybercriminelles et des pertes qui en découlent.")

CSDE

Council to Secure the Digital Economy

securingdigitaleconomy.org