CSDE

Council to Secure the Digital Economy

GUIDE INTERNATIONAL SUR LA SÉCURITÉ DES BOTNETS ET DES IOTS 2020

USTELECOM
THE BROADBAND ASSOCIATION

Consumer Technology Association™

AVIS

Le Guide international de sécurité des botnets et de l'IdO a été élaboré pour faciliter l'atténuation des botnets et d'autres menaces automatisées et distribuées par le biais d'une participation volontaire et d'une collaboration entre des parties prenantes disparates dans l'ensemble 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 des communications (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 personnes 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 consommateur, où l'analyse coûts-avantages peut différer considérablement de celle d'une grande entreprise. 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.

DÉCLARATION DE COPYRIGHT

01 / Résumé

Depuis la publication l'année dernière du Guide international anti-botnet 2018 par le CSDE, l'industrie a continué à intensifier ses efforts pour repousser les attaques distribuées. Cependant, les acteurs malveillants ont également intensifié leurs efforts. La version de cette année du guide a été rafraîchie et mise à jour tout du long, mais deux ajouts importants dans le guide 2020 méritent d'être soulignés. Tout d'abord, la section 3 contient une nouvelle et importante analyse de l'évolution de la menace des botnets au cours de l'année écoulée. Voici quelques-unes des principales conclusions de notre analyse :

- Les botnets adoptent de plus en plus de stratégies qui les rendent plus efficaces pour causer des dommages tout en évitant la détection.
- Les botnets ciblent plus fréquemment les appareils IoT d'entreprise et autres appareils IoT dotés de processeurs et d'architectures plus complexes.
- Les botnets de crypto-monnaies sont en augmentation, et leurs opérateurs se livrent souvent une concurrence féroce.
- Les botnets sont de plus en plus utilisés pour la fraude commerciale et de détail.
- Les robots des médias sociaux falsifient les preuves sociales et diffusent des contenus protégés par le droit d'auteur ou dont la distribution est illégale. - Nous commençons à voir des attaques DDoS IPv6, avec au moins un exemple avéré.

Deuxièmement, les parties de la section 5 qui traitent des dispositifs et des systèmes de dispositifs, ainsi que de l'installation des systèmes domestiques et des petites entreprises, ont bénéficié de l'élaboration par le CSDE du principal consensus industriel mondial sur la sécurité de l'IdO. S'appuyant sur les contributions techniques de centaines d'experts en sécurité de milliers d'entreprises différentes, le CSDE a réuni 20 grandes organisations de cybersécurité et de technologie, des associations industrielles, des consortiums et des organismes de normalisation pour identifier les exigences de sécurité de base pour le marché de l'IdO en pleine croissance. Cet effort, connu sous le nom de "Convene the Conveners" ou "C2", visait à relever quatre défis :

1. Promouvoir une harmonisation mondiale pour éviter la fragmentation des spécifications et des exigences de sécurité.
2. Travailler avec les forces émergentes du marché mondial qui favorisent naturellement les dispositifs et les systèmes sécurisés.
3. Développer un langage commun cohérent sur ces questions qui soit convaincant pour les différents publics politiques et techniques.
4. Contribuer à l'élaboration de politiques au niveau international et aux États-Unis, y compris au niveau des États.

Le résultat de cet effort historique, le Consensus C2 sur les capacités de base en matière de sécurité des dispositifs IoT, ou "Base de consensus C2", a été publié le 17 septembre 2019. Le C2 Consensus Baseline est un ensemble commun de capacités de sécurité des dispositifs qui peuvent être appliquées à tous les nouveaux dispositifs IoT qui se connectent à l'internet - des capacités de meilleures pratiques qui sont largement applicables, verticalement et horizontalement, sur tous les marchés. Il s'applique à toute la gamme des nouveaux appareils IoT, en tenant compte du large spectre de complexité des appareils, quel que soit l'environnement de déploiement. La base de référence se veut flexible et non prescriptive. En fonction d'une variété de facteurs, dont l'appareil

complexité, facilité de gestion du dispositif, profil de risque, cas d'utilisation et contexte - les capacités de sécurité décrites dans la ligne de base peuvent être réalisées de diverses manières, l'essentiel étant que la capacité de base ultime soit réalisée d'une manière applicable au dispositif spécifique.

Cette année, le guide s'inspire également du vaste processus multipartite du NIST sur la sécurité de base des dispositifs IoT. Le projet NISTIR 82591 et l'effort C2 sont en accord matériel sur les capacités de base des dispositifs, avec des recommandations supplémentaires pour les capacités de l'organisation, les informations des clients et les activités du cycle de vie des deux côtés.

Enfin, nous devons souligner que les entreprises membres du CSDE ont également élaboré un plan de coordination industrielle en cas d'attaque massive de botnet, inspiré de l'incident de 2016 du botnet Mirai basé sur l'IoT, qui a mis hors service des parties importantes d'Internet aux États-Unis et en Europe. Ce plan est inclus dans notre rapport intitulé "Cyber Crisis : Foundations of Multi-Stakeholder Coordination ou "Fondations de la crise cybernétique". Le rapport envisage des stratégies pour un total de 12 événements importants en matière de cybersécurité.

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 unique - 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 l'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. [2]
Malheureusement, plus le nombre de personnes, d'entreprises et d'appareils connectés augmente, plus le potentiel de ces attaques malveillantes augmente. 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 on estime qu'ils atteindront 20 milliards d'appareils connectés d'ici 2020. Avec cette surface d'attaque importante et croissante, ce n'est pas une coïncidence si le coût global des cyber-attaques est en hausse. On s'attend à ce que ces pertes atteignent des billions de dollars. Les botnets sont le moteur de ces pertes à l'échelle industrielle, et ils constituent une menace persistante qui cherchera à évoluer et à s'adapter dans les années à venir.

IBM Security Intelligence rapporte que l'activité des variantes de Mirai a presque double entre 2018 et 2019.

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 rester en tête des menaces sophistiquées actuelles. 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 botnets 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 qui sont guidées par les puissantes forces du marché mondial et qui sont aussi agiles et adaptables que les cybermenaces à atténuer, plutôt que des mécanismes de conformité du régulateur 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 certaines composantes ou parties prenantes choisies.
- 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.

Guide international de la sécurité des botnets et de l'IdO : 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 dispositifs IoT, (4) l'installation de systèmes pour les particuliers et les petites entreprises, et (5) les entreprises. Pour chacun de ces composants, 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. Aux fins du présent 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 nuage, d'hébergement web, de diffusion 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 objets tangibles au concept numérique. Nous recommandons des pratiques de base et des capacités avancées pour l'infrastructure, notamment :
   - 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. Le développement de logiciels. [3] Le logiciel est un élément de plus en plus omniprésent dans 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 se composent généralement de pratiques de base et de capacités avancées, à savoir
   - Pratiques de développement "Secure-by-Design
   - Gestion de la vulnérabilité de la sécurité
   - Transparence des processus de développement sécurisés

3. Dispositifs IoT . 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. 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 les "choses" d'extrémité dans l'IoT, nous recommandons des pratiques de base et des capacités avancées à inclure :
   - Développement sécurisé
   - Capacités sécurisées
   - Gestion du cycle de vie des produits

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 périmés et piratés

Perspectives d'avenir . Tout comme la publication du Guide 2018 n'était qu'une première étape, le présent Guide s'inscrit dans la stratégie permanente du CSDE visant à impliquer un large ensemble de parties prenantes, y compris les gouvernements de pays partageant les mêmes idées, afin de promouvoir les pratiques de base et les capacités avancées, et nous continuerons à nous projeter dans l'avenir en fonction de ce que l'évolution de la menace exige. Comme indiqué dans le Guide 2018, nous mettrons à jour, publierons et promouvrons une nouvelle version du Guide chaque année. À partir de cette année, le titre de notre Guide reflète l'année à venir, il s'agit donc de l'édition 2020.

Si les efforts déployés cette année pour lutter contre les botnets se concentrent sur la sécurité des dispositifs IoT, en raison de l'urgence de la situation.
une base de référence largement acceptée, tous les botnets importants ne ciblent pas les appareils connectés - en fait, certains des botnets les plus importants au monde ont été créés à partir d'appareils connectés.
les botnets les plus destructeurs ne ciblent pas les appareils connectés. Ainsi, bien qu'il Il est clair que le futur des botnets est étroitement lié à l'avenir de la sécurité de l'IdO, et le CSDE va continuer à prendre l'initiative sur ce front, nous allons également explorer d'autres moyens que les botnets et autres menaces distribuées peuvent être réduits de façon spectaculaire grâce au leadership de nos membres. En reconnaissant la nature complexe et stratifiée de la menace des botnets, les entreprises du CSDE s'attaqueront à ces menaces sur plusieurs fronts.

The digital economy has been an engine for commercial growth and quality-of-life improvements across the world and may already represent 20% of global economic value.

02 / Introduction

Les membres du Council to Secure the Digital Economy (CSDE) 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 dont bénéficient une grande partie 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.

Depuis la publication du Guide international anti-botnet 2018, les membres du CSDE - Akamai, AT&T, Centur yLink, Cisco, Ericsson, IBM, Intel, NT T, Oracle, Samsung, SAP, Telefónica et Verizon - soutenus par USTelecom et la Consumer Technology Association (CTA), ont encouragé l'adoption d'une sécurité améliorée sur le marché mondial dans les infrastructures, les logiciels, les appareils et d'autres segments de l'économie numérique, afin d'unir l'industrie au niveau mondial dans la lutte contre les botnets malveillants.

Le monde a pris note. En 2019, le Forum sur la gouvernance de l'Internet de l'ONU a reconnu le CSDE pour avoir pris des mesures significatives afin de lutter contre les botnets et d'autres menaces automatisées et distribuées par le biais d'une approche collaborative et globale de l'écosystème, où la sécurité est une priorité partagée. Nous avons également été reconnus dans la Botnet Roadmap du gouvernement américain comme des contributeurs clés à la lutte. Notre projet global a un impact dans de nombreuses régions du monde, notamment en Europe, en Asie et en Amérique latine, où les membres du CSDE font des affaires.

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 chaque continent. Selon certaines estimations, elle représenterait déjà 20 % de la valeur économique mondiale7. [7] 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.[8] La croissance de l'économie numérique est continuellement alimentée par l'adoption par les entreprises et les consommateurs de technologies nouvelles et émergentes. [9] Gérer en toute sécurité les opportunités présentées Cette croissance impressionnante représente un défi et une responsabilité pour tous les acteurs de la communauté des technologies de l'information et des communications (TIC).

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[10], de mener des attaques par déni de service[11] et de diffuser artificiellement de la désinformation corrosive sur les médias sociaux12. [12] 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. [13] Il n'y a jamais eu autant de systèmes vulnérables qu'aujourd'hui, 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.[14] 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 à mesure qu'elles déploient des appareils. Néanmoins, des appareils non sécurisés continuent d'affluer sur le marché sans que les systèmes en place soient conçus pour les sécuriser. [15] En outre, il est désormais possible pour des acteurs malveillants relativement peu qualifiés de louer un puissant botnet pour des activités néfastes à grande échelle. [16]

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. [17] 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.) [18]

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 freinent 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 normatives des régulateurs sont rarement efficaces, mais elles sont en fait généralement contre-productives par rapport à l'objectif de sécurité. [19] Les solutions dynamiques et flexibles qui reposent sur des normes consensuelles volontaires, qui répondent aux exigences 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.

La publication du Guide 2018 n'était qu'une première étape. Nous engageons actuellement un large éventail de parties prenantes, y compris des gouvernements de pays partageant les mêmes idées, afin de promouvoir les pratiques de base et les capacités avancées du Guide. En outre, nous continuerons à mettre à jour, à publier et à promouvoir une nouvelle version du Guide chaque année.

Nouveaux éléments dans le Guide 2020. La version de cette année du Guide a été rafraîchie et mise à jour dans son ensemble, mais deux ajouts importants dans le Guide 2020 méritent une attention particulière. Tout d'abord, la section 3 contient une nouvelle et importante analyse de l'évolution de la menace des botnets au cours de l'année écoulée. Voici quelques-unes des principales conclusions de notre analyse :

- Les botnets adoptent de plus en plus de stratégies qui les rendent plus efficaces pour causer des dommages tout en évitant la détection.
- Les botnets ciblent plus fréquemment les appareils IoT d'entreprise et autres appareils IoT dotés de processeurs et d'architectures plus complexes.
- Les botnets de crypto-monnaies sont en augmentation, et leurs opérateurs se livrent souvent une concurrence féroce.
- Les botnets sont de plus en plus utilisés pour la fraude commerciale et de détail.

‣ Les robots des médias sociaux falsifient les preuves sociales et diffusent des contenus protégés par le droit d'auteur ou dont la distribution est illégale. ‣ Nous commençons à voir des attaques DDoS IPv6, avec au moins un exemple avéré.

Deuxièmement, les parties de la section 5 qui traitent des dispositifs et des systèmes de dispositifs, ainsi que de l'installation de systèmes domestiques et de petites entreprises, ont bénéficié de l'élaboration par le CSDE du principal consensus industriel mondial sur la sécurité IoT. S'appuyant sur les contributions techniques de centaines d'experts en sécurité de milliers d'entreprises différentes, le CSDE a réuni 20 grandes organisations de cybersécurité et de technologie, des associations industrielles, des consortiums et des organismes de normalisation pour identifier les exigences de sécurité de base pour le marché de l'IdO en pleine croissance. Cet effort, connu sous le nom de "Convene the Conveners" ou "C2", visait à relever quatre défis :

1. Promouvoir une harmonisation mondiale pour éviter la fragmentation des spécifications et des exigences de sécurité.
2. Travailler avec les forces émergentes du marché mondial qui favorisent naturellement les dispositifs et les systèmes sécurisés.
3. Développer un langage commun cohérent sur ces questions qui soit convaincant pour les différents publics politiques et techniques.
4. Contribuer à l'élaboration de politiques au niveau international et aux États-Unis, y compris au niveau des États.

Le résultat de cet effort historique, le Consensus C2 sur les capacités de base en matière de sécurité des dispositifs IoT ou "Consensus C2", est le suivant
Baseline ", a été publié le 17 septembre 2019. La ligne de base du consensus C2 est un ensemble commun de sécurité des dispositifs.
capacités pouvant être appliquées à tous les nouveaux dispositifs IoT qui se connectent à l'internet - capacités liées aux meilleures pratiques
qui sont largement applicables, verticalement et horizontalement, sur tous les marchés. Elle s'applique à la gamme variée de nouveaux produits IoT
dispositifs, s'adaptant au large éventail de
la complexité du dispositif, quel que soit le déploiement l'environnement. La ligne de base est destinée à être flexible et non prescriptive. En fonction d'un une variété de facteurs - de la complexité du dispositif, gestion des dispositifs, profil de risque, cas d'utilisation et le contexte - les capacités de sécurité
La capacité de la ligne de base décrite peut être obtenue de diverses manières, l'essentiel étant que la capacité de la ligne de base finale soit obtenue d'une manière applicable à l'appareil spécifique.

Based on a study of 180 countries and territories, Verizon reported that 84% of botnets involved in data breaches targeted the finance and insurance industries.

Cette année, le guide s'inspire également du vaste processus multipartite du NIST sur la sécurité de base des dispositifs IoT. Le projet NISTIR 825920 et l'effort C2 sont en accord matériel sur les capacités de base des dispositifs, avec des recommandations supplémentaires pour les capacités de l'organisation, les informations des clients et les activités du cycle de vie des deux côtés.

Enfin, nous devons souligner que les entreprises membres du CSDE ont également élaboré un plan de coordination industrielle en cas d'attaque massive de botnet, inspiré de l'incident de 2016 du botnet Mirai basé sur l'IoT, qui a mis hors service des parties importantes d'Internet aux États-Unis et en Europe. Ce plan est inclus dans notre rapport intitulé "Cyber Crisis : Foundations of Multi-Stakeholder Coordination ou "Fondations de la crise cybernétique". Le rapport envisage des stratégies pour un total de 12 événements importants en matière de cybersécurité.

03 / L'évolution des botnets : Bilan de l'année

Comme c'était le cas lors de la publication du Guide international anti-botnet 2018, la catégorie la plus importante de menaces automatisées et distribuées pour l'écosystème mondial de l'internet et des communications est celle des botnets - de vastes réseaux d'ordinateurs et d'appareils compromis connectés à l'internet qui communiquent avec des ser vers 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 dispositifs 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. [21]

Botnets : Un problème mondial persistant. Alors que les entreprises du CSDE travaillent en permanence avec la communauté mondiale pour exercer une pression toujours plus forte sur les opérateurs de botnets, ces acteurs malveillants ne restent pas inactifs. Ils ne veulent pas voir leurs opérations démantelées, et ils voient dans les actions de nos entreprises une menace directe pour leurs profits et autres objectifs critiques. Au cours de l'année 2019, nous avons observé diverses tendances qui nous amènent à conclure que, si des progrès sont réalisés dans la lutte contre les botnets, les défis s'intensifient.

Nos adversaires sont attentifs à chacun de nos gestes et font évoluer leurs stratégies de manière intelligente.
réponse. Les opérateurs de botnets inventent constamment de nouveaux outils, adoptent de nouvelles techniques et étudient la manière dont nous combattons leur
des bots perturbateurs, afin de contrer nos efforts. Nous sommes aux prises avec des bots très motivés et de plus en plus nombreux.
des ennemis sophistiqués, notamment des États-nations et des organisations criminelles à grande échelle, qui sont très bien armés.
financés. Ces organisations se sont effectivement protégées de toute attribution, tout en continuant à faire d'énormes gains financiers mal acquis par des méthodes criminelles.

Dans cette section, nous examinerons comment la menace des botnets a évolué au cours de l'année écoulée. Voici quelques-unes des principales conclusions de notre analyse :

- Les botnets adoptent de plus en plus de stratégies qui les rendent plus efficaces pour causer des dommages tout en évitant la détection.
- Les botnets ciblent plus fréquemment les appareils IoT d'entreprise et autres appareils IoT dotés de processeurs et d'architectures plus complexes.
- Les botnets de crypto-monnaies sont en augmentation, et leurs opérateurs se livrent souvent une concurrence féroce.
- Les botnets sont de plus en plus utilisés pour la fraude commerciale et de détail.
- Les robots des médias sociaux falsifient les preuves sociales et diffusent des contenus protégés par le droit d'auteur ou dont la distribution est illégale. - Nous commençons à voir des attaques DDoS IPv6, avec au moins un exemple avéré.

Mirai ne mourra pas : plus de 60 variantes, l'activité double presque. Depuis que le code source du botnet Mirai a été divulgué en ligne il y a trois ans, les acteurs malveillants n'ont cessé d'expérimenter et de créer leurs propres versions améliorées. En juillet 2019, le botnet Mirai comptait au moins 63 variantes confirmées22 et il est très possible que d'autres n'aient pas encore été découvertes.

IBM Security Intelligence rapporte que l'activité des variantes de Mirai a presque doublé entre 2018 et 2019.[23] Dans un inter view sur les nouveaux exploits IoT, publié en mars 2019, un chercheur d'AT&T Cybersecurity a déclaré : " Chaque fois que nous examinons un nouveau malware IoT - c'est presque inévitablement une nouvelle variante de Mirai. Chaque jour, nous voyons de nouvelles variantes de Mirai avec des charges utiles différentes... "[24] L'activité liée à Mirai avait diminué après une cyberattaque historique en 2016 qui a mis hors service des portions importantes d'Internet aux États-Unis et en Europe, mais cette résurgence indique que le logiciel malveillant continue de représenter une menace sérieuse.

Les différentes variantes de Mirai sont contrôlées par des opérateurs qui se font concurrence pour dominer les appareils IoT vulnérables. Comme on peut s'y attendre compte tenu de la course aux armements technologiques que les opérateurs de botnets mènent sur plusieurs fronts - contre les forces de l'ordre et les uns contre les autres - les botnets les plus récents sont généralement plus ingénieux que Mirai. [25] Echobot, par exemple, est une variante de Mirai découverte en 2019 qui utilise au moins vingt-six exploits pour infecter les appareils. [26]

Dans certains cas, les créateurs de botnet combinent le code de Mirai avec celui d'autres sources pour parvenir à leurs fins. Par exemple, Gafgyt, qui, selon les données d'IBM X-Force, représente 27 % de tous les logiciels malveillants ciblant les appareils IoT[27], est généralement considéré et étudié comme distinct de Mirai, bien qu'il partage une partie de son code source ayant fait l'objet d'une fuite.

Le rapport sur les menaces 2019 de CenturyLink28 contient une comparaison de Gafgyt, Mirai et d'autres logiciels malveillants de botnet IoT basée sur les données des Black Lotus Labs de Centur yLink. [29] Les données révèlent que le temps de fonctionnement moyen de Gafgyt et Mirai est en baisse. Cela s'explique notamment par le fait que davantage de chercheurs et d'équipes de lutte contre les menaces suivent le mouvement des logiciels malveillants, que les chercheurs s'améliorent dans l'identification des variantes de logiciels malveillants IoT conçues pour échapper à la détection et que les fournisseurs s'améliorent dans le suivi proactif des menaces sur leurs réseaux. [30]

Risque accru pour les entreprises et les dispositifs à haute complexité. Si les entreprises ont toujours joué un rôle important dans l'approche globale de l'écosystème visant à réduire les réseaux de zombies, elles risquent de plus en plus de subir des dommages et des pertes. Nous assistons à une expansion rapide du paysage des menaces liées aux botnets, et des données récentes d'IBM X-Force révèlent que les systèmes d'entreprise sont infectés plus fréquemment par des variantes de Mirai. [31] Les données de Telefónica indiquent que les entreprises sont plus susceptibles d'être infectées par un botnet au cours des deux premiers mois suivant le déploiement d'un nouveau service. [32]

Les violations de données sont facilitées par les botnets si souvent que le rapport d'enquête sur les violations de données 2019 de Verizon a analysé séparément les attaques par botnet "pour éviter d'éclipser" les autres types d'incidents. N'importe quel secteur d'activité peut être ciblé. Cependant, certaines industries sont clairement plus exposées aux attaques de botnet. Sur la base d'une étude portant sur 180 pays et territoires, Verizon a indiqué que 84 % des botnets impliqués dans des violations de données ciblaient les secteurs de la finance et de l'assurance ;
10 % visaient les industries de l'information ; 33 et 5 % les industries des services professionnels, scientifiques et techniques. L'étude ne fait pas de distinction entre les botnets IoT et les autres botnets.

Dans le passé, les botnets basés sur l'IdO infectaient principalement les appareils et systèmes connectés présents dans les foyers, tels que les caméras, les enregistreurs vidéo, les appareils d'éclairage et les thermostats. Mais il est logique que, du point de vue des criminels, toute nouvelle catégorie d'appareils IoT - que ce soit à la maison, au niveau de l'entreprise ou ailleurs dans l'écosystème - constitue un nouveau bataillon dans leur armée de botnets. De nombreuses parties prenantes possédant des appareils connectés, et pas seulement les entreprises, sont exposées à un risque accru.

Par exemple, au cours de l'année 2019, Black Lotus Labs de Centur yLink a dressé le profil de TheMoon, un botnet IoT qui cible les vulnérabilités des routeurs dans les réseaux à large bande. 34 Bien que cette menace particulière ait été atténuée, elle montre à quel point la sécurité de l'IoT a des répercussions sur les infrastructures et l'écosystème dans son ensemble.

En février 2019, les chercheurs en sécurité ont découvert des échantillons de Mirai affectant un ensemble de processeurs et d'architectures qui ne pouvaient pas être ciblés auparavant. 35 Nous pouvons maintenant nous attendre à des infections de plus de types de routeurs, de capteurs en réseau, de radios et de microprocesseurs pour les signaux numériques. 36 Des développements comme ceux-ci ouvrent la porte à des botnets plus importants.

Les experts estiment que les futurs vecteurs d'attaque pourraient inclure de plus en plus de systèmes IoT industriels et de vêtements connectés37 ; il sera donc essentiel que l'industrie et le gouvernement se coordonnent pour identifier les capacités de sécurité qui reconnaissent les considérations uniques associées aux différents niveaux de complexité.

Botnets intelligents et automatisés : Swarmbots et Hivenets. Imaginez des milliers d'abeilles qui essaient d'atteindre une seule cible. C'est, par essence, un swarmbot. Les swarmbots peuvent souvent surpasser les défenses traditionnelles par leur seul volume. 38 Pour ne rien arranger, ces bots sont dirigés par une intelligence artificielle appelée hivenet.

Les Hivenets sont des "botnets qui pensent par eux-mêmes" et ont la capacité d'apprendre pendant une attaque. Cette capacité d'apprentissage en temps réel est en grande partie à l'origine de leur dangerosité. Alors que les botnets traditionnels devaient attendre les ordres de leurs opérateurs40, le hivenet coordonne automatiquement les stratégies en fonction de ce que les swarmbots apprennent.

Les bots partagent des informations sur les vulnérabilités découvertes et d'autres informations stratégiques afin d'accroître l'intelligence collective de la ruche. Les bots coordonnent et partagent également les ressources de manière automatique. Les bots individuels peuvent être équipés de différents outils ; lorsque le hivenet découvre une vulnérabilité, le swarmbot doté de l'outil approprié est mobilisé. 41

En déployant la technologie basée sur les essaims, les opérateurs de botnet peuvent augmenter considérablement l'efficacité d'une attaque en réduisant le temps nécessaire pour infiltrer un dispositif ou un système de dispositifs. L'une des principales raisons pour lesquelles les criminels ont besoin d'une plus grande efficacité est de surpasser les outils de sécurité réseau qui sont déployés de plus en plus fréquemment sur le marché mondial. 42 Nous sommes dans une course aux armements technologiques à long terme, et la technologie basée sur les essaims est l'effort des criminels pour monter en puissance parce que leurs anciens outils s'avèrent de plus en plus inefficaces.

Emotet est de retour avec plus de 200 000 courriels et mots de passe volés. Talos de Cisco rapporte qu'après une pause de plusieurs mois, le botnet Emotet est revenu en force en septembre 2019.43 Emotet envoie un volume élevé de spam à des utilisateurs du monde entier, les incitant à libérer des charges utiles malveillantes, dont les suivantes
le cheval de Troie TrickBot et le ransomware Ryuk, qui sont tous deux connus pour s'enfoncer profondément dans les réseaux des victimes, augmentant ainsi les dommages potentiels. 4 4

NT T utilise actuellement des captures de données netflow et exploite la connaissance de 40 % du trafic Internet mondial pour analyser l'infrastructure et les acteurs de la menace derrière TrickBot, qui, à la fin de l'année dernière, a été reconnu comme la principale menace pour les entreprises. 45 Comme TrickBot est souvent téléchargé après une infection par Emotet, l'atténuation de TrickBot peut contribuer à limiter le potentiel destructeur d'Emotet.

Souvent, les courriels envoyés par Emotet semblent provenir de contacts légitimes. Ils peuvent contenir des détails sur des conversations réelles auxquelles les destinataires ont participé. Emotet est connu pour citer des fils de discussion antérieurs et même envoyer des courriels de suivi comme le ferait un être humain. De telles tactiques rendent le botnet de plus en plus difficile à détecter par les filtres anti-spam et les êtres humains. 46

Emotet obtient les informations nécessaires pour tromper les destinataires des e-mails en s'introduisant dans les comptes de messagerie et en volant les listes de contacts et les e-mails des ordinateurs des victimes. Dans son étude d'Emotet, Talos de Cisco a découvert 202 675 combinaisons uniques de nom d'utilisateur et de mot de passe. Talos de Cisco indique également qu'après avoir analysé Emotet dans un bac à sable de logiciels malveillants appelé Threat Grid pendant 10 mois, le botnet malveillant a tenté d'envoyer du spam près de 19 000 fois48. 48

Si les publications d'actualités technologiques ont qualifié Emotet de "botnet le plus destructeur du monde "49 et de "botnet le plus dangereux d'aujourd'hui "50, il n'est pas le seul spambot à fort volume actuellement actif. Par exemple, Gamut et Necurs, des spambots qui, il y a quelques années seulement, représentaient 97 % du trafic de spam sur Internet, continuent de causer des problèmes. 51

En 2019, Cisco rapporte que le botnet Gamut a envoyé des spams de rencontres et de relations intimes, ainsi que des publicités pour des produits pharmaceutiques et des offres d'emploi. 52 Necurs est passé d'un botnet qui envoie des chevaux de Troie bancaires et des ransomwares à un botnet qui permet également le proxing de trafic, le cr yptomining et le lancement d'attaques DDoS. Une analyse réalisée par Centur yLink révèle que Necurs est principalement présent dans les pays en développement53. 53 Toutefois, comme les réseaux de zombies ignorent les frontières juridictionnelles, ces infections peuvent avoir des retombées importantes dans toutes les régions du monde.

Botnets à louer : désormais disponibles sur le Dark Web et les médias sociaux. Sur le Dark Web (zones de l'internet accessibles à l'aide d'un logiciel spécifique), il existe des marchés criminels où les cybercriminels peuvent louer des botnets à bas prix. Cet arrangement, appelé "malware-as-a-ser vice" (MaaS), met des outils destructeurs à la disposition d'un plus grand nombre d'acteurs malveillants. 54 Certains des criminels qui louent un botnet n'ont pas les compétences techniques nécessaires pour créer leur propre botnet. Cependant, d'autres considèrent la location d'un botnet comme une décision commerciale purement pragmatique. Comme les entreprises légitimes, les entreprises criminelles sont intéressées par le retour sur investissement et sont prêtes à donner la priorité aux investissements qui rapportent le plus. 55 Parfois, les criminels ayant des compétences techniques avancées louent des botnets pour compléter leurs armées déjà existantes - dans ce cas, on peut considérer les botnets loués comme des mercenaires.

Dans le rapport 2019 Cyber Crisis Foundations, le CSDE documente le cas d'une entreprise de télécommunications libérienne qui a fait l'objet d'un procès après avoir engagé un hacker criminel pour lancer des attaques DDoS contre un rival afin d'obtenir un avantage concurrentiel déloyal. 56 Le pirate a utilisé un botnet personnalisé basé sur Mirai et a loué des caméras de sécurité et des routeurs infectés auprès d'autres pirates. 57 Au plus fort de l'attaque, la plupart des internautes du pays ont été privés d'accès à Internet, ce qui a renforcé les préoccupations mondiales concernant la sécurité de l'IdO. 58

Si vous pensez que toutes les activités malveillantes se déroulent dans le secret du dark web, sachez que les créateurs de botnets sont de plus en plus nombreux à faire de la publicité pour leurs créations sur des plateformes grand public. Parfois, les créateurs vont même jusqu'à louer des botnets qui sont

encore en développement, alors que des criminels avides font la queue pour s'assurer une place. Par exemple, les créateurs de Cayosin - un botnet décrit comme "Frankenstein" parce qu'il est fabriqué à partir de différents morceaux de logiciels malveillants open source (dont Mirai) - ont fait la publicité de leur projet sur YouTube et Instagram, bafouant ouvertement la loi et facturant un faible coût de location pour inciter les criminels à devenir leurs clients. 59

En utilisant les médias sociaux, les créateurs de botnets sont en mesure de réaliser des études de marché dans le but d'augmenter leurs profits - ils demandent parfois ouvertement l'avis des clients sur les services fournis, afin d'améliorer le service et d'établir une relation avec leurs clients criminels. 60 Il s'agit d'un changement marqué dans l'évolution culturelle des criminels de botnet.

Les bots furtifs utilisent des astuces pour éviter la détection. Les développeurs de botnets font constamment évoluer leurs stratégies pour que les bots restent cachés et actifs plus longtemps. Un récent rapport d'Akamai explique que "les bots peuvent représenter jusqu'à 60 % du trafic web global, mais moins de la moitié d'entre eux sont effectivement déclarés comme bots - ce qui rend le suivi et le blocage difficiles." 61 Un autre facteur de complication est que ces bots ne sont pas tous malveillants, ce qui rend difficile l'éradication des comportements criminels lorsque l'automatisation est détectée.

Par exemple, pour éviter d'être détectés lorsqu'ils visitent un site web, les robots malveillants se font passer pour des navigateurs et des applications mobiles populaires ou, dans certains cas, ils se font passer pour de bons robots. Certains robots trafiquent les propriétés des navigateurs pour usurper les "caractéristiques de l'empreinte digitale" qui ont tendance à être mises sur une liste blanche, ou trafiquent les cookies, soit en les supprimant, soit en vendant de bons cookies pour qu'ils paraissent légitimes63. 63

Nous avons également constaté l'augmentation constante des "attaques lentes et discrètes", où les robots essaient de passer inaperçus,
le vol inlassable d'une grande quantité d'informations au fil du temps. 6 4 Lorsqu'ils utilisent cette méthode, les bots changent d'adresse IP ou utilisent plusieurs adresses IP. Cela leur permet de contourner les limitations de débit sans se faire remarquer ; les adresses IP multiples envoient un petit nombre de requêtes par heure. 65

Les bots utilisent également d'autres techniques pour contourner les limites de débit lorsqu'ils restent "bas et lents". De plus en plus fréquemment, les opérateurs de botnets rendent le trafic malveillant anonyme en l'acheminant par des connexions résidentielles à large bande et sans fil. 66 Les botnets modifient également leurs adresses IP via des proxies en se cachant dans des réseaux anonymes, comme les VPN et Tor 67 - y compris une variante de Mirai récemment découverte. 68 Lorsque votre ennemi peut se cacher dans la foule, sans s'exposer, la tâche de le détecter et de s'en défendre est considérablement plus difficile.

Les réseaux de zombies ont recours à une autre astuce : faire le mort. Le botnet Necurs, analysé par les Black Lotus Labs de Centurylink, s'arrête de fonctionner à différents intervalles. Dans un cas observé, Necurs a été actif pendant trois semaines, s'est tu pendant deux semaines, puis s'est réactivé. 69 En 2019, Necurs est apparu largement inactif pendant plusieurs mois, ne se mettant en action qu'une fois par semaine pendant de brèves périodes. 70 Necurs s'est avéré résistant à diverses tentatives de sinkholing - des pièges pour les botnets déployés par les forces de l'ordre ou les chercheurs en sécurité - grâce à son algorithme de génération de domaines (DGA). Cependant, l'analyse du DGA du botnet révèle aux chercheurs les domaines qui seront générés à l'avenir, ce qui leur permet d'inspecter le trafic DNS et réseau correspondant et de déployer des stratégies d'atténuation. 71

Les bots fraudent les détaillants et les annonceurs en ligne, en se faisant passer pour des humains. Un récent rapport d'Akamai sur l'état de la sécurité sur Internet7 2 révèle que les bots malveillants représentent désormais près de la moitié de la bande passante Internet dirigée vers les détaillants en ligne. 7 3 À la lumière de ce fait qui donne à réfléchir, le rapport qualifie les bots d'"outils de destruction massive (de détail)".

ces années, les criminels utilisent de[illegible]aux de zombies pour commettre des fraudes publicitaires en envoyant des bots à la place de véritables [illegible]mains vers des destinations en ligne. Cela coûte des millions de dollars aux annonceurs et offre aux utilisateurs des expériences de navigation sur le web de moins bonne qualité. 74 Les bots ont également été utilisés pour d'autres activités à but lucratif, comme l'achat de marchandises ou de billets pour des événements populaires et leur vente au rabais. 75

Au début de l'année, les experts en sécurité d'Oracle ont découvert une importante opération de fraude impliquant DrainerBot, qui s'est propagée via un kit de développement logiciel (SDK) présent dans des centaines d'applications et de jeux pour téléphones mobiles. Une fois installées sur les téléphones d'utilisateurs peu méfiants, les applications infectées utilisaient plus de 10 Go de données par mois (même si le téléphone était en mode veille) et faisaient croire aux annonceurs qu'ils recevaient du trafic humain. 76

En 2019, il est beaucoup plus difficile de dire si une activité en ligne est humaine. Par le passé, en cas de soupçons, il était relativement facile d'identifier des comportements non humains tels que l'ouverture et la fermeture de millions de fenêtres. 7 7 Cependant, l'activité des bots malveillants ressemble de plus en plus à une véritable navigation web humaine, à tel point que même les experts ont du mal à faire la différence.

Les **botnets sociaux diffusent de la désinformation et des liens illégaux.** La capacité du trafic des botnets à ressembler au trafic humain ordinaire a des implications qui vont au-delà de la fraude des détaillants et des annonceurs. Les botnets abusent des médias sociaux de différentes manières, allant de l'usurpation de l'identité de millions de personnes à la facilitation de l'accès à des contenus protégés par des droits d'auteur ou dont la distribution est illégale.

Dans le guide de l'année dernière, nous avons constaté que les réseaux de zombies peuvent jouer un rôle dans la diffusion de désinformations corrosives qui peuvent priver le public de la possibilité de prendre des décisions éclairées. Les robots qui imitent le comportement humain peuvent potentiellement être utilisés pour influencer les opinions humaines sur à peu près n'importe quel sujet, des tendances musicales à la politique, en falsifiant les preuves sociales. 78

Pour un exemple courant de botnets diffusant des contenus protégés par le droit d'auteur, nous pouvons nous tourner vers le sport. En décembre 2018, Telefónica a publié un rapport de tendance sur la "détection des botnets Twitter dans les événements sportifs". 79 Les bots diffusent massivement des liens vers des contenus diffusés illégalement en streaming, interférant avec les bénéfices des détenteurs de droits.

Mettre un frein aux botnets qui exploitent les médias sociaux ne sera pas une tâche facile. En septembre 2019, le rapport de transparence de Twitter a révélé que la plateforme avait supprimé des milliers de comptes ayant des liens apparents avec des campagnes de médias sociaux soutenues par l'État. 80 Au total, la plateforme a purgé des millions de faux comptes. 81 Pourtant, les botnets apprennent, s'adaptent et sont constamment mis à niveau pour échapper aux interdictions et poursuivre leurs opérations sans être détectés.

Les bots se multiplient pour extraire des crypto-monnaies anonymes. L'essor de la cr yptocurrency est devenu un carburant pour l'activité des botnets. En 2018, la Cyber Threat Alliance a constaté une augmentation de 459 % des logiciels malveillants de minage de cr yptocurrency82, et il est possible qu'à la fin de 2019, nous soyons confrontés à des chiffres tout aussi choquants.

Les opérations de minage des botnets sont motivées par le profit. Ainsi, lorsque la crypto-monnaie Monero a triplé de valeur à l'été 2019, l'activité des botnets a connu une hausse notable. 83 En général, les criminels préfèrent les crypto-monnaies comme Monero et ZCash qui sont relativement anonymes, plutôt que le bitcoin qui est plus facile à tracer pour les forces de l'ordre. 84

Bien que les systèmes infectés des victimes continuent généralement de fonctionner, le crime n'est pas sans victime ; la pression supplémentaire exercée sur l'infrastructure informatique peut avoir de graves conséquences, notamment des dommages physiques. 85 Les victimes peuvent constater un ralentissement des performances et une augmentation du temps de latence car les ressources sont détournées au profit des criminels. Les opérations commerciales peuvent être affectées négativement et les victimes peuvent constater des factures d'énergie plus élevées. 86

Les guerres de territoire des botnets se déplacent vers le cloud. La concurrence que se livrent les criminels pour s'emparer du plus grand nombre possible d'appareils et de systèmes donne souvent lieu à des "guerres de territoire" entre botnets. Les botnets infectent les appareils déjà infectés par d'autres botnets - et suppriment leurs rivaux - afin d'accroître leur propre puissance et leurs profits.

En 2019, nous avons assisté à une escalade de la rivalité entre Rocke et Pascha, des groupes de piratage de cr yptomining qui se disputent la domination de l'environnement de cloud computing Linux. 87 Les deux groupes utilisent des ressources cloud mal acquises pour faire avancer les opérations de cr yptomining. Pendant ce temps, Smominru, un autre botnet de cr yptomining, a supprimé des rivaux des ordinateurs Windows 7. 88 Alors que deux autres bots de cr yptomining, Fbot et Trinity, ont poursuivi une lutte entamée l'année dernière pour contrôler des dizaines de milliers d'appareils Android non sécurisés. 89

Les bots qui suppriment d'autres bots devenant de plus en plus courants et les profits étant en jeu, les opérateurs de botnets sont soumis à une pression importante pour combattre leurs rivaux à l'aide des outils les plus récents, ou du moins pour prendre des mesures pour se défendre. Par exemple, certains botnets corrigent activement les failles de sécurité après s'être introduits dans un appareil, afin d'empêcher un rival de s'y introduire.

La demande de puissants botnets capables de mettre hors d'état de nuire leurs rivaux s'est répercutée sur les marchés criminels du dark web, entraînant la prolifération de logiciels malveillants puissants comme Mylobot, qui dispose d'un nombre sans précédent d'outils. 90

Alors que les pirates criminels s'inquiètent de voir leurs rivaux les rendre obsolètes, ils doivent également prendre en compte la menace que représente pour eux le fait de ne pas avoir accès à l'information.

des opérations menées par des "cyber justiciers". Des botnets comme BrickerBot91 et Hajime92 ont été conçus pour effacer les botnets malveillants

et améliorer ostensiblement la sécurité d'un système infecté. Bien que les intentions derrière ces botnets ne sont pas sur le surface malveillante, le justicier
Les botnets brisent néanmoins la
les lois de nombreux pays.

> **Sometimes, criminals with advanced technical proficiency will rent botnets to supplement their already-existing armies — in these cases, one can think of the rented botnets as mercenaries.**

L'avenir de la sécurité d'IPv6 et l'internet des objets. L'IPv6 est un protocole internet défini par l'Internet Engineering Task Force (IETF)93 et a été créé pour remplacer à terme l'ancien protocole IPv4. À mesure que le nombre d'internautes et d'appareils connectés augmente dans le monde, les réseaux fournissent de plus en plus de connectivité IPv695 et, dans de nombreux cas, IPv6 et IPv4 sont déployés ensemble.
Le rapport d'Akamai sur l'état de la sécurité Internet note cependant que " parce que l'IPv6 est encore considéré comme une minorité du trafic, il ne constitue pas un argument de vente majeur pour un certain nombre d'outils de sécurité. Toutes les organisations ne considèrent pas que l'espace IPv6 vaut la peine d'être surveillé, même lorsque la capacité est présente "96 .

Les botnets comme Mirai obtiennent de nouveaux bots par le biais de balayages automatisés de l'espace d'adressage IPv4, et les dispositifs vulnérables sont généralement infectés quelques minutes après leur connexion à Internet. [97] En revanche, l'analyse de l'espace d'adressage IPv6 a été considérée comme extrêmement difficile en raison de sa taille. [98] Néanmoins, depuis des années, les experts avertissent que des vulnérabilités non découvertes dans le protocole IPv6, combinées à la croissance de l'IdO, pourraient permettre des attaques massives de botnet. [99]

Il existe désormais au moins un cas documenté d'attaque DDoS IPv6, qui a utilisé une technique connue sous le nom de DNS.
amplification au lieu d'un botnet. Bien qu'il ne s'agisse pas d'un incident majeur, la question doit être posée : l'IPv6 pourrait-il entraîner des attaques DDoS plus nombreuses et plus importantes au fil du temps ? L'augmentation des attaques de botnets IPv6 présenterait des défis uniques qui ne sont pas faciles à résoudre. Par exemple, le nombre incroyablement élevé d'adresses IPv6 (plus de 8 000 fois plus qu'IPv4) pourrait permettre aux attaquants de dépasser la mémoire des systèmes de sécurité conçus pour traiter les menaces basées sur IPv4. [101]

Conclusion. Alors que l'industrie fait des progrès tangibles dans la lutte contre les botnets, la menace a continué d'évoluer et de croître. Dans un avenir proche, les problèmes de sécurité mondiale liés aux botnets pourraient être exacerbés par la migration vers le cloud et la croissance de l'IdO - deux évolutions qui augmentent radicalement la surface d'attaque que les acteurs malveillants peuvent cibler. Pour lutter contre cette menace qui évolue rapidement, nous avons besoin d'un mouvement mondial, fondé sur le marché, en faveur d'une sécurité accrue dans tous les segments de l'économie numérique. Dans le même temps, nous avons besoin de politiques qui encouragent l'innovation et permettent à l'industrie d'évoluer de manière aussi souple et dynamique que les adversaires.

04 / Lutte contre les menaces automatisées et distribuées dans un écosystème Internet diversifié

Le défi fondamental que représente la lutte contre les botnets dans l'écosystème mondial de l'internet, extrêmement diversifié, complexe et interdépendant, demeure : 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, mais que personne ne les contrôle, qui est responsable du nettoyage des botnets malveillants qui menacent les fonctions de base sur lesquelles tout le monde compte ?

La réponse est que toutes les parties prenantes doivent prendre leurs responsabilités, et pas seulement dans le but altruiste de nettoyer le 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.

L'atténuation des réseaux de zombies nécessite une approche réfléchie et holistique. Les différentes parties de cet écosystème complexe
doivent - pour leur bien individuel et collectif - approfondir et aiguiser leur compréhension de leur propre responsabilités et comment elles complètent celles
d'autres. Et dans les cas où les lignes
sont peu claires ou inconnues, les parties prenantes doivent travailler ensemble pour les clarifier. En l'absence d'une telle les stratégies de lutte contre les réseaux de zombies seront revenir à l'erreur des solutions utopiques
concentré sur un ou deux éléments de la
L'idée que les fournisseurs d'accès à Internet devraient simplement fermer tous les réseaux de zombies, que des milliards d'appareils devraient être universellement sécurisés ou que les consommateurs devraient devenir des utilisateurs omniscients de la technologie.

A recent Akamai State of the Internet Security report reveals that malicious bots now account for nearly half of the internet bandwidth directed at online retailers.

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 à travers les marchés des consommateurs et des entreprises du secteur privé, les universités, la société civile et les gouvernements du monde entier doit mettre en œuvre des méthodes d'atténuation à tous les niveaux pour accroître sa sécurité. C'est ce que vise à faire ce Guide international de la sécurité des botnets et de l'IdO.

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 d'une analyse
des menaces mondiales en évolution rapide, des vulnérabilités à l'échelle 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 qui sont guidées par les puissantes forces du marché mondial et qui sont aussi agiles et adaptables que les cybermenaces à atténuer, plutôt que des mécanismes de conformité du régulateur 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 parties prenantes 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, construits sur un cadre qui prend des mesures collectives contre les mauvais acteurs et récompense les contributions des acteurs responsables.

Aperçu de l'écosystème mondial de l'internet et des communications. Comme indiqué plus haut, l'économie numérique repose sur - et a été rendue possible par - un écosystème mondial complexe de l'Internet et des 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.

La complexité et la diversité du "système de systèmes" que constitue l'écosystème de l'internet et des communications associées font qu'il est impossible de fournir un ensemble d'orientations qui s'appliquent uniformément à toutes les parties prenantes. Plusieurs rapports importants du gouvernement et du secteur privé 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. [102] 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 composants de l'écosystème de manière à faciliter l'identification et la mise en œuvre de pratiques anti-botnet parmi les groupes de parties prenantes qui le composent. Plus précisément, le guide s'articule autour des cinq types de fournisseurs, prestataires et utilisateurs suivants :

1. Infrastructure
2. Développement de logiciels
3. Dispositifs IoT
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'elle soit réelle ou perçue. 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 composantes de l'écosystème

A. INFRASTRUCTURE

Aux fins du présent 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 fourniture 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 objets 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 à ses 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 fournisseurs d'accès à large bande proposent un antivirus dans le cadre de leur offre, et nombre d'entre eux notifient 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 dorsale 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 ser vers 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 alors correspondre le nom de domaine avec une adresse IP.

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 le DNS for warding. Les fournisseurs de DNS mettent aussi régulièrement à jour leurs services 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 services proxy. Le terme CDN est utilisé pour décrire de nombreux types de services de diffusion de contenu, tels que le téléchargement 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 il la reçoit.
au 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 de rendu et les performances 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 à un serveur de cache responsable de la livraison du contenu.

Fournisseurs de cloud et d'hébergement

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 croissante 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'exécuter une grande variété de fonctions informatiques. Les réseaux en nuage étant décentralisés, ils peuvent généralement résister à la perturbation de nombreux composants de réseau. Cette caractéristique architecturale rend le cloud plus résistant aux réseaux de zombies 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. Comme le cloud se situe en amont de la cible d'une attaque par rapport aux FAI, 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 observé qu'en raison de la complexité de l'écosystème, aucun outil unique ne sera toujours efficace pour atténuer les menaces[103], 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. [104] 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 protégés contre les attaques et les vulnérabilités potentielles (c'est-à-dire les surfaces d'attaque) qui peuvent exposer 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 exploiter les flux de données et les mécanismes de partage d'informations de tiers fiables, tant au sein de leur secteur qu'entre les 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. [105]

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 vrai virus, les logiciels malveillants peuvent s'adapter et évoluer lorsqu'ils passent d'un hôte à l'autre. [106] Une limite plus évidente de l'analyse des signatures est qu'elle nécessite une connaissance préalable du logiciel malveillant, ce qui signifie que l'analyse des signatures n'est pas toujours possible.

L'efficacité de l'analyse des signatures dépend de la rapidité des mises à jour et du partage des informations dans l'ensemble de l'écosystème. Idéalement, l'analyse des 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. [107]

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 les 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 lutter contre 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. [108]

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 pour 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, la cause de ce changement de comportement n'est pas toujours évidente au premier abord. Cependant, il existe des indicateurs connus indiquant qu'un logiciel peut être malveillant, par exemple lorsqu'il tente d'obtenir des privilèges élevés ou interagit 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. [109]

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.

† 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.

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 honeypots 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.

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 est 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. En filtrant le mauvais trafic à son entrée dans le réseau du fournisseur (c'est-à-dire le filtrage à l'entrée, BCP38 et BCP84),[111] 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 d'entrée comme une meilleure pratique. [112] 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'adresses IP, y compris les entreprises. Les fournisseurs, tels que 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 protocole BCP38.

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 la meilleure façon pour les fournisseurs d'accroître la résilience. [113]

Enfin, dans un environnement réseau, les listes de contrôle d'accès 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. [114] Dans certains contextes, les listes de contrôle d'accès 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. [115]

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 problèmes que les autres.
les perturbations du trafic légitime. Par exemple, les centres d'épuration commerciaux peuvent nettoyer le trafic en
en filtrant les éléments malveillants et en envoyant le trafic légitime à sa destination. Les petits fournisseurs peuvent former des partenariats avec de 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. [116] 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 le serveur 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. Frottage

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 l'épuration est gourmande en ressources par rapport aux autres solutions, plusieurs grands fournisseurs proposent l'épuration 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 flowspec

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. [117]

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 M3A AWG a révélé que les appels téléphoniques et le courrier postal sont les moyens les plus efficaces d'entrer en contact avec les utilisateurs. [118] 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. [119] Les pairs peuvent être notifiés par 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 leur ordre - 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. Les actions répressives de ce type nécessitent des ressources importantes et des analyses médico-légales poussées. Les saisies de domaines à grande échelle peuvent également nécessiter des efforts coordonnés au niveau international. [120] 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. [121]

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

Le logiciel est un élément de plus en plus omniprésent dans tous les autres composants de l'écosystème abordé dans ce guide. Comme indiqué tout au long de ce guide, il existe une grande variété de processus de développement complexes et d'interdépendances qui stimulent l'innovation et l'amélioration des logiciels dans les principaux utilisateurs systémiques de logiciels mis en évidence dans le guide : l'infrastructure, les dispositifs IoT, les installateurs de systèmes et les entreprises. Par conséquent, cette section n'a pas pour but de présenter les différentes pratiques de sécurité de base et les capacités avancées qui sont pertinentes.
au développement de logiciels spécialisés dans chaque partie de l'écosystème. Il 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 consister en ces pratiques.

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 . [122]

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. Cependant, 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 faire appel à 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. [123]

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. [124] Cependant, un cadre développé en partenariat entre le gouvernement et les parties prenantes de l'industrie pourrait contribuer à normaliser la terminologie et les processus, renforçant ainsi la confiance du marché. Le NIST travaille actuellement en partenariat avec SAFECode et d'autres parties prenantes pour élaborer une publication spéciale sur les processus et pratiques de développement de logiciels sécurisés. La NTIA convoque un processus multipartite pour étudier comment les organisations peuvent communiquer des informations sur les composants logiciels tiers et offrir une plus grande transparence. [125]

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 IOT

Cette édition 2020 du guide bénéficie des travaux réalisés dans le cadre du Consensus C2 sur les capacités de base en matière de sécurité des dispositifs IoT[126] , un projet connexe organisé par le CSDE. Le CSDE a convoqué vingt grands organismes de normalisation, des alliances techniques et des groupes de la société civile pour tirer parti de la grande expertise de ces organisations en matière de cybersécurité. Le livre blanc du Consensus C2 sur les capacités recommandées a été publié en septembre 2019.

Dans cette mise à jour 2020 du guide, le CSDE réaffirme les pratiques du guide 2018 mais réorganise le matériel et reformule les conseils pour s'aligner sur le Consensus C2 et les autres efforts de l'industrie. Deux pratiques supplémentaires sont ajoutées au guide de 2018 sur la base des résultats du Consensus C2 (journalisation des événements et documentation de l'intention du dispositif).

Pratiques de base et capacités avancées pour les dispositifs IoT

1. UN DÉVELOPPEMENT SÛR

La sécurité doit être intégrée au processus de développement dès la planification des exigences et jusqu'à la qualification et la mise en service. [127] Cette section énumère les pratiques de développement qui sont importantes pour la sécurité des dispositifs IoT mais qui ne sont généralement pas observables en dehors de l'organisation.

a. Processus de cycle de vie du développement sécurisé

Dans le processus SDL, chaque phase de développement comporte des activités de sécurité qui peuvent être réalisées manuellement ou automatiquement. [128]

Pratiques de base : Un processus de cycle de développement sécurisé (SDL) doit être mis en place.

Bien que les éléments spécifiques d'une SDL puissent varier, les SDL devraient inclure les éléments de sécurité suivants : identification et élimination des menaces ; normes de codage ; exigences relatives aux logiciels tiers ; tests et validation des contrôles et des capacités de sécurité des logiciels ; identification et traitement des nouvelles vulnérabilités.

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 Model129) ; les documents du BSIMM sont open source et peuvent constituer une ressource pour cet effort.

b. 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 : 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 doivent être utilisés pour développer, compiler, construire et maintenir les logiciels. Il convient également d'utiliser des langages à mémoire sécurisée.

Capacités avancées : Les techniques de test telles que le fuzzing, l'exécution symbolique, le sandboxing, l'analyse statique et l'analyse dynamique doivent être utilisées pour compléter la chaîne d'outils axée sur la sécurité, afin de trouver les vulnérabilités pendant le processus de développement.

2. DES CAPACITÉS SÉCURISÉES

Cette section énumère les capacités du dispositif qui sont généralement des propriétés observables d'un dispositif après son expédition et son installation. Dans certaines architectures de système, ces propriétés importantes du dispositif peuvent se trouver non pas dans le dispositif lui-même, mais dans une passerelle ou un concentrateur qui fait partie de la structure globale. Lorsqu'un dispositif utilise une technologie câblée ou sans fil particulière, il a besoin d'un concentrateur ou d'une passerelle pour s'interfacer avec l'Internet général. Les propriétés ci-dessous peuvent parfois se trouver sur le concentrateur ou la passerelle plutôt que sur le dispositif, tout en restant pleinement efficaces car il n'y a pas d'accès au dispositif si ce n'est via le concentrateur ou la passerelle.

a. Identificateurs de dispositifs

L'identité d'un appareil joue un rôle tout au long de son cycle de vie. Les identifiants sont utilisés pour connecter les appareils à un ou plusieurs réseaux, les enregistrer, les authentifier, les autoriser, leur attribuer des listes d'accès et une politique, les contrôler et les gérer dans le cadre de l'exécution de services et d'applications. Les identifiants peuvent également aider à comprendre ce qui s'est passé après qu'un dispositif ou un réseau ait été compromis.

Pratiques de base : Le dispositif doit être associé à une valeur unique qui est distincte et qui distingue le dispositif de tous les autres dispositifs.

Capacités avancées : La sécurité de l'identifiant du dispositif doit être renforcée par des protections cryptographiques supplémentaires pour la confidentialité, l'intégrité et la disponibilité.

b. Accès sécurisé

Les produits de l'IdO 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.

Pratiques de base : Le dispositif doit être soigneusement protégé en exigeant l'authentification de l'utilisateur pour lire ou modifier le logiciel, le micrologiciel et la configuration, y compris des moyens pour garantir des identifiants uniques au dispositif pour l'accès administratif, et en protégeant l'accès aux interfaces.

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 envisagé.

c. Les données sont protégées

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 d'amorçage sécurisé, etc. ; voir également la discussion sur la cryptographie en ce qui concerne la discussion sur la sécurité liée au matériel.

Pratiques de base : La confidentialité et l'intégrité des données au repos et en transit doivent être protégées. À cette fin, les communications de données doivent être cryptées, sauf dans les cas où l'analyse des risques indique le contraire. Les données sensibles doivent être stockées sous forme cryptée.

En général, les mécanismes de sécurité disponibles dans le système utilisé, quel qu'il soit, doivent être utilisés pour protéger les données au repos et en transit.

Capacités avancées : Les versions les plus récentes des protocoles et des mécanismes de sécurité doivent être sélectionnées avec soin ; notez que la version la plus récente d'une spécification peut ne pas rendre obsolète une version antérieure. L'organisation responsable de la maintenance de la spécification pertinente (pour le protocole ou le mécanisme de sécurité) doit être utilisée pour déterminer l'applicabilité de la version.

La mémoire sécurisée peut être utilisée à la place du cryptage pour les informations stockées. Il convient d'utiliser des méthodes de clé de chiffrement conformes à la norme NIST FIPS 140-2 ou ISO/IEC 24759. [130]

d. Protocoles acceptés par l'industrie

Une bonne cr yptographie est difficile. Une cr yptographie qui a été examinée et testée par des experts a beaucoup plus de chances de réussir. Les protocoles acceptés par l'industrie sont passés par ce processus et ont intégré l'expérience des experts.

Pratiques de base : Utilisation de protocoles sécurisés et largement utilisés, à l'exclusion des versions et protocoles dépréciés et remplacés, pour les communications vers et depuis le dispositif.

Capacités avancées : La mémoire sécurisée peut être utilisée au lieu du cryptage pour les informations stockées. Il convient d'utiliser des méthodes de chiffrement conformes ou équivalentes à la norme NIST FIPS 140-2 ou ISO/IEC 24759. [131]

e. Validation des données

Les données qui peuvent être fournies par un facteur extérieur peuvent être conçues pour inclure des caractères spéciaux au-delà des caractères alphanumériques de base. Des caractères comme ".", "\", "%" et " :" peuvent avoir des conséquences inattendues pour le développeur. Les chaînes de données malveillantes font partie de nombreux exploits.

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 s'arranger pour qu'elle soit utilisée directement comme code, commande ou autre entrée du flux d'exécution. La longueur, le type de caractère et les valeurs ou plages acceptables de l'entrée doivent être validés. Les sorties d'un sous-système vers un autre ou vers un autre site doivent également être filtrées.

Capacités avancées : Toutes les données provenant de l'extérieur du dispositif qui seront traitées en interne sont validées à l'entrée et canonisées à la sortie de chaque étape du traitement interne au dispositif.

f. Enregistrement des événements

La journalisation est importante pour l'analyse médico-légale et la compréhension en temps réel des défaillances du système. Lorsque quelque chose ne va pas, il est important de comprendre quelle chaîne d'événements a conduit à la panne et quels sont les dispositifs touchés. La journalisation vers un système externe est souhaitable mais pas toujours réalisable.

Pratiques de base : Les événements de cybersécurité pertinents doivent être enregistrés (sous réserve de l'espace mémoire disponible), sécurisés et accessibles aux utilisateurs autorisés. Les événements pertinents sont propres à chaque application, mais on peut citer comme exemples les tentatives de connexion échouées ou les résultats négatifs de contrôles de cybersécurité tels que la mesure du temps de démarrage ou la vérification du hachage.

g. Cryptographie

Pratiques de base : Lorsque des méthodes cryptographiques sont utilisées pour assurer l'intégrité et la confidentialité des données, l'authentification des droits et la non-répudiation des demandes, elles doivent être choisies en fonction du risque évalué. La mise en œuvre doit utiliser des méthodes cryptographiques ouvertes, publiées, éprouvées et évaluées par des pairs, avec des sélections appropriées de paramètres, d'algorithmes et d'options.

Dans la mesure du possible, les méthodes cryptographiques doivent pouvoir être mises à jour.

Les méthodes obsolètes sont à éviter.

Il convient d'examiner comment la sécurité liée au matériel s'intègre dans les cycles de développement sécurisé des produits actuels et futurs.

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 pour un attaquant de localiser le secret. Le secret doit néanmoins être protégé par d'autres moyens tels que le contrôle d'accès et le cryptage.

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

En ce qui concerne les racines de 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.

h. Patchabilité

Cette capacité peut être assez difficile du point de vue technique et de la faisabilité. Cependant, aucun produit ne peut être considéré comme parfaitement sûr depuis sa fabrication jusqu'à la fin de sa vie utile. Jusqu'à ce que l'appareil soit pris hors ligne ou mis hors service, des mises à jour peuvent être nécessaires pour traiter les exploits nouvellement découverts. L'industrie offre
solutions : Certaines entreprises proposent des "plateformes" IoT qui incluent la mise à jour des logiciels à distance.

Pratiques de base : 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. 132

i. Reprovisionnement

La possibilité de ramener un appareil à un état "vierge" connu permet de supprimer les données sensibles d'un appareil lorsqu'il change de propriétaire, par exemple lors de la vente d'une maison pour les appareils de maison intelligente, ou lors du recyclage de toutes sortes d'appareils.

Pratiques de base : Le fabricant fournit aux utilisateurs autorisés la capacité de sécuriser les éléments suivants reconfigurer et redéployer un dispositif après sa mise sur le marché, notamment pour remettre le produit aux valeurs par défaut d'usine ou à un point de restauration autorisé, et supprimer en toute sécurité les données collectées par le dispositif (qui ne sont pas essentielles à son fonctionnement), dans un délai défini par l'organisation.

j. Signalisation de l'intention du dispositif

Pour des raisons similaires à celles de la documentation de l'intention du dispositif (voir ci-dessous), la propagation des botnets peut être considérablement réduite par des protocoles tels que le descripteur d'utilisation du fabricant (MUD). 133 Parmi les autres outils, citons OMA-DM134 et TR-69135 (ces deux dernières étant applicables dans les cas où les dispositifs peuvent être gérés directement), les exigences de sécurité, notamment les profils de sécurité de l'Open Connectivity Forum (Black, Blue et Purple), et des propositions telles que IoTSense. 136

Capacités avancées : L'appareil prend en charge le processus d'authentification de l'appareil, l'autorise avec des informations d'identification et le configure pour communiquer dans le domaine de sécurité approprié.

k. Embarquement du réseau de dispositifs

Si un appareil a accès au réseau, il doit être autorisé à cet accès. Les appareils non autorisés dans les environnements domestiques et d'entreprise créent des faiblesses dans la sécurité du réseau. Un processus d'accueil sûr et défini réduit les inconvénients de la connexion d'un appareil au réseau et lui permet de participer sous autorisation.

Capacités avancées : Le dispositif prend en charge un protocole permettant au dispositif de fournir des informations aux routeurs ou aux pare-feu en amont concernant l'utilisation prévue du réseau. De manière équivalente, le dispositif fournit des heuristiques liées à son propre comportement en fonctionnement normal en vue de l'analyse du réseau.

3. GESTION DU CYCLE DE VIE DES PRODUITS

La gestion du cycle de vie des produits (PLM) 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.

a. Traitement des vulnérabilités

Les vulnérabilités existent. Une organisation doit disposer de processus actifs pour les détecter, tels que des efforts internes, le partage des menaces et l'ouverture à la divulgation extérieure (éthique).

Pratiques de base : Les fournisseurs - fabricants et détaillants - doivent créer une politique et un processus de vulnérabilité de sécurité pour identifier, prioriser, atténuer et, le cas échéant, divulguer les vulnérabilités de sécurité connues dans leurs produits.

b. Mises à jour et divulgation d'EoL/EoS

Cette capacité doit être considérée avec soin au sein de l'organisation. Elle est liée au traitement des vulnérabilités, au cycle de vie des produits, aux conditions de service, etc.

Pratiques de base : Les fournisseurs de dispositifs doivent avoir une politique de support de sécurité définie qui inclut le traitement de toutes les vulnérabilités de sécurité en fin de vie (EoL) ou en fin de service (EoS), si des mises à jour seront disponibles et comment, et ce qu'il faut faire avec le dispositif à ce moment-là.

c. Documentation de l'intention du dispositif

L'usage réseau conçu et prévu d'un appareil (ports, protocoles, sites à visiter, niveaux de trafic de données attendus, communications avec d'autres appareils) est une information importante pour déterminer si l'appareil a été compromis, y compris dans un botnet.

Pratiques de base : Le fabricant du dispositif fournit publiquement la documentation sur l'utilisation du réseau telle qu'elle a été conçue pour le dispositif, soit dans la documentation du produit, soit par d'autres moyens pour les utilisateurs du dispositif.

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'alarme, 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
le dispositif. Une bonne installation permet d'obtenir la "meilleure sécurité disponible" à partir 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.

Les informations ci-dessous s'inspirent largement de The Connected Home Security System. [137]

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 de systèmes de gestion des mots de passe, qui constituent un stockage sécurisé des mots de passe. Ces systèmes déchargent les utilisateurs de la tâche de mémoriser et de gérer les mots de passe et de 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 contrôler les mises à jour logicielles.

b. Protocoles

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. Liaisons 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 ou WPA3 (la version la plus récente). Le WPS doit être désactivé. Il ne faut pas utiliser 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 exponentiellement croissant 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. 138 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. Les efforts déployés par la Coalition pour la cybersécurité en vue d'élaborer et de faire progresser les profils de prévention et d'atténuation des attaques DDoS et des botnets dans le cadre du Cybersecurity Framework139 sont peut-être les plus pertinents pour le présent guide, car ils visent à aider les entreprises et d'autres organisations à traiter et à atténuer les attaques 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 dans 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. [140]

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.

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 pour le service de lutte contre la menace des botnets et autres menaces automatisées et distribuées. [141]

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 des 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/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. [142] 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 très fructueux, de nombreux clients n'auront pas l'expertise technique nécessaire pour sécuriser leurs propres réseaux. Plutôt que d'ignorer 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. [143] 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. [144] 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 support de réserve/de secours capable de répondre efficacement aux incidents de cybersécurité et de maintenir un niveau de sécurité raisonnable. Les entreprises doivent choisir des fournisseurs commerciaux dont les produits et services comprennent 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 sélectionner des fournisseurs commerciaux capables de fournir une réponse automatisée ou par défaut. 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. [145]

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 début 2017, lorsque Google a commencé à exiger de tous ses employés - plus de 85 000 au total - qu'ils utilisent des clés de sécurité physiques, pas un seul compte lié au travail d'un employé n'a été hameçonné. 146

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 d'adhésion/de déplacement/de départ et la coordination des événements de changement entre des 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 24 heures pour les accès privilégiés et les accès aux ressources du cloud.

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 service d'authentification centralisé pour les applications Web et SaaS avec une signature unique qui nécessite une authentification 2FA (step-up authentication) 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) : les logiciels malveillants déposés sur les postes de travail par spear phishing à l'aide d'infos sur les réseaux sociaux et d'e-mails se comportent différemment et peuvent indiquer qu'un poste de travail et des informations d'identification privilégiées ont été compromis.

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 a pris fin. [147] A étroitement

Le problème le plus courant du point de vue de l'assistance technique est celui des logiciels piratés. Aux États-Unis, près d'un ordinateur personnel sur cinq est piraté.

des ordinateurs utilisent des logiciels piratés, alors qu'en Chine, le pourcentage d'ordinateurs personnels dotés de logiciels piratés

dépasse souvent 70 %. [148] Bien sûr, les fabricants ne corrigent normalement pas les logiciels piratés, ce qui signifie qu'ils restent

vulnérables aux exploits connus. [149] Les entreprises doivent éviter les logiciels piratés et réduire le nombre total de logiciels piratés.

les vulnérabilités de 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. [150]

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

06 / Prochaines étapes et conclusion

La publication de la version 2020 de ce guide constitue la poursuite d'une campagne stratégique sans précédent menée par l'industrie contre les botnets et autres menaces automatisées et distribuées. Le CSDE, USTelecom 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, l'économie numérique a été un moteur de la croissance commerciale et de l'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 offertes 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 souples, 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 continuer à mettre à jour, publier et 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.

Par exemple, si les efforts de cette année pour lutter contre les botnets se concentrent sur la sécurité des appareils IoT, en raison du besoin urgent d'une base de référence largement acceptée, tous les botnets importants ne ciblent pas les appareils connectés - en fait, certains des botnets les plus destructeurs au monde ne ciblent pas du tout les appareils connectés. Ainsi, s'il est clair que l'avenir des botnets est étroitement lié à celui de la sécurité de l'IdO, et que le CSDE continuera à jouer un rôle moteur sur ce front, nous explorerons également d'autres moyens de réduire considérablement les botnets et autres menaces distribuées grâce au leadership de nos membres. En reconnaissant la nature complexe et stratifiée de la menace des botnets, les entreprises du CSDE s'attaqueront à ces menaces sur plusieurs fronts.

Dans l'immédiat, nos prochaines étapes dans les mois à venir consisteront à nous engager 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) afin de 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, Centur yLink, Cisco, Ericsson, IBM, Intel, NT T, Oracle, Samsung, SAP, Telefonica et Verizon. Le CSDE est coordonné par USTelecom et la Consumer Technology Association (CTA).

À propos de USTelecom

USTelecom est la principale association commerciale représentant les fournisseurs de services et les fournisseurs de l'industrie des télécommunications. Sa base de membres diversifiée 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 la Consumer Technology Association

La Consumer Technology Association (CTA)™ est l'association professionnelle qui représente l'industrie américaine des technologies grand public, d'une valeur de 377 milliards de dollars, qui soutient plus de 15 millions d'emplois aux États-Unis. Plus de 2 200 entreprises -
80 Certains sont des petites entreprises et des start-ups, d'autres font partie des marques les plus connues au monde - bénéficient des avantages de l'adhésion au CTA, notamment la défense des politiques, les études de marché, l'éducation 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 Nat'l Inst. of Standards and Tech, NISTIR 8259 (Draft), Core Cybersecurity Feature Baseline for Securable IoT Devices : A Starting Point for IoT Device Manufacturers (juillet 2019), https://csrc.nist.gov/publications/ detail/nistir/8259/draft.

2 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.

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

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 qui se débrouillent seuls, ou par des professionnels : intégrateurs, installateurs d'alarme, etc. Dans l'idéal, 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 afin d'obtenir la "meilleure sécurité disponible" du produit fabriqué.

5 Consumer Technology Association, The Connected Home Security System, https://www.cta.tech/Membership/Member-Groups/Smart-Home-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 en augmentation exponentielle de systèmes de dispositifs IoT, les entreprises de tous types - gouvernement, secteur privé, universitaire et à but non lucratif - ont un rôle essentiel à jouer dans la sécurisation de l'écosystème numérique. Bien que les entreprises soient souvent la cible d'attaques automatisées et distribuées, elles doivent faire face à de nombreux défis.
ainsi que les tentatives d'exfiltration de données, leurs vastes systèmes peuvent également être détournés pour accroître l'impact des attaques DDoS et autres attaques distribuées sur les 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'écosystèmeLes fournisseurs et prestataires qui ont élaboré ce guide sont de grandes entreprises mondiales. 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.
La mise en place d'un système de gestion de l'information et de la communication (SGC) dans les services de l'UE permettra d'accroître l'innovation, la sophistication et la rentabilité de ces services.

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

8 Ir ving 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.

9 Paul Tentena, Artificial Intelligence to Double Digital Economy to 23 Trillion by 2025, East African Business Week (30 mai 2018), https://www. busiweek.com/artificial-intelligence-to-double-digital-economy-to-23-trillion-by-2025/.

10 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-cr yptomining-botnet-behind-ever-shifting-proxy-ser vice ("[Les réseaux axés sur les opérations de minage de cr yptocurrency ont été l'une des formes les plus actives d'infections par des logiciels malveillants en 2018").

11 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-ser vice.

12 Michael Newberg, pas moins de 48 millions de comptes Twitter 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.

13 JP Buntinx, Top 4 Largest Botnets to Date , Null T X (7 janvier 2017), https://themerkle.com/top-4-largest-botnets-to-date/.

14 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/#48d7f78e67f725230968 67f7 (citant HIS Markit IoT Trend Watch 2018, disponible sur https://ihsmarkit.com/industr y/ telecommunications.html) ; voir aussi Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016 (Feb. 7, 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.

15 Jan-Peter Kleinhans, Internet of Insecure Things : Can Security Assessment Cure Market Failures", Stiftung Neue Verantwortung (déc. 2008).
2017), https://www.stiftung-nv.de/sites/default/files/internet _of_ insecure_things.pdf.

16 Bill Connor, Ransomware-As-A-Service : The Next Great Cyber Threat ?", Forbes (17 mars 2017), https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-ser vice-the-next-great-cyber-threat/#14a38e5b4123.

17 Andy Greenberg, The White House Blames Russia for NoPetya, the 'Most Costly Cyber Attack in History', Wired (15 fév. 2018) https://www. wired.com/stor y/white-house-russia-notpetya-attribution/ ; Damien Sharkov, Russia Accused of 1.2 Billion NoPetya Cyberattack, Newsweek (15 fév. 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 (discutant de la façon dont le malware NotPetya a causé plus de 10 milliards de dollars de dommages).

18 Alex Zaharov-Reutt, Cyber Crime, Data Breaches to Cost Businesses 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.

19 Commc'n Sec., Reliability and Interoperability Council IV Working Group 4, Final Report on Cybersecurity Risk Management and Best Practices 4 (Mar. 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 ").

20 Nat'l Inst. of Standards and Tech, NISTIR 8259 (Draft), Core Cybersecurity Feature Baseline for Securable IoT Devices : A Starting Point for IoT Device Manufacturers (juillet 2019), https://csrc.nist.gov/publications/ detail/nistir/8259/draft.

21 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.").

22 Charles DeBeck, Joshua Chung et Dave McMillen, I Can't Believe Mirais : Tracking the Infamous IoT Malware, SecurityIntelligence (18 juillet 2019), https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/.

23 Charles DeBeck, Joshua Chung et Dave McMillen, I Can't Believe Mirais : Tracking the Infamous IoT Malware, SecurityIntelligence (18 juillet 2019), https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/.

24 Mark Mayne, New Mirai variant targets enterprises with 11 new exploits, SC Media (19 mars 2019), https://www.scmagazineuk.com/new-mirai-variant-targets-enterprises-11-new-exploits/article/1579535.

25 Voir SentinelOne, Mirai Botnet Descendants Will Lead to Even Bigger Internet Outages, CSO (22 déc. 2016), https://www.csoonline.com/ article/3153031/mirai-botnet-descendants-will-lead-to-even-bigger-internet-outages.html.

26 Larry Cashdollar, Latest Echobot : 26 Infection Vectors, Akamai (13 juin 2019, 11:17 AM), https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html.

27 Charles DeBeck, Joshua Chung et Dave McMillen, I Can't Believe Mirais : Tracking the Infamous IoT Malware, SecurityIntelligence (18 juillet 2019), https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/.

28 2019 Threat Report, CenturyLink 5-7, https://www.centurylink.com/ asset/business/enterprise/report/2019-threat-research-report.pdf (dernière visite le 8 octobre 2019).

29 2019 Threat Report, CenturyLink 5-7, https://www.centurylink.com/ asset/business/enterprise/report/2019-threat-research-report.pdf (dernière visite le 8 octobre 2019).

30 2019 Threat Report, CenturyLink 16, https://www.centurylink.com/ asset/business/enterprise/report/2019-threat-research-report.pdf (dernière visite le 8 octobre 2019).

31 Charles DeBeck, Joshua Chung et Dave McMillen, I Can't Believe Mirais : Tracking the Infamous IoT Malware, SecurityIntelligence (18 juillet 2019), https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/.

32 Warick Ashford, Phishing top security threat to business, Computerweekly.com (12 août 2019, 4:00 PM), https://www.computerweekly.com/news/252468231/Phishing-top-security-threat-to-business.

33 Incident Classification Patterns and Subsets, Verizon, https://enterprise. verizon.com/resources/reports/dbir/2019/incident-classification-patterns-subsets/ (dernière visite le 8 octobre 2019).

34 A New Phase of TheMoon, CenturyLink (31 janvier 2019), https://blog. centurylink.com/a-new-phase-of-themoon/.

35 Sergiu Gatlan, Mirai Botnet Variants Targeting New Processors and Architectures, BleepingComputer, (9 avril 2019, 8:40 AM), https://www. bleepingcomputer.com/news/security/mirai-botnet-variants-targeting-new-processors-and-architectures/.

36 Sean Gallagher, New variants of Mirai botnet detected, targeting more IoT devices, Ars Technica (9 avr. 2019, 1:49 PM), https://arstechnica.com/ information-technology/2019/04/new-variants-of-mirai-botnet-detected-targeting-more-iot-devices/.

37 Charles DeBeck, Joshua Chung et Dave McMillen, I Can't Believe Mirais : Tracking the Infamous IoT Malware, SecurityIntelligence (18 juillet 2019), https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/.

38 Derek Manky, The Evolving Threat Landscape - Swarmbots, Hivenets, Automation in Malware, CSO (29 août 2018, 9h00), https://www. csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots-hivenets-automation-in-malware.html.

39 Derek Manky, Rise of the 'Hivenet' : Botnets That Think for Themselves, DarkReading (16 février 2018, 10:30 AM), https://www.darkreading.com/ vulnerabilities---threats/rise-of-the-hivenet-botnets-that-think-for-themselves/ a/d-id/1331062.

40 Derek Manky, Rise of the 'Hivenet' : Botnets That Think for Themselves, DarkReading (16 février 2018, 10:30 AM), https://www.darkreading.com/ vulnerabilities---threats/rise-of-the-hivenet-botnets-that-think-for-themselves/ a/d-id/1331062.

41 Derek Manky, The Evolving Threat Landscape - Swarmbots, Hivenets, Automation in Malware, CSO (29 août 2018, 9h00), https://www. csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots-hivenets-automation-in-malware.html.

42 Derek Manky, The Evolving Threat Landscape - Swarmbots, Hivenets, Automation in Malware, CSO (29 août 2018, 9h00), https://www. csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots-hivenets-automation-in-malware.html.

43 Colin Grady, William Largent & Jaeson Schultz, Emotet is back after a summer break, Cisco Talos Intelligence Group (17 septembre 2019), https://blogs. cisco.com/security/talos/emotet-is-back-a-a-summer-break.

44 Dan Goodin, World's most destructive botnet returns with stolen passwords and email in tow, Ars Technica (19 septembre 2019, 14 h 45), https:// arstechnica.com/information-technology/2019/09/worlds-most-destructive-botnet-returns-with-stolen-passwords-and-email-in-tow/.

45 Analyzing the botnet infrastructure and threat actors behind TrickBot, NTT (28 mars 2019), https://technical.nttsecurity.com/post/102fhgo/analyzing-the-botnet-infrastructure-and-threat-actors-behind-trickbot.

46 Dan Goodin, World's most destructive botnet returns with stolen passwords and email in tow, Ars Technica (19 septembre 2019, 14 h 45), https:// arstechnica.com/information-technology/2019/09/worlds-most-destructive-botnet-returns-with-stolen-passwords-and-email-in-tow/.

47 Colin Grady, William Largent et Jaeson Schultz, Emotet is back after a summer break, Cisco Talos Intelligence Group (17 septembre 2019), https://blog. talosintelligence.com/2019/09/emotet-is-back-after-summer-break.html.

48 Colin Grady, William Largent et Jaeson Schultz, Emotet is back after a summer break, Cisco Talos Intelligence Group (17 septembre 2019), https://blog. talosintelligence.com/2019/09/emotet-is-back-after-summer-break.html.

49 Dan Goodin, World's most destructive botnet returns with stolen passwords and email in tow, Ars Technica (19 sept. 2019, 2:45 PM), https://arstechnica.com/information-technology/2019/09/worlds-most-destructive-botnet-returns-with-stolen-passwords-and-email-in-tow/.

50 Catalin Cimpanu, Emotet, today's most dangerous botnet, comes back to life, ZDNet (16 septembre 2019), https://www.zdnet.com/article/emotet-todays-most-dangerous-botnet-comes-back-to-life/.

51 Catalin Cimpanu, les botnets Necurs et Gamut représentent 97 % des cas de contamination par le virus de la grippe aviaire. les courriers électroniques indésirables d'Internet, BleepingComputer (12 mars 2018, 5:20 AM), https://www.bleepingcomputer.com/news/security/necurs-and-gamut-botnets-account-for-97-percent-of-the-internets-spam-emails/.

52 Courriel : Click with Caution, Cisco 31, https://www.cisco.com/c/dam/ fr/us/products/collateral/security/email-security/email-threat-report.pdf (dernière visite le 8 oct. 2019)

53 2019 Threat Report, Centur yLink 19, https://www.centur ylink.com/ asset/business/enterprise/report/2019-threat-research-report.pdf (dernière visite le 8 octobre 2019).

54 Chris Bing, You can Now Buy a Mirai-Powered Botnet on the Dark Web, CyberScoop (27 oct. 2016), https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web.

55 Derek Manky, The Evolving Threat Landscape - Swarmbots, Hivenets, Automation in Malware, CSO (29 août 2018, 9h00), https:// www.csoonline.com/article/ 3301148 /the-evolving-threat-landscape-swarmbots-hivenets-automation-in-malware.html.

56 Catalin Cimpanu, Liberian ISP sues rival for hiring hacker to attack its network, ZDNet (14 janvier 2019), https://www.zdnet.com/article/liberian-isp-sues-rival-for-hiring-hacker-to-attack-its-network.

57 Catalin Cimpanu, Liberian ISP sues rival for hiring hacker to attack its network, ZDNet (14 janvier 2019), https://www.zdnet.com/article/liberian-isp-sues-rival-for-hiring-hacker-to-attack-its-network.

58 Catalin Cimpanu, Liberian ISP sues rival for hiring hacker to attack its network, ZDNet (14 janvier 2019), https://www.zdnet.com/article/liberian-isp-sues-rival-for-hiring-hacker-to-attack-its-network.

59 Curtis Franklin Jr., New Botnet Shows Evolution of Tech and Criminal Culture, DarkReading (4 février 2019, 18h30), https://www.darkreading. com/attacks-breaches/new-botnet-shows-evolution-of-tech-and-criminal-culture/d/d-id/1333792.

60 Curtis Franklin Jr., New Botnet Shows Evolution of Tech and Criminal Culture, DarkReading (4 février 2019, 18h30), https://www.darkreading. com/attacks-breaches/new-botnet-shows-evolution-of-tech-and-criminal-culture/d/d-id/1333792.

61 Akamai, Retail Attacks and API Traffic, State of the Internet Security 5, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf (dernière visite le 8 octobre 2019).

62 Akamai, Retail Attacks and API Traffic, State of the Internet Security 5, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf (dernière visite le 8 octobre 2019).

63 Akamai, Retail Attacks and API Traffic, State of the Internet Security 18, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf (dernière visite le 8 octobre 2019).

64 Jay Coley, Bots try to break the internet, and other trends for 2019, TechRadar (21 février 2019), https://www.techradar.com/news/bots-try-to-break-the-internet-and-other-trends-for-2019.

65 Akamai, DDoS et attaques d'applications, État de la sécurité Internet 17, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf (dernière visite le 8 octobre 2019).

66 The Rise of "Bulletproof" Residential Networks, KrebsonSecurity (19 août 2019), https://krebsonsecurity.com/2019/08/the-rise-of-bulletproof-residential-networks.

67 Akamai, DDoS et attaques d'applications, État de la sécurité Internet 18, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf (dernière visite le 8 octobre 2019).

68 Charlie Osborne, New Mirai botnet lurks in the Tor network to stay under the radar, ZDNet (1er août 2019), https://www.zdnet.com/article/new-mirai-botnet-lurks-in-the-tor-network-to-stay-under-the-radar.

69 Tara Seals, Necurs Botnet Evolves to Hide in the Shadows, with New Payloads, Threatpost (Mar. 1, 2019, 10:41 AM), https://threatpost.com/necurs-botnet-hide-payloads/142334.

70 Casting Light On The Necurs Shadow, CenturyLink (28 février 2019), https://blog.centurylink.com/casting-light-on-the-necurs-shadow.

71 Casting Light On The Necurs Shadow, CenturyLink (28 février 2019), https://blog.centurylink.com/casting-light-on-the-necurs-shadow.

72 Voir Akamai, Retail Attacks and API Traffic, État des lieux de l'Internet. Sécurité 5, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf (dernière visite le 8 octobre 2019).

73 The Rise of "Bulletproof" Residential Networks, Krebs on Security (19 août 2019), https://krebsonsecurity.com/2019/08/the-rise-of-bulletproof-residential-networks.

74 Robin Kurzer, Oracle découvre une autre opération de fraude majeure affectant les utilisateurs d'Android et les annonceurs mobiles, Marketing Land (20 févr. 2019, 7:00 AM), https://marketingland.com/oracle-discovers-another-major-fraud-operation-affecting-android-users-and-mobile-advertisers-257322.

75 Conor Reynolds, Botnet Attacks : From DDoS to Hivenets and Sextoration, CBR (29 août 2019), https://www.cbronline.com/feature/botnet-attacks-changing-theatre.

76 Robin Kurzer, Oracle découvre une autre opération de fraude majeure affectant les utilisateurs d'Android et les annonceurs mobiles, Marketing Land (20 févr. 2019, 7:00 AM), https://marketingland.com/oracle-discovers-another-major-fraud-operation-affecting-android-users-and-mobile-advertisers-257322.

77 Jeff Stone, Des attaques DDoS à la fraude publicitaire : Smarter bots are copying human behavior, CyberScoop (10 déc. 2018), https://www.cyberscoop.com/ smart-botnet-human-behavior-ddos-ad-fraud-methbot.

78 Jeff Stone, Des attaques DDoS à la fraude publicitaire : Smarter bots are copying human behavior, CyberScoop (10 déc. 2018), https://www.cyberscoop.com/ smart-botnet-human-behavior-ddos-ad-fraud-methbot.

79 Voir Telefonica, Etisalat & Singtel, détection de botnets sur Twitter en événements sportifs, rapport sur les tendances, https://www.elevenpaths.com/wp-content/ uploads/2018/12/twitter-botnets-detection-in-sports-events. pdf (dernière visite le 8 octobre 2019).

80 Christine Fisher, Twitter interdit des milliers de comptes soutenus par l'État qui diffusent de la désinformation, Engadget (20 septembre 2019), https://www.engadget. com/2019/09/20/twitter-bans-state-backed-misinformation.

81 Ben Collins & Shoshana Wodinsky, Twitter pulls down bot network that pushed pro-Saudi talking points about disappeared journalist, NBCNews (Oct. 18, 2018, 6:39 PM), https://www.nbcnews.com/tech/tech-news/exclusive-twitter-pulls-down-bot-network-pushing-pro-saudi-talking-n921871.

82 Jessica Lyons Hardcastle, Cyber Threat Alliance Reports 459% Spike in Cryptomining Malware, SDxCentral (21 septembre 2018, 13:18 PM), https://www. sdxcentral.com/articles/news/cyber-threat-alliance-459-spike-cryptomining-malware/2018/09.

83 Catalin Cimpanu, Crypto-mining malware saw new life over the summer as Monero value tripled, ZDNet (18 sept. 2019), https://www.zdnet.com/ article/crypto-mining-malware-saw-new-life-over-the-summer-as-monero-value-tripled.

84 Michael Nadeau, Qu'est-ce que le cryptojacking ? How to prevent, detect, and recover from it, CSO (2 août 2019, 3:00 AM), https://www.csoonline.com/ article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html.

85 The Illicit Cryptocurrency Mining Threat, Cyber Threat Alliance 4, https:// www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf (dernière visite le 8 octobre 2019).

86 The Illicit Cryptocurrency Mining Threat, Cyber Threat Alliance 15, https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf (dernière visite le 8 octobre 2019).

87 Catalin Cimpanu, Two crypto-mining groups are fighting a turd war on over unsecured Linux servers, ZDNet (10 mai 2019), https://www.zdnet.com/ article/two-crypto-mining-groups-are-fighting-a-turf-war-over-unsecured-linux-servers/.

88 Lucian Constantin, Secrets of latest Smominru botnet warrant revealed in new attack, CSO (18 sept. 2019, 6:00 AM), https://www.csoonline.com/ article/3439400/secrets-of-latest-smominru-botnet-variant-revealed-in-new-attack.html.

89 Catalin Cimpanu, Deux réseaux de zombies se disputent le contrôle de milliers de personnes.
de dispositif Android non sécurisé, ZDNet (2 nov. 2018), https://www.zdnet.com/ article/two-botnets-are-fighting-over-control-of-thousands-of-unsecured-android-devices.

90 Tara Seals, Mylobot Botnet Emerges with Rare Level of Complexity, Threatpost (20 juin 2018, 13 h 12), https://threatpost.com/mylobot-botnet-emerges-with-rare-level-of-complexity/132967.

91 Catalin Cimpanu, A mysterious grey-hat is patching people's outdated MikroTik routers, ZDNet (12 oct. 2018), https://www.zdnet.com/article/a-mysterious-grey-hat-is-patching-peoples-outdated-mikrotik-routers.

92 Mark Samuels, Vigilante White-Hate Hacker Boosts IoT Device Security, SecurityIntelligence (20 avr. 2017, 1:31 PM), https://securityintelligence.com/ news/vigilante-white-hat-hacker-boosts-iot-device-security.

93 RFC 2460 Network Working Group, Internet Protocol, Version 6 (IPv6) Specification, IEFT (Dec. 1998), https://tools.ietf.org/html/rfc2460.

94 Marek Šimon et Ladislav Huraj, A Study of DDoS Reflection Attack on Internet of Things in IPv4/IPv6 Networks, SpringerLink, https://link.springer.com/chapter/10.1007/978-3-030-19807-7_12 (dernière visite le 10 octobre 2019).

95 Erik Nygren, Six ans après le lancement mondial d'IPv6 : L'entrée dans le
Majority Phases, Akamai (6 juin 2018, 12:00 PM), https://blogs.akamai. com/2018/06/six ans-depuis-le-lancement-du-monde-ipv6-entrant-dans-les-majorités.html.

96 Akamai, Retail Attacks and API Traffic, State of the Internet Security 4, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf (dernière visite le 10 octobre 2019).

97 Kelly Hill, Netscout : IoT devices under attack within minute of turn-up, RCRWrielessNews (6 août 2019), https://www.rcr wireless.com/20190806/ internet-of-things/netscout-iot-devices-under-attack-within-minutes-of-turn-up.

98 Martin Zeiser & Aleksandar Nikolich, IPv6 unmaking via UPnP, Cisco (Mar. 18, 2019), https://blog.talosintelligence.com/2019/03/ipv6-unmasking-via-upnp.html.

99 Rene Paap, IPv6 And the Growing DDoS Danger, DarkReading (2 nov. 2015, 10:30 AM), https://www.darkreading.com/attacks-breaches/ipv6-and-the-growing-ddos-danger/a/d-id/1322942.

100 Kieren McCarthy, It's begun : 'First' IPv6 denial-of-service attacks puts IT bods on notice, The Register (3 mars 2018, 9:30 AM), https://www.theregister. co.uk/2018/03/03/ipv6_ddos/.

101 Mark Mayne, "First true' nativeIPv6 DDoS attack spotted in wild", SCMedia (28 février 2018), https://www.scmagazineuk.com/first-true-native-ipv6-ddos-attack-spotted-wild/article/1473177.

102 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, NIST (22 mai 2018), disponible sur https://csrc.nist.gov/publications/detail/white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the-president/draft ; 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 (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/projects/ botnet.html.

103 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://csrc.nist.gov/publications/detail/white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the-president/draft.

104 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, y compris 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 sur 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.

105 Voir, par exemple, États-Unis, Système de partage d'indicateurs automatisé (AIS) du DHS, https://www.us-cert.gov/ais (dernière consultation le 17 octobre 2018) ; Royaume-Uni, Partenariat de partage d'informations sur la cybersécurité (CiSP), https://www.ncsc.gov. uk/section/keep-up-to-date/cisp (dernière consultation le 17 octobre 2018) ; Japon, Cyber Clean Center, https://www.telecom-isac.jp/ccc/en_index.html (dernière consultation le 17 octobre 2018) ; Nouvelle-Zélande, CORTEX, https://www.gcsb.govt.nz/our-work/ information-assurance/cortex-faqs (dernière consultation le 17 octobre 2018).

106 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.

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

108 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 (comparaison des deux différents types d'analyse heuristique) ; voir également John Aycock, Computer Viruses and Malware

74(2006) (expliquant que la seule différence entre l'heuristique statique et l'heuristique dynamique est " la façon dont les données sont recueillies " et que, sinon, les données sont identiques).

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

110 Nat'l Inst. of Standards and Tech, Advanced DDoS Mitigation Techniques (18 oct. 2017) ("Depuis bien plus d'une décennie, 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.

111 Ferguson & D. Senie, Network Ingress Filtering : Défier le déni 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.

112 Id.

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

114 Voir Cisco, Listes de contrôle d'accès (dernière mise à jour le 17 juillet 2018), https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/asdm79/firewall/ asdm-79-firewall-config/access-acls.html.

115 Voir Cisco, Policing and Shaping Overview (dernière mise à jour le 23 novembre 2017), https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/ configuration/15-mt/qos-plcshp-15-mt-book/qos-plcshp-oview.html.

116 Voir généralement, par exemple, Guy Bruneau, DNS Sinkhole, SANS.
Institute (7 août 2010), https://isc.sans.edu/forums/diar y/DNS+Sinkhole+ISO+Version+20/21153/.

117 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.

118 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/news/independent-georgia-tech-study-reveals-best-ways-to-tell-customers- "you're-botted" (dernier accès le 17 octobre 2018) ; voir également Commc'n Sector Coordinating Council, Botnet Whitepaper 24-25 (17 juillet 2017) (énumérant les multiples moyens par lesquels les fournisseurs d'infrastructures peuvent avertir les utilisateurs, notamment le courriel, l'appel téléphonique, le courrier postal, le message texte, la notification par navigateur Web, le walled garden et d'autres méthodes comme les médias sociaux), disponible à l'adresse https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

119 Voir Ctr. for Democracy and Tech, Comments to the NIST Models pour faire progresser la notification volontaire des entreprises aux consommateurs concernant l'utilisation illicite d'équipements informatiques par des botnets et des logiciels malveillants connexes (14 novembre 2011) (exprimant son inquiétude quant à la pratique consistant à " couper ou à
d'interférer autrement avec la connexion Internet d'un client " pour obliger botnet remediation), disponible à l'adresse https://www.nist.gov/sites/default/files/. documents/itl/CDT-Comments-on-BotNet-FRN-11-14-11.pdf ; Elec. Frontière
Found, Comments to the NIST Models to Advance Voluntary Corporate Notification aux consommateurs concernant l'utilisation illicite d'équipement informatique par Botnets and Related Malwares 5 (14 nov. 2011) (expliquant comment des ordinateurs non infectés peuvent être utilisés dans le cadre de la lutte contre le terrorisme).
les parties pourraient voir leur accès à Internet affecté par la quarantaine), disponible à l'adresse suivante
https://www.nist.gov/sites/default/files/documents/itl/AT-Ts-Comments-to-BotNet-FRN-11-14-11.pdf.

120 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.

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

122 Voir SAFECode, Fundamental Practices for Secure Software Development (mars 2018), https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_ Secure_Software_Development _ March_2018.pdf.

123 Arora et al, An Empirical Analysis of Software Vendors' Patching Behavior : Impact of Vulnerability Disclosure, Carnegie Mellon University (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.

124 Voir SAFECode, Principles for Software Assurance Assessment (2015), disponible sur https://safecode.org/wp-content/uploads/2015/11/SAFECode_Principles_for_Software_Assurance_Assessment.pdf.

125 Nat'l Inst. of Standards and Tech, NTIA Software Component Transparency (21 oct. 2019), https://www.ntia.doc.gov/SoftwareTransparency.

126 Council to Secure the Digital Economy, The C2 Consensus on IoT Device Security Baseline Capabilities (2019), https://securingdigitaleconomy.org/ wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

127 La planification précoce des exigences et la certification finale 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.

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

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

130 Pour plus de normes internationales, voir l'Institut national des normes et technologies (NIST), 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).

131 Id.

132 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).

133 Fabricant Utilisation Description Spécification, IETF (19 mars 2019), https://datatracker.ietf.org/doc/rfc8520/.

134 Voir l'aperçu de la gestion des dispositifs de l'OMA (20 avril 2018), http://www.
openmobilealliance.org/wp/overviews/dm_overview.html.

135 Voir CPE WAN Management Protocol, Broadband Forum (mars 2018), https://www.broadband-forum.org/download/TR-069.pdf.

136 Bruhadeshwar Bezawada et al, IoTSense : Behavioral Fingerprinting of IoT Devices, Université d'État du Colorado (avril 2018), https://arxiv.org/ pdf/1804.03852.pdf.

137 Consumer Technology Association, The Connected Home Security System, https://cta.tech/Membership/Member-Groups/TechHome-Division/ Device-Security-Checklist.aspx (dernière visite le 10 octobre 2018).

138 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.

139 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).

140 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 automatiquement les mises à jour critiques du système d'exploitation et des applications installées"). (nov. 2011), disponible à l'adresse https://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

141 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://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8192.pdf.

142 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.

143 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.elevenpaths.com/technology/anti-ddos/index.html (dernière visite le 3 novembre 2019) ; NTT, DDoS Protection Service, https://www.ntt.com/en/services/network/gin/transit/ddos.html (dernière visite le 14 mai 2018).

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

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

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

148 Voir BSA The Software Alliance, Seizing Opportunity Through License Compliance : BSA Global Software Survey 6-7 (2016), https://globalstudy.bsa. org/2016/.

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

150 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.")

Pour de plus amples informations sur le Conseil pour la sécurité de l'économie numérique (securingdigitaleconomy.org) ou des informations sur ce rapport, veuillez contacter :

Robert Mayer
Vice-président principal - Cybersécurité
USTelecom
rmayer@ustelecom.org

Mike Bergman
Vice-président - Technologie et normes
Association pour la technologie des consommateurs
mbergman@cta.tech

CSDE

Council to Secure the Digital Economy

securingdigit aleconomy.org