Présentation de solution

Sécuriser les équipements IoT pour une protection optimale contre les attaques

L'attaque par déni de service distribué (DDoS) lancée contre l'infrastructure de services DNS de la société Dyn en octobre 2016 a été analysée en détail dans le *Rapport sur le paysage des menaces – Avril 2017* de McAfee Labs.

Les pirates ayant utilisé le protocole DNS pour lancer leur attaque, il était extrêmement difficile pour les solutions de sécurité de distinguer le trafic légitime des paquets malveillants. Pour ne rien arranger, le trafic légitime et celui de l'attaque provenaient de millions d'adresses IP disséminées partout dans le monde.

En plein essor, ce type d'attaque DDoS est favorisé par une sécurisation inadaptée de l'infrastructure de l'Internet des objets (IoT). Le logiciel malveillant Mirai utilisé au cours de l'attaque contre Dyn exploitait un large éventail d'équipements IoT mal sécurisés, notamment des enregistreurs numériques, des imprimantes, des caméras de surveillance, des réfrigérateurs, des thermostats, etc. Une fois l'équipement IoT infecté, le logiciel malveillant propageait l'infection à d'autres pour former un réseau de robots (botnet) et utiliser leurs ressources de traitement combinées pour exécuter l'attaque DDoS.

D'après l'équipe de sécurité de Dyn, des dizaines de millions d'équipements IoT malveillants faisaient partie du botnet Mirai au pic de l'attaque.

Il n'est guère facile de savoir si un équipement réseau a été infecté ni d'identifier le stade de l'infection — déclenchement du code, propagation latérale, communication avec le serveur de contrôle ou recrutement de robots pour le lancement d'attaques DDoS. Il est toutefois intéressant de respecter certaines recommandations pour sécuriser vos équipements IoT et protéger votre réseau approuvé.

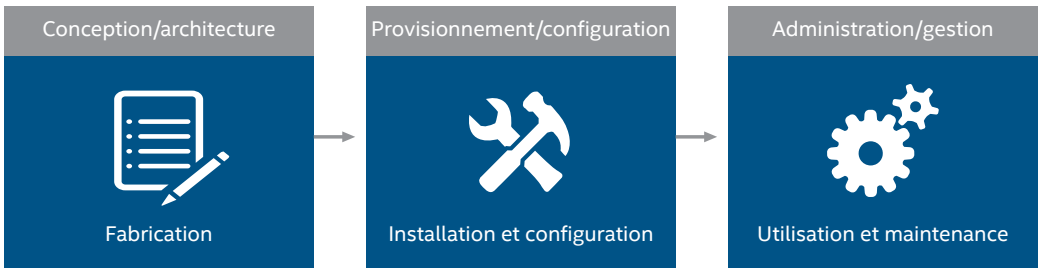
Comment sécuriser les équipements IoT

Pour prendre le contrôle des équipements IoT, les pirates choisissent généralement la solution de facilité, c'est-à-dire des identifiants faibles. Cela dit, ils peuvent aussi s'adapter et craquer des mots de passe forts ou contourner d'autres contrôles de sécurité. C'est la tendance souvent observée pour de nombreux vecteurs d'attaque.

Intel Security recommande de bloquer les exploits connus ainsi que les stratagèmes probablement utilisés par les pirates dans un avenir proche. Suivez les trois recommandations ci-dessous pour protéger les équipements IoT, de la fabrication à la mise au rebut :

intel Security

Sécurisation des équipements IoT



Les fonctions et contrôles de sécurité doivent être intégrés aux produits dès le départ.

L'installation et la configuration doivent respecter les meilleures pratiques.

Une supervision et une maintenance responsables permettent de bénéficier d'équipements sécurisés et à jour.

1. **Concevez les équipements IoT en intégrant dès le départ la sécurité.** Les fabricants d'équipements IoT doivent intégrer la sécurité à l'architecture, aux interfaces et à la conception de leurs produits. Développez des concepts et des fonctions de sécurité élémentaires, par exemple la séparation des données et du code, la communication entre parties approuvées, la protection des données au repos et en cours d'utilisation et l'authentification des utilisateurs. À l'avenir, les produits seront plus puissants, stockeront de plus grands volumes de données et proposeront davantage de fonctionnalités. Il faut que les produits puissent recevoir des mises à jour de sécurité, intégrer des fonctions de verrouillage, de validation de version et d'approbation de logiciels, en plus de posséder des configurations par défaut conformes aux meilleures pratiques du secteur. Tout commence par le fabricant : la durabilité du produit doit être intégrée à sa conception. Le matériel, les micrologiciels, les systèmes d'exploitation et les logiciels doivent être conçus pour résister à un environnement hostile. Lorsqu'ils envisagent l'achat d'un équipement IoT, les acheteurs doivent se poser la question suivante : « Le fabricant a-t-il conçu et construit l'équipement IoT en pensant à la sécurité ?
2. **Optez pour une configuration et un provisionnement sécurisés.** La plupart des équipements IoT doivent être configurés et provisionnés lors de l'installation. L'identification et l'authentification des équipements jouent un rôle essentiel dans ce processus en deux étapes. Il est important que les configurations par défaut respectent les meilleures pratiques de sécurité et soient faciles à comprendre pour les utilisateurs. Il faut prévoir des règles qui interdisent les mots de passe par défaut, exigent la signature des correctifs et des mises à jour, le chiffrement des données et la sécurisation des connexions Internet. Pour les entreprises, la limitation de l'accès réseau, l'application rapide des correctifs et une exécution d'applications limitée aux logiciels autorisés contribuent grandement à la sécurité des équipements IoT. Pour les équipements capables de les prendre en charge, l'implémentation de logiciels de sécurité, par exemple la protection antimalware, les systèmes de prévention des intrusions et même les pare-feux locaux, renforce la protection des équipements. Il est également utile de configurer des outils de détection et de télémétrie pour détecter les attaques contre les systèmes ou une utilisation non prévue par l'entreprise. Il faut mettre en œuvre des stratégies de confidentialité, de rétention des données, d'accès distant, de sécurité et de mise hors service.
3. **Mettez en place des procédures d'administration et de gestion adéquates.** Lorsque les équipements appartiennent à des particuliers, ceux-ci doivent avoir le contrôle ultime de leur gestion. Les fabricants et les fournisseurs de services en ligne jouent un rôle dans l'activation, mais ce sont les propriétaires qui doivent garder le contrôle de l'équipement et de ce qu'il peut faire. Le provisionnement est différent de l'administration. Ainsi, au cours de l'installation de caméras de surveillance, il est logique de se connecter au site du fabricant pour obtenir les derniers correctifs ou encore configurer le stockage dans le cloud. Mais les clients ne souhaitent pas que ces systèmes de surveillance soient contrôlés par les fabricants. Ces derniers ne doivent pas être en mesure de faire fonctionner l'équipement sans l'autorisation de l'acheteur. Les propriétaires doivent être seuls autorisés à mettre l'appareil sous tension et hors tension et à sélectionner les services en ligne auxquels ils veulent se connecter. Pour cela, il faut mettre en œuvre des méthodes d'identification et d'authentification utilisateur appropriées.

Les mots de passe par défaut courants devraient être interdits car n'importe qui pourrait prendre le contrôle de l'équipement en tant qu'administrateur. Imaginez si Windows était fourni avec un mot de passe de connexion par défaut sur chaque système. La sécurité tournerait rapidement au cauchemar car de nombreux utilisateurs ne le modifieraient jamais et les pirates pourraient se connecter très aisément. Les systèmes IoT doivent avant tout être capables d'authentifier leur propriétaire. Les fonctions de gestion doivent par ailleurs être étendues afin d'autoriser les propriétaires à définir des limites, des politiques relatives aux données et des paramètres de confidentialité plus restrictifs que ceux de n'importe quel éditeur tiers potentiel. Des mises à jour de sécurité signées doivent être automatiquement installées dès leur publication. Les propriétaires avertis doivent être en mesure de configurer des limites pour les connexions entrantes et sortantes, les types de données, les ports et les paramètres de sécurité. L'équipement doit inclure des outils de journalisation des erreurs et des activités inattendues ou inhabituelles, qui peuvent transmettre les journaux à un système approuvé ou permettre de les consulter localement. Par ailleurs, un système de notification d'alarmes à distance, via e-mail ou SMS, est une fonctionnalité très utile sur certains équipements. Enfin, une fonction de réinitialisation est indispensable dans le cas d'une compromission irrécupérable ou d'un transfert de propriété.

Stratégies et procédures à mettre en place pour sécuriser les équipements IoT

- **Renseignez-vous sur le niveau de sécurité de l'équipement IoT.** Avant d'acheter un équipement IoT, vérifiez si ce dernier, ou la société qui le fabrique, a rencontré des problèmes. Une recherche rapide sur Internet peut suffire. Une recherche sur le site web de la FTC (Federal Trade Commission) révèlera toutes les sanctions ou actions en justice préalables. Dans le cadre de ces recherches, vous découvrirez peut-être que certaines entreprises ignorent les problèmes de sécurité de leurs produits, alors que d'autres adoptent une démarche plus proactive.
- **Maintenez à jour tous les logiciels de vos équipements IoT.** Cette pratique très simple permet souvent d'éliminer les vulnérabilités, surtout celles découvertes récemment et portées à l'attention du public. Mettez en place une procédure de déploiement des patchs et correctifs, et vérifiez si ceux-ci ont été correctement appliqués.
- **Pour les équipements IoT plus anciens auxquels il n'est pas possible d'appliquer des correctifs, limitez le risque** en implémentant une technologie de listes blanches, qui verrouille les systèmes et empêche l'exécution de programmes non autorisés.
- **Isolez les équipements IoT du reste du réseau** à l'aide d'un pare-feu ou d'un système de prévention des intrusions. Désactivez les ports et les services superflus sur ces systèmes pour limiter les points d'entrée possibles d'une infection. Mirai exploite les ports non utilisés.
- **Remplacez les mots de passe par défaut par des mots de passe forts.** Les mots de passe faibles et par défaut représentent la principale menace posée aux équipements IoT. Prenez de bonnes habitudes en la matière, par exemple en choisissant des mots de passe longs et en mélangeant caractères spéciaux, majuscules, minuscules et chiffres. Optez toujours pour des mots de passe forts, difficiles à deviner.
- **Tirez parti des options de sécurité des équipements IoT.** Certains équipements proposent des configurations avancées : pensez à en profiter. D'autres peuvent offrir une option de mise en réseau isolée, similaire à un réseau Wi-Fi invité fonctionnant en parallèle à votre réseau principal. Ce n'est qu'un exemple, d'autres fonctionnalités sont possibles selon les produits.
- **Connectez les équipements IoT à l'aide d'un Wi-Fi sécurisé.** Créez des mots de passe forts et utilisez les protocoles de sécurité les plus récents, p. ex. WPA2.
- **Limitez l'accès physique aux équipements IoT.** La manipulation directe des équipements peut également conduire à leur piratage.
- **Désactivez la fonction Universal Plug and Play (UPnP).** De nombreux équipements IoT prennent en charge UPnP, ce qui les rend visibles sur Internet et les exposent à des infections par des logiciels malveillants. Si possible, désactivez cette fonction.
- **De temps à autre, débranchez l'équipement IoT puis redémarrez-le.** Les logiciels malveillants sont généralement stockés dans une mémoire volatile et peuvent être éliminés en arrêtant, puis en redémarrant l'équipement.

Comment les produits Intel Security peuvent protéger les systèmes et réseaux contre les attaques exploitant les équipements IoT

En plus de respecter les meilleures pratiques susmentionnées pour vos équipements IoT, vous pouvez faire appel aux produits Intel Security pour limiter les risques d'infection des équipements par des logiciels malveillants et bloquer les activités des botnets. Les configurations des produits Intel Security proposées ci-dessous permettent de sécuriser les équipements IoT et de protéger les systèmes et réseaux contre les attaques lancées à l'aide de ces équipements.

McAfee VirusScan® Enterprise 8.8 ou McAfee Endpoint Security 10

- Maintenez les fichiers DAT à jour.
- Assurez-vous que McAfee Global Threat Intelligence (McAfee GTI) est activé, car ce système reconnaît plus de 600 millions de signatures de logiciels malveillants uniques.
- Développez des règles de protection de l'accès pour bloquer l'installation et les charges actives des logiciels malveillants.
  - Reportez-vous aux articles de la base de connaissances consacrés aux règles de protection de l'accès : KB81095 et KB54812.
  - Reportez-vous aux meilleures pratiques de configuration de McAfee VirusScan Enterprise 8.8 : PD22940.
  - Reportez-vous aux meilleures pratiques de configuration de McAfee Endpoint Security : KB86704.

McAfee Host Intrusion Prevention

- La solution McAfee Host Intrusion Prevention peut empêcher la propagation des logiciels malveillants. Par l'utilisation de signatures IPS personnalisées, vous pouvez créer des règles empêchant les opérations sur fichiers (création, écriture, exécution, lecture, etc.) générées par les logiciels malveillants.
- Activez la signature 3894 de McAfee Host Intrusion Prevention : Access Protection—Prevent svchost.exe executing non-Windows executables (Protection à l'accès - Empêcher le lancement de fichiers exécutables non-Windows par svchost).
- Activez les signatures 6010 et 6011 de McAfee Host Intrusion Prevention pour bloquer immédiatement les injections.
- Pour ce faire, il existe deux types de sous-règles :
  1. Créez une signature IPS personnalisée à l'aide du moteur Files et d'une sous-règle répondant aux critères suivants :
     - Name: <insérer le nom>
     - Rule type: Files
     - Operations: Create, Execute, Read, Write
     - Parameters: Include - Files - <chemin d'accès/nom de fichier du logiciel malveillant>
       - Le nom de fichier doit inclure un chemin d'accès. Pour remplacer le chemin d'accès par un caractère générique, insérez « **\ » avant le nom du fichier, et pour remplacer la lettre du lecteur, insérez « ?:\ » (par exemple « **\nom_de_fichier.exe » ou « ?:\nom_de_fichier.exe »).
       - Le paramètre « Files » ne prend pas en charge les hachages MD5 ; uniquement le format chemin d'accès/nom de fichier.
       - Vous pouvez également indiquer le type de lecteur si vous souhaitez limiter le chemin d'accès à un lecteur spécifique (par exemple disque dur, CD, USB, réseau, disquette).
     - Executables: Ce critère peut rester vide, sauf si vous souhaitez limiter la signature à des processus spécifiques qui exécutent l'opération sur fichier (par exemple explorer.exe, cmd.exe, etc.).

2. Créez une signature IPS personnalisée à l'aide du moteur Program et d'une sous-règle répondant aux critères suivants :
   - Name: <insérer le nom>
   - Rule type: Program
   - Operations: Run target executable
   - Parameters: <laisser vide>
   - Executables: Ce critère peut rester vide, sauf si vous souhaitez limiter la signature à un processus spécifique comme l'exécutable source (par exemple pour empêcher explorer.exe d'exécuter un fichier Target Executable tel que notepad.exe).
   - Target Executables: Définissez les propriétés du fichier exécutable dont vous souhaitez empêcher l'exécution (par exemple si vous souhaitez bloquer l'exécution de notepad.exe, indiquez le chemin d'accès/nom du fichier exécutable). Vous pouvez définir l'exécutable à l'aide d'un ou de plusieurs critères (description du fichier, nom du fichier, empreinte, signataire).

McAfee SiteAdvisor® Enterprise ou McAfee Web Protection

- Utilisez les informations sur la réputation des sites web pour signaler aux utilisateurs les sites distribuant des logiciels malveillants.

McAfee Threat Intelligence Exchange et McAfee Advanced Threat Defense

- Configuration des stratégies McAfee Threat Intelligence Exchange :
  - Commencez en mode d'observation. Lorsque des processus suspects sont identifiés sur des terminaux, utilisez des marqueurs système pour appliquer les stratégies de mise en œuvre de McAfee Threat Intelligence Exchange.
  - Nettoyez au niveau « Known malicious » (Malveillant connu).
  - Bloquez au niveau « Most-likely malicious » (Très probablement malveillant). (Un blocage au niveau « Unknown » (Inconnu) offrirait une meilleure protection mais peut également alourdir la charge administrative initiale.)
  - Configurez l'option « Submit files to McAfee Advanced Threat Defense » (Envoyer les fichiers à McAfee Advanced Threat Defense) aux niveaux « Unknown » (Inconnu) et inférieurs.
  - Stratégie McAfee Threat Intelligence Exchange Server : Acceptez les réputations McAfee Advanced Threat Defense pour les fichiers qui n'ont jamais été rencontrés par McAfee Threat Intelligence Exchange.
- Intervention manuelle dans McAfee Threat Intelligence Exchange :
  - Appliquez les règles en matière de réputation des fichiers (selon le mode de fonctionnement). « Most likely malicious » (Très probablement malveillant) : choisissez de nettoyer/supprimer.
  - « Might be malicious » (Potentiellement malveillant) : bloquer.
- La réputation d'entreprise (organisationnelle) peut outrepasser McAfee GTI :
  - Vous pouvez choisir de bloquer un processus indésirable, par exemple une application non prise en charge ou vulnérable.
  - Marquez le fichier comme « Might be malicious » (Potentiellement malveillant).
- Vous pouvez également choisir d'autoriser un processus indésirable à des fins de test.
  - Marquez le fichier comme « Might be trusted » (Potentiellement approuvé).

McAfee Advanced Threat Defense

- Fonctionnalités de détection :
  - Détection basée sur les signatures : McAfee GTI contient plus de 600 millions d'échantillons.
  - Détection basée sur la réputation : McAfee GTI.
  - Émulation et analyse statique en temps réel : Utilisées pour la détection sans signatures.
  - Règles YARA personnalisées.
  - Analyse statique complète du code : Reconstitue la logique du code pour évaluer les attributs et les jeux d'instructions, et effectuer un examen approfondi du code source sans l'exécuter.
  - Analyse dynamique dans un environnement restreint de type sandbox.

- Créez des profils d'analyse sur les systèmes et programmes susceptibles d'être ciblés par les logiciels malveillants :
  - Systèmes d'exploitation courants, Windows 7, Windows 8, Windows 10
  - Applications Windows installées (Word, Excel) avec macros activées
- Autorisez les profils d'analyse à accéder à Internet :
  - De nombreux échantillons exécutent un script à partir d'un document Microsoft, qui établit une connexion sortante et active le logiciel malveillant. Autoriser les profils d'analyse à accéder à Internet permet d'améliorer les taux de détection.

McAfee Network Security Platform

- Les stratégies par défaut de McAfee Network Security Platform contiennent des signatures permettant d'identifier le réseau Tor, qui peut être utilisé pour transférer des fichiers associés aux logiciels malveillants.
- Intégration avec McAfee Advanced Threat Defense pour les nouvelles variantes des attaques :
  - Configurez l'intégration avec McAfee Advanced Threat Defense dans la stratégie pour les logiciels malveillants avancés.
  - Configurez McAfee Network Security Platform pour envoyer les fichiers .exe, Microsoft Office, Java Archive et PDF à McAfee Advanced Threat Protection pour inspection.
  - Vérifiez que la configuration de McAfee Advanced Threat Protection est appliquée au niveau des capteurs.
- Mettez à jour les règles de détection des rappels (pour contrer les botnets).

McAfee Web Gateway

- Activez l'inspection McAfee Gateway Anti-Malware.
- Activez McAfee GTI pour tirer parti du service de réputation des fichiers et des URL.
- Intégrez la solution avec McAfee Advanced Threat Defense pour bénéficier de fonctions sandbox et de détection des menaces de type « jour zéro ».

VirusTotal Convicter : intervention automatisée

- Convicter est un script Python déclenché par le système de réponse automatisée de McAfee ePolicy Orchestrator® (McAfee ePO) pour référencer un fichier générant un événement de menace McAfee Threat Intelligence Exchange avec VirusTotal.
- Notez que vous pouvez modifier le script pour recouper les événements avec d'autres modules McAfee Threat Intelligence Exchange, tels que GetSusp.
- Si le seuil de confiance dans la communauté est atteint, le script définit automatiquement la réputation de l'entreprise. Seuil d'identification positive suggéré : 30 % des éditeurs, dont deux éditeurs majeurs, doivent confirmer.
- Filtre : « Target File Name Does Not Contain (Le nom du fichier cible ne contient pas) : McAfeeTestSample.exe ».
- GetSusp est un outil gratuit dont le support est assuré par la communauté. (Le support n'est pas pris en charge par Intel Security.)

McAfee Endpoint Threat Defense and Response

- McAfee Endpoint Threat Defense and Response détecte et neutralise les menaces avancées. Lorsqu'il est utilisé en association avec des flux d'informations sur les menaces tels que McAfee GTI, Dell SecureWorks ou ThreatConnect, les nouvelles menaces peuvent être recherchées et éliminées avant qu'elles n'aient l'occasion de se propager.
- Les collecteurs personnalisés vous permettent de créer des outils spécifiques afin de rechercher et d'identifier les indicateurs de compromission associés aux logiciels malveillants.
- L'utilisateur intègre des déclencheurs et des réactions pour définir les actions exécutées lorsque des conditions spécifiques sont remplies. Par exemple, lorsque des hachages ou des noms de fichiers sont détectés, une action de suppression peut être automatiquement exécutée.

Autres lectures conseillées

Livre blanc : *More Confidence, Safety, and Security in the Digital World (Plus de confiance et de sécurité dans le monde numérique)*

Best Practices for how to use Host IPS rules for a malware outbreak (Meilleures pratiques pour utiliser les règles McAfee Host Intrusion Prevention en cas d'attaque par logiciel malveillant) : KB84507

SIEM Orchestration. How McAfee Enterprise Security Manager can drive action, automate remediation, and increase situational awareness (Comment McAfee Enterprise Security Manager peut effectuer des actions, automatiser les mesures de correction et améliorer la connaissance situationnelle) : PD24830

Livre blanc : *La sécurité au-delà des signatures*

FAQs for Network Security Platform. Advanced Malware Detection (Questions fréquentes sur McAfee Network Security Platform – Détection des logiciels malveillants avancés) : KB75269

Guide produit McAfee Web Gateway. Filtrage de contenu web : PD26339

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com