

Les aspirateurs robots Ecovacs piratés

Des pirates informatiques inconnus exploitent les vulnérabilités récemment découvertes dans les aspirateurs robots Ecovacs pour espionner leurs propriétaires et leur causer des ennuis.

Kaspersky Team

9 Jan 2025



Imaginez : vous vous levez la nuit pour aller boire un verre d'eau, vous marchez dans un couloir non éclairé, quand, dans l'obscurité, une voix commence à vous crier dessus. Ce n'est pas agréable, vous en conviendrez. C'est pourtant la nouvelle réalité pour les propriétaires d'aspirateurs robots vulnérables, qui peuvent être contrôlés par des pirates informatiques pour être transformés de domestiques en malotrus. Et ce n'est pas tout : les pirates informatiques peuvent également contrôler le robot à distance et accéder à sa caméra en direct.

Le danger est bien présent : on a récemment vu des cas de cyberviolence détournant des aspirateurs robots vulnérables pour faire des farces aux gens (et pire). Lisez la suite pour en savoir plus.

Comment fonctionne un robot aspirateur

Commençons par le fait qu'un aspirateur robot moderne est un véritable ordinateur sur roues, fonctionnant la plupart du temps sous Linux. Il est équipé d'un puissant processeur ARM multicœur, d'une bonne partie de la mémoire vive, d'un disque flash de grande capacité, du Wi-Fi et du Bluetooth.

Hardware

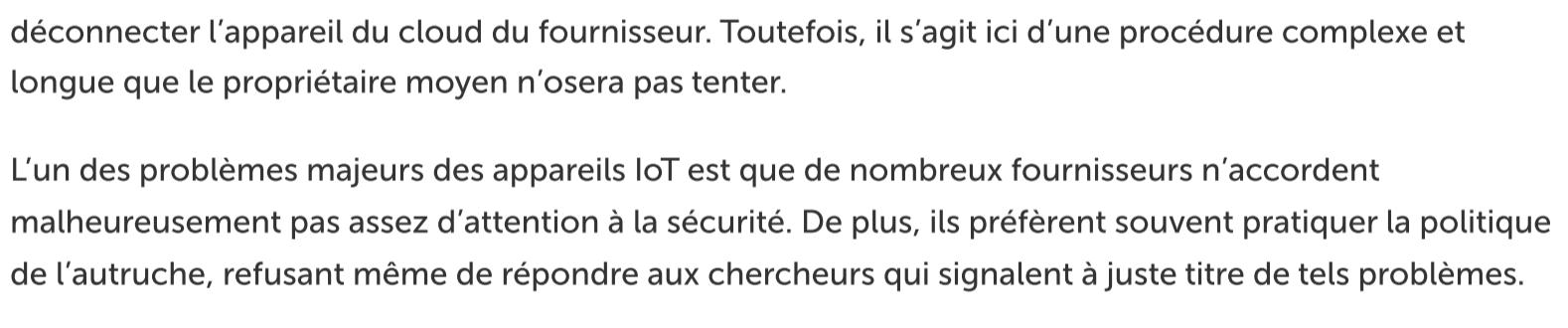


L'aspirateur robot d'aujourd'hui est un véritable ordinateur sur roues [Source](#)

Bien entendu, l'aspirateur robot moderne est équipé de capteurs partout : infrarouge, lidar, mouvement, caméra (il y en a bien souvent plusieurs), et certains modèles sont également dotés de microphones pour la commande vocale.

Hardware: Deebot X1

- Sensors
 - Lidar
 - Microphone array
 - Camera+Line Lasers
 - Lots of IR distance sensors



L'Ecovacs DEEBOT X1 n'a pas seulement une caméra, mais toute une gamme de microphones [Source](#)

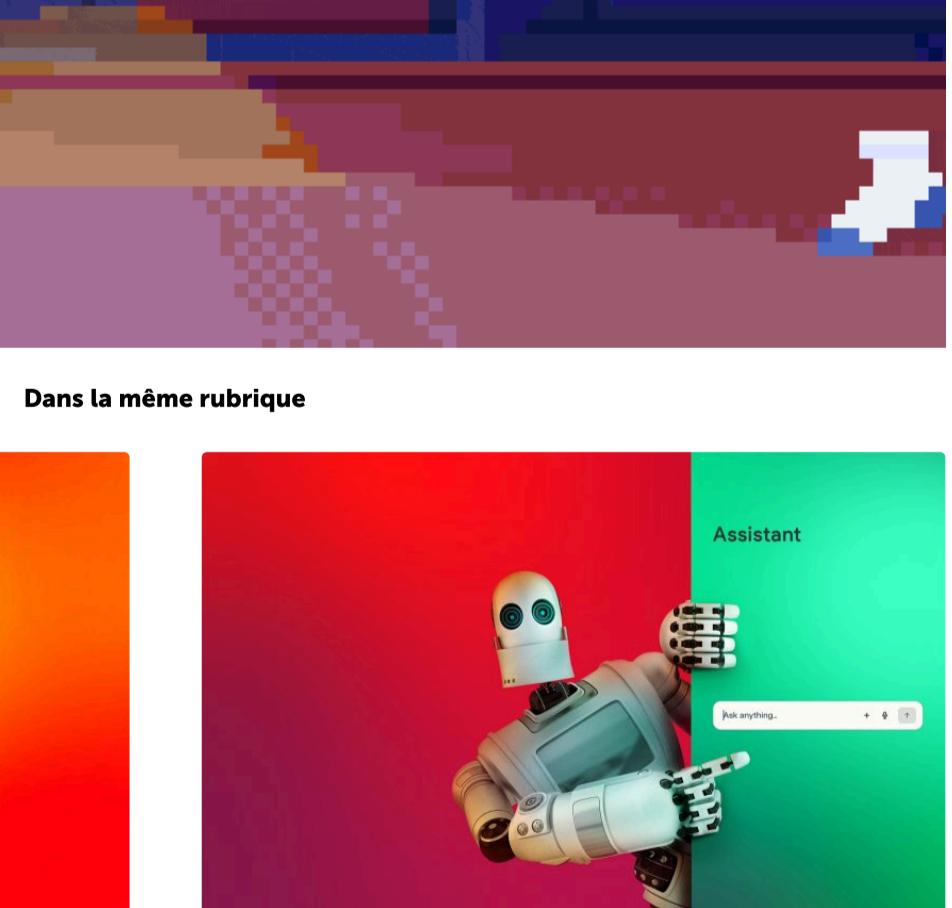
Bien entendu, tous les aspirateurs robots modernes sont en permanence connectés à l'infrastructure cloud du fournisseur. Dans la plupart des cas, ils communiquent étroitement avec ce cloud, en envoyant de nombreuses données collectées pendant leur fonctionnement.

Vulnérabilité des aspirateurs et tondeuses robots Ecovacs

Le premier rapport portant sur les vulnérabilités des aspirateurs et tondeuses robots Ecovacs est apparu en août 2024, lorsque les chercheurs en sécurité Dennis Giese (connu pour avoir [piraté un aspirateur robot Xiaomi](#)) et Braelynn Luedtke ont donné une conférence à la DEF CON 32 sur la rétro-ingénierie et le piratage des robots Ecovacs.

Goat G1 Lawnmowing Robot

- Released
 - 2023 in EU, AU
 - 2024 in US (G1-GX)
- Navigation
 - GPS
 - Visual, ToF
 - UWB Beacons
- Features:
 - Optional LTE
 - Remote view/Patrol



L'Ecovacs GOAT G1 peut également être équipé d'un GPS, d'un système LTE et d'un module Bluetooth à longue portée [Source](#)

Dans leur exposé, Dennis Giese et Braelynn Luedtke ont décrit plusieurs méthodes de piratage des aspirateurs robots Ecovacs et de l'application mobile que les propriétaires utilisent pour contrôler ces appareils. Ils ont notamment constaté qu'un pirate informatique potentiel pouvait accéder au flux à partir de la caméra et du microphone intégrés du robot.

Il y a deux raisons à cela. Tout d'abord, si l'application est utilisée sur un réseau non sécurisé, des pirates informatiques risquent d'intercepter le jeton d'authentification et de communiquer avec le robot.

Ensuite, bien qu'en théorie le code PIN défini par le propriétaire de l'appareil sécurise le flux vidéo, dans la pratique, il est authentifié côté application, si bien qu'il peut être contourné.

Live video ap(p)oocalypse

Le code PIN permettant de sécuriser le flux vidéo d'un aspirateur robot Ecovacs est authentifié côté application, ce qui rend le mécanisme extrêmement vulnérable [Source](#)

Les chercheurs sont également parvenus à obtenir un accès root au système d'exploitation du robot. Ils ont découvert qu'il était possible d'envoyer une charge utile malveillante au robot via Bluetooth, qui, sur certains modèles Ecovacs, se déclenche après un redémarrage programmé, tandis que sur d'autres, elle reste activée en permanence. En théorie, le chiffrement devrait permettre de s'en prémunir, mais Ecovacs utilise une clé statique qui est la même pour tous les appareils.

En disposant de ces informations, un intrus peut obtenir les priviléges root dans le système d'exploitation de n'importe quel robot Ecovacs vulnérable et le pirater à une distance allant jusqu'à 50 mètres. C'est précisément ce qu'ont fait les chercheurs. Quant aux tondeuses robots, elles peuvent être piratées à plus de 100 mètres de distance, car elles disposent de systèmes Bluetooth plus puissants.

Si l'on ajoute à cela le fait que les aspirateurs robots d'aujourd'hui sont de véritables ordinateurs fonctionnant sous Linux, on comprend comment des pirates informatiques peuvent se servir d'un robot infecté pour pirater d'autres à proximité. En théorie, les pirates pourraient même créer un ver de réseau pour infecter automatiquement des robots n'importe où dans le monde.

Robot worm scenario

La vulnérabilité Bluetooth des robots Ecovacs pourrait entraîner une chaîne d'infection [Source](#)

Dennis Giese et Braelynn Luedtke ont informé Ecovacs des vulnérabilités trouvées, mais n'ont reçu aucune réponse. Selon les chercheurs, l'entreprise a bien tenté de combler certaines failles, mais sans grand succès et en ignorant les vulnérabilités les plus critiques.

Comment les aspirateurs robots Ecovacs ont été piratés pour de vrai

Il semble que la conférence DEF CON ait suscité un grand intérêt dans la communauté des pirates informatiques, à tel point que quelqu'un semble avoir poussé l'attaque un peu plus loin et l'avoir déployée sur les aspirateurs robots Ecovacs dans le monde réel. Selon des informations récentes, des

Cookibot

by Unicenter

appareils connectés DEF COM DEF CON Internet des objets IoT menaces piratage robots

sécurité Vulnérabilités

Conseils

Vulnérabilité Pixnapping : captures d'écran impossibles à bloquer sur votre téléphone Android

Le passeur des codes à usages uniques Android détecte partout des chevauchements. Elles permettent d'écarter les applications sans autorisation spéciale du système d'exploitation. En quoi consiste cette vulnérabilité et que pouvez-vous faire pour vous protéger ?

Enfin, n'oubliez pas qu'un robot connecté au même réseau peut s'en servir, servir de relais, téléviseurs intelligents, etc. Il est donc toujours judicieux de migrer les appareils IoT (en particulier les aspirateurs robots) vers un réseau privé et d'installer une protection fiable sur l'ensemble des appareils, dans la mesure du possible.

Protection avancée pour les utilisateurs avancés

Une grande partie de votre vie étant en ligne, il est important de la sécuriser.

kaspersky

appareils connectés DEF COM DEF CON Internet des objets IoT menaces piratage robots

sécurité Vulnérabilités

Conseils

Comment se prémunir contre le piratage des aspirateurs robots ?

En un mot : vous ne pouvez pas. Malheureusement, il n'existe pas de méthode universelle de protection contre le piratage des aspirateurs robots. Malheureusement, il n'existe pas de méthode universelle de protection contre les vulnérabilités des aspirateurs robots.

En revanche, il existe quelques méthodes pour empêcher les pirates informatiques de pirater vos robots. Pour commencer, il est recommandé de déconnecter l'appareil du cloud du fournisseur. Toutefois, il s'agit ici d'une procédure complexe et longue que le propriétaire moyen n'osera pas tenter.

L'un des problèmes majeurs des appareils IoT est que de nombreux fabricants n'accordent malheureusement pas assez d'attention à la sécurité. De plus, ils préfèrent souvent pratiquer la politique de l'autruche, refusant même de répondre aux chercheurs qui signalent à juste titre de tels problèmes.

Pour limiter les risques, essayez de mener vos propres recherches sur les pratiques de sécurité du fournisseur en question avant tout. Si certains d'entre eux réussissent à protéger leurs produits, et bien, installez toujours les mises à jour du micrologiciel : les nouvelles versions suscitent généralement au moins quelques-unes des vulnérabilités que les pirates informatiques sont susceptibles d'exploiter pour pirater n'importe quel robot.

Enfin, n'oubliez pas qu'un robot connecté au même réseau peut s'en servir, servir de relais, téléviseurs intelligents, etc. Il est donc toujours judicieux de migrer les appareils IoT (en particulier les aspirateurs robots) vers un réseau privé et d'installer une protection fiable sur l'ensemble des appareils, dans la mesure du possible.

Protection avancée pour les utilisateurs avancés

Une grande partie de votre vie étant en ligne, il est important de la sécuriser.

kaspersky

appareils connectés DEF COM DEF CON Internet des objets IoT menaces piratage robots

sécurité Vulnérabilités

Conseils

Vulnérabilité Pixnapping : captures d'écran impossibles à bloquer sur votre téléphone Android

Le passeur des codes à usages uniques Android détecte partout des chevauchements. Elles permettent d'écarter les applications sans autorisation spéciale du système d'exploitation. En quoi consiste cette vulnérabilité et que pouvez-vous faire pour vous protéger ?

Enfin, n'oubliez pas qu'un robot connecté au même réseau peut s'en servir, servir de relais, téléviseurs intelligents, etc. Il est donc toujours judicieux de migrer les appareils IoT (en particulier les aspirateurs robots) vers un réseau privé et d'installer une protection fiable sur l'ensemble des appareils, dans la mesure du possible.

Protection avancée pour les utilisateurs avancés

Une grande partie de votre vie étant en ligne, il est important de la sécuriser.

kaspersky

appareils connectés DEF COM DEF CON Internet des objets IoT menaces piratage robots

sécurité Vulnérabilités

Conseils

Vulnérabilité Pixnapping : captures d'écran impossibles à bloquer sur votre téléphone Android

Le passeur des codes à usages uniques Android détecte partout des chevauchements. Elles permettent d'écarter les applications sans autorisation spéciale du système d'exploitation. En quoi consiste cette vulnérabilité et que pouvez-vous faire pour vous protéger ?

Enfin, n'oubliez pas qu'un robot connecté au même réseau peut s'en servir, servir de relais, téléviseurs intelligents, etc. Il est donc toujours judicieux de migrer les appareils IoT (en particulier les aspirateurs robots) vers un réseau privé et d'installer une protection fiable sur l'ensemble des appareils, dans la mesure du possible.

Protection avancée pour les utilisateurs avancés

Une grande partie de votre vie étant en ligne, il est important de la sécuriser.

kaspersky

appareils connectés DEF COM DEF CON Internet des objets IoT menaces piratage robots

sécurité Vulnérabilités

Conseils

Vulnérabilité Pixnapping : captures d'écran impossibles à bloquer sur votre téléphone Android

Le passeur des codes à usages uniques Android détecte partout des chevauchements. Elles permettent d'écarter les applications sans autorisation spéciale du système d'exploitation. En quoi consiste cette vulnérabilité et que pouvez-vous faire pour vous protéger ?

Enfin, n'oubliez pas qu'un robot connecté au même réseau peut s'en servir, servir de relais, téléviseurs intelligents, etc. Il est donc toujours judicieux de migrer les appareils IoT (en particulier les aspirateurs robots) vers un réseau privé et d'installer une protection fiable sur l'ensemble des appareils, dans la mesure du possible.

Protection avancée pour les utilisateurs avancés

Une grande partie de votre vie étant en ligne, il est important de la sécuriser.

kaspersky

appareils connectés DEF COM DEF CON Internet des objets IoT menaces piratage robots

sécurité Vulnérabilités

Conseils

Vulnérabilité Pixnapping : captures d'écran impossibles à bloquer sur votre téléphone Android

Le passeur des codes à usages uniques Android détecte partout des chevauchements. Elles permettent d'écarter les applications sans autorisation spéciale du système d'exploitation. En quoi consiste cette vulnérabilité et que pouvez-vous faire pour vous protéger ?

Enfin, n'oubliez pas qu'un robot connecté au même réseau peut s'en servir, servir de relais, téléviseurs intelligents, etc. Il est donc toujours judicieux de migrer les appareils IoT (en particulier les aspirateurs robots) vers un réseau privé et d'installer une protection fiable sur l'ensemble des appareils, dans la mesure du possible.

Protection avancée pour les utilisateurs avancés

Une grande partie de votre vie étant en ligne, il est important de la sécuriser.

kaspersky

appareils connectés DEF COM DEF CON Internet des objets IoT menaces piratage robots

sécurité Vulnérabilités

Conseils

Vulnérabilité Pixnapping : captures d'écran impossibles à bloquer sur votre téléphone Android

Le passeur des codes à usages uniques Android détecte partout des chevauchements. Elles permettent d'écarter les applications sans autorisation spéciale du système d'exploitation. En quoi consiste cette vulnérabilité et que pouvez-vous faire pour vous protéger ?

Enfin, n'oubliez pas qu'un robot connecté au même réseau peut s'en servir, servir de relais, téléviseurs intelligents, etc. Il est donc toujours judicieux de migrer les appareils IoT (en particulier les aspirateurs robots) vers un réseau privé et d'installer une protection fiable sur l'ensemble des appareils, dans la mesure du possible.

Protection avancée pour les utilisateurs avancés

Une grande partie de votre vie étant en ligne, il est important de la sécuriser.

kaspersky

Solutions pour les particuliers	TPE 150 EMPLOYS	PME 51 999 EMPLOYS	Grande entreprise 1 000 EMPLOYS ET
Kaspersky Standard	Kaspersky Small Office Security	Kaspersky Next	Kaspersky Next
Kaspersky Plus	Kaspersky Endpoint Security Cloud	Kaspersky Endpoint Security for Business Select	Cybersecurity Services
Kaspersky Premium	Kaspersky Endpoint Security for Business Advanced	Kaspersky Endpoint Security for Business Advanced	Threat Management and Defense
Toutes les solutions	Tous les produits	Tous les produits	Endpoint Security Hybrid Cloud Security Cybersecurity Training Threat Intelligence Toutes les solutions

© 2025 AO Kaspersky Lab. Tous droits réservés. • Politique de confidentialité • Politique anticorruption
• Contrat de licence grand public • Contrat de licence entreprises • Cookies

Nous contacter • À propos • Partenaires • Blog • Communiqués de presse

Securelist • Eugene Personal Blog • Encyclopédie de Kaspersky



This website uses cookies
We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

[Show details](#)

[Cookiebot by Ubersmith](#)