# 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

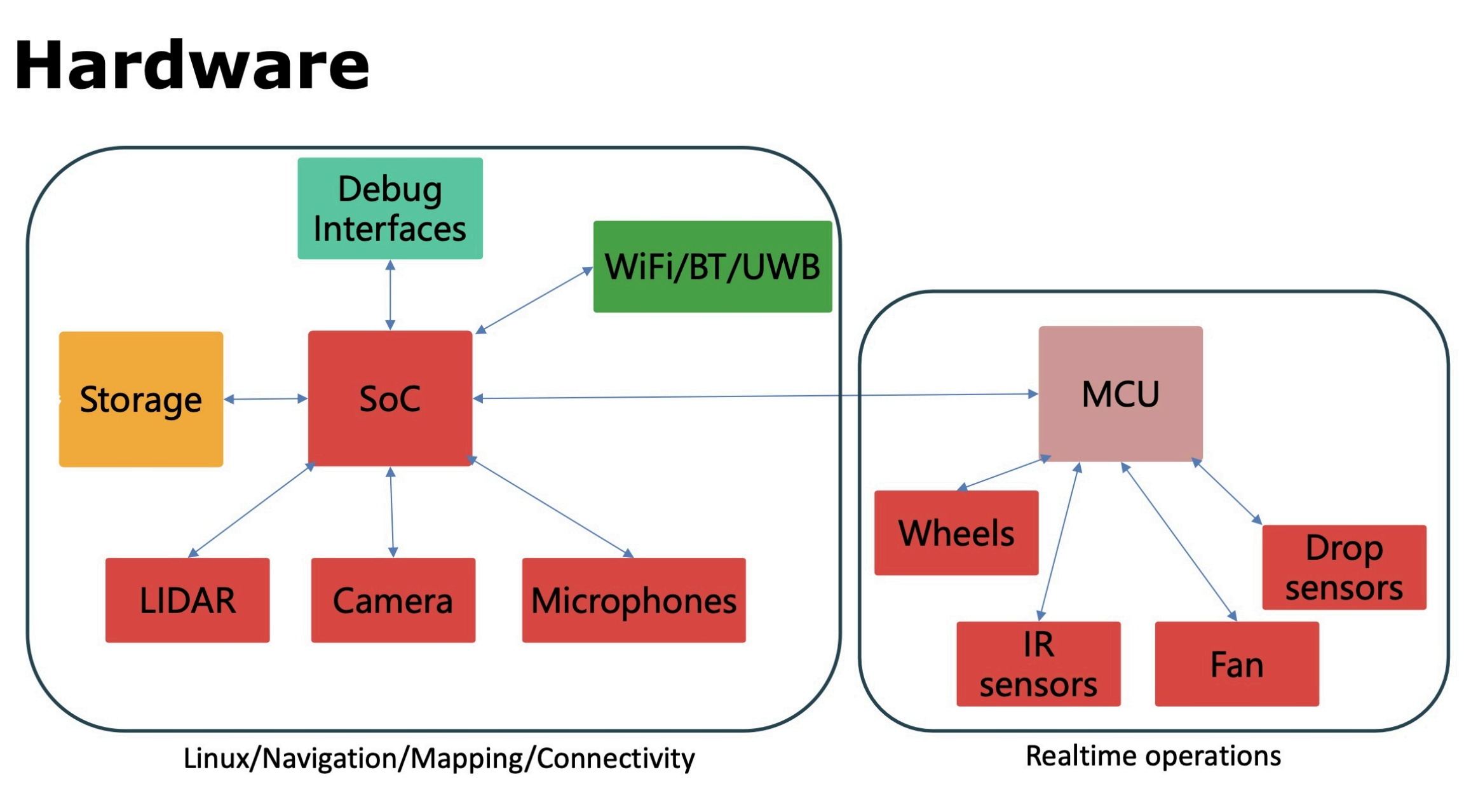
9 Jan 2025

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 très 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.

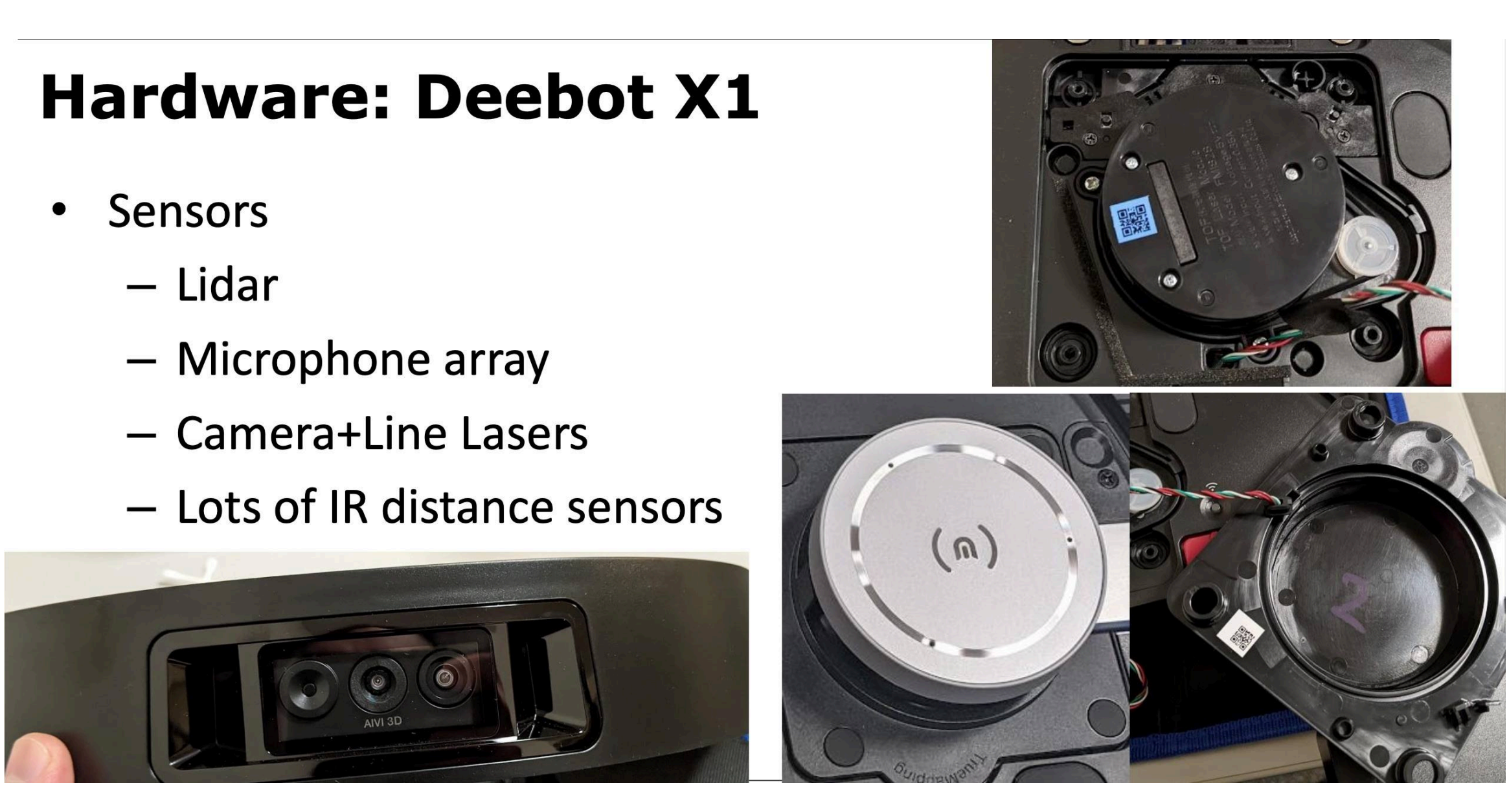
## Comment fonctionne un robot aspirateur

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.



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.



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.

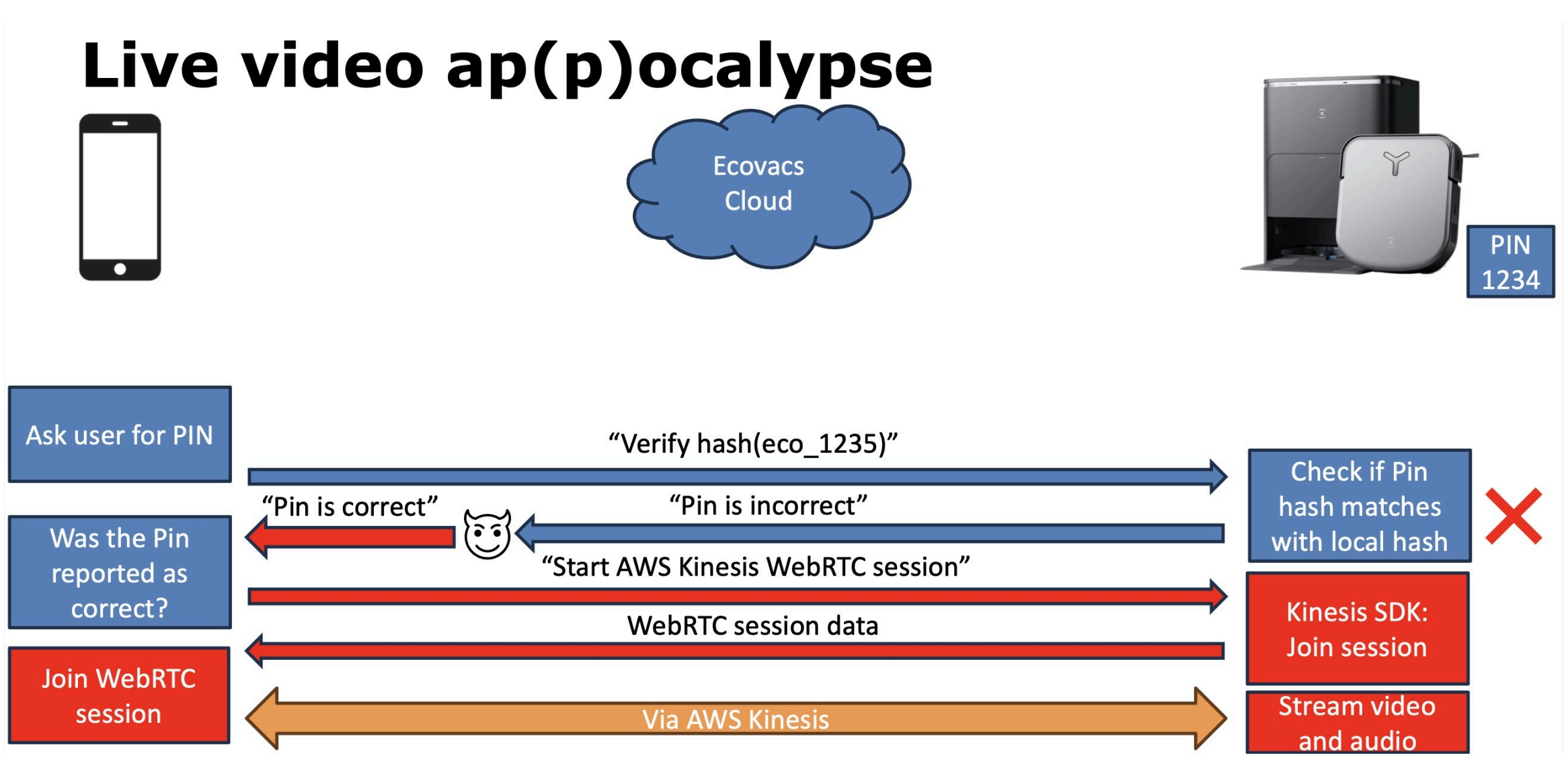
## Vulnérabilité des aspirateurs et tondeuses robots Ecovacs

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 rétroingénierie et le piratage des robots Ecovacs.

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.



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 privilèges 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 en 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.

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 propriétaires de plusieurs villes américaines ont été victimes de piratages informatiques et ont eu des ennuis avec leurs robots domestiques.

Lors d'un incident survenu dans le Minnesota, un Ecovacs DEEBOT X2 s'est mis à bouger tout seul et à faire des bruits étranges. Inquiet, son propriétaire s'est connecté à l'application Ecovacs et a constaté que quelqu'un était parvenu à accéder au flux vidéo et à la fonction de contrôle à distance. Pensant qu'il s'agissait d'un problème logiciel, il a modifié le mot de passe, redémarré le robot et s'est assis sur le canapé pour regarder la télévision avec sa femme et son fils.

Toutefois, le robot s'est remis à bouger presque immédiatement, cette fois en émettant un flux continu d'injures racistes via ses haut-parleurs. Ne sachant que faire, le propriétaire a éteint le robot, l'a emmené dans le garage et l'a laissé là. Malgré cette situation difficile, il est reconnaissant aux pirates d'avoir révélé si clairement leur présence. Selon lui, le pire aurait été qu'ils se contentent de surveiller secrètement sa famille à travers le robot, sans se dévoiler.

Piratage d'un flux vidéo en direct d'un aspirateur robot Ecovacs Source

Dans une affaire similaire, cette fois en Californie, un autre robot Ecovacs DEEBOT X2 a poursuivi un chien autour de la maison, en émettant de nouveau des obscénités. Un troisième cas a été signalé au Texas, où, vous l'aurez deviné, un aspirateur robot Ecovacs s'est égaré et a proféré des insultes à l'encontre de ses propriétaires.

Le nombre exact de piratages des aspirateurs robots Ecovacs reste inconnu. L'une des raisons, évoquée plus haut, est que les propriétaires peuvent ne pas en être conscients : il se peut que les pirates informatiques observent tranquillement leur quotidien par le biais de la caméra intégrée.

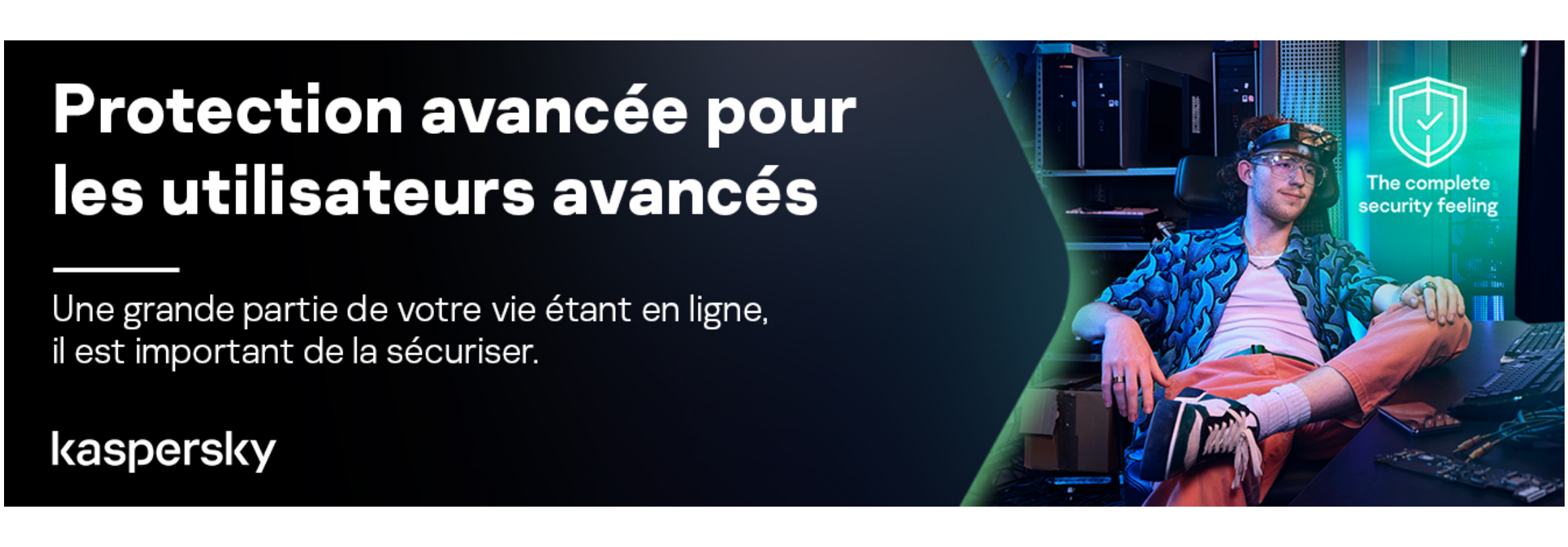
## Comment se prémunir contre le piratage des aspirateurs robots ?

En un mot : vous ne pouvez pas. Malheureusement, il n'existe pas de méthode universelle de protection contre le piratage des aspirateurs robots qui permette de résoudre toutes les situations. Pour certains modèles, il est théoriquement possible de les pirater soi-même, d'obtenir un accès root et 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 fournisseurs 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 achat. Certains d'entre eux réussissent plutôt bien à sécuriser leurs produits. Et, bien sûr, installez toujours les mises à jour du micrologiciel : les nouvelles versions éliminent généralement au moins quelques-unes des vulnérabilités que les pirates informatiques sont susceptibles d'exploiter pour prendre le contrôle de votre robot.

Enfin, n'oubliez pas qu'un robot connecté au réseau Wi-Fi domestique peut, s'il est piraté, servir de tremplin à une attaque contre d'autres appareils connectés au même réseau (smartphones, ordinateurs, téléviseurs intelligents, etc.). Il est donc toujours judicieux de migrer les appareils IoT (en particulier les aspirateurs robots) vers un réseau invité et d'installer une protection fiable sur l'ensemble des appareils, dans la mesure du possible.



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

Dans la même rubrique

Qu'advient-il des données volées lors d'une attaque de phishing ?

Le voleur d'informations a rejoint la partie

Lire l'article suivant

## Ce que nous réserve l'année 2025

Nous allons évoquer les tendances et les cybermenaces à venir en 2025.

7 Jan 2025

## Conseils

Conseils

### L'IA et la nouvelle réalité de la sextorsion

L'IA générative a fait passer les techniques de sextorsion à un tout autre niveau : désormais, n'importe quel utilisateur des réseaux sociaux peut en être victime. Comment pouvez-vous vous protéger, vous et vos proches ?

26 Jan 2026

Conseils

### Infrastructure informatique oubliée : pire encore que le Shadow IT

Comment éliminer la menace que représentent pour les organisations les serveurs et services sans propriétaire, les bibliothèques obsolètes et les API non sécurisées.

8 Jan 2026

Conseils

### Sécurité informatique : les bons réflexes à adopter en 2026

Huit résolutions numériques pour la nouvelle année que vous devez absolument tenir.

30 Déc 2025

Conseils

# Le voleur d’informations a rejoint la partie

Une nouvelle vague d’attaques ClickFix propageant un voleur d’informations sur macOS publie des guides d’utilisation malveillants sur le site officiel de ChatGPT en utilisant la fonction de partage de conversation du chatbot.

20 Déc 2025

**Solutions pour les particuliers**

- Kaspersky Standard
- Kaspersky Plus
- Kaspersky Premium
- Toutes les solutions

**TPE**
1 50 EMPLOYS

- Kaspersky Small Office Security
- Kaspersky Endpoint Security Cloud
- Tous les produits

**PME**
51 999 EMPLOYS

- Kaspersky Next
- Kaspersky Endpoint Security Cloud
- Kaspersky Endpoint Security for Business Select
- Kaspersky Endpoint Security for Business Advanced
- Tous les produits

**Grande entreprise**
1 000 EMPLOYS ET

- Kaspersky Next
- Cybersecurity Services
- Threat Management and Defense
- Endpoint Security
- Hybrid Cloud Security
- Cybersecurity Training
- Threat Intelligence
- Toutes les solutions