Les bornes de recharge, nouveau terrain de jeu des cybercriminels

Miio, spécialiste européen de la recharge des véhicules électriques, alerte sur les risques de cyberattaques liés aux bornes de recharge et partage des conseils simples pour s'en protéger.

À l'occasion du mois de Sensibilisation à la Cybersécurité, miio, spécialiste européen de la recharge des véhicules électriques, alerte contre un risque encore largement sous-estimé : les bornes de recharge deviennent une cible privilégiée des cybercriminels.

Avec près de six millions de véhicules 100% électriques en circulation dans l'Union européenne selon Eurostat, les infrastructures de recharge s'intègrent désormais pleinement à l'écosystème numérique. Reliées à des applications, à des services de paiement et à des réseaux connectés, elles peuvent devenir des points d'entrée pour des attaques ciblées. Escroqueries via QR codes, bornes compromises ou vols de données clients, la menace évolue au même rythme que le marché.

miio appelle à faire preuve de vigilance sans pour autant céder à l'inquiétude. L'entreprise rappelle que la cybersécurité n'est pas un frein à la mobilité électrique, mais un élément clé pour instaurer la confiance et accompagner son développement. Elle partage aujourd'hui les principaux risques observés sur le terrain et les bons réflexes à adopter pour les éviter.

Des QR codes frauduleux jusque sur les parkings

Les arnaques par QR code, aussi appelées quishing, se multiplient sur les parkings et les aires de service. En collant un code piégé sur une borne de recharge, les escrocs peuvent rediriger le conducteur vers un faux site de paiement pour dérober ses coordonnées bancaires ou installer un logiciel malveillant sur son smartphone. L'année dernière dans le Loiret, plusieurs automobilistes ont été piégés en scannant un de ces codes sur une borne publique et ont ainsi perdu des dizaines d'euros. Le bon réflexe consiste à lancer la recharge uniquement depuis l'application officielle de l'opérateur et de vérifier attentivement l'adresse d'un site avant toute saisie.

Des bornes vulnérables aux attaques à distance

Des chercheurs en cybersécurité ont montré qu'une borne mal configurée pouvait être utilisée pour manipuler la facturation, interrompre une recharge ou exécuter du code à distance. Ces tests, menés lors d'événements de hacking Pwn2Own Automotive 2024, rappellent qu'un appareil connecté doit être maintenu à jour et surveillé. Miio recommande de privilégier les bornes d'opérateurs reconnus et de signaler toute anomalie, notamment une déconnexion inattendue ou un message d'erreur.

Les opérateurs de recharge aussi visés

Les cybercriminels s'attaquent désormais aux opérateurs eux-mêmes. En novembre 2024, une fuite massive de données a été détectée sur le dark web après le piratage de plusieurs réseaux de recharge mal sécurisés. Plus de 116 000 d'enregistrements ont ainsi été exposés, y compris des noms, des numéros de série de véhicules et la localisation précise des bornes utilisées. Il est conseillé aux utilisateurs de vérifier régulièrement les moyens de paiement enregistrés et de rester attentifs aux communications officielles des opérateurs.

Phishing, fausses applications et Wi-Fi publics

L'essor de la mobilité électrique attire également de nouvelles arnaques en ligne. Des mails promettant des réductions ou des applications imitant les originales peuvent chercher à piéger les utilisateurs. Dans certains parkings ou aires de services, des connexions Wi-Fi publiques mal sécurisées peuvent également intercepter des échanges. Les conducteurs doivent donc installer uniquement les applications officielles depuis les boutiques d'applications vérifiées. Il est également plus prudent de passer par une connexion mobile ou un VPN afin d'éviter les Wi-Fi publics pour gérer son compte de recharge.

Un enjeu de confiance numérique

La sécurité de la recharge repose sur une combinaison de vigilance utilisateur et de bonnes pratiques techniques. Les conducteurs doivent se méfier des QR codes suspects, éviter les connexions non sécurisées et maintenir à jour leurs applications. De leur côté, les opérateurs ont un rôle essentiel à jouer en renforçant l'authentification, le chiffrement des échanges et la supervision des bornes. Une approche partagée de la cybersécurité entre usagers, fabricants et gestionnaires est la clé pour garantir la confiance dans la mobilité électrique.

« La recharge doit rester simple et sûre. Quelques réflexes suffisent déjà pour éviter la plupart des risques : passer uniquement par l'application officielle, vérifier l'URL avant tout paiement, éviter le Wi-Fi public et signaler toute anomalie. La cybersécurité n'est pas un frein à la mobilité électrique, c'est la condition de sa confiance », explique Rafael Ferreira, Chief Technology Officer et cofondateur de miio.

À propos de miio

Lancée en mai 2019, miio est une start-up spécialisée dans la mobilité électrique. Elle est présente dans 7 pays européens : l'Allemagne, la Belgique, l'Espagne, la France, l'Italie, les Pays-Bas et le Portugal, qui regroupent une communauté de plus de 400 000 utilisateurs. miio simplifie la recharge des véhicules électriques des particuliers aussi bien que des flottes professionnelles, grâce à une application qui permet de simuler les prix et les temps de recharge, d'effectuer des paiements automatisés et d'interagir avec une vaste communauté, sans avoir à se déplacer jusqu'aux bornes. miio collabore également avec l'écosystème

européen de la mobilité pour améliorer l’accès à un réseau fiable et efficace, sur la voie publique comme à domicile, et accompagner l’essor des véhicules électriques.

L'application miio est disponible gratuitement sur le Play Store, l'App Store et en version Web.