Les Secrets des Mots de Passe : L’Essence des IA Révélée !

Les Risques de Sécurité dans l’Entraînement des Modèles d’Intelligence Artificielle

Une récente recherche menée par *Truffle Security* a révélé une fuite alarmante de près de **12 000 informations confidentielles**, incluant des clés API et des mots de passe. Ces données ont été trouvées dans **Common Crawl**, un vaste ensemble de données utilisé pour l’entraînement d’intelligences artificielles, notamment des modèles de langage comme ChatGPT.

Des Données Sensibles Découvertes dans le Corpus

Les chercheurs, scrutant 400 téraoctets de données issues de plus de 2,67 milliards de pages web, ont mis en lumière ce problème croissant. Selon leur analyse, le corpus contient **11 908 informations sensibles**. Les analyses ont été effectuées à l’aide de TruffleHog, un outil conçu pour détecter des secrets apparemment oubliés dans le code et les données en ligne.

> *« Nous avons soupçonné que des identifiants codés en dur pouvaient influencer le comportement des modèles d’IA. » — Truffle Security*

Cette découverte présente des risques cruciaux : les modèles d’IA, entraînés sur des données compromises, pourraient

produire des résultats ayant des implications sérieuses en matière de sécurité.

Les Défaillances des Développeurs

Le rapport de *Truffle Security* pointe du doigt des erreurs potentielles commises par les développeurs. En intégrant directement des identifiants sensibles dans le code HTML et JavaScript, les risques associés se multiplient. Certaines clés ont été retrouvées à plusieurs reprises, ce qui augmente considérablement la portée de la faille de sécurité.

En réponse, *Truffle Security* a pris l'initiative de contacter toutes les entreprises concernées par les clés exposées. Grâce à leur assistance, ces sociétés ont pu rapidement *révoquer et générer de nouvelles clés* pour protéger leurs services.

> *Pour suivre l'actualité de 01net, abonnez-vous à notre fil d'actualités sur Google Actualités et via WhatsApp.*

Source :

Truffle Security

Source : www.01net.com

→🔗 Accéder à CHAT GPT en cliquant

dessus