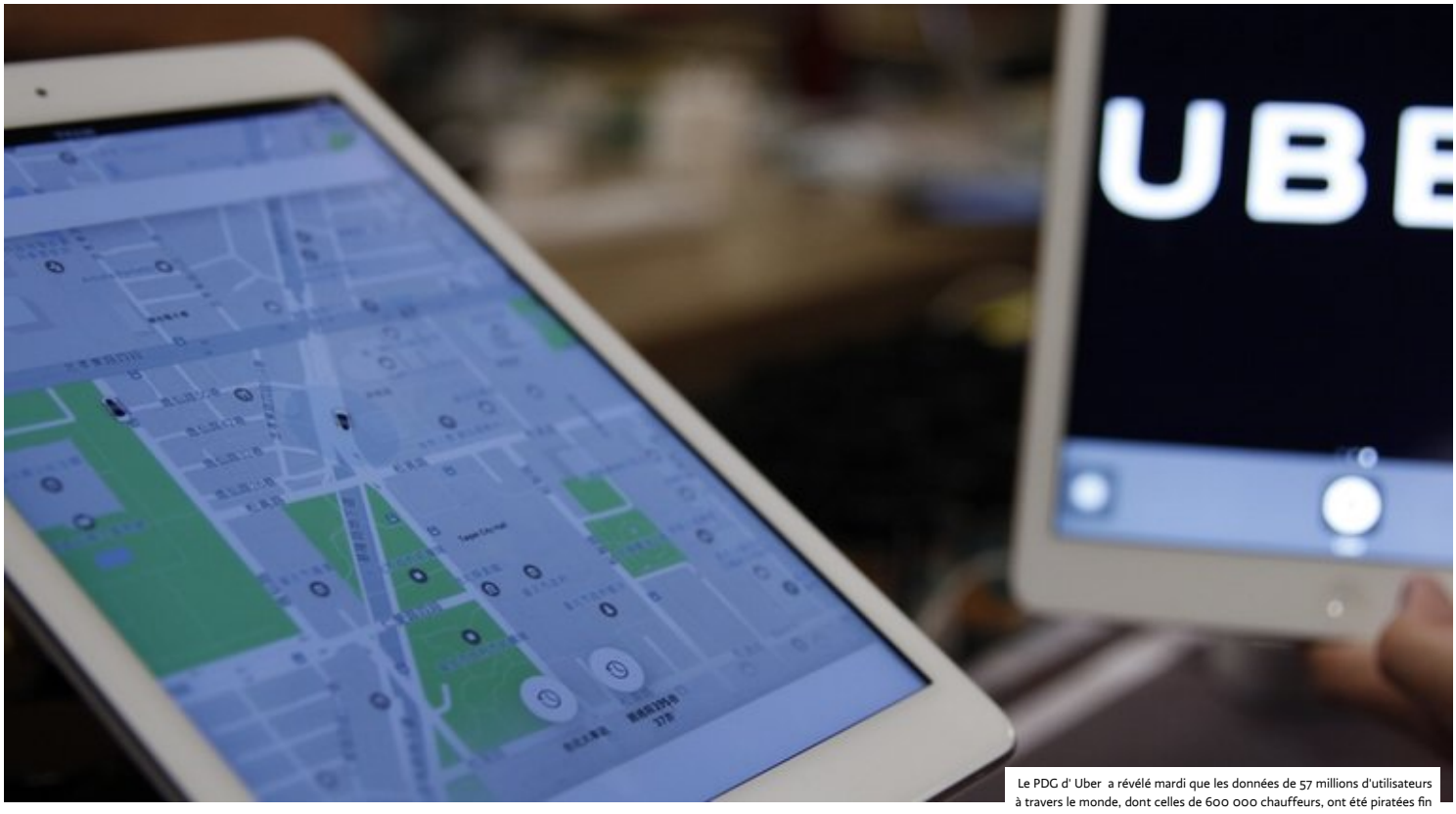
LE TEMPS



Le PDG d' Uber a révélé mardi que les données de 57 millions d'utilisateurs à travers le monde, dont celles de 600 000 chauffeurs, ont été piratées fin 2016
© RITCHIE B. TONGO

TECHNOLOGIE

Les données volées chez Uber, un piratage en réalité si banal

La société de transport s'est fait dérober les données de 57 millions de clients. Il y a eu plus d'un milliard de victimes en 2016

3 minutes de lecture

Technologies **Transports**

Anouch Seydtaghia
Publié mercredi 22 novembre 2017 à 11:45, modifié mercredi 22 novembre 2017 à 14:22.

C'est un scandale de plus pour Uber. Mais c'est surtout un scandale de plus pour toutes les entreprises qui stockent de manière peu professionnelle les données de leurs clients. Dans la nuit de mardi à mercredi, la société américaine de mise en relation entre chauffeurs privés et passagers a admis s'être fait dérober plus de 58 millions de sets de données. Ainsi, des informations concernant 57 millions de clients ont été volées, en plus des informations concernant 600 000 chauffeurs.

C'est le nouveau directeur d'Uber, Dara Khosrowshahi, qui a annoncé la nouvelle via un communiqué. Le vol est intervenu en 2016, mais le responsable ne l'aurait appris que récemment. Non seulement la société basée à San Francisco a caché ce vol aux autorités, mais en plus elle a payé, via deux employés licenciés entre-temps, 100 000 dollars aux pirates pour qu'ils se taisent et détruisent les données.

Un impact planétaire, mais les nationalités ne sont pas précisées

De quelles données s'agit-il? Pour les clients, il s'agit des adresses e-mail et de leurs numéros de téléphone mobile. Pour les chauffeurs, il s'agit de leurs noms et numéros de permis de conduire. Uber promet que ni l'historique des trajets, ni les numéros de cartes et de comptes bancaires, ni les numéros de sécurité sociale n'ont été dérobés.

Lire aussi: Insensible aux scandales, Uber croît sans cesse

Uber ne précise pas la nationalité des victimes, mais tout le monde peut se sentir concerné. Il y a un an, la société affirmait avoir 40 millions d'utilisateurs réguliers, un chiffre qui a sensiblement augmenté depuis.

Ces 58 millions de victimes rejoignent une longue liste d'internautes piratés. Dans son rapport 2017 sur la cybersécurité, la société américaine Symantec affirmait que 1,12 milliard de personnes s'étaient fait voler des données en 2016, contre 563 millions l'année précédente. En 2016, 1209 cas de vol ont été répertoriés, dont 15 «méga-vols», comme les appelle Symantec, soit des cas avec plus de 10 millions d'identifiants volés en une fois.

Des données disponibles ensuite sur le Dark Web

Autre élément intéressant: les 58 millions de victimes du vol de données chez Uber vont sans doute rejoindre d'autres victimes. Selon Symantec, on trouve déjà des données de clients d'Uber pour un dollar pièce sur le Dark Web, sans doute issues d'un vol intervenu il y a plusieurs mois. «Nos chercheurs ont montré que les pirates s'intéressent de plus en plus à des comptes liés à des médias, tels Netflix et Spotify, avec des prix allant de 10 cents de dollars à 10 dollars par compte», écrit Symantec dans son rapport.

Il s'agit ainsi d'un business en pleine expansion et toutes les données ont leur importance, car elles permettent, avec un peu d'ingénierie sociale, d'accéder ensuite à des données bancaires ou de cartes de crédit. Que penser du cas de la nuit dernière? «Ces hackers ne font probablement pas partie du crime organisé», estime Steven Meyer, directeur de la société de sécurité genevoise ZENData. «Les données ont été vendues bien en dessous du prix du marché et il existe de nombreux outils pour scanner Github afin de trouver des identifiants.» Github est un service web d'hébergement et de gestion de développement de logiciels. Les pirates auraient piraté ce service pour ensuite accéder aux données privées stockées sur un espace Amazon Web Services.

«Former les développeurs»

Selon Steven Meyer, «il n'y a pour l'heure aucune indication que les données ont été vendues sur le Dark Web». Mais ensuite, «les données volées pourraient être utilisées pour faciliter d'autres activités criminelles, car les numéros de téléphone sont souvent utilisés dans les processus d'authentification forte.» De nombreux services exigent en effet une authentification par mot de passe, puis par SMS. Le spécialiste insiste: «Il faut former correctement les développeurs et s'assurer qu'ils comprennent les risques et conséquences de leurs actions.»

Anouch Seydtaghia
@Anouch

Journaliste éco/finance, spécialisé dans les nouvelles technologies, intéressé par les voitures autonomes, la cybersécurité et les start-up