

Près de 10 millions de données de santé en vente sur le Dark Web

Les données ont une valeur, mais certaines plus que d'autres. Les informations médicales font partie de celles-là. Sur le Dark Web, il est fréquent de voir surgir de temps en temps des bases de données de santé. Sauf que, cette fois, le volume concerné est peu banal : un pirate connu sous le nom de « thedarkoverlord » a mis en vente une base contenant plus de 10 millions de dossiers d'assurés sociaux.

Plusieurs lots de données sont en vente. Le plus fourni comprend 9,3 millions de dossiers d'assurance-maladie de patients américains. Il est en vente pour 750 bitcoins, soit environ près de 500 000 euros. Les informations comprennent les noms, adresses mails, numéros de téléphone, dates de naissance et numéros de sécurité sociale.



Plusieurs lots à des prix variés

Le pirate revendique également d'autres vols de données issus de 3 régions en particulier : 48 000 enregistrements sont basés à Farmington dans le Missouri, 397 000 entrées proviennent d'Atlanta en Géorgie (probablement via des organismes comme Blue Cross Blue Shield et United Healthcare) et 210 000 données sont issues du Midwest américain. Les prix demandés pour ces informations vont de 60 bitcoins (environ 40 000 dollars) pour Farmington, à 300 bitcoins (195 000 dollars) pour Atlanta en passant par 170 bitcoins (110 000 dollars) pour le Midwest. Soit un total de près de 850 000 dollars pour l'ensemble des données.

Difficile de vérifier la validité des lots de données mis en vente. Déjà, le pirate semble nouveau sur la plateforme, car aucun point ne lui est attribué, une méthode pour reconnaître les hackers expérimentés. Le site MotherBoard a réussi à récupérer des échantillons et a contacté les personnes touchées. Les informations étaient bonnes, ce qui laisse penser que la base est globalement valide. Dans un entretien avec nos confrères, le pirate explique avoir dérobé les informations en exploitant une faille de type zero day dans le protocole UDP, utilisé pour le contrôle à distance d'un PC. Il précise que certaines données étaient accessibles en clair, donc non chiffrées, contrairement aux exigences fédérales en matière de confidentialité.

A lire aussi :

[Nos données de santé \(mal\) protégées par l'indésirable SHA-1](#)

[Les données de santé, une manne pour les hackers](#)

Crédit Photo : Vladyslav Starozhylov-Shutterstock