

Cyberattaques : pourquoi vos données de santé sont si fragile



Article rédigé par *Le Figaro*, le 14 mars 2021

Source [Le Figaro] Les cyberattaques sur les établissements de santé se multiplient depuis le début la crise sanitaire. Les pirates n'hésitent pas à revendre les données médicales de centaines de milliers de patients en ligne.

La démonstration est saisissante. Au bout du fil, un hacker nous liste en hurlant de rire les noms et informations personnelles de médecins d'un grand hôpital français qu'il a pu récupérer grâce à une faille de sécurité. Toujours au téléphone, un autre homme, spécialiste de la cybercriminalité, déniche en quelques secondes les pseudonymes et mots de passe de plus de 300 professionnels de santé un peu partout dans le pays. Sur le dark web, la face cachée et souvent sombre d'internet, il faut peu de temps à ces initiés pour parcourir d'immenses bases de données médicales où figurent les numéros de sécurité sociale, adresse et antécédents médicaux de patients et professionnels de santé. Les cyberattaques sur des établissements de santé se sont multipliées depuis le début de l'année 2020, avec notamment une [fuite de 500.000 dossiers médicaux au mois de février 2021](#), et pas une semaine ne passe aujourd'hui sans qu'[un de ces établissements ne soit visé par une attaque](#).

Si ces données de santé ont de la valeur pour les pirates, c'est d'abord parce qu'elles sont « réelles et sincères » explique Nicolas Arpagian, auteur de *La cybersécurité* (PUF) et administrateur de [la plateforme gouvernementale d'assistance aux victimes de cyberattaques](#). « Si demain je m'inscris pour une newsletter, je peux donner de fausses informations, mais les données de santé sont de vraies données : un vrai nom, un vrai groupe sanguin, de vrais antécédents médicaux... » Mieux, selon Nicolas Arpagian, ces données ne sont pas « substituables » : « Si je me fais pirater ma carte bleue, je peux changer de code. Mais je ne pourrai pas changer mon groupe sanguin »

Retrouvez l'intégralité de l'article [en cliquant ici](#)

14/03/2021 07:00