Les données de santé, une manne pour les hackers

Mis à jour le 23 avril, à 14h55. Avec des précisions sur le nombre et la nature des données dérobées à Labio, puis mises en ligne, suite aux demandes de l'avocat de cette société, maître Paul Nicoud.

Le vol et la diffusion récente d'une liste d'identifiants de connexion, immédiatement rendus inutilisables par les laboratoires de biologie médicale **Labio**, et de résultats d'examens du groupe par des pirates informatiques de **Rex Mundi**, n'est que la partie émergée de l'iceberg. En témoignent les attaques qui ont récemment ciblé des assureurs santé outre-Atlantique.

La semaine dernière, la mutuelle américaine **Premera Blue Cross** a confirmé avoir été victime d'une attaque informatique au cours de laquelle les données personnelles de **11 millions d'utilisateurs** ont été exposées, informations médicales incluses. L'attaque avait été repérée en début d'année 2015. En février dernier, c'est l'assureur américain **Anthem** qui a annoncé avoir été la cible d'une cyberattaque durant laquelle les identités, les coordonnées, les informations bancaires et les numéros de sécurité sociale de plus de **78 millions de clients** et employés ont été compromis.

Des marchés souterrains lucratifs pour les hackers

Le secteur de la santé serait moins bien préparé que d'autres. « *D'autres industries souvent ciblées par des attaques informatiques, tels que le commerce de détail ou la banque, ont élevé leur niveau de protection en ligne. Le secteur de la santé, en revanche, est à la traîne en matière de sécurité informatique* », a expliqué à *Computerworld* Jeff Schmidt, CEO de la société de conseil spécialisée JAS Global Advisors.

Pour les hackers, les données de santé seraient donc un nouvel eldorado. Les numéros de sécurité sociale, par exemple, peuvent s'échanger pour **quelques centaines de dollars** chacun aujourd'hui, contre une poignée de dollars pour un numéro de carte bancaire qui ne vaudra plus grand chose une fois le vol signalé, d'après l'éditeur et spécialiste du chiffrement de données PKWare.

La **revente d'informations sanitaires** à des acteurs de l'écosystème capables d'en tirer profit, l'industrie pharmaceutique notamment, est une autre possibilité. Les entreprises et leurs clients victimes de cyberattaques peuvent également faire l'objet d'un **chantage** direct. Les hackers de Rex Mundi ont eux-mêmes réclamé une rançon de **20 000 euros** à Labio en contrepartie d'une non-diffusion des données dérobées.

Le laboratoire français a refusé et les données concernées (une liste de 15 000 identifiants de connexion, immédiatement rendus inutilisables par les laboratoires Labio, et une dizaine de résultats d'examens) ont été publiées le 17 mars dernier sur un site de Rex Mundi accessible depuis le réseau Tor.

Lire aussi :
Pourquoi les hôpitaux US sont dans la ligne de mire des hackers
Pour FireEye, la Chine finance une razzia sur les données de santé US

crédit photo © Eugene Sergueev-Shutterstock