AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

772 millions de dossiers e-mails hackés

Contenu

I. Contexte

772 millions d'adresses email et 21 millions de mots de passe piratés sont en circulation sur le Dark web. C'est tout simplement l'une des plus grosses fuites de données qu'on n'ait jamais connues. Elle a été baptisée « Collection #1 ». Ces emails et mots de passe sont issus de différents sites web et services en ligne et sont contenus dans un fichier archive d'une taille de 87 Go. Selon les estimations, les informations auraient été extraites à partir de 2890 sites web. Pastebin a publié une liste présumée des répertoires concernés.

II. Risques et implications

Après le nettoyage des fichiers bruts, on peut recenser près de 2,7 milliards d'adresses concernées. Parmi elles, ce sont près de 773 millions de mails qui ont été réellement piratés, auxquels sont associés 21 millions de mots de passe. Pourtant, on exclu les mots de passe sous forme hachée. D'après ces précisions, environ 140 millions de mails n'étaient pas encore enregistrés dans la base de données. Par ailleurs, plus de 10 millions de mots de passe sont également nouveaux. La fuite est vraiment importante. Son niveau se rapproche de celle révélée par Yahoo il y a quelques années (https://www.phonandroid.com/yahoo-les-donnees-de-500-millions-dutilisateurs-ont-ete-piratees.html)

Sergey Lozkhin, chercheur en cybersécurité au sein du GReAT chez Kaspersky Lab, commente cette faille : « Cette quantité de données massives, récoltée par le biais d'une faille de données a été produite sur une longue période, ce qui signifie qu'un certain nombre d'informations sont susceptibles d'être obsolètes aujourd'hui. Cependant, il est de notoriété commune que malgré la prise de conscience croissante face au danger, les individus continuent d'utiliser les mêmes mots de passe, et les réutilisent même sur un grand nombre de sites Internet. De plus, cette collection de données peut facilement être transformée en une simple liste d'emails et de mots de passe, de fait les attaquant n'auraient qu'à écrire une ligne de code sur un programme informatique assez simple pour vérifier la fonctionnalité de ces mots de passe sur d'autres comptes en ligne. Les conséquences d'un accès aux comptes peuvent aller d'un phishing très fructueux, puisque les criminels n'ont qu'à envoyer des emails malveillants à la liste de contacts de la victime, à des attaques ciblées visant à dérober l'intégralité de l'identité digitale de la victime ou de l'argent, ou encore à la compromission des informations envoyées sur tous les réseaux sociaux »

III. Comment se protéger ?

Il est urgent que toutes les personnes qui utilisent leurs mots de passe de messagerie pour d'autres activités en ligne prennent les mesures suivantes, aussi vite que possible :

1- Vérifier si les comptes de messageries ont été exposés en se rendant sur le site https://haveibeenpwned.com/
2- Changer les mots de passe des comptes les plus importants et sensibles (tels que les banques en ligne, les plateformes de paiement en ligne ou les réseaux sociaux), de préférence en utilisant un gestionnaire de mots de passe
3- Implémenter l'authentification multi-facteurs dès que possible. »