# 68 millions de comptes Dropbox menacés ?

La semaine dernière, Dropbox invitait ses utilisateurs qui avaient ouvert un compte avant la mi-2012 sans en avoir changé le mot de passe depuis à le faire. La raison ? Le service de stockage en ligne reconnaissait que des identifiants avaient pu être dérobés à partir d'un ou plusieurs sites tiers. Mais Dropbox assurait n'avoir constaté aucune attaque des comptes utilisateurs concernés et leur conseillait, par sécurité, de modifier leur mot de passe.

Si l'affaire apparaissait comme anecdotique, elle prend une toute autre ampleur quand le vol concerne plus de 68 millions de comptes. C'est du moins ce qu'a révélé le site Motherboard qui dit avoir obtenu une sélection de fichiers contenant adresses e-mails et mots de passe hachés. Des comptes valides aux dires du chercheur en sécurité Troy Hunt, par ailleurs directeur régional chez Microsoft, qui a épluché les fichiers reçus par Motherboard. *« Il ne fait aucun doute que la violation de données contient les mots de passe valides de Dropbox, vous ne pouvez tout simplement pas inventer ce genre de chose »*, assure-t-il sur son blog.

## Dropbox reconnaît mais minimise

De son côté, Dropbox ne nie pas l'existence de ce fichier de comptes qui circule sur la toile. *« La liste des adresses e-mail avec les mots de passe hachés est réelle »*, reconnaît l'entreprise. Qui s'était bien gardée d'indiquer le volume de clients compromis. Pour ne pas les inquiéter ? *« Nous n'avons aucune information relative au fait que les comptes d'utilisateurs Dropbox ont été abusés »*, ajoute le service. Tout en reconnaissant que c'est parce que *« nous avons d'abord entendu des rumeurs au sujet de cette liste [de fichiers piratés] il y a deux semaines »* que l'alerte a été lancée. Le changement des mots de passe devrait normalement protéger les potentielles victimes des risques de futures violations de comptes.

Dropbox en profite pour inviter les utilisateurs qui utiliseraient le mot de passe de leur compte de stockage en ligne sur d'autres services à les changer également pour éviter que les pirates n'étendent leur périmètre d'attaque. Comme ce fut probablement le cas avec l'affaire Linkedin également piraté en 2012 et qui mettait à risque des comptes Twitter. Vous pouvez vérifier si vos comptes sont exposés à un vol de données depuis le très utile site Have I been pwned ?.

---

**Lire également**
Près de 10 millions de données de santé en vente sur le Dark Web
Via beta Facebook, un hacker accède à n'importe quel compte
Shard : un test ambigu pour les mots de passe partagés
Que se passe-t-il après un vol de données ?