Dropbox accessible pendant 4 heures sans mot de passe

L'image de la sécurité du cloud vient de prendre une nouvelle claque. Lundi 20 juin, une vulnérabilité a été repérée sur le service de stockage et de partage de fichiers en ligne **Dropbox**. Pendant 4 heures, cette faille de sécurité a permis à n'importe quel internaute de pouvoir se connecter à n'importe quel compte Dropbox sans mot de passe.

Il suffisait de saisir, à sa guise, l'identifiant d'un compte utilisateur pour s'y connecter et avoir accès à ses données. **Peu importe le mot de passe saisi**, Dropbox a ainsi ouvert les portes de son service à tout intrus, pendant une demi journée.

On vient tout juste de l'apprendre et pourtant, les faits se sont déroulés **dans la nuit du dimanche 19 à lundi 20 juin**, en pleine nuit à Paris. Aux Etats-Unis, où le service compte plus de 10 millions d'inscrits, la lune cédait sa place au soleil. Autant dire que le créneau avait tout d'une heure de pointe sur les serveurs américains de Dropbox rapporte *ITespresso.fr*. Ce ne fut vraisemblablement pas le cas. Sur le blog officiel, **Arash Ferdowsi**, directeur du service technique, a tout de même présenté toutes ses excuses pour une erreur « *qui n'aurait jamais dû se produire*».

Désabusé, il a toutefois tenu à relativiser le désagrément, en précisant que « ***tout au plus 1% des utilisateurs se sont connectés durant ce laps de temps*** ». Sur les 25 millions d'inscrits que compte Dropbox, la plupart dormaient donc sur leurs deux oreilles, tandis que 250.000 d'entre eux se connectaient, chacun à son compte personnel, comme si de rien n'était.

A l'origine, **un bug dans le mécanisme d'authentification** désactivait l'algorithme de contrôle des mots de passe. Seul l'identifiant était contrôlé. Détecté à 2h40 (heure de Paris), le problème a été résolu dans la minute, mais il remontait à la dernière mise à jour du code, vers 22h50 la veille.

Déjà miné par l'enquête lancée par la Federal Trade Commission contre sa politique de confidentialité, Dropbox déclare avoir la situation en main. **On ignore encore si certains comptes ont été infiltrés**, mais Arash Ferdowski a précisé qu'un log (enregistrement) est actuellement à l'étude. Le document répertorie toutes les connexions effectuées durant la période critique, de 22h50 à 2h40.

Certains comptes Premium peuvent contenir jusqu'à **100 Go de données**. En cas de suspicion concernant l'un d'entre eux, Dropbox promet d'en avertir les possesseurs et de prendre les mesures jugées nécessaires. En attendant, cet incident montre que la sécurité du cloud repose quasiment entièrement sur la qualité de son fournisseur, lequel n'est jamais à l'abri d'un bug…