14 septembre 2016
Conseils d'ami

Piratage massif : comment vous protéger si vous faites partie des 68 millions d'utilisateurs de Dropbox dont les données sont désormais en vente sur le Dark Web

De nombreuses données personnelles piratées en 2012 sont actuellement revendues sur le "Dark Web". Attention, les vôtres s'y trouvent peut-être...Et si ce n'est pas le cas, voici quelques conseils pour éviter que cela ne vous arrive un jour.

Avec Frédéric Mouffle

Atlantico : Après le hacking de 68 millions de comptes Dropbox dont les données personnelles sont désormais en vente actuellement sur le "Dark Web", lesquelles d'entres elles sont, selon vous, le plus revendues et pourquoi ?

Frédéric Mouffle : La compromission des données liées à Dropbox date de 2012. A l'époque, on parlait de suspicion concernant d'autres plateformes telles que LinkedIn, Myspace ou Tumblr… Dropbox a d'ailleurs à l'époque initié une réinitialisation des mots de passe des utilisateurs accompagné d'un mail explicatif.

Si les élements sont exploitables, les identifiants Dropbox donnent l'accès à l'espace de stockage des utilisateurs. Ce qui signifie que si vous y stockez des données suffisamment sensibles **-** telles des données bancaires ou personnelles **-** vous serez peut être impacté. Pourquoi peut être ? Parce qu'**il faut plusieurs mois, voire plusieurs années, pour vérifier** : premièrement, si les mots de passe sont toujours d'actualité; deuxièmement, pour consulter tous les fichiers (ils peuvent être nombreux : dans ce cas, 68 millions de comptes multipliés par le nombre de fichiers stockés), afin de voir si ces données sont exploitables par ceux qui ont réussi à y accéder, etc.

L'accès à ces données peut ainsi être monétisé de plusieurs façons. **Ce qui se vend bien est l'accès à divers comptes (Mail, Facebook, PayPal, etc..), mais aussi l'accès aux fichiers de type "*état civil*" pour les spécialistes de l'usurpation d'identité**, le "cyber**-** chantage" via des fichiers ou des photos compromettantes, les données professionnelles ou médicales, le "*cybersquating*" sur votre espace personnel pour y stoker des scripts ou autres codes malicieux, mais encore des sites internet de spam. Il y a bien d'autres possibilités que je n'évoquerais pas ici pour des raisons évidentes…

Existe-t-il des moyens de récupérer les données personnelles piratées en vente sur le "Dark Web" ?

Il existe des moyens de récupérer la base de données dont une partie a été diffusée sur *Pastebin* en octobre 2014, des données qui portaient sur seulement 7 millions de comptes. **Concernant les données personnelles déjà en vente, il est malheureusement impossible d'arrêter le processus** surtout s'il s'agit de fichiers ou d'images, pour peu que vous soyez une personne exposée (politique, acteur, chanteur, VIP, personnel qualifié, etc.).

Pour les utilisateurs ayant une "hygiène de vie numérique" réfléchie,**changer ses mots de passe régulièrement réduit fortement la possibilité d'être impacté**. Il faut cependant noter que le piratage de 2012 compromet les mots de passe à un instant T. Le décryptage des mots de passe (qui sont la plupart du temps stockés de manière cryptées via l'algorithme MD5), est rendu quasi instantané sur des mots de passe simple de type ″123456″ (il y en a encore beaucoup, malheureusement…).

Si celui-ci a été changé avec un mot de passe plus complexe, vous êtes en théorie beaucoup moins exposé car le décryptage sera plus long à réaliser par l'intrus. Le pirate préfèrera se concentrer sur les mots de passe simples qui donnent une indication sur l'importance que porte l'utilisateur à la complexité de son mot de passe, et donc, à la plus grande probabilité de pouvoir avoir accès à d'autres comptes de la victime visée. Il y a bien d'autres chemins pour accéder frauduleusement à votre mot de passe: par exemple, votre machine a pu être infectée par un *malware*, et dans ce cas, l'attaquant a accès à tous les fichiers de votre machine incluant les divers mots de passe enregistrés et stockés dans les navigateurs ou dans les autres applications. La question centrale est plutôt de comprendre le *modus operandi* des attaquants et de savoir quelles mesures ont été mises en place par ces entreprises pour éviter ce type d'attaques malveillantes.

Un volume non négligeable d'utilisateurs ont recours au même mot de passe pour les services en ligne qu'ils utilisent tous les jours. Ce qui à mon sens, est une stratégie très risquée et une négligence impardonnable dont les pirates savent se saisir pour en tirer parti. Ils testeront donc ce mot de passe sur votre boite mail et tous les comptes associés, tels que Facebook, Gmail, etc… Comptes qu'ils auront pu identifier en analysant les fichiers contenus sur votre espace personnel. Des gestionnaires de mots de passe à l'instar de LastPass ou 1password pour ne citer qu'eux, comme la double authentification, sont également une solution relativement efficace et rapide à mettre en place…

Le site https://haveibeenpwned.com/ permet à tout un chacun de vérifier si ses données d'identifications Dropbox ont pu être compromises. Le site https://www.leakedsource.com/ peut également être utilisé pour couvrir un plus large spectre sur les autres plateformes ayant également été victimes de piratage.

Au vu de ce piratage, faudrait-il arrêter d'utiliser ce type de stockage en ligne ? Si oui, par quoi le remplacer ?

Le stockage en ligne est pratique et gratuit. Cependant, la confiance repose sur le fait que la société qui héberge vos données soit suffisamment solide pour garantir l'intégrité et la confidentialité de celles-ci.

Pour la plupart des utilisateurs, ces questions ne se posent pas car ils ignorent le plus souvent totalement ce qui se passe en "*backoffice"*, dans les coulisses. Il est possible de stocker des données chiffrées sur Dropbox, mais dans ce cas, il n'est pas possible d'avoir accès à ces mêmes données en cas d'intrusion malveillante. **Le stockage de ses données en local reste une solution sûre à condition de respecter les règles de bon sens**, à savoir être vigilant avant d'ouvrir une pièce jointe ou de cliquer sur un lien pouvant être compromis ou "infecté", et maintenir ses systèmes d'exploration à jour.

Propos recueillis par Chloé Chouraqui