Shard : un test ambigu pour les mots de passe partagés

Au mois de juin, plusieurs vols massifs de données ont défrayé la chronique sur des sociétés célèbres, Linkedin, MySpace, Tumblr. Au total pas moins de 642 millions de comptes ont été livré au public avec les identifiants et les mots de passe. Certes, les bases de données volées étaient pour la plupart relativement anciennes. Mais le risque le plus grand portait sur la réutilisation des mots de passe sur d'autres sites et donc d'avoir accès à des données supplémentaires pour les cybercriminels.

Or, il n'y a rien de plus fastidieux pour un utilisateur de savoir si son mot de passe subtilisé est utilisé sur d'autres plateformes comme Facebook, LinkedIn, Reddit, Twitter ou Instagram. Un développeur, Philip O'Keefe, a réalisé un outil en ligne de commandes disponible sur GitHub. Baptisé Shard, il permet aux utilisateurs de tester son mot de passe sur d'autres sites. Il a créé ce programme après avoir découvert que son mot de passe de 8 caractères générés aléatoirement était dans le vol de 177 millions de mots de passe de Linkedin. « *J'utilisais ce mot de passe pour m'authentifier sur de nombreux services* », explique dans un mail adressé à nos confrères d'*Ars Technica*. Et d'ajouter que « *c'était très difficile de me rappeler sur quels sites, je l'avais utilisé et être obligé de le changer à chaque fois. Maintenant, je me sers d'un gestionnaire de mots de passe* ».

Un outil potentiellement dévoyé

Philip O'Keefe a développé Shard dans une optique d'aide aux personnes, mais il est facile d'imaginer un usage moins philanthrope et plus néfaste. Techniquement, l'outil est capable de vérifier un nombre illimité d'identifiants volés sur des sites. Une mise à jour du code pourrait permettre à des attaquants de faire de même pour des comptes bancaires ou des services financiers. Avec un peu de travail, il serait possible d'ajouter des caractères aléatoires dans les mots de passe testés comme par exemple, « p @ $$ w0rd11 » et « p @ $$ w0rd22 ».

Seul point de limitation de la part des sites testés, bloquer l'adresse IP unique qui essaye de se connecter un grand nombre de fois et s'appuyer sur une authentification spécifique (captcha, questions, etc.). Faible obstacle pour des cybercriminels ayant accès à des botnets pour contourner cette mesure. Philip O'Keefe reconnaît qu' « *il est difficile pour les sites de bloquer le trafic provenant de cet outil, car il ressemble à un trafic normal comme si un utilisateur se connecte à l'aide d'un navigateur* ».

A lire aussi :

Que se passe-t-il après un vol de données ?

Des millions de comptes Twitter à risque après le piratage de Linkedin

Crédit Photo : scyther5-Shutterstock