

1,2 milliard de mots de passe volés par des pirates russes

Le *New York Times* [explique](#) qu'un groupe de pirates russes, baptisé Cybervor, aurait rassemblé la plus large collection d'identifiants de connexion jamais réalisée. Ils auraient collecté 4,5 milliards d'identifiants dont **1,2 milliard de comptes utilisateurs** (noms et mots de passe de connexion) uniques, reliés à **plus de 500 millions d'adresses e-mail**.

Le casse du siècle pour cette douzaine de pirates, qui ont ciblé des sites tous azimuts, du plus gros au plus insignifiant. Près de **420 000 sites web** seraient concernés par cette attaque sans précédent.

« Les pirates n'ont pas seulement ciblé des entreprises américaines, ils ont ciblé tous les sites web qu'ils pouvaient, allant des sociétés du Fortune 500 à de très petits sites », confirme **Alex Holden**, fondateur et chef de l'information responsable de la sécurité de Hold Security, société qui [a dévoilé cette affaire](#).
« Et la plupart de ces sites sont encore vulnérables. »

Une méthode proche de l'audit de sécurité

Dans sa note de sécurité, Hold Security indique que la méthodologie employée par Cybervor s'apparente à de l'audit de site à travers des tests sur la vulnérabilité aux injections SQL.

[Pour aller plus loin, lire : [5 questions pour comprendre le vol de 1,2 milliard d'identifiants](#)]

Les cybercriminels ont automatisé ces tests en s'appuyant sur un botnet capable de mener à grandes échelles de tests de pénétrations et de glaner ainsi un maximum de données sensibles.

Du spam... pour le moment

Les pirates n'ont jusqu'alors pas cherché à vendre leur base d'identifiants de connexion, indique le *New York Times*. Ils se bornent actuellement à l'utiliser afin de diffuser du spam, par e-mail et sur les réseaux sociaux.

Il est toutefois probable que cette immense base de données se retrouvera prochainement sur le marché. Les informations qu'elle renferme sont en effet précieuses pour les criminels souhaitant spammer ou voler l'identité des internautes. Elles intéresseront également les services marketing les moins scrupuleux.

A lire aussi :

[Sécurité : des chercheurs favorables à la réutilisation des mots de passe](#)

[Une nouvelle affaire de vol de millions de mots de passe](#)

[Quiz Silicon.fr – Fuites de données, petits secrets et grands scandales](#)