Piratage de Yahoo : les données sont à vendre depuis août 2016

Désormais connu de tous, le piratage de la base de données des utilisateurs a commencé à apparaître à la lumière en août dernier, quand Andrew Komarov, le responsable du renseignement (sic) de la firme américaine InfoArmor a découvert qu'un collectif de hackers d'Europe de l'Est offrait cette gigantesque base de données sur le marché noir, expliquent nos confrères de *Bloomberg*. Le responsable d'InfoArmor, société qui effectue un suivi des transactions sur le Darknet, assure que trois acheteurs ont récupéré la base, payant environ 300 000 $ chacun : deux spammers bien connus et une organisation apparemment davantage tournée vers l'espionnage. Cet acheteur mystère a, en effet, vérifié la présence de 10 personnalités du monde des affaires et de la politique (américaines et autres) avant de se porter acquéreur. Le lot est aujourd'hui toujours à vendre, mais son prix a chuté (entre 20 000 et 50 000 $), depuis que Yahoo a initié le processus de remplacement des mots de passe.

InfoArmor assure avoir obtenu une copie de la base via la surveillance d'un groupe de cybercriminels (baptisé Group E), rodés à la revente de données dérobés à de grands services Internet (comme MySpace, Dropbox ou le réseau social russe VK.com). La société américaine dit avoir alerté, au cours des derniers mois, les autorités américaines, mais aussi australiennes, canadiennes, britanniques et celles de l'Union européenne. Andrew Komarov explique n'avoir pas sonné l'alarme auprès de Yahoo directement, redoutant de voir le portail freiner une enquête qui pouvait menacer le rapprochement avec Verizon.

Une opération de reconnaissance ?

L'histoire ne dit pas en revanche ce qu'il est advenu des données en question durant les trois années qui ont séparé leur vol (en août 2013) et leur découverte par Andrew Komarov. Ni entre quelles mains elles ont circulé durant cette période. Rappelons que les informations exfiltrées de Yahoo comprennent les noms des utilisateurs, les dates de naissance, les numéros de téléphone, les mots de passe (chiffrés avec une technologie obsolète), les questions de sécurité ainsi que les e-mails de back-up. Des informations particulièrement utiles dans le cadre d'opérations d'espionnage, relève la presse américaine ; en effet, plusieurs millions de ces adresses de récupération appartiennent à des employés civils ou militaires de douzaines de pays dans le monde (dont plus de 150 000 Américains).

Plusieurs voix dans la communauté de la cybersécurité américaine estiment que ce vol de la base de données géante de Yahoo pourrait n'être qu'une opération de reconnaissance. « I*nactifs ou pas, un milliard de comptes utilisateurs et de mots de passe hachés constituent une mine d'or pour de futures attaques par phishing* », estime ainsi, dans les colonnes du *New York Times*, Oren Falkowitz, un ancien analyste de la NSA qui dirige désormais une start-up en cybersécurité, Area 1.

Yahoo et les fuites à répétition

Yahoo a dévoilé ce qui est à ce jour la plus vaste fuite de données connue il y a de cela 2 jours, après avoir été averti voici environ un mois par les autorités américaines qui disposaient d'échantillons des données dérobées. Yahoo indique ne pas savoir qui a compromis ses systèmes en 2013. Rappelons que le portail Internet a aussi été victime, en septembre dernier, d'un second piratage de sa base de données, remontant à 2014 et concernant environ 500 millions de comptes. Selon les premiers éléments communiqués par la société de Santa Clara, il s'agirait d'une attaque distincte, probablement menée par un service de renseignement étranger.

La révélation du vol de données massif qui frappe Yahoo intervient en pleine cyber-guerre froide entre les Etats-Unis et la Russie, suite aux attaques attribuées à cette dernière afin de déstabiliser le camp démocrate durant la récente campagne présidentielle. Le président sortant, Barack Obama, vient d'annoncer que les Etats-Unis avaient l'intention de riposter aux manoeuvres russes.

A lire aussi :

Fuite de données Yahoo : pourquoi les spécialistes tombent des nues

Verizon va réviser sa proposition de rachat de Yahoo

Piratage de Yahoo : des employés savaient dès 2014

crédit photo © igor.stevanovic / shutterstock