Piratage de Yahoo : des employés savaient dès 2014

Dès 2014, des employés de Yahoo savaient que leur entreprise avait été victime d'un piratage sophistiqué mené par un hacker téléguidé par un Etat étranger. C'est ce qu'indique la firme dans un document officiel déposé auprès du gendarme de la bourse américaine, la SEC (Securities and Exchange Commission). Sans toutefois préciser si l'information avait, à l'époque, été remontée jusqu'à la direction de la société.

Le portail Internet explique que la faille, reconnue publiquement le 22 septembre dernier, concerne « *au moins 500 millions de comptes utilisateurs* ». Les informations dérobées comprennent les noms, adresses e-mail, numéros de téléphone, dates de naissance, les mots de passe hachés (la plupart avec Bcrypt) et, parfois, les questions de sécurité et leurs réponses. Celles-ci sont tantôt chiffrées, tantôt en clair, précise Yahoo.

« *Notre enquête à date indique que les informations volées ne comprennent pas des mots de passe non protégés, des données de paiement ou des coordonnées bancaires* », ajoute la firme, qui reste toutefois prudente, admettant entre les lignes ne pas être encore totalement sûre du niveau de compromission de ses systèmes lors de cette attaque.

Cookies pour contourner les mots de passe

Yahoo précise avoir identifié un « *acteur sponsorisé par un Etat ayant eu accès au réseau de l'entreprise fin 2014* ». Sans toutefois donner d'indications sur son identité. Le portail assure qu'un comité interne, auquel participe un expert en analyse d'attaques informatiques, enquête sur l'étendue de la prise de conscience de cette intrusion en interne dès 2014. Par ailleurs, Yahoo reconnaît qu'un assaillant, probablement le même groupe de hackers, a très probablement créé des cookies qui ont pu lui permettre de « *contourner la nécessité d'entrer un mot de passe pour accéder à certains comptes d'utilisateurs ou informations sur ces comptes* ». Des phrases sibyllines qui peuvent laisser penser à des opérations d'espionnage découlant de la fuite de données…

Le 7 novembre, les autorités américaines ont par ailleurs remis aux équipes du portail des données issues d'un hacker prétendant détenir des informations sur certains comptes Yahoo. La firme, avec l'aide d'experts tiers, est en train d'analyser ses éléments, explique-t-elle dans son document remis à la SEC.

Le rachat par Verizon mis en danger

Yahoo explique que cette faille majeure dans sa sécurité se traduit pour l'instant par des dépenses d'environ un million de dollars, intégrées à son dernier trimestre fiscal clos le 30 septembre dernier. L'entreprise, qui n'avait pas d'assurance en matière de cybersécurité, s'attend toutefois à voir cette facture enfler au cours des prochains trimestres, du fait des investigations encore en cours. Par ailleurs, l'entreprise fait face à ce jour à 23 procès collectifs aux Etats-Unis, intentés par

des utilisateurs.

Surtout, l'affaire joue un rôle central dans le processus de rachat de Yahoo par Verizon (pour 4,8 milliards de dollars). En effet, la portail n'a reconnu publiquement la fuite de données que deux mois après avoir finalisé ses discussions avec l'opérateur. Et la fuite n'avait pas été mentionnée durant lesdites négociations. S'il s'avère que les dirigeants de Yahoo étaient au courant de ce qui reste à ce jour la plus grande fuite de données touchant une entreprise avant de parapher l'accord avec Verizon, ce dernier aurait un argument solide pour casser le deal ou – à minima – demander un rabais significatif. Le mois dernier, des dirigeants de l'opérateur ont déjà publiquement affirmé que la fuite de données diminuait la valeur de Yahoo. Le rachat du portail doit, en principe, être conclu en début d'année prochaine.

A lire aussi :

Piratage Yahoo : des critiques et des scénarios alternatifs

Espionnage de mails chez Yahoo : un programme existant customisé

Espionnage des e-mails : Yahoo pouvait-il refuser d'aider la NSA ?

Crédit photo : Neon Tommy via Visual Hunt / CC BY-SA