Yahoo : les données volées ont servi à fabriquer de faux cookies

Marissa Mayer a beau avoir fait une croix sur ses primes pour les redistribuer à ses salariés, la pilule reste difficile à avaler pour les utilisateurs de Yahoo. Dévoilées à l'occasion de la publication des résultats annuels du portail Internet, les conclusions du comité indépendant qui a enquêté sur la fuite de donnée massives qu'a connu le service en 2014 montrent que les équipes de Yahoo, au moins celles en charge de la sécurité et du juridique, étaient au courant, dès le mois de décembre de cette même année, du fait qu'un acteur « *sponsorisé par un Etat* » avait dérobé une copie de sauvegarde d'un fichier contenant des données personnelles d'utilisateurs (e-mails, téléphones et mots de passe hachés). Si le comité confirme ainsi de premières indications données par la firme dès novembre dernier, il ne se prononce pas sur le fait de savoir si les informations relatives à cette fuite ont été « *communiquées et comprises* » à l'extérieur de l'équipe de sécurité. Rappelons que c'est seulement en septembre 2016 que la firme a publiquement dévoilé sa mésaventure.

Plus grave : les données dérobées par ces hackers d'Etat en 2014 ont bien été activement exploitées. Pas moins de 32 millions de comptes ont en effet été victimes, en 2015 et 2016, de tentatives de détournement, via de faux cookies. Les enquêteurs confirment que certains de ces cookies détournés, depuis invalidés par Yahoo, sont reliés au même acteur sponsorisé par un Etat. Le portail ajoute que les comptes de 26 individus en particulier ont été pris pour cible par ces assaillants non identifiés, via une exploitation de l'outil de gestion de comptes maison. Ces personnes ont été averties de la tentative de détournement de leurs données. Comme l'a montré le hacking du directeur de campagne d'Hillary Clinton, John Podesta, les comptes mails individuels de personnalités peuvent renfermer des informations de grande valeur. En particulier pour un Etat souhaitant exercer un chantage sur ces personnes ou lancer une campagne de déstabilisation.

Ronald Bell se fait sonner les cloches

« *Bien que d'importantes mesures de sécurité supplémentaires aient été mises en place en réponse à ces incidents, il semble que certains cadres supérieurs n'aient pas bien compris ou enquêté et n'aient donc pas agi de façon suffisamment déterminée, au regard des connaissances que l'équipe de sécurité des systèmes d'information avait de l'affaire* », écrit Yahoo dans son rapport remis au gendarme des bourses américaines (la Securities and Exchange Commission). Les conclusions du comité d'enquête, qui parle de défaillances internes dans la communication, le management, l'enquête ou encore le reporting interne, coûtent certes à Marissa Meyer son bonus, mais elles se traduisent surtout par la démission (sans compensation) de Ronald Bell, le directeur juridique, qui porte donc le chapeau de ce fiasco.

Rappelons que Yahoo n'a publiquement reconnu cette fuite massive de données –environ 500 millions d'utilisateurs touchés – qu'après la mise en vente d'une copie de la base de données volée sur le marché noir du Web. Ce premier scandale en cachait en réalité un autre, puisque le portail a ensuite découvert un second vol de données, encore plus massif (environ 1 milliard d'utilisateurs cette fois). Cette seconde fuite, d'une ampleur inédite dans l'histoire d'Internet, remonte à août

2013, mais n'a été rendu publique qu'en fin d'année dernière, les autorités américaines ayant alors fourni au portail une copie des données exfiltrées à cette occasion. Le rapport du comité indépendant ne fournit pas d'information sur la façon dont ce vol massif de données a été perpétré.

32 millions de faux cookies

Yahoo enquête également sur une attaque contre certains de ses utilisateurs, passant par des cookies forgés par un hacker ou groupe de hackers non identifié. Ici, le comité d'enquête établit une relation entre cette activité malveillante et le hacking de 2014. « *Nous pensons qu'une partie de cette activité est reliée au même acteur sponsorisé par un Etat et soupçonné d'être à l'origine de l'incident de sécurité de 2014* », écrit Yahoo. De façon troublante, le portail semble indiquer que les 32 millions de comptes visés par ces faux cookies ne résultent pas tous d'une exploitation des données qui lui ont été dérobé en 2014.

Rappelons que les révélations sur ces fuites à répétition ont eu un impact très direct sur la valeur du portail, ce dernier ayant été contraint d'accorder 350 millions de dollars de rabais à son acheteur, Verizon. La transaction doit être bouclée au cours du second trimestre.

A lire aussi :

Des systèmes IT toujours compromis chez Yahoo ?

Fuite de données Yahoo : pourquoi les spécialistes tombent des nues

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

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