Piratage Yahoo : des critiques et des scénarios alternatifs

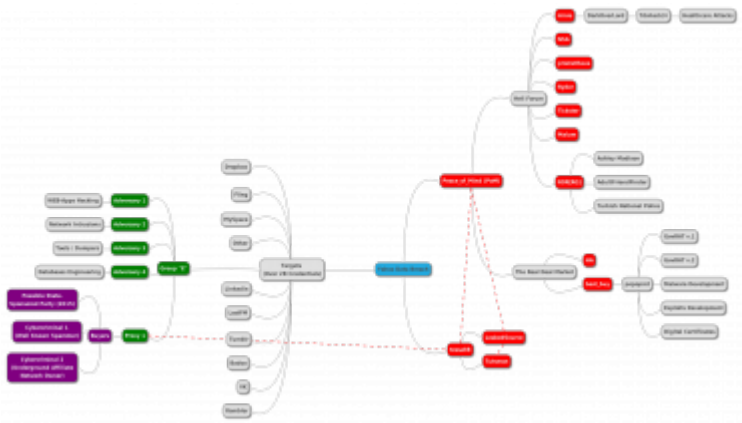
Après le piratage de plus de 500 millions de comptes, les langues se délient et les doutes surgissent autour de Yahoo. La première critique concerne les efforts menés par le site en matière de sécurité. A la mi-2012, Marissa Mayer dote l'entreprise d'une équipe dédiée à la cybersécurité. Cette dernière, appelée dans le milieu « *l'équipe de paranoïaques* », gagne ses lettres de noblesse et fait référence dans la communauté. Mais les relations entre Alex Stamos, patron de l'équipe et la CEO ne sont pas au beau fixe.

Il reproche à Marissa Mayer de ne pas prendre des mesures de sécurité basiques comme un reset automatique des mots de passe de l'ensemble des comptes, en cas de vol massif de données. Le manque de ressources financières et de mise en œuvre des politiques de sécurité proactive ont eu raison de la patience d'Alex Stamos qui a rejoint les rangs de Facebook.

Pas de parrainage étatique, mais des pirates d'élite

Les experts en sécurité ont de plus en plus de mal à admettre que le piratage de Yahoo soit lié à un Etat-nation. Juste après l'annonce du délit, des spécialistes émettaient des doutes sur cette affirmation. Pourquoi un Etat irait vendre une telle base de données ? Les attaques menées par des gouvernements ne se font pas dans un but lucratif et surtout sans publicité.

Une récente recherche de la firme ArmorInfo dresse un scénario plus traditionnel pour expliquer le vol de données. Selon elle, les serveurs de Yahoo ont été victimes d'un piratage par une équipe expérimentée de pirates. Il s'agirait du même groupe qui se cache derrière les offensives menées contre LinkedIn, MySpace, Tumblr, VK, etc. La société de sécurité dresse deux profils de ce groupe, il peut s'agir d'anciens membres du « Hell Forum » ou de blackhats originaires de l'Europe de l'Est (cf schéma ci-dessous)



Pour ArmorInfo, ce groupe communique par l'intermédiaire de deux porte-paroles connus sous les pseudo, Tessa88 and Peace_of_Mind. Ces derniers sont chargés de vendre sur le Dark Web des échantillons de comptes compromis. Autre élément souligné par InfoArmor, Yahoo aurait sous-estimé le volume de comptes dérobés, avec une compromission pouvant aller jusqu'à 1 milliard de

comptes compromis.

Une affaire politique et financière

En tout cas, l'affaire a pris une tournure politique, car 6 sénateurs réclament des comptes à Yahoo. Ils ne comprennent pas le retard « *inacceptable* » de communication de la part de Yahoo sur cet évènement de sécurité. L'intrusion date de l'année 2014, ce qui signifie que « *pendant 2 ans, des millions de comptes de citoyens américains ont été compromis* », rapportent les élus démocrates. Cette question de délai intéresse aussi la SEC. Le gendarme boursier a reçu lors de la volonté de rachat des activités web de Yahoo par Verizon des documents montrant que le portail n'avait pas connaissance de violation de son système d'information. Verizon a été averti seulement 2 jours avant la communication officielle de Yahoo. La SEC pourrait donc se pencher sur le timing et le libellé des documents de Yahoo.

A lire aussi :

Piratage de Yahoo : après la stupeur, le procès

200 millions de comptes Yahoo en vente sur le Dark Web

crédit photo © Lusoimages – shutterstock