02 mars 2017
Hacking

Un milliard de comptes Yahoo piratés : ce qu'il faut savoir si vous avez peur d'être concerné

Révélée au grand jour ces derniers mois, l'affaire des piratages des comptes mail de Yahoo ne cesse de prendre de l'ampleur, alors que le géant américain vient d'annoncer que près d'un milliard de comptes seraient concernés.

Avec Frédéric Mouffle
Avec Franck DeCloquement

Atlantico : Ce mercredi 14 décembre, Yahoo a révélé avoir subi en août 2013 un important piratage ayant compromis les informations d'au moins un milliard de comptes. Quelles sont les implications de cette nouvelle révélation, tant pour Yahoo que pour ses utilisateurs ?

Frédéric Mouffle : Ces révélations sont aujourd'hui admise par la société Yahoo ayant déjà été victime de ce piratage en 2013. Yahoo avait fait le choix d'utiliser des moyens obsolètes pour sécuriser le stockage des mots de passes des utilisateurs Yahoo, ne pouvait pas ignorer que l'algorithme MD5 utilisé était vulnérable depuis les années 2000. D'ailleurs d'autres grandes entreprises avait elle aussi, sous-estimer l'importance du choix de l'algorithme dont les failles sont pourtant connus et ont elle aussi (LinkedIn, Vtek, Myspace… subi les assauts des pirates.

Le problème pour les utilisateurs c'est que même en changeant votre mot de passe, vous n'aurez pas la garantie de voir vos login et mot de passe mis à disposition sur le Darknet ou Pastebin. Tant que la sécurité du stockage ne sera pas garantie, Yahoo risque de perdre beaucoup de ses utilisateurs, la confiance étant déjà bien entamée.

Nombre d'utilisateurs utilisent le même mot de passe pour l'accès a d'autres services en ligne ce qui signifie qu'une attaque par rebond est tous a fait envisageable. Ces révélations tombent on ne peut plus mal pour Yahoo qui en en phase de finalisation de cession pour un montant de 4.8 MDS à la société Verison. Actuellement, Vérizon, repreneur de la société investigue de son coté sur les causes de ce piratage et préviens déjà que ces problématiques graves auxquelles Yahoo doit faire face serait de nature à faire diminuer significativement la valeur de la société. Il est probable que l'on descende au-dessous des 3 MD$.

Franck Decloquement : Il y a un évidemment un risque non nul d'être concerné, dès lors que l'on est le dépositaire d'un compte Yahoo... Ces comptes contiennent des données personnelles confidentielles pouvant être liées aux mails que nous pouvons envoyer à des destinataires très divers. Au sein desquels on retrouve des écrits amicaux, certes, mais aussi des données à vocation professionnelle, des mails destinés à notre banque, *et cætera*...

Il est – dès lors – très important de savoir si ces données liées aux comptes utilisateurs ont été toutes corrompues. Pour le percevoir il faut être particulièrement attentif aux éventuels signes d'activités résiduelles suspectes sur ses comptes. Si les données ont effectivement été corrompues, la meilleure des choses à faire c'est de changer de mot de passe aussi radicalement et rapidement que

possible. Il est aussi pertinent de lier le moins possible les mots de passes d'une boite mail possiblement infectée avec ceux d'autres comptes, afin d'éviter la réplication frauduleuse des identifiants et mots de passe de proche en proche. C'est une technique simple et de bon sens, en plus d'être la seule à la portée de l'utilisateur lambda... Pour le reste, il appartient à l'opérateur de réagir en fonction de la nature de la menace et de la profondeur de l'attaque.

En sait-on davantage sur les hackers à l'origine de ce piratage massif de données ?

Frédéric Mouffle : Nous supposons, parmi les communiqués officiels et les diverses enquêtes menées aux Etats-Unis, qu'il y aurait eu 2 piratages massifs réalisés selon Yahoo, par deux groupes distincts. Le premier proche de services d'Etat, qui selon moi est peu crédible, au vu des failles présentes. Nul besoin d'être un service d'Etat pour ce type d'offensive, les bons outils et tout devient possible. Beaucoup plus probable : un groupe de cybercriminels baptisé Group E agiraient depuis les pays de l'Est.

La suspicion d'une attaque par un service d'Etat est peut-être une façon pour Yahoo d'obtenir une aide significative de l'Etat et de se poser plus en victime, recentrant le débat sur des problématiques géopolitiques espérant ainsi limiter l'impact de leur incompétence à sécuriser leur système d'information. Ce qui est sûr c'est que les données étaient en vente des 2013 sur le darknet.

Plusieurs piratages ont concernés Yahoo ces dernières années, en 2012 Yahoo avoue s'être fait pirater 450 000 comptes.

2013 : attaques via les cookies, plusieurs milliers d'utilisateurs voient leur boîte mail utiliser pour faire du spam.

2014 : Yahoo réinitialise les mots de passe expliquant qu'une de ses bases a été subtilisée chez un de ses services tiers.

2015 : des pirates accèdent aux serveurs de Yahoo et diffusent, via les services de régie publicitaire de Yahoo, des publicités pièges (attaque dite malvertising)

2016 : le site motherboard annonce avoir eu accès à 200 millions de comptes valide

Ce qu'on leur souhaite c'est de pouvoir mettre un terme à leurs problématiques de sécurité et proposer des services à la hauteur des autres grandes entreprises du même secteur.

Que sait-on aujourd'hui de cet événement vieux de deux ans ? Comment l'expliquer ?

Franck Decloquement : Cette affaire remonte en effet à deux ans, mais Yahoo n'a commencé à communiquer publiquement sur le sujet que ce jeudi 22 septembre 2016. Concrètement, il s'agit de la captation de 500 millions de comptes utilisateurs (mots de passe, identifiants, IP, profils de comptes utilisateur, identifications des numéros de téléphones, etc). Cela signifie que les données de ces comptes – noms, adresses, e-mails et boites mails, numéros de téléphones, comptes bancaires, liens avec d'autres utilisateurs, *et cætera* – ont été, selon Yahoo, captées indûment par un piratage massif de données personnelles. Et ceci, sur une très grande échelle… Les informations propres à des millions de comptes utilisateurs peuvent être potentiellement compromises à l'heure où nous rédigeons cet interview.

Yahoo, dans son communiqué, explique que l'attaque pourrait être le fruit d'une manœuvre étatique adverse, ou d'un acteur "parrainé" par une puissance étatique étrangère... Yahoo étant une entreprise américaine, il est donc sous-entendu dans cette communication institutionnelle qu'il pourrait s'agir d'une intrusion Russe ou Chinoise… C'est du moins ce que l'on peut comprendre entre les lignes, en lisant à mi-mot les première déclarations des communicants de Yahoo.

Pour tous les utilisateurs, cette intrusion et ce vol de données à très grande échelle sont susceptibles de se traduire par des agissements suspects sur leurs comptes personnels Yahoo, des actions hiératiques notamment, et dans la durée Cela inclut notamment la réception ou l'envoi de mails suspects n'ayant aucun rapports avec les communications du propriétaire du compte, des vols d'informations bancaires, etc... Il est, par conséquent, primordial de réinitialiser immédiatement les mots de passe de ces comptes si cela n'avait pas été fait depuis les deux dernières années d'utilisation.... Dans un article publié sur le *New York Times* relatif à cette affaire, Alex Holden – fondateur d'une société spécialisée en cyber-sécurité – explique que les informations volées chez Yahoo sont désormais en libre circulation sur ce qu'il appelle le "web souterrain". Il s'agit bien entendu ici du *"Dark Web"* ou transitent et s'échangent schématiquement, des millions de tera octets de données volées ou extraites frauduleusement, par les pirates du monde entier... Selon lui, il s'agit d'une des *"plus grandes violations de la vie privée des gens connue jusqu'à présent."* C'est effectivement l'une des plus grosses opérations frauduleuse de captation de comptes utilisateurs et d'adresses contemporaines. Nous n'avons cependant pas plus d'éléments à l'heure actuelle.

Plusieurs hypothèses peuvent pourtant être avancées. La première d'entre elles est c'est celle d'un État qui ferait appel aux services de hackers spécialisés, doués de grandes compétences techniques pour participer à ce vol de données globalisé. C'est celle avancée par le communiqué de Yahoo. Une autre hypothèse, qui n'est pas explorée dans ce communiqué pourrait tourner autour du rachat par Verizon de Yahoo. Verizon cherche en effet à racheter Yahoo. Et la proposition d'acquisition du célèbre opérateur américain est, jusqu'à présent cotée à 4.8 milliards de dollars. Il va de soi que ce prix de vente pharaonique de Yahoo risque d'être très fortement revu à la baisse, compte tenue de cette annonce d'intrusions massive dans le dispositif sécuritaire de Yahoo. À ce titre, rien n'exclut la possibilité d'une opération de "guerre de l'information", ou d'une opération capitalistique agissant sur la réputation, et visant à faire chuter le prix de l'opérateur convoité par Verizon… Rien n'est à exclure en la matière.

Un audit très complet a sans aucun doute été réalisé pour agréer le prix estimatif de cette vente, à auteur des 4.8 milliards de dollars proposés pour le rachat de Yahoo. Ces audits ont lieu avant ou pendant les opérations de rachats et se penchent évidemment sur la dimension sécuritaire. Tout particulièrement dans le cadre d'un opérateur où il est d'importance vitale de garantir la sécurisation de l'infrastructure technique, au risque de perdre en route la confiance des utilisateurs des services en ligne proposés par la marque. Il est probable que cette captation frauduleuse, qui date de 2014, ait été initialement découverte par Yahoo, puisque volontairement occultée ensuite pour éviter "l'onde de choc réputationnelle". Verizon a pu découvrir cette action massive de piratage justement à la suite d'un audit de sécurité des installations techniques de la société Yahoo qu'elle souhaite acquérir, opération diligentée dans l'hypothèse d'un prochain rachat. Il est important de garder à l'esprit que des spécialistes surveillent quotidiennement le *Dark Web* – un peu comme l'on pourrait écouter les signaux d'un sous-marin en eaux troubles – pour détecter à temps ce qui peut en émaner et impacter les firmes, les utilisateurs ou les États.

Quels sont les enjeux consécutifs à une telle faille de sécurité ? Qu'en est-il concrètement, tant pour les consommateurs que pour l'entreprise concernée, ici Yahoo ?

Franck Decloquement : Le premier enjeu est évidemment sécuritaire… L'un des plus grands opérateurs mondiaux s'est fait dérober à son insu, 500 millions de comptes utilisateurs… et possiblement les millions de données qui s'y rattachent. C'est tout simplement gigantesque si toutefois les déclarations de l'opérateur s'avèrent exactes. Il s'agit ni plus ni moins d'une crise majeure pouvant très largement impacter la confiance que portent les clients des services en ligne de Yahoo. Rappelons-nous de l'affaire ORANGE, avec laquelle il est possible de dresser un rapide parallèle : Après avoir sondé le *Dark Web*, il s'est avéré que le nombre de comptes volés et déclarés par l'opérateur Français était très largement en-deçà de la réalité. Les pertes occasionnées étaient beaucoup plus importantes en vérité. Hélas, pourrions-nous dire.

Très souvent, pour ne pas mettre en péril la valorisation de son activité, un opérateur victime d'une telle attaque en minimise les réalités et les conséquences... Il n'en reste pas moins que cela traduit et soulève de nombreux questions : sécurisation des services d'une part, mais également continuation de l'activité dès lors que l'on sait les comptes utilisateurs possiblement corrompus. Dans cette situation, on demande aux utilisateurs de changer leurs mots de passe, *a minima*, de surveiller les activités frauduleuses qui pourraient s'effectuer à travers leur compte personnel. Il est important qu'ils soient attentifs à tous les signes susceptibles d'être interprétés comme la poursuite d'une opération offensive frauduleuse, depuis leur compte mail, visant à instrumentaliser leurs informations personnelles (mail amicaux, identifications bancaires, informations confidentielles, etc). Par conséquent, une telle faille de sécurité ne peut pas être anodine et ses conséquences peuvent s'étaler sur plusieurs années.

N'oublions pas que les informations récupérées peuvent-êtres vendues à des tiers. C'est une situation susceptible de concerner tout à chacun. Cependant, une telle agression numérique – si elle devait être le fait d'un État à la manœuvre – viserait prioritairement des cibles précises à travers la masse des données recueillies. En outre, quand un État se lance dans ce type d'action régalienne, tout l'intérêt de la démarche est de faire cela en secret, sans éveiller les soupçons... De manière à pouvoir se rendre maître des choses, et d'agir impunément sur la durée à l'encontre de cibles prédéterminées. Le fait que l'information ait ainsi fuité et soit relayée de la sorte, et pour partie possiblement commercialisée sur le *Dark Web* (ce qui reste à confirmer), ne fait pas parti des "habitudes" d'actions ciblées des services d'États quand ils s'essayent à ce type d'opération. Ces éléments de réflexion pourraient partiellement décrédibiliser l'hypothèse d'une opération étatique. Mais il faut toutefois rester extrêmement prudent en la matière. Comparaison n'étant pas raison.

Dans l'ordre des scénarios rocambolesques possible, on pourrait également faire l'hypothèse d'une opération de "guerre de l'information" opposant deux États en rivalité de puissance, dont l'activité secrète affleure à cette occasion. Gardons aussi à l'esprit que Verizon, qui projette de racheter Yahoo, a été mis en cause dans l'affaire Snowden. Il pourrait tout à fait s'agir ici d'un signal "amical" facétieux envoyé par une puissance étrangère à cet opérateur américain – et les services d'État qui la soutienne – à la façon "d'un prêté, un rendu"… Pour l'heure, et faute d'informations complètes et sérieuses, on ne peut que divaguer en la matière, à l'instar d'un scénariste de fiction.