LesEchos.fr

Date : 12/10/2016
Heure : 00:32:28
Journaliste : Nicolas Richaud/ Anais Moutot

www.lesechos.fr
Pays : France
Dynamisme : 0

Visualiser l'article

Yahoo! Retour sur le « hack » du siècle

Le « Yahoo!gate » sonne comme la énième fausse note du règne de la PDG du groupe, Marissa Mayer. - Photo Bloomberg

Le 22 septembre dernier, le groupe californien révélait avoir été victime d'un piratage massif de données, remontant à 2014. Une attaque imputée à « une entité parrainée par un Etat », mais qui pourrait bien être le fait de hackers isolés. Un épisode ravageur pour sa réputation.

Qui a piraté plus d'un demi-milliard de comptes chez Yahoo! ? C'est la devinette à laquelle tente de répondre toute la Silicon Valley depuis que l'entreprise californienne a annoncé, il y a bientôt trois semaines, qu'au moins la moitié de ses utilisateurs avaient été victimes de l'attaque informatique la plus importante jamais rendue publique par une société. Noms, adresses e-mail, numéros de téléphone, mots de passe « hachés » par le biais d'un algorithme et, dans certains cas, questions et réponses de sécurité prévues en cas d'oubli du mot de passe : le butin est copieux. L'ex-fleuron du Web des années 1990 évoque une intrusion perpétrée fin 2014 par une entité « *parrainée par un Etat* ». S'il ne précise pas lequel, tous les regards se tournent

vers la Russie, après son implication supposée dans plusieurs affaires récentes de piratage aux Etats-Unis : plate-forme du Parti démocrate en juillet, bases de données d'électeurs en Arizona et dans l'Illinois en août, e-mails de l'ancien secrétaire d'Etat Colin Powell en septembre...

Mais de nombreux experts en cybersécurité contestent cette hypothèse. *« I Ils ne veulent pas apparaître comme ayant été négligents. Si c'est un Etat plutôt qu'un petit groupe de hackers qui est responsable de la fraude, ils espèrent que cela les rendra moins coupables »* , estime Troy Hunt, un expert en cybersécurité travaillant chez Microsoft et créateur du site Have I Been Pwned (« Ai-je été hacké ? »), un service gratuit qui permet d'être prévenu en cas de piratage de son compte. Plutôt qu'une attaque directe provenant d'une entité liée à un Etat, plusieurs experts estiment, eux, que l'intrusion a été commise par un groupe de cybercriminels russes et/ou d'Europe de l'Est. Ils remontent pour cela à une petite annonce publiée sur The Real Deal au début du mois d'août, proposant un paquet de données issues de comptes Yahoo!. The Real Deal est l'une des places de marché interlopes du « darknet », cette composante d'Internet non indexée par les moteurs de recherche classiques (Google Search, Qwant, Yahoo!...), à laquelle tout un chacun peut se connecter de manière anonyme grâce à des logiciels spécifiques comme Freenet, I2P ou, le plus connu d'entre eux, Tor. Avec AlphaBay, The Real Deal fait partie de ces « marketplaces » qui ont pris la suite de Silk Road, alias « l'eBay de la drogue », après son démantèlement par le FBI il y a trois ans.

L'auteur de cette petite annonce ? Peace, un revendeur de données qui se dit russe dans une interview faite via messagerie privée par le magazine « Wired ». Le personnage est, semble-t-il, lié à de nombreux autres faits d'armes sur la plate-forme - revente au mois de mai de données de plus de 100 millions de comptes LinkedIn, 360 millions de comptes Myspace et 65 millions de comptes du réseau de blogs Tumblr (propriété de Yahoo!), puis, en juin, de 100 millions de comptes VK, le « Facebook russe », et de 33 millions de comptes Twitter, y compris celui de Mark Zuckerberg, dont le mot de passe était « dadada »...

La prudence est cependant de mise tant l'inconnu et l'anonymat sont la norme sur le « darknet ». La problématique est la même lorsque des internautes se réclament du mouvement des Anonymous. Impossible de savoir qui et combien de personnes se cachent derrière le masque de Guy Fawkes : deux personnes opérant depuis leur garage ou plusieurs centaines. Ici, il en va de même avec Peace. Le cabinet de cybersécurité InfoArmor, qui vient de rendre un rapport sur le sujet, penche cependant pour un individu qui aurait obtenu la base de données Yahoo! par l'intermédiaire de Tessa88. Derrière ce pseudonyme féminin se cacherait un autre jeune homme vivant dans le sud de la Russie, comme Peace, selon Vitali Kremez, expert du cabinet de cybersécurité Flashpoint Intel.

En mai, Peace aurait contacté Tessa88 pour lui proposer un *« partenariat »* , selon InfoArmor. Ce dernier lui envoie alors les données, et Peace les met en vente, apparemment sans l'accord de Tessa88.

Des données vendues au rabais

Dans une interview à Motherboard, celui-ci assure qu'il les avait fournies à Peace uniquement pour qu'il les analyse. Au final, la majorité des données Yahoo! correspond à *« des comptes inactifs, supprimés ou inexistants »* , selon InfoArmor. Leur prix indique d'ailleurs clairement que ces données sont vendues au rabais - 3 bitcoins, soit environ 1.800 dollars pour 200 millions de comptes, un tarif très bas et *« qui ne peut s'expliquer rationnellement »* , note InfoArmor. Il faut dire que les bases de données auparavant mises en ligne par Tessa88 n'étaient pas de premier choix. Celles des comptes du service de stockage Dropbox, qu'il prétendait avoir obtenues en avril, correspondaient en fait à celles de Tumblr, selon LeakedSource, un site qui archive ce type de fuites et propose un service payant de recherche. D'après InfoArmor, Peace, dont la réputation a pâti de cette collaboration avec Tessa88, a tenté de se débarrasser au plus vite de son « pack » Yahoo! en le bradant.

Les liens s'enchevêtrent et sont difficiles à démêler entre les deux affaires. Les données Yahoo! mises en ligne par Peace correspondent à un plus petit nombre de comptes que le chiffre annoncé par Yahoo! - 200 millions contre 500 millions - et datent de 2012, non de 2014. La semaine dernière, Bob Lord, le responsable de la sécurité chez Yahoo!, a affirmé que les faits revendiqués par Peace n'étaient pas confirmés ni liés au piratage de 2014, mais qu'ils avaient conduit son service à enquêter et à découvrir une autre faille. Yahoo! aurait-il déjà été piraté massivement auparavant ? *« On ne saura sûrement jamais la vérité »* , tranche Troy Hunt. Car la chaîne de récupération et de distribution des données est extrêmement complexe et compte moult intermédiaires. Il y a d'abord les hackers, qui trouvent des failles dans les systèmes de protection logiciels des serveurs, puis les revendent sur le « darknet » à d'autres pirates cherchant à accéder à des bases de données.

Ces derniers passent ensuite régulièrement par des intermédiaires comme Peace pour revendre les lots. *« Chacun a des compétences différentes, comme dans la vraie vie, entre un développeur informatique et un commercial »* , explique Troy Hunt. Ils se chargent d'abord de faire des « deals » exclusifs pour des acheteurs cherchant des cibles spécifiques puis publient le tout publiquement sur le « darknet » à un tarif discount. De quoi récolter des sommes entre 10.000 et 20.000 dollars par lot, selon les dires de Peace rapportés par « Wired ».

Leurs acheteurs sont en majorité des cybercriminels qui savent en faire un usage protéiforme. Ils peuvent ainsi profiter du fait qu'une majorité des internautes optent pour un seul et même mot de passe pour se connecter à différents services. D'un mot de passe LinkedIn, ils peuvent ainsi aboutir facilement à un compte PayPal ou Amazon, par exemple. *« Cela peut aussi donner lieu à de l'usurpation d'identité et à la création de faux passeports »* , note Marc-Antoine Ledieu, avocat au barreau de Paris et spécialiste des technologies de l'information. *« Certains cybercriminels achètent ces données en vue de procéder à des attaques de type "ransomware"* [un logiciel malveillant qui chiffre les données présentes sur un ordinateur en vue de demander une rançon à l'utilisateur ciblé pour les rendre de nouveau accessibles, NDLR] *sur des organisations professionnelles et des particuliers visés avec précision grâce aux données acquises »* , précise Luc d'Urso, patron de Wooxo, éditeur français de solutions de protection des données. Des géants de la tech tels que Facebook ou Amazon peuvent aussi chercher à récupérer ce type de données, selon Troy Hunt et Didier Perrot, PDG d'inWebo, une entreprise fabriquant des outils d'authentification multifactoriels. Leur objectif ? Comparer les adresses e-mail et mots de passe de la base de données hackée avec la leur et prévenir rapidement les utilisateurs qui utilisent des mots de passe identiques pour qu'ils les changent... et éviter le piratage de leurs comptes.

Ce « hack » hors norme sonne, en tout cas, comme la énième fausse note du règne crépusculaire de Marissa Mayer. Yahoo! risque de devoir en plus faire face à une série de nouvelles questions, après les informations dévoilées dans la presse ces derniers jours : d'après le « New York Times », la société aurait utilisé son filtre pour les spams et la pédopornographie pour scanner les e-mails de ses utilisateurs à la recherche de la signature d'une organisation terroriste. Reuters évoque, lui, la création d'un logiciel spécifique sur ordre du FBI ou de la NSA...

Une sécurité défaillante

Cet été, le groupe a conclu la vente de la majorité de ses actifs (moteur de recherche, régie publicitaire, sites d'information) à Verizon pour 4,8 milliards de dollars, après des mois de négociation et d'enchères. L'opération doit normalement être conclue début 2017 mais certains termes du contrat, dont le prix, pourraient être remis en question - selon le « New York Post », Verizon chercherait déjà à obtenir un rabais de 1 milliard de dollars -, en fonction des réponses qu'apportera Yahoo! à plusieurs interrogations non élucidées : pourquoi la fraude, qui remonte à 2014, n'a-t-elle été découverte que maintenant ? La direction a-t-elle caché le piratage à son

repreneur ? Les sénateurs américains réclament des explications à l'entreprise, l'un d'eux souhaitant même l'ouverture d'une enquête du gendarme boursier américain (SEC).

Dans le « Yahoo! gate », la problématique du degré de défaillance du groupe est au centre de l'attention. Entre Marissa Mayer et les « paranoids », surnom donné en interne aux équipes de sécurité informatique du groupe (car rémunérées pour être paranoïaques), les relations étaient à couteaux tirés. La PDG aurait cherché à raboter le budget de ce département en raison du trou d'air traversé par son groupe. *« Ce sont presque toujours des groupes en difficulté qui se sont fait pirater ces derniers mois, que ce soit Myspace ou Yahoo!. Ils ne peuvent plus faire les dépenses nécessaires pour tester leur sécurité informatique tous les jours »* , souligne Frans Imbert-Vier, patron d'Ubcom et consultant en cybersécurité. Pour couronner le tout, Marissa Meyer aurait été informée de l'affaire début juillet mais aurait refusé qu'un e-mail soit envoyé à tous les utilisateurs de Yahoo! pour qu'ils réinitialisent leurs mots de passe, selon le « Financial Times ». Une pratique pourtant considérée comme le minimum syndical après un piratage de masse, et qu'a d'ailleurs employée LinkedIn il y a près de cinq mois. Mais, d'après le « New York Times », la patronne de Yahoo! craignait que cela effraie les utilisateurs et que ces derniers désertent plus encore les services de son groupe en décrépitude... Pas sûr que l'hémorragie s'arrête de sitôt.

Les points à retenir
La moitié au moins des utilisateurs de Yahoo! ont été victimes de l'attaque informatique la plus importante jamais rendue publique par une société.

La chaîne de récupération et de distribution des données, extrêmement complexe, ne permet pas de déterminer à l'heure actuelle si ce piratage est le fait d'un Etat, d'un groupe de hackers ou d'un élément isolé.

Quoi qu'il en soit, ce « Yahoo! gate » pose plusieurs interrogations : pourquoi cette fraude, ancienne, n'a-t-elle été découverte que maintenant ? Le piratage a-t-il été caché par la direction, alors que Yahoo! mettait en vente la majorité de ses actifs ?