Hacking, une étude de cas.

Les attaques de Yahoo.

Présenté à

M. Claude D'Amours

Dans le cadre du cours de

CSI2911F

Pratique professionnelle

Par

Maxime Côté-Gagné (8851539)

Stéphane Rurema (8862803)

Université d'Ottawa

Le 6 avril 2016

Résumé

Le sujet de ce projet était d'étudier un cas d'hacking et voir les conséquences à long et court terme que cela a amenées sur les différentes personnes touchées. Nous avons donc choisi de parler de la compagnie Yahoo et des deux attaques subies qui ont touché un grand nombre de leurs utilisateurs.

Abréviations

AOL - America Online

HTTP - Hypertext Transfer Protocol

HTTPS - HyperText Transfer Protocol Secure

IP - Internet Protocol

MD5 - Message Digest 5

FBI - Federal Bureau of Investigation

FSB - Service fédéral de sécurité de la fédération de Russie

2FA - Two-factor authentication

SMS - Short Message Service

Table des matières

Introduction

Tout d'abord, il faut commencer par définir ce que signifie le terme « hacking » avant de pouvoir en parler. Selon le Larousse en ligne, un hacker est une « personne qui, par jeu, goût de défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique. » [7] Il existe une quantité immense de cas d'hacking et le nombre de victimes ou personnes touchées par ces attaques peut varier d'une dizaine à des millions de gens. Pour ce projet, nous avons décidé de parler d'un des cas les plus importants, vu qu'il a touché des milliards d'utilisateurs, il s'agit du hack de la compagnie Yahoo!. Fondé en 1994 par Jerry Yang et David Filo, Yahoo! est un fournisseur de services internet. Le site internet offre plusieurs services comme un moteur de recherche, service de messagerie, annuaire et une branche d'actualité. Seule la partie du service de messagerie avait été touché dans les attaques dont nous allons discuter. Même si la compagnie a perdu assez d'influences de nos jours, il ne faut pas oublier qu'ils ont été pendant un long moment une grande force dans le monde informatique, et faisait de la compétition avec Google [5].

Développement

Yahoo! se fait attaquer

Tout d'abord, la compagnie Yahoo! n'a pas subi une attaque mais bien deux attaques qui ont pris quelques années avant d'être annoncée au public. Le 22 septembre 2016, Yahoo! annonce avoir été la victime d'une attaque qui a touché 500 millions de ses utilisateurs, à ce moment, ils disent que les attaquants sont hors de leur service, mais rien n'est dit sur les moyens utilisés pour voler les informations des comptes [1]. Après cela, le 14 Décembre de la même année, il révèle une autre attaque qui a eu lieu en 2013, donc avant la première, qui aurait touché 1 milliards

d'utilisateurs. C'est aussi à ce moment, qu'il dévoile que l'attaque de 2014 a surement été réalisé à partir de faux cookies, pour obtenir les informations de comptes mais cette attaque (qui a eu lieu en 2013), est différente et n'a aucun rapport avec celle de 2014[2]. Après avoir dévoilé ces attaques, Yahoo! a contacté toutes les personnes qui étaient touché de changer leur mot de passe le plus rapidement possible et d'utiliser plusieurs moyens de vérification de compte. Selon la compagnie, la seule information qui a été volé lors des attaques était : nom, date de naissance, adresse, numéro de téléphone, mot de passe (crypté/haché), émail, question secrète et sa réponse. Aucune information bancaire n'aurait été volé et aucun mot de passe non crypté, mais cela n'empêchait pas aux hackers d'accéder aux comptes et de voir toute l'information reliée. Yahoo! fut racheté par Verizon au prix de 4.48 milliards de dollars en juin 2017, même si Verizon était conscient des attaques qui venait d'être annoncé, ils ont quand même gardé leur offre d'acheter la compagnie. Cependant, le premier prix annoncé était 4.8 milliards, donc 320 millions de plus que le prix final, à cause des attaques de 2013 et 2014. La raison pour laquelle Verizon voulait acheter Yahoo! était qu'avec leur précédent achat de AOL (America Online) et Yahoo!, il comptait créer une compagnie pour développer leur marché de télécommunication [8]. Bref, après son achat, en Octobre 2017, Verizon annonça que leur recherche prouvait que tous les comptes des utilisateurs existants lors de l'attaque de 2013 ont été compromis, ce qui signifie qu'au lieu des 1 milliards annoncés, il s'agissait de 3 milliards. Ainsi, les autres personnes qui n'était pas inclus dans le premier diagnostic furent contacter pour renforcer la sécurité de leur compte et vérifier les possibles fuites d'informations [3].

Méthodes Utilisées

Spear-Phishing

L'incident survenu en août 2013 a pu être réalisé à l'aide d'une méthode d'hacking très répandue, le spear-phishing. Le spear-phishing ou le harponnage est une dérivée de l'hameçonnage, mais contrairement à ce dernier, la seule différence entre ces deux techniques de l'ingénierie sociale est le nombre d'utilisateurs touchés par ce message. Dans le cas d'un hameçonnage traditionnel, le ou les messages vont être destinés aux plus grands nombres de personnes possibles et pour le cas d'un harponnage, il sera spécifique pour des personnes sélectionnées par le responsable. Ce message peut prendre diverses formes, mais la plus connue est un email usurpateur dont on demandera des renseignements personnels, de cliquer sur un lien ou bien de télécharger un fichier. En d'autres mots, c'est une arnaque. [9] Il peut aussi être très difficile à distinguer d'un vrai email, parce que dans la plupart des cas ils seront très bien réalisés par le responsable pour que la victime ait le plus de confiance en ce message. Celle utilisée pour le cas de Yahoo! lors de l'incident de 2013 fut un simple email envoyé à un responsable de la sécurité chez Yahoo! [10] qui aurait usurpé l'identité d'un quelqu'un d'importance chez Yahoo!, nous ne savons pas qui est la personne dont l'identité a été usurpé ou le nombre d'employés touchés par cette technique lors de cet incident. Cet email aurait réussi à faire croire à l'employé qu'il devait télécharger un fichier pour faire une mise à jour connexe en arrière-plan. En réalité ce fichier aurait laissé place à l'installation d'une *backdoor* par l'hackeur sur les serveurs de Yahoo! sans que l'employé se rende compte de ce qu'il venait de se passer. La *backdoor* créée aurait donner la chance à l'hackeur d'avoir accès à l'outil permettant la gestion des comptes utilisateurs de Yahoo!, ce qui est en d'autres mots avoir accès à toutes les informations personnelles des utilisateurs, donc la base de données contenant ces informations. Yahoo! a tout de même précisé que les données bancaires n'ont pas été touchées par cette intrusion dut au fait qu'elles étaient stockées dans une autre base de données. L'efficacité de

cette technique peut s'avérer très efficace si les personnes l'utilisant sont très futées malgré qu'elle demande un attaquant sophistiqué et déterminé pour qu'elle soit parfaitement exécuté. Pour ce cas, elle fut très efficace, car l'intégralité des comptes Yahoo! furent touchés.

Vol par cookie

Selon les résultats des investigations réalisées par Yahoo! et les autorités concernées, l'incident de 2014 a été réalisé à partir d'un vol par cookie. [11] Les cookies ou les témoins de connexions sont un protocole de communication HyperText Transfer Protocol(HTTP) via un navigateur internet tel que Google Chrome, Mozilla Firefox, etc. Ces témoins peuvent renfermer des données des utilisateurs qui visitent un site web. Ces données peuvent être une adresse IP (Internet Protocol) qui permet de localiser et de distinguer les ordinateurs visitant un site internet ou bien encore seulement pour enregistrer des données personnelles d'un utilisateur tel que son identifiant de connexion, son mot de passe et des d'autres détails à son propos. Dans la plupart des cas, un cookie sera utilisé par un site web dans le but d'enregistrer les informations de connexions de l'utilisateur pour une prochaine session. Pour qu'un vol par cookie soit réalisable, il faut que le site internet en question ait une connexion internet non sécurisé ou bien qu'elle ait une connexion sécurisée et cryptée (HyperText Transfer Protocol Secure(HTTPS)) non parfaitement réalisé, donc elle posséderait une faille. Chez Yahoo! en 2014, le site n'était pas entièrement sous une connexion dîtes HTTPS ce qui a laissé place à un hackeur la possibilité d'intercepter les connexions effectuées à l'aide d'un cookie et de les falsifier. Même si les mots de passes étaient hachés, il était tout de même possible à un hackeur d'utiliser les faux cookies pour se connecter aux comptes touchés par ce type de vol. L'efficacité de ces méthodes dépends du nombre d'utilisateurs qui décident d'enregistrer leurs informations sur leur ordinateur à l'aide d'un cookie lorsque demandé. Pour le cas de Yahoo!, un demi-milliard de comptes furent touchés par cette méthode utilisée en 2014.

[12] Ce n'est pas autant que l'attaque réalisé en 2013 à l'aide d'un harponnage par email, mais c'est tout de même énormément d'informations personnelles qui ont été dérobées.

Encryptions des données

C'est quoi le hachage?

Le hachage est une fonction à sens unique utilisé en informatique qui consiste à convertir une chaîne de données en une autre chaîne de caractères aléatoires dépendant l'algorithme qui est utilisé. Cette nouvelle chaîne créée est appelée *hash* en anglais. [13] En temps normal, les informations hachées ne peuvent pas être converties au texte brut d'origine sauf si l'algorithme a été cracké ce qui permettrait d'effectuer une reconversion. Peu importe l'algorithme utilisé pour crypter les données, un hackeur trouvera toujours une façon de la compromettre.

MD5:

L'algorithme Message Digest 5(MD5) est une fonction de hachage cryptographique créé par Ronald Rivest en 1991. Elle consiste à faire 4 fois 16 itérations de la chaîne de données qui générera un hash en hexadécimal de 32 caractères quel que soit la taille de la chaîne de données et comme le but d'une fonction de hachage, les données cryptées en MD5 ne peuvent pas, en théorie, se faire cracker. [14] En 1996, une faille a été découverte dans l'algorithme mettant alors cette méthode de hachage obsolète pour toute utilisation en cryptographie ou en cyber sécurité. Cependant certains vont encore utiliser cet algorithme malgré le fait qu'il existe plusieurs façons de découvrir les données qui ont été haché à l'aide de cette méthode. Yahoo! est un de ceux qui ont décidé d'utiliser cette technique pour crypter les mots de passes de ces utilisateurs dans leur base de données malgré la menace des attaques par force brute qui existait déjà lors de l'incident d'août 2013.

Bcrypt:

L'algorithme Bcrypt est une autre fonction de hachage basé sur l'algorithme Blowfish créé en 1999 et utilisé par Yahoo! depuis 2014. [1] Elle a l'avantage d'être une fonction adaptative, ce qui la permet d'augmenter son nombre d'itérations pour la rendre plus lente et ainsi plus résistante à des attaques par force brute malgré l'augmentation de la puissance de calcul des ordinateurs de nos jours. Comparativement à l'algorithme MD5, Bcrypt n'est, pour le moment, toujours pas craqué à ce qu'on sait, ce qui veut dire que pour l'incident de Yahoo! par vol de cookies en 2014, les attaquants ne pouvaient techniquement pas revenir à la forme normale des données cryptées, mais ils pouvaient encore utiliser les cookies falsifiés pour prendre contrôle des comptes utilisateurs touchés par cette attaque. Aujourd'hui, l'algorithme est toujours présent pour crypter les données des utilisateurs, surtout les mots de passes, car elle reste une protection avancée contre les techniques avancées pour cracker des mots de passes.

Les motivations derrières ces deux cybers attaques

Pour ce qui en ait des motivations et des responsables derrières ces deux hacks, les éléments restent assez flous. En mars 2017, quatre suspects se sont fait inculpés par le département américain de la Justice pour le piratage de Yahoo! en 2014. D'après le FBI, deux agents du FSB sont en cause pour avoir recruté des cybercriminels pour infiltrer le site Yahoo!. [15] À ce jour, aucune information n'a été trouvé pour le plus gros incident, celui de 2013.

D'après les autorités américaines se chargeant des deux cas de piratage de Yahoo!, plus précisément le FBI [16], les responsables auraient décider de s'attaquer à Yahoo! à cause de sa grande importante base de données. Elle contient beaucoup d'informations personnelles dû à son grand nombre de comptes, plus de trois milliards d'utilisateur ayant chacun un email, un nom, un

mot de passe, une adresse, etc. Ces informations pouvant être recueillis pour être utilisés pour, par exemple, une usurpation d'identité, essayer de soutirer de l'argent à ces personnes ayant un compte compromis ou encore pour essayer de faire une attaque de force brute avec les mots de passes contre un site internet ou une application. De plus, l'outil de gestion des comptes utilisateurs de Yahoo! permettant d'avoir accès à la totalité de la base de données peut être une des motivations des hackers pour avoir fait cette action en août 2013.

Conclusion

Pour conclure, Yahoo! a été victime de la plus grande cyberattaque que le monde a connu dont la totalité de ses utilisateurs ont été victimes. Soit plus de 3 milliards de comptes ont été touchés par l'attaque de 2013 effectuée par un email qui est en grande partie une erreur humaine dû à notre facilité à se faire manipuler ou pour ce cas, se faire arnaquer, et plus de 500 millions autres se sont fait avoir par les cookies falsifiés lors de l'incident de 2014 qui est encore une autre erreur humaine. Ces deux hacks ont eu des conséquences sur le prix de ventes de Yahoo! lors du rachat par Verizon d'une marge considérable. Yahoo! n'est pas la seule entreprise à se faire pirater, par exemple, Equifax, une entreprise de crédit très importante, en a été victime en automne 2017 [17], et même si des protections contre ce type d'attaque sont mise en place par les entreprises, les pirates informatiques trouveront ont moyens de parvenir à ces fins. Bref, en tant que consommateur le meilleur moyen de se protéger contre de telle attaque reste d'avoir des mots de passes variés et compliqués pour nos différents comptes et, si possible, d'utiliser la vérification à deux étapes(2FA) qui nous demande un code lors d'une connexion, en plus de notre mot de passe, que l'on reçoit par un message texte(SMS) ou sur une application dédiée.

Références

[1] «Yahoo Security Notice September 22, 2016», Yahoo, https://help.yahoo.com/kb/account/sln28092.html, consulté le 11 Mars 2018.

[2] «Yahoo Security Notice December 14, 2016», Yahoo, https://help.yahoo.com/kb/account/SLN27925.html, consulté le 11 Mars 2018.

[3] «Yahoo 2013 Account Security Update FAQs», Yahoo, https://ca.help.yahoo.com/kb/SLN28451.html?impressions=true, consulté le 11 Mars 2018.

[4] «Yahoo Security Notices», Yahoo, https://help.yahoo.com/kb/account/sln27927.html, Consulté le 25 Mars 2018.

[5] «Yahoo! American Company», Encyclopaedia Britannica, https://www.britannica.com/topic/Yahoo-Inc, consulté le 22 Mars 2018.

[6] «L'Historique de Yahoo», CPENAVAIRE, https://www.lesechos.fr/01/02/2008/lesechos.fr/300238788_l-historique-de-yahoo.htm#, consulté le 22 Mars 2018.

[7] Dictionnaire de Français Larousse, http://www.larousse.fr/dictionnaires/francais/hacker/38812, consulté le 2 Avril 2018.

[8] Hamza Shaban, «It's official: Verizon finally buys Yahoo», Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2017/06/13/its-official-verizon-finally-buys-yahoo/?utm_term=.32a594677a20, consulté le 22 Mars 2018.

[9] «What is Spear Phishing? - Definition, Kaspersky Lab, https://usa.kaspersky.com/resource-center/definitions/spear-phishing, consulté le 21 mars 2018.

[10] Martyn Williams, «Inside the Russian hack of Yahoo: How they did it», IDG Communications,https://www.csoonline.com/article/3180762/data-breach/inside-the-russian-hack-of-yahoo-how-they-did-it.html, 4 Octobre 2017.

[11] Swati Khandelwal, «It's 3 Billion! Yes, Every Single Yahoo Account Was Hacked In 2013 Data Breach»,The Hacker News, https://thehackernews.com/2017/02/yahoo-hack.html, 3 octobre 2017.

[12] Mohit Kumar, «Yahoo Confirms 500 Million Accounts Were Hacked by 'State Sponsored' Hackers», https://thehackernews.com/2016/09/yahoo-data-breach.html, 22 Septembre 2016.

[13] «C'est quoi le hachage ?», Culture Informatique, https://www.culture-informatique.net/cest-quoi-hachage/, consulté le 15 mars 2018.

[14] «Comment ça marche ?», MD5ONLINE.ORG, http://www.md5online.fr/, consulté le 2 Avril 2018.

[15] Marc Zaffagni, «Yahoo! reconnaît que 3 milliards de comptes ont été piratés en 2013», Futura Sciences, https://www.futura-sciences.com/tech/actualites/securite-yahoo-reconnait-3-milliards-comptes-ont-ete-pirates-2013-64447/, 4 Octobre 2017.

[16] Martyn Williams, «Inside the Russian hack of Yahoo: How they did it», IDG Communications,https://www.csoonline.com/article/3180762/data-breach/inside-the-russian-hack-of-yahoo-how-they-did-it.html, 4 Octobre 2017.

[17] Katie Lobosco , «How to find out if you're affected by the Equifax hack», http://money.cnn.com/2017/09/07/pf/victim-equifax-hack-how-to-find-out/index.html, 11 Septembre 2017.