Faculté des Sciences Aix Marseille Université
163 Avenue de Luminy Case 901
13288 Marseille
Téléphone : 04 91 82 90 00

Présentation d'une cyber-attaque

Attaque de comptes vérifiés Twitter 07/2020

Quentin PLA
Équipe PL – FSI-8

Vendredi 4 décembre 2020

ERDI – MASTER 1 Informatique – Aix-Marseille Université

Résumé

Le mercredi 15 juillet 2020, le réseau social Twitter est touché par une cyber-attaque massive touchant un grand nombre d'utilisateurs, dont des comptes certifiés de grandes personnalités publiques américaines.

Les pirates ont employé une attaque de type hameçonnage en usurpant l'identité de comptes certifiés, afin de convaincre les utilisateurs d'effectuer des virements de cryptomonnaie via une adresse donnée, permettant de doubler la somme versée.

Pour y parvenir, ils ont réussi à accéder à un outil interne de Twitter par le biais d'employés manipulés, afin de prendre le contrôle de dizaines de comptes pour y publier un message et empocher plus de cent mille dollars en quelques heures seulement.

Abstract

On Wednesday, July 15, 2020, the social network Twitter was hit by a massive cyber-attack affecting a large number of users, including certified accounts of major American public figures.

The hackers used a phishing attack by usurping the identity of certified accounts in order to convince users to make cryptomoney transfers via a given address, doubling the amount paid.

To achieve this, they managed to access an internal Twitter tool through manipulated employees, in order to take control of dozens of accounts to publish a message and collect more than one hundred thousand dollars in just few hours.

Mots-Clés

Mot(s)-Clé(s)	Signification
Ransomware	Logiciel de rançon prenant en otage des données personnelles
Phishing	Technique d'hameçonnage en usurpant une identité afin de tromper l'utilisateur
Malware	Logiciel malveillant nuisant à un système informatique
Spyware	Logiciel espion collectant des données personnelles sans consentement de l'utilisateur
Code PIN	Code confidentiel comprenant quatre chiffres ou plus
DDOS	Attaque par déni de service dont le but est de rendre un système informatique indisponible durant un temps spécifique
Tweet	Message bref utilisé sur le réseau social Twitter
Cryptographie	Technique d'écriture qui consiste à rédiger un message de manière cryptée
Blockchain	Technologie de stockage et de transmission d'informations sans organe de contrôle
Adresse Bitcoin	Adresse utilisée pour désigner la destination d'un paiement en cryptomonnaie Bitcoin. Elle peut être considérée comme l'équivalent d'un numéro de compte Iban.

Table des matières

Table des illustrations

Introduction

Le mercredi 15 juillet 2020, une cyber-attaque massive a lieu sur le réseau social Twitter touchant cent trente comptes certifiés, afin d'extorquer l'argent des utilisateurs de la plateforme via des virements de cryptomonnaie.

Pour présenter cette attaque, je me suis renseigné sur différents sites internet français et américains expliquant le déroulement de celle-ci et donnant leur point de vue.

Afin d'aborder le sujet, une définition du mot cyber-attaque, ainsi que les différentes formes dans lesquelles vous pourrez la retrouver seront présentées. Quelques exemples célèbres seront également disponibles afin d'avoir un aperçu de l'impact de ces attaques virtuelles dans le monde réel. Vous trouverez ensuite la présentation détaillée de cette cyber-attaque, dont le contexte, les sécurités utilisées par Twitter, l'attaque ainsi que les moyens employés par les cybercriminels, le déroulement de celle-ci ainsi que les répercussions et pertes engendrées.

Le rapport a été rédigé et organisé de telle sorte à ce que la lecture reste agréable, en incluant des images liées aux paragraphes et en effectuant des liaisons logiques entre chaque partie afin que la présentation de cette attaque soit la plus compréhensible possible.

Je vous souhaite une bonne lecture.

Qu'est-ce qu'une cyber-attaque ?

1.1. Définition

Le préfixe « cyber » désignant tout ce qui est de l'ordre d'internet et du numérique, une cyber-attaque signifie un acte de malveillance mis en place sur des systèmes informatiques. Ces systèmes peuvent être représentés sous plusieurs formes comme par exemple un ordinateur, un serveur, un périphérique, un smartphone ou encore un objet connecté.

Les attaques peuvent atteindre n'importe qui, que ce soit un particulier ou une entreprise, de manière directe ou indirecte. Nous pouvons les retrouver sous quatre formes distinctes dont la cybercriminalité, l'espionnage, l'atteinte à l'image et le sabotage.

1.2. Cybercriminalité

La motivation principale des attaquants consiste à dérober des informations personnelles, le but étant de les exploiter afin de parvenir à leur fin ou de les revendre si elles ne leur sont pas utiles, comme par exemple des coordonnées bancaires.

Les internautes sont les plus vulnérables car internet regorge de sites malveillants falsifiants leur identité en se faisant passer pour une entreprise (ex. Amazon), une administration (ex. CAF) ou encore un organisme financier (ex. BNP Paribas). C'est ce que l'on appelle une attaque par « hameçonnage » ou encore « phishing ».


Crédit Mutuel

Madame, Monsieur,

Vous devez vous connecter à votre compte de **crédit mutue**l dès que possible et accepter **les nouvelles conditions** pour confirmer et / ou mettre à jour vos données personnelles.

Avec cette étape, nous pouvons nous assurer que votre adresse électronique et votre numéro de téléphone ne sont pas utilisés sans votre consentement.

Vous devez accéder au service en ligne en cliquant sur le lien ci-dessus:

Espace Client

Suivez les conseils ci-dessous pour confirmer et / ou mettre à jour vos informations personnelles:

- 1 Connectez-vous à votre espace sécurisé avec vos identifiants personnels.
- 1 Accepter les nouvelles conditions et suivez les étapes

Si vous avez des questions, votre agence de crédit mutuel sera toujours disponible pour vous aider.

Cordialement,

L'équipe Crédit Mutuel

Image 1 : Exemple d'hameçonnage de l'organisme Crédit Mutuel par e-mail

Un deuxième type d'attaque appelé « rançongiciel » ou « ransomware » consiste à crypter les données personnelles d'une victime en attendant que celle-ci paie une rançon fixée par le pirate afin de débloquer la situation et que la victime puisse récupérer ses données.

Ces deux types de cyber-attaques ne sont pas réellement ciblées, les internautes naïfs sont les plus touchés, voilà pourquoi elles sont les plus répandues sur internet.

1.3. Espionnage

Contrairement à la cybercriminalité, les attaques liées à l'espionnage sont très ciblées. En effet, l'intention principale étant de dérober un maximum de données sensibles en toute discrétion, elles touchent majoritairement les entreprises. Parfois, celles-ci se rendent compte qu'elles ont été espionnées seulement des années plus tard après le début de l'attaque.

Afin d'y parvenir, les pirates utilisent une cyber-attaque nommée « point d'eau » consistant à utiliser une faille de sécurité par le biais de sites internet peu sécurisés souvent consultés par l'entreprise ciblée, afin d'y introduire du code malveillant et d'infecter les machines pour débuter l'espionnage sans élever de soupçon. Certains cybercriminels utilisent également « l'hameçonnage » comme vu précédemment, mais de manière ciblée en envoyant des mails contenant un lien vers un site malveillant à des adresses e-mail spécifiques.

Les pirates pourront ainsi obtenir des informations précieuses et avoir un contrôle total de la machine infectée.

1.4. Atteinte à l'image

Certains pirates souhaitent décrédibiliser l'image d'une organisation en s'y prenant de deux manières.

La première consiste à bloquer l'accès d'un site internet en saturant les ports du serveur lié grâce à une multitude de requêtes envoyées vers celui-ci, c'est ce que l'on appelle une attaque « DDOS ». De ce fait, il est impossible pour les internautes d'y accéder pendant un certain temps, pouvant varier de quelques minutes à plusieurs heures, voir dans le pire des cas à quelques jours. La deuxième attaque par « défiguration » a pour but de défigurer l'apparence physique d'un site internet, afin que les pirates puissent répandre le message qu'ils souhaitent faire passer en monopolisant le serveur du site web, c'est-à-dire qu'ils disposent d'un contrôle total et d'un accès complet aux données de celui-ci. Ainsi, chaque internaute se connectant au site web sera exposé au message et ne pourra accéder aux services initiaux proposés par le site internet. Les plus ciblés sont ceux dont l'affluence est très élevée afin de toucher un maximum d'internautes. Les messages passés par les cybercriminels sont souvent d'ordre politique ou idéologique.

Ces attaques sont généralement peu conséquentes car il n'y a pas vraiment de danger lié à l'économie et à la vie d'une entreprise ou d'une organisation.

1.5. Sabotage

Contrairement aux attaques de décrédibilisation vu précédemment, celles dont le but principal est de saboter des systèmes informatiques engendrent des conséquences dramatiques sur l'économie et la vie d'une organisation. Elles peuvent rapidement mener celles-ci à la faillite, le personnel étant également touché car ils risquent de perdre leur emploi et de finir au chômage.

Les pirates font passer leur attaque comme étant une « panne organisée » ciblant l'ensemble ou une majorité des systèmes informatiques ayant pour but de modifier ou d'effacer un maximum de données sensibles contenues dans ceux-ci.

Les moyens d'attaques utilisés sont nombreux et sophistiqués de telle sorte à ce que les cibles ne soient pas toujours préparées face à ces actes de malveillance.

1.6. Exemples célèbres

Parmi les cyber-attaques les plus connues dans le monde, nous pouvons citer « WannaCry », un ransomware de chiffrement très sophistiqué qui a pu atteindre un grand nombre d'internautes et d'organisations grâce aux réseaux sociaux. Cette épidémie a pu faire le tour des chaines d'informations à cause de son importance, en effet, à peine quatre jours ont suffi pour infecter plus de deux cent mille ordinateurs à travers le monde. Parmi les victimes, nous pouvons retrouver des usines ainsi que des hôpitaux qui ont été contraint d'arrêter leur activité pour cause de matériel informatique inutilisable.

Image 2 : Ransomware WannaCry

Une deuxième attaque, s'intitulant « DarkHotel » a pu faire prendre conscience que les réseaux publics sont peu sécurisés et qu'il faut donc se protéger au maximum face aux vulnérabilités. Les cybercriminels déploient un spyware dans le réseau public de l'hôtel avant l'arrivée des clients, afin qu'une fois connectés au réseau, un message impose l'installation d'une mise à jour, étant en fait un logiciel malveillant ayant pour but d'enregistrer chaque saisie provenant du clavier. C'est une attaque d'hameçonnage ciblée en faisant passer un malware comme étant une mise à jour bénigne qui permet d'espionner sans lever de soupçon les clients dans l'hôtel.

Présentation de la cyber-attaque

1.7. Contexte

1.7.1. Réseau social Twitter

Twitter a été fondé par un groupe de quatre membres dont Jack Dorsey, Evan Williams, Biz Stone et Noah Glass qui a vu le jour le 21 mars 2006. Le siège social se trouve à San Francisco aux États-Unis et actuellement l'entreprise dispose d'un effectif d'environ trois mille neuf cents employés.

Image 3 : Logo Twitter

C'est un réseau social gratuit permettant d'envoyer des « tweets » représentés par de courts messages. Ce service est devenu rapidement populaire puisqu'en moins de dix ans, il regroupait déjà plus de trois cents millions d'utilisateurs actifs mensuels. De nos jours, il en regroupe plus de trois cents trente millions et chaque jour plus de cinq cents millions de tweets sont publiés. Il est majoritairement utilisé pour rapidement partager de courtes informations.

Grâce à ces chiffres, nous pouvons remarquer que Twitter est un réseau social de grande ampleur disposant d'un nombre élevé d'utilisateurs actifs chaque jour, voilà pourquoi une sécurité accrue est nécessaire pour détecter et éviter les cyber-attaques qui pourraient compromettre les données personnelles de chaque utilisateur inscrit sur la plateforme.

1.7.2. Les cryptomonnaies

Elles sont représentées par des devises virtuelles décentralisées utilisant des algorithmes cryptographiques reposant sur un protocole informatique nommé « blockchain ». Il s'agit d'une base de données infalsifiable stockant toutes les informations liées aux transactions effectuées afin d'assurer la fiabilité et la traçabilité de celles-ci. Ce registre étant publique, tout utilisateur peut avoir accès à l'historique des transactions effectuées. Chaque transaction est indélébile, il est donc simple de retracer l'ensemble des échanges effectuées par un utilisateur.

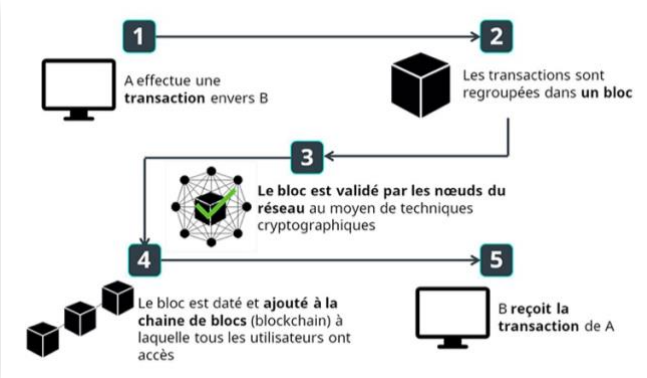

Image 4 : Fonctionnement du protocole "blockchain" utilisé pour les cryptomonnaies

Ces monnaies peuvent être stockées dans un portefeuille numérique, permettant d'effectuer des transactions grâce à son identifiant unique, comme par exemple une adresse Bitcoin, qui peut être partagée, servant à réaliser des achats et ventes de cryptomonnaies via des plateformes d'échanges en ligne.

1.7.3. Les cybercriminels

Cette cyber-attaque a été préméditée par un groupe de pirates grâce à l'aide de quelques employés de Twitter manipulés, qui ont pu les aider en fournissant un accès à un système interne à la plateforme : « Nous avons détecté ce que nous pensons être une attaque coordonnée d'ingénierie sociale par des personnes qui ont réussi à cibler certains de nos employés ayant accès aux systèmes et outils internes » d'après le réseau social.

1.7.4. Les victimes de l'attaque

Nous pouvons recenser les quelques employés manipulés par les pirates.

Plus de cent trente comptes Twitter certifiés représentant de grandes personnalités publiques américaines ont été ciblés. Nous pouvons citer Bill Gates, Barack Obama ou encore Kim Kardashian, mais également de multiples firmes américaines comme Apple ou encore Uber.

Cependant, elles ne sont pas les seules victimes de cette attaque. En effet, de nombreux utilisateurs de la plateforme ont été touchés et sont tombés dans le piège établi par les cybercriminels.

1.8. Enjeu des attaquants

L'enjeu principal des attaquants était de générer un maximum de bénéfices en extorquant les utilisateurs par le biais d'une escroquerie et de plusieurs adresses Bitcoin qui leur était proposées afin d'y verser la somme d'argent qu'ils souhaitaient.

De cette manière, les pirates n'incitant pas les victimes à envoyer une somme d'argent précise, ils pouvaient percevoir une grande quantité de faibles montant provenant de milliers d'utilisateurs et ainsi maximiser leurs gains.

1.9. Sécurités mises en place par Twitter

Le réseau social a mis en place de nombreux moyens de sécurité afin de le protéger un maximum face aux nombreuses cyber-attaques dont il peut faire face.

Tout d'abord pour éviter la cybercriminalité, la plateforme a mis en place un système de détection de liens potentiellement dangereux lorsqu'un utilisateur saisit un lien dans un tweet. Une recherche va être effectuée dans une base de données contenant des liens signalés comme étant malveillants afin de vérifier s'il est dangereux.

Il permet ainsi de bloquer les attaques d'hameçonnage et les liens menant vers des logiciels malveillants comme des ransomwares.

De plus, l'authentification à double facteurs est disponible afin de renforcer la sécurité lors de la connexion à un compte en demandant un code éphémère envoyé par SMS sur le mobile de l'utilisateur. De cette manière, si celui-ci se fait dérober ses données personnelles, le pirate se retrouvera bloqué lors d'une tentative de connexion sur le compte de la victime.

Une fonctionnalité supplémentaire permet également de sécuriser au maximum un compte en obligeant l'utilisateur à s'authentifier avec un code PIN pour chaque action qui sera effectuée concernant un tweet, comme par exemple pour la publication ou la suppression.

1.10.Moyens employés par les attaquants

Afin de mettre en place la cyber-attaque, les cybercriminels ont réussi à s'octroyer un outil interne à Twitter via le personnel de l'entreprise, en utilisant leurs identifiants afin de contourner le dispositif de sécurité d'authentification à deux facteurs.

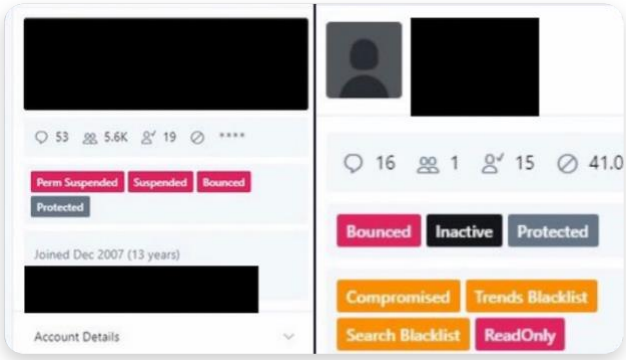

Image 5 : Outil interne du réseau social Twitter

Sa fonction principale étant de superviser l'ensemble des comptes utilisateurs du service, il permettait notamment d'avoir un contrôle total sur les données personnelles disponibles, comme par exemple la possibilité de modifier une adresse e-mail et un mot de passe associés à un compte.

De ce fait, les pirates avaient un contrôle total sur l'ensemble des comptes disponibles de la plateforme, ils ont donc décidé de cibler les comptes les plus suivis par les utilisateurs, qui sont pour la grande majorité des comptes dit « certifiés » représentant de grandes personnalités publiques, afin de toucher un maximum de personnes et ainsi maximiser les gains de l'escroquerie.

1.11.Cyber-attaque utilisée

Les assaillants ont décidé d'utiliser une attaque de type hameçonnage d'une manière différente de celles que l'on peut voir habituellement, le but ici n'étant pas de rediriger les victimes vers des sites internet malveillants.

Grâce à l'outil interne de Twitter qu'ils ont pu s'octroyer, rendant toutes les sécurités liées aux comptes inefficaces, les criminels ont réussi à prendre le contrôle de plusieurs comptes certifiés en modifiant l'adresse mail et le mot de passe de chaque compte, afin de publier un tweet en usurpant ainsi leur identité afin de convaincre les internautes de la véracité du tweet publié et donc de les faire tomber plus facilement dans le piège.

L'ingéniosité de l'escroquerie se trouve dans le message publié par les attaquants, car comme nous avons pu le voir précédemment, Twitter utilisant une sécurité permettant de bloquer les liens dangereux, ils ont donc décidé de la détourner en ne mettant aucun lien, mais uniquement des adresses de portefeuilles de cryptomonnaie qui ne sont donc pas bloquées.

1.12. Déroulement de l'attaque

Dans l'après-midi du mercredi 15 juillet, les criminels commencent à prendre le contrôle de cent trente comptes certifiés disposant de millions d'abonnés, grâce à l'outil qu'ils disposent. Pendant plusieurs heures, un message alléchant écrit en anglais, apparait sur ces comptes Twitter certifiés, dont le sujet était une proposition afin de doubler la somme d'argent que les utilisateurs verseraient à une adresse liée à un porte-monnaie de cryptomonnaies.

La majorité des utilisateurs ne disposant pas de porte-monnaie virtuel, donc ne comprenant pas le but de ce message, l'ont ignoré. Cependant, quelques-uns d'entre eux en possédant un, sont tombés dans le piège et ont alors effectué un virement vers l'adresse indiquée en espérant obtenir le double du montant versé. Ainsi, près de trois cents personnes ont cédé à la tentation de l'escroquerie et se sont faites piégées avant l'intervention de la plateforme.

Image 6 : Exemple de tweet issu de l'escroquerie

Le réseau social a pu rapidement se rendre compte de la supercherie et a donc décidé d'agir en verrouillant les comptes compromis afin d'en reprendre le contrôle, de

révoquer l'accès aux outils internes permettant de bloquer les pirates dans leur avancement et d'empêcher les utilisateurs de tweeter ou de modifier leur mot de passe.

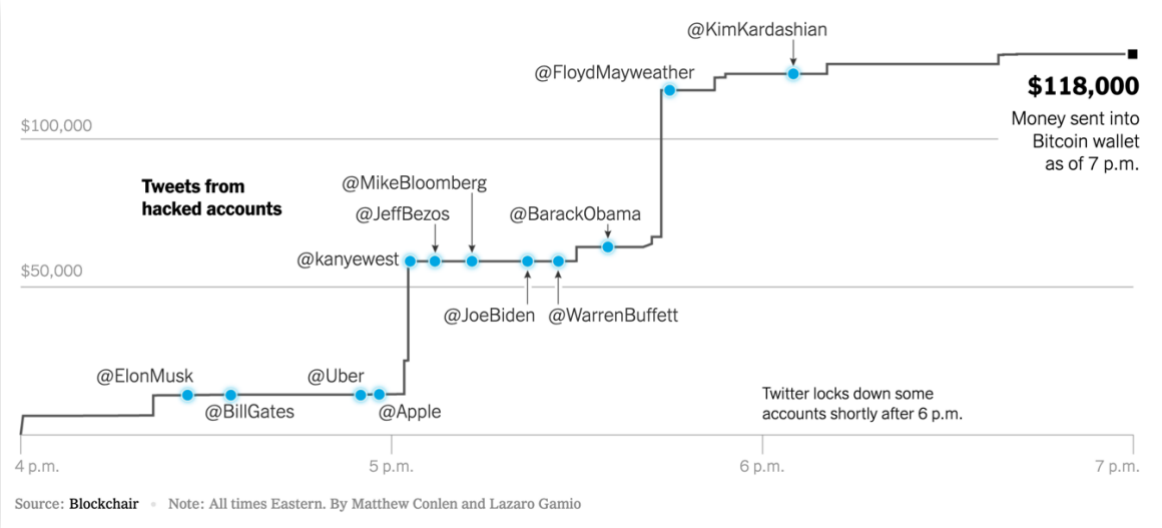

Image 7 : Déroulement de la cyber-attaque

1.13. Répercussions de l'attaque sur Twitter

Le réseau social travaille toujours avec les forces de l'ordre afin de déterminer qui sont les auteurs de cette cyber-attaque.

De nombreuses équipes internes travaillent en permanence afin d'améliorer la sécurité de la plateforme et de leurs systèmes.

Les employés ont eu droit à une formation supplémentaire concernant les tactiques d'ingénierie sociale afin d'éviter qu'ils puissent se faire manipuler à nouveau comme ils ont pu l'être fait par les pirates.

Twitter se dit gêné, déçu et désolé à propos de cette cyber-attaque qui a eu lieu.

Un jour plus tard après l'attaque, le cours de la bourse du réseau social n'a pas été impacté car il aura seulement reculé d'environ un pour cent.

1.14. Gains empochés par les attaquants

Grâce à cette cyber-attaque, les attaquants ont pu s'empocher plus de cent mille dollars en quelques heures via des virements de cryptomonnaie.

De plus, grâce à l'outil interne, ils ont pu récupérer l'historique complet des actions effectuées sur le réseau social de certains comptes, comprenant leur données personnelles, les messages privés qu'ils ont pu envoyer ainsi que toutes les interactions effectuées sur d'autres tweets.

Selon Twitter, il est également possible que les pirates aient pu revendre certains noms d'utilisateurs déjà utilisés à d'autres utilisateurs souhaitant les obtenir.

1.15.Indemnisation des victimes

Malheureusement, aucune des victimes touchées ont pu être indemnisées.

Le problème étant lié au fait que lorsqu'une transaction de cryptomonnaie est validée, il n'est plus possible de faire un retour arrière. Comme cela a été dit précédemment, le protocole blockchain étant décentralisé, aucune autorité ne peut intervenir.

Pour la majorité de ceux qui utilisent les cryptomonnaies, ce problème est un avantage car il n'y a aucun moyen d'interférer une transaction.

Conclusion

Cette cyber-attaque massive au sein du réseau social Twitter a réussi à prendre une ampleur phénoménale en quelques heures seulement, grâce au piratage de nombreux comptes certifiés très suivis. Malheureusement, de nombreux utilisateurs sont tombés dans le piège et les pirates ont pu récolter plus de cent mille dollars. Cependant, la plateforme fut réactive et a su réagir à temps, avant que l'attaque dégénère, mais les victimes n'ont pu être indemnisées, du fait que la devise des virements était en cryptomonnaie.

Je trouve que les cybercriminels ont établi une bonne stratégie pour leur attaque, mais assez peu de personnes utilisent les cryptomonnaies, ainsi beaucoup moins d'elles ont été tentées par le piège. S'ils avaient utilisé un autre service anonyme permettant de récolter de l'argent, comme par exemple une cagnotte en ligne anonyme, ils auraient peut-être pu récolter plus d'argent, mais auraient dû l'utiliser sous forme de bons d'achat, ce qui est inconvénient.

L'entreprise a très bien réagi face à l'attaque grâce aux protocoles mis en œuvre afin de rétablir la situation. Elle a averti les utilisateurs de chacune de ses démarches durant l'attaque afin de limiter la panique, ce qui est une très bonne démarche selon moi.

Ce travail m'a apporté quelques connaissances supplémentaires par rapport aux types de cyber-attaques existantes et les méthodes employées par les cybercriminels afin d'arriver à leurs fins. Il m'a également forcé à vérifier l'authenticité des informations trouvées sur internet en les comparant sur de nombreux sites internet français et américains afin d'avoir un contenu de qualité.

Bibliographie

GOUVERNEMENT [En ligne]. Page consultée le 14 novembre 2020. Disponible sur : https://www.gouvernement.fr/risques/risques-cyber
Cmentreprise [En ligne]. Page consultée le 14 novembre 2020. Disponible sur : https://cmentreprise.fr/cyber-assurance/definition-cyber-attaque/#cybercriminalite
Global Security Mag [En ligne]. Kaspersky Lab, page publiée en février 2019 [consultée le 15 novembre 2020]. Disponible sur : https://www.globalsecuritymag.fr/Le-passage-de-la-quantite-a-la,20190207,84334.html
Futura-Sciences [En ligne]. Page consultée le 15 novembre 2020. Disponible sur : https://www.futura-sciences.com/tech/definitions/securite-attaque-point-eau-16369/
SNOW, John. Kaspersky [En ligne]. Page publiée le 6 novembre 2018 [consultée le 15 novembre 2020]. Disponible sur : https://www.kaspersky.fr/blog/five-most-notorious-cyberattacks/11130/
COËFFÉ, Thomas. Blog du modérateur [En ligne]. Page publiée le 20 mai 2018 [consultée le 18 novembre 2020]. Disponible sur : https://www.blogdumoderateur.com/chiffres-twitter/
Wikipédia [En ligne]. Page mise à jour le 18 novembre 2020 [consultée le 18 novembre 2020]. Disponible sur : https://fr.wikipedia.org/wiki/Twitter
Le Monde [En ligne]. Le Monde avec AFP, page publiée le 16 juillet 2020 [consultée le 21 novembre 2020]. Disponible sur : https://www.lemonde.fr/pixels/article/2020/07/16/bill-gates-elon-musk-un-piratage-vise-les-comptes-twitter-de-personnalites-et-d-entreprises_6046297_4408996.html

STATT, Nick. THE VERGE [En ligne]. Page publiée le 15 juillet 2020 [consultée le 21 novembre 2020]. Disponible sur : https://www.theverge.com/2020/7/15/21326656/twitter-hack-explanation-bitcoin-accounts-employee-tools
COX, Joseph. VICE [En ligne]. Page publiée le 16 juillet 2020 [consultée le 21 novembre 2020]. Disponible sur : https://www.vice.com/en/article/jgxd3d/twitter-insider-access-panel-account-hacks-biden-uber-bezos
INA, Fried. AXIOS [En ligne]. Page publiée le 16 juillet 2020 [consultée le 21 novembre 2020]. Disponible sur : https://www.axios.com/twitters-big-hack-bares-broad-dangers-b6c05341-c2a6-468e-b719-5b52b411c941.html
RAYMOND, Grégory. CAPITAL [En ligne]. Page publiée le 16 juillet 2020 [consultée le 21 novembre 2020]. Disponible sur : https://www.capital.fr/entreprises-marches/les-hackers-de-twitter-ont-ils-empoche-de-largent-et-pourra-t-on-les-retrouver-1375530
NANDAGOPAL, Rajan. The Indian EXPRESS [En ligne]. Explained Desk, page publiée le 18 juillet 2020 [consultée le 21 novembre 2020]. Disponible sur : https://indianexpress.com/article/explained/twitter-hack-explained-bitcoin-us-elections-politicians-celebrities-6508127/
Twitter [En ligne]. Page consultée le 22 novembre 2020. Disponible sur : https://help.twitter.com/fr/safety-and-security
RICHAUD, Nicolas. Les Echos [En ligne]. Page publiée le 17 juillet 2020 [consultée le 22 novembre 2020]. Disponible sur : https://www.lesechos.fr/tech-medias/medias/cyberattaque-de-twitter-130-comptes-ont-ete-pirates-1224375
MESSÉANT, Élodie. LA TRIBUNE [En ligne]. Page publiée le 17 novembre 2020 [consultée le 23 novembre 2020]. Disponible sur : https://www.latribune.fr/entreprises-finance/banques-finance/industrie-financiere/les-cryptomonnaies-l-argent-des-criminels-862460.html

Futura-Sciences [En ligne]. Page consultée le 23 novembre 2020. Disponible sur :

https://www.futura-sciences.com/tech/definitions/informatique-cryptomonnaie-18278/

Twitter [En ligne]. Twitter Inc, page publiée le 18 juillet 2020 [consultée le 24 novembre 2020]. Disponible sur :

https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html

FRENKEL Sheera, POPPER Nathaniel, CONGER Kate, SANGER David E. The New York Times [En ligne]. Page publiée le 15 juillet 2020 [consultée le 24 novembre 2020]. Disponible sur :

https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html