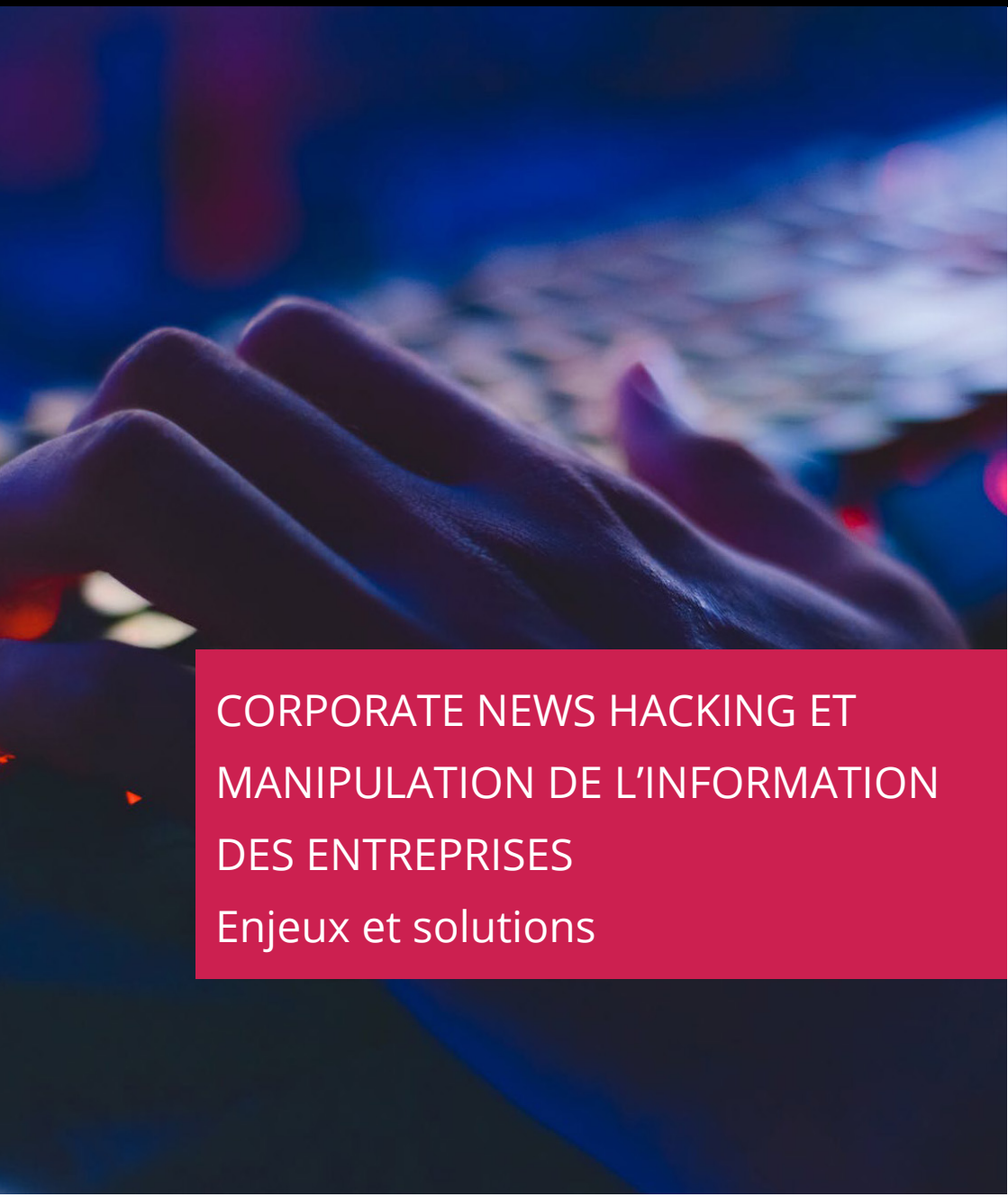
wiztrust



CORPORATE NEWS HACKING ET MANIPULATION DE L'INFORMATION DES ENTREPRISES

Enjeux et solutions

Paris, le 21 Mai 2019

#Hackcorp

SOMMAIRE

INTRODUCTION

Les entreprises et les médias sont confrontés à un nouveau et même défi. Comment assurer la confiance dans l'information face aux *fake news*, aux usurpations d'identité et à l'effet amplificateur des robots et des réseaux sociaux ? Ces enjeux sont plus aigus encore pour les entreprises cotées et les services financiers.

La teneur de l'information économique et financière affecte directement la valeur des entreprises concernées. L'impact d'une information mal gérée ou détournée est instantané et peut provoquer des effets extrêmement violents. En 2016, la valeur de Vinci a chuté de près de 20% en quelques minutes après la reprise par Bloomberg d'une fausse information sur les performances de l'entreprise. Sept milliards d'euros se sont volatilisés avant que l'action ne remonte laissant une baisse nette à la clôture de 3,76%.

Il existe plusieurs « méthodes » permettant de manipuler l'information. Leur complexité technologique est variable, depuis l'envoi d'un faux communiqué rédigé via un banal traitement de texte jusqu'au hacking plus sophistiqué des systèmes d'information des autorités de marché, en passant par la manipulation de plusieurs canaux de diffusion de l'information. L'imagination et l'ingéniosité des hackers est sans limite.

Comme leurs méthodes, les motivations des « manipulateurs » sont multiples.
Certains sont des activistes chevronnés désirant attirer l'attention sur la cause qu'ils défendent. Les *hoax* ou canulars plus ou moins malveillants sont l'une de leurs pratiques préférées. Ce sont par exemple les Yes Men qui, en janvier 2019, ont détourné la lettre annuelle de Larry Fink, le CEO de BlackRock, pour annoncer la sortie progressive du leader mondial de l'asset management du secteur des énergies fossiles. Information fausse reprise notamment par le Financial Times… Même les médias référents ont été dupés.
D'autres sont des escrocs patentés à l'affut des plus-values générées par les variations violentes de la valeur des entreprises dont ils manipulent l'information et le cours de l'action.

Sans sombrer dans le catastrophisme ou une paranoïa aigue, il devient essentiel de comprendre ces phénomènes pour mieux les anticiper et se préparer à les contrer.

Nous avons choisi d'organiser ce livre blanc autour d'une série de cas réels, plus ou moins médiatisés, mais illustrant bien les différentes mécaniques de « *corporate news hacking* ».

Dans ce livre blanc, Wiztopic recense les profils de ces malfaiteurs, présente un récit des faits avérés depuis une décennie et mène une réflexion sur la manière pour les entreprises de se protéger.

C'est sur ces analyses que Wiztopic a développé Wiztrust.

Créée en France par les ingénieurs de Wiztopic, Wiztrust est aujourd'hui la première plateforme de certification et de vérification de l'information des entreprises. Wiztrust s'appuie sur la *blockchain* pour permettre aux entreprises de certifier les informations qu'elles diffusent et à leurs destinataires, journalistes, analystes et investisseurs, d'en vérifier l'authenticité.

La technologie bouleverse l'environnement des communicants. Elle est au cœur de la manipulation de l'information des entreprises. Elle est aussi au cœur des solutions apportées à ces nouveaux enjeux.

Jérôme Lascombe et Raphaël Labbé

Fondateurs de Wiztopic

TEMPS RÉEL ET AMPLIFICATION SOCIALE DE L'INFORMATION

Le temps de l'information est en pleine accélération et les médias économiques et financiers, notamment les agences d'information financière, ont souvent peu de temps pour vérifier l'authenticité d'une annonce. Les robots producteurs de contenus excluent toute vérification « humaine » de l'information avant sa diffusion.

Dans un contexte où la crédibilité des journalistes est parfois contestée, le haut niveau de technicité des hacks avec plusieurs faux communiqués, des sites imités à la quasi-perfection ainsi que des emails ressemblant de près à des contenus sécurisés, laisse les médias dans une situation critique où la vérification devient un travail complexe et chronophage.

L'information *corporate* est aujourd'hui diffusée par des canaux multiples, via un communiqué de presse reçu par email, parfois un *tweet*, qui mènera lui-même à un communiqué de presse ou la newsroom du site de l'entreprise émettrice. La synchronisation de la diffusion laisse parfois à désirer lorsque les équipes communication sont organisées par canaux (relations presse, social, digital, communication interne).

Nos experts constatent que la mécanique de *news hacking* s'est développée ces dernières années et combine en règle générale, tous ces canaux. Une attaque bien organisée consiste souvent en un faux communiqué envoyé via une fausse adresse email, avec un lien pointant vers un faux espace presse et un faux numéro de téléphone permettant d'appeler un faux service de presse. Dans ce cas, même si le journaliste appelle pour vérifier l'information, il obtiendra la confirmation qu'elle est authentique, alors même qu'elle est fausse.

Quand une information paraît importante, elle doit être traitée au plus vite. Pour un média, avoir la primeur de la publication est un enjeu économique et de réputation. C'est sur ce temps court que comptent les fraudeurs ou les activistes, lorsqu'ils envoient à la presse de fausses informations, en reprenant le graphisme des documents originaux, l'identité des émetteurs habituels, des adresses e-mail et des noms de domaine très approchants et suffisamment trompeurs.

Les auteurs de *corporate news hacking* comptent également sur le rythme effréné de cette « course à la news » pour planifier leur action. En effet, presque tous les cas recensés par nos experts suivent deux modèles principaux. Une partie des faux communiqués, font état d'un événement extraordinaire, imprévisible, requérant une communication de crise immédiate, dont l'urgence et le contenu ne peuvent pas être ignorés par la presse. Ces attaques peuvent intervenir à n'importe quel moment et parient sur l'ampleur du « buzz » potentiel pour se soustraire à la vigilance des journalistes.

Dans de nombreux autres cas, la diffusion du faux communiqué se fait légèrement en amont d'une échéance très attendue, comme la publication d'une lettre aux investisseurs régulière ou de résultats financiers. Plutôt que de jouer sur l'urgence d'une crise soudaine, ces attaques se fondent sur l'anticipation par les médias d'éléments de communication ordinaires. La réception d'un communiqué d'apparence véridique et répondant à une échéance régulière, a des chances d'échapper à une vérification approfondie.

Le travail de vérification est d'autant plus important que chaque fausse information diffusée par un media, *a fortiori* d'envergure internationale, a le potentiel d'être reprise quasi-instantanément par d'autres rédactions, chaînes d'info en continu ou media en ligne. A cette propagation s'ajoute l'effet amplificateur des réseaux sociaux, où un article, une vidéo ou même le moindre *tweet* ou *post* d'un journaliste peut être repris et commenté des milliers de fois en quelques minutes. Selon une étude du MIT publiée dans le journal Science, le 9 mars 2018, les *fake news* se diffusent d'ailleurs plus rapidement et plus largement que les véritables informations.

Les réseaux sociaux, toujours alertes et dont les algorithmes favorisent l'émergence d'informations spectaculaires, sont de formidables caisses de résonnance pour les *fake news*. Ils en amplifient les effets dans la sphère économique. Les investisseurs surveillent ces réseaux en temps réel pour en suivre le « sentiment » et s'y adapter aussi rapidement que possible.

LES MOTIVATIONS : ACTIVISME ET APPÂT DU GAIN

Le travail de recensement des cas de *corporate news hacking* que nous avons effectué révèle deux typologies de motivations.

C'est tout d'abord l'activisme (ou hacktivisme), aux visées diverses, souvent écologiques ou anti-libérales. Il s'agit de manipuler la communication d'une entreprise pour la déstabiliser, la tourner en dérision, attirer l'attention du public sur ses pratiques jugées néfastes, influencer son management, appeler au *boycott* de ses produits… Ces pratiques sont souvent qualifiées de *hoax*, ou canular malveillant (« *prank* »), parfois de « satirisme de guerrilla ».

L'appât du gain est un autre moteur de ces hacks. Lorsque les attaques ne portent pas un message revendicateur, politique ou social, leurs auteurs cherchent souvent à diffuser une fausse information dans le but d'influencer les marchés financiers, après avoir pris des positions pour profiter des mouvements provoqués par la fausse information. Ces opérations sont dirigées vers les sociétés cotées avec des stratégies différentes en fonction de la taille des cibles. Du classique *pump & dump* sur de très petites capitalisations, les *hackers* vont parfois jusqu'à utiliser des produits dérivés comme dans le cas du *hacking* de la communication de Vinci.

La technique du *pump and dump* vise à abuser les petits actionnaires à la recherche de tendances haussières sur des titres modestes. Elle consiste tout d'abord à accumuler des actions de société dites « *penny stocks* », à faible valeur et à forte volatilité potentielle, avant d'encourager les marchés financiers à l'achat de ces titres via la diffusion d'une fausse information prometteuse de gain pour ensuite les revendre au plus haut.

La mécanique peut aussi être inversée. Le fraudeur mise sur la baisse d'une valeur, diffuse une information négative entraînant une chute du cours, profite de cette chute puis dément l'information peu après pour profiter du rebond du cours une fois la supercherie révélée.

Dans les deux cas, de confortables gains peuvent être engrangés, parfois en tout anonymat, les attaques les mieux organisées ayant recours à des produits dérivés, comme les ETF, pour profiter des mouvements d'un indice sans être traçable par les autorités financières.

La propagation de fausses informations peut aussi prendre la forme plus grossière de « spam boursier » ou diffusion massive de fausses informations par email, misant sur la crédulité des investisseurs recevant ces messages.

Les tentatives de manipulation des marchés ou de déstabilisation des entreprises ne sont pas récentes mais les nouveaux médias ont considérablement accéléré la transmission et la diffusion des informations. Quant au mode de diffusion, c'est le communiqué de presse qui est le plus souvent utilisé. Dans une étude récente intitulée *Market manipulation and suspicious stock recommendations on social media*, l'universitaire Thomas Renault écrit : « Les canaux les plus utilisés par les fraudeurs pour propager des fausses informations sont les communiqués de presse (73,3 %), suivi des e-mails ou newsletters (34 %), les sites internet (32 %) et les forums (10,6 %) ».

LES RISQUES : DES ATTAQUES À FAIBLES COÛTS MAIS À FORTS ENJEUX

La multiplication des cas de *corporate news hacking* (ou hacking de communication d'entreprise) s'explique, en partie, par la disproportion entre les coûts d'une attaque pour son auteur et pour sa cible. Réussir à faire relayer par la presse un faux communiqué ne requiert que peu de ressources, surtout en comparaison des répercussions potentielles sur l'entreprise, la valeur de son action et sa réputation. En outre les auteurs de *corporate news hacking* ne sont que très rarement identifiés et inquiétés par la justice.

Certaines attaques menées par des groupes d'activistes écornent, parfois durablement, l'image d'une entreprise, diffusant au grand public des révélations, réelles ou non, détruisant plusieurs années de relations publiques et de RSE. Cependant d'autres cas ont occasionné des dommages financiers quantifiables.

En particulier, le cas de Vinci est l'un des plus révélateurs : le 22 novembre 2016, suite à la publication d'un faux communiqué annonçant des irrégularités dans ses comptes et le licenciement de son directeur financier, l'action du groupe dévisse. En 7 minutes, la capitalisation du groupe chute de 7 milliards d'euros, avant que sa cotation soit suspendue. Même après les démentis, l'action de Vinci perd tout de même près de 4% en clôture, après une journée pourtant positive pour le CAC 40.

La chute de la valeur de l'un des leaders mondiaux de la construction contraste avec les coûts minimes nécessaires pour orchestrer la fausse information et la rendre crédible : envoyer un faux email est gratuit, construire le site miroir vinci.group est l'affaire de quelques heures, il a été hébergé aux Pays-Bas pour 22,50€, une fausse ligne téléphonique peut être mise en place grâce à une carte prépayée pour 5€. En arrondissant le coût probable de l'attaque à 30€, chaque euro dépensé a eu un impact immédiat de plus de 233 millions d'euros pour Vinci.

Les recours pour les entreprises victimes sont, quant à eux, très limités. Vinci a bien porté plainte contre X, le lendemain de l'attaque, et l'Autorité des Marchés Financiers a mené sa propre enquête sur l'usurpation de l'identité du groupe, sans aboutir à ce jour, si ce n'est la communication de nouvelles recommandations et bonnes pratiques. Cependant, il ne serait pas surprenant, dans un futur proche, alors que les pratiques de *fact checking* se normalisent, de voir des entreprises victimes d'une fausse communication se retourner contre l'organisme de presse l'ayant publiée, amplifiée et légitimée.

Risques et ressources limités pour un impact maximal, le *corporate news hacking* est représentatif d'un type de cyberattaque en plein essor qui nécessite de la part de ses cibles potentielles l'adoption de nouvelles pratiques et d'outils innovants.

DEPUIS 2010, DES MANIPULATIONS À RÉPÉTITIONS

Nous avons pris le parti de présenter une sélection des cas de manipulation d'informations les plus représentatifs. Certains ont fait la Une des médias, notamment quand ils sont l'œuvre d'activistes recherchant une visibilité médiatique. D'autres cas ont été gérés plus discrètement et sont passés inaperçus. C'est le cas de manipulations boursières ayant été peu médiatisés.

2019

BLACKROCK

BlackRock et son dirigeant Larry Fink sont la cible d'une usurpation d'identité. À quelques jours de la parution attendue et annoncée de sa lettre annuelle officielle, une fausse lettre du CEO de BlackRock est diffusée via un faux e-mail et un faux mini-site très similaires aux canaux officiels de l'entreprise américaine. Le plus important gestionnaire d'actifs au monde, avec 6 300 Md$ d'actifs sous gestion, est victime d'un *hoax*. Ce dernier annonçait un virage de l'entreprise vers un engagement pour le climat sans précédent. Ce simple e-mail a réussi à duper plusieurs médias de référence, notamment le Financial Times et Cnbc news.

2016

FITBIT

FitBit est la victime d'un trader amateur peu scrupuleux. Ce dernier dépose un faux dossier à la SEC annonçant que Fitbit étudiait une offre d'achat d'une société d'investissement chinoise dénommée ABM Capital. Se faisant passé pour un employé d'ABM, le trader va même jusqu'à ouvrir un compte au système de dépôt de la SEC EDGAR pour annoncer qu'ABM offrait 12,5$ par action de Fitbit, qui cotait au même moment moins de 9$. Le cours de bourse de Fitbit bondit de 100 millions de dollars.
L'auteur de cette fraude, Robert Walter Murray, a écopé de 2 ans de prison ferme.

VINCI

Vinci a été victime d'une usurpation d'identité. Un faux communiqué de presse annonçait une révision à la baisse des résultats du groupe et le licenciement de son Directeur Financier, conduisant à un *flash crash*. L'action de Vinci chute de plus de 18 %. Un faux démenti a ensuite été envoyé pour faire remonter ce même cours avant que le groupe n'envoie son (vrai) démenti. L'information fut relayée également par deux faux sites internet. Une fausse information reprise par plusieurs médias, dont l'agence Bloomberg. Difficile de savoir qui a bénéficié de cette opération, s'il s'agit d'une escroquerie ou d'un *hoax*. La Dépêche a rapporté que l'initiative avait été revendiquée par des opposants à l'aéroport de Notre-Dame-des-Landes.

2016

PFIZER

Pfizer, la veille du 1er avril, annonce dans un communiqué rapidement repris par le Washington Post, que le géant pharmaceutique allait cesser d'augmenter le prix de ses médicaments. Le faux communiqué, peut-être un poisson d'avril, fait suite à plusieurs mois de controverses sur les pratiques tarifaires des groupes pharmaceutiques. Malgré de rapides démentis et le retrait de l'article, le cours de Pfizer trébuche et perd 2%.

2015

RYANAIR

Ryanair est la cible d'artistes et d'activistes. Un faux communiqué de presse annonce que la compagnie aérienne transporterait des réfugiés depuis la côte grecque et l'Europe de l'Est vers les pays les plus fortunés de l'UE. Le *hoax* est l'œuvre de Luther Blissett, une association italienne qui entend dénoncer les dérives de la société médiatique. Cette campagne bénéficiait d'un site internet dédié, ryanfair.org. France Info cite le slogan frauduleux que le communiqué arborait : « Notre mission : rendre le voyage aérien accessible au plus grand nombre ».

2014

G4S

G4S, groupe britannique leader mondial dans les services de sécurité, envoie aux journalistes un communiqué de presse annonçant que ses comptes sont erronés et que son Directeur financier a été licencié. Le Telegraph, suspectant un faux, alerte G4S, le communiqué contenant plusieurs fautes de grammaire et citant par erreur le nom du précédent CFO. Entre-temps l'information avait été reprise par plusieurs journalistes sur Twitter, puis relayée par des chaînes d'information en continu.

INTEL

Intel, après avoir annoncé un investissement de 6 milliards de dollar en Israël, est la victime d'un faux communiqué de presse, appuyé par un faux site web et un faux numéro de téléphone, révélant l'annulation de l'investissement. Raison invoquée : la politique de responsabilité sociale d'Intel est en contradiction avec « les récents assauts d'Israël sur Gaza ». Selon Business Insider, l'auteur du faux communiqué répondait même au téléphone pour confirmer la nouvelle.

2013

BANQUE EUROPÉENNE D'INVESTISSEMENT

La Banque européenne d'investissement, la veille de la présentation de ses résultats, est la cible d'un faux communiqué de presse qui annonce la fin des financements pour les centrales à charbon. Le journal L'Echo précise que les activistes environnementaux, auteurs du faux communiqué de presse, avaient poussé la supercherie jusqu'à donner le numéro de téléphone d'un pseudo porte-parole de la BEI, qui répondait aux appels des journalistes.

2013

SAMSUNG / FINGERPRINT CARDS

Un communiqué frauduleux prétend que Fingerprint Cards, société suédoise cotée, va être rachetée par le géant sud-coréen pour 650 millions de dollars. Résultat : une hausse de 50 % de la valeur de Fingerprint Cards, soit 200 millions de dollars. Reuters note que l'affaire a fait grand bruit et que Cision, la société de diffusion via laquelle le faux communiqué fut diffusé, a chuté de plus de 5% en bourse.

SPENCER PHARMACEUTICAL

Spencer Pharmaceutical est victime d'une authentique opération de *pump and dump* menée par l'escroc canadien Jean-François Amyot. Ce dernier fit croire, à grands coups de faux communiqués, que cette société avait reçu une offre d'achat de 245 millions de dollars provenant du Moyen-Orient. Fait original, comme le note PR Week, Amyot s'était servi, pour disséminer ses fausses nouvelles, de deux sociétés de relations publiques qu'il contrôlait, IAB Media et Hilbroy. Le fraudeur a été condamné à plus de 7 millions de dollars de dommages et intérêts par la justice américaine.

ANZ

ANZ, un grand groupe bancaire océanien, est pris pour cible par un activiste environnemental, Jonathan Moylan. Celui-ci diffuse un faux communiqué de presse prétendant que la banque allait retirer un financement de plus d'un milliard de dollars à un projet de mine de charbon mené par la société Whitehaven. Comme le relate le média australien ABC, la secousse médiatique fit plonger la valeur du groupe minier Whitehaven de 314 millions.

2012

BANK OF AMERICA

Bank of America est victime d'activistes qui font croire, avec un faux communiqué de presse et un faux site web, que Brian Moynihan, le CEO de la banque déclarait : « Aujourd'hui, il faut l'admettre, notre banque ne fonctionne plus ». Business Insider relève que le communiqué, pour davantage de réalisme, était faussement signé par BusinessWire.

GOOGLE / ICOA

Google est connu pour sa stratégie d'acquisition de sociétés. Un faux communiqué annonce que le moteur de recherche va mettre la main sur ICOA, un fournisseur de *hot spots wifi*. L'action ICOA (une *penny stock*), dont la valeur est multipliée par 5. L'escroc à l'origine de ce faux communiqué aurait fait alors une belle plus-value estimée à plus d'un million de dollars, rappelle BuzzFeed News.

2012

SHELL

Shell est attaquée par des activistes écologistes qui publient un faux communiqué de presse, mettent en ligne un faux site web agrémenté d'une vidéo. Les numéros de téléphone figurant sur le pseudo-site internet étaient des faux. Selon CNEWS, les militants voulaient protester contre le forage du groupe dans l'Arctique.

2011

GENERAL ELECTRIC

General Electric est, à son tour, la cible d'un *hoax*. Le groupe n'ayant pas payé d'impôts l'année précédente, le faux communiqué de presse insinuait que, pris de remords, GE allait verser 3,2 milliards au Trésor américain. L'annonce est relayée par l'agence AP. Le Washington Post relève que, malgré une deuxième dépêche corrigeant son erreur, l'action de la société, qui ne cessait de grimper, a reculé de près d'un demi-point. Le groupe d'activistes « Yes Men » était derrière cette manipulation.

2010

CHEVRON

Chevron est la victime de trois groupes d'activistes, Amazon Watch, RAN, et les Yes Men. Avec un message en forme de *mea-culpa*, ce *hoax* reposait sur un faux communiqué de presse et un faux site internet annonçant : « Les compagnies pétrolières doivent nettoyer leurs dégâts, [Chevron] est d'accord ! ». Comme le note PR Daily, plusieurs médias dont Fast Company ont relayé le faux communiqué.

GENERAL MILLS

General Mills est la cible d'une usurpation d'identité corporate avec la publication d'un faux communiqué prétendant que le président Obama avait ordonné une enquête sur la société suite au retrait du marché de plusieurs produits. Adweek souligne que le communiqué frauduleux avait été diffusé via PRNewswire, mis en cause à l'époque pour le défaut de vérification des contenus soumis par certains nouveaux clients. WSJ Online, Fox Business News et Dow Jones Newswire avaient repris l'info.

KOCH INDUSTRIES

Koch Industries, le conglomérat industriel américain, connu pour financer de nombreuses initiatives remettant en question le changement climatique, est attaqué par des activistes. Les « Youth for Climate Truth » diffusent un faux communiqué pointant vers un faux site. Comme le relatait à l'époque le New York Times, ils prétendaient que les frères Koch allaient cesser leur soutien aux organisations semant le doute sur le changement climatique comme Americans for Prosperity, the Fraser Institute, the Foundation for Research on Economics and the Environment, parmi d'autres.

QUELS ENSEIGNEMENTS EN TIRER ?

Une analyse des cas ici sélectionnés, qu'ils soient l'œuvre d'activistes ou d'escrocs, révèle quelques constantes.

1. Les médias n'ont pas pu vérifier l'information avant de la publier, par manque de temps ou de moyens fiables de vérification. Même quand ils ont tenté de vérifier son authenticité en appelant la société concernée, ils ont souvent été mis en relation avec de fausses messageries de services de presse, voire de faux services de presse ou de fausses agences de relations publiques répondant au téléphone pour valider l'information.

2. Quand une agence de presse publie une information, elle la valide et lui confère une crédibilité telle qu'il n'est plus besoin pour le lecteur ou pour d'autres médias de la vérifier. Le média qui reprend une fausse information contribue à son « blanchiment » pour les lecteurs, surtout si la fausse information est reprise pour la première fois.

3. Le contenu de l'information diffusée est certes faux mais il reste toujours plausible, même dans les cas de canulars.

4. Le format préféré reste le communiqué de presse, finalement assez facile à détourner et souvent très efficace.

5. Les canaux d'émission de la fausse information sont généralement multiples : fausses adresses emails, faux espaces presse ou sites Internet, faux numéros de téléphone. Cette combinaison rend la vérification illusoire quand on ne connaît pas déjà l'émetteur.

6. Les *newswires* ou organismes de diffusion d'information réglementée n'empêchent pas le *corporate news hacking*. Ils ont même tendance à amplifier ses effets en donnant une apparente crédibilité à des informations fausses sans les avoir vérifiées.

7. Même les systèmes les plus sécurisés comme les bases de données de la SEC peuvent aussi être manipulés.

COMMENT LES ENTREPRISES PEUVENT-ELLES SE PROTÉGER ?

Assurer la fiabilité de l'information pour préserver l'image et les intérêts des entreprises exposées, c'est d'abord favoriser une vérification facile et rapide de l'information originale. Cette fiabilité repose non seulement sur la responsabilité de vérification de l'information que portent les médias mais aussi sur l'entreprise émettrice qui doit prévenir le *corporate news hacking*. Ce sont ces dernières qui, *in fine*, en subissent la plupart des conséquences.

La première chose à faire afin de se protéger de ces risques est de « certifier » son information dès son émission. En lui donnant un certificat d'authenticité infalsifiable, son destinataire pourra vérifier l'information aussi facilement que possible. C'est ce que les entreprises font avec Wiztrust en ancrant leurs communiqués de presse ou autres contenus photos et vidéo dans la blockchain. Les destinataires de ces contenus peuvent en vérifier l'authenticité, en deux clics, sur wiztrust.com.

La distinction du canal de diffusion du communiqué de celui de sa vérification prévient également l'essentiel des hacks. Pour les entreprises et les médias, la certification par la blockchain est la manière la plus fiable de prévenir la publication de fausses informations.

Prévenir le *corporate news hacking* c'est aussi multiplier les canaux de diffusion simultanée du contenu pour faciliter sa vérification. Une manière de se préparer est de toujours privilégier une diffusion multicanale, programmée et simultanée de l'information. C'est ce que font les entreprises qui utilisent Wiztopic la plateforme de gestion et de distribution de l'information des entreprises cotées.

Il est toujours plus difficile de « hacker » 8 ou 10 canaux officiels (emails, newsrooms, sites corporate, comptes sociaux, etc.) plutôt qu'une petite fraction d'entre eux. Ces différents canaux, sécurisés de manière différentes, permettent aussi de vérifier l'authenticité de l'émetteur par recoupement en passant de l'un à l'autre.
Dans un contexte bouleversé par la technologie, la confiance relative à l'information corporate et financière devient la priorité n°1 pour les professionnels de l'information, qu'ils en soient les émetteurs, institutions financières ou entreprises cotées, ou les destinataires, médias, analystes et investisseurs.

A PROPOS

Wiztrust a été créée par Wiztopic, l'éditeur de la plateforme logicielle des équipes communication du secteur de la finance et des sociétés cotées. Avec Wiztopic, elles gèrent, diffusent et mesurent la performance de leurs contenus. En toute simplicité, sécurité et conformité.
En savoir plus : www.wiztrust.com

CONTACT :

Agathe Chabert

agathe@wiztopic.com
06 42 76 34 42

SUIVEZ NOUS !

wiztrust