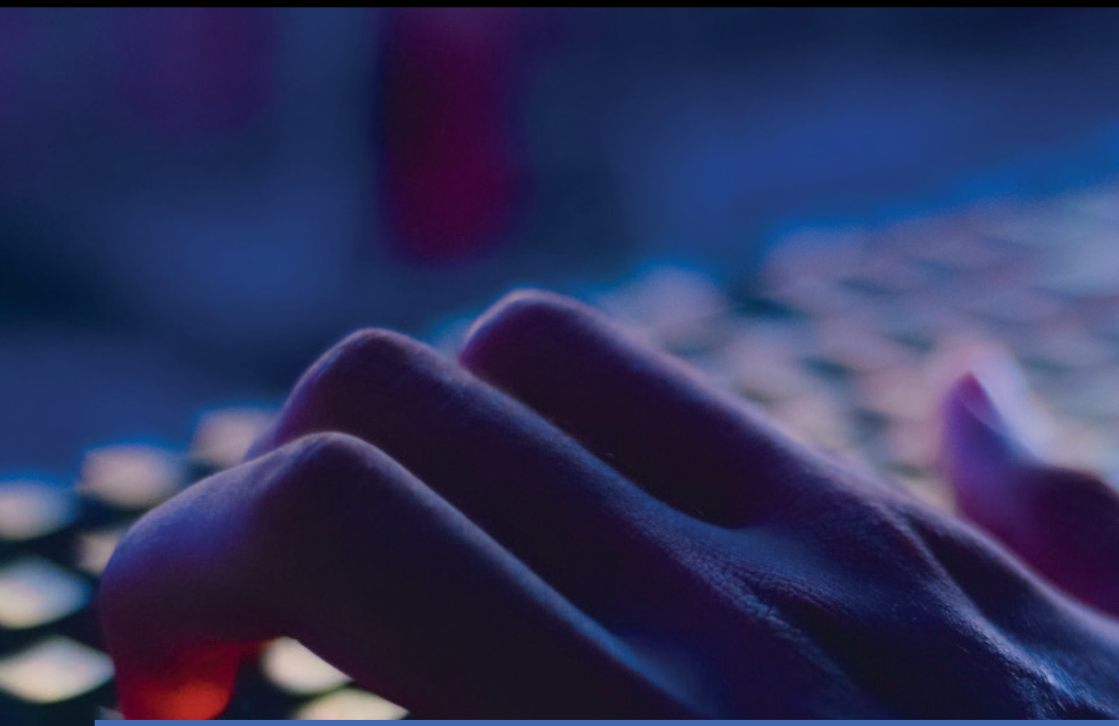
wiztrust

un partenaire de EURONEXT CORPORATE SERVICES



DÉSINFORMATION ET MANIPULATION DE L'INFORMATION DES ENTREPRISES

Enjeux et solutions

Mai 2022

Certifié avec wiztrust

TABLE DES MATIÈRES

INTRODUCTION

Les entreprises et médias sont confrontés à un nouveau défi. Comment assurer la confiance dans une ère de désinformation ? Les sociétés cotées et les institutions financières du monde entier sont les plus exposées à ces menaces croissantes.

En effet, l'article 221-4 du règlement général de l'Autorité des Marchés Financiers stipule que : « L'information financière réglementée est transmise aux médias dans son intégralité et d'une manière qui garantisse la sécurité de la transmission, minimise le risque de corruption des données et d'accès non autorisé, et apporte toute certitude quant à la source de l'information transmise.»

L'information économique et financière impacte directement la valeur des entreprises concernées.
Les faux articles et les campagnes d'information montées de toutes pièces ont des effets néfastes non seulement sur la réputation d'une entreprise, mais aussi sur sa stabilité financière et les intérêts de ses actionnaires.

Il existe plusieurs « méthodes » permettant de manipuler l'information des entreprises. 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, surtout quand les auteurs de ces attaques utilisent non seulement de multiples techniques, mais leurs actions ont des motivations très diverses. Certains sont des activistes novices, d'autres des manipulateurs chevronnés désirant attirer l'attention sur la cause qu'ils défendent. Ces canulars ou hoax malveillants sont parmi les meilleurs outils de leur arsenal d'influence.

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 et CNBC… 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. Quand ces variations impliquent des crypto-monnaies, ces escrocs peuvent s'enrichir en quelques minutes tout en étant difficile à démasquer.

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 spécialistes de la manipulation de l'information, présente un récit des faits avérés et mène une réflexion sur la manière pour les entreprises de se protéger.

L'équipe d'experts de Wiztopic a analysé les mécanismes de piratage de l'information des entreprises pour concevoir une solution leur permettant de protéger leur communications externe. C'est sur ces travaux 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 très simplement les informations qu'elles diffusent et à leurs destinataires, journalistes, analystes et investisseurs, d'en vérifier en temps réel l'intégrité et 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

Co-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. En outre 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 dont l'URL est similaire à l'authentique, et un faux numéro de téléphone permettant d'appeler un faux service de presse. Dans ce cas, même si un journaliste scrupuleux 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 et l'identité des émetteurs habituels.

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 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 récemment dans le journal Science, 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 », une sorte de nouveau «consensus social» 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, ou plus récemment la valeur de crypto-monnaies, 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.

Plusieurs types d'activistes sont connus pour leurs initiatives en matière de manipulation de l'information des entreprises. Les Yes Men, un groupe activiste spécialisée dans la production de fausses nouvelles, a ciblé plusieurs multinationales par ses attaques. Par exemple, la fabrication d'un faux communiqué de presse de General Electric envoyé ou encore la diffusion d'une fausse information sur BlackRock usurpant l'identité de son dirigeant, Larry Fink.
Plus récemment, les Fixers ont manipulé la communication de Vanguard pour mettre en évidence le comportement environnemental douteux des assets managers.

Le groupe Extinction Rebellion, un mouvement international de désobéissance civile en lutte contre le dérèglement climatique cible aussi les acteurs de la finance. Il a récemment manipulé l'information du plus important fonds de pension suédois, AP7. Le groupe activiste a diffusé un faux communiqué de presse à plusieurs médias internationaux. L'un de ses membres s'est fait passer pour le dircom de l'entreprise.
L'été dernier, le groupe Galp au Portugal a fait l'objet de manipulation d'informations qui combinait à la fois une fausse annonce et de l'activisme urbain pour dénoncer son implication au Mozambique.

En outre, la technique du pump and dump vise à abuser les petits actionnaires à la recherche de tendances haussières sur des «penny stocks». Elle consiste tout d'abord à accumuler des actions de ces petites sociétés 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 d'une part et pour sa cible d'autre part. 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 2016, le géant pharmaceutique Pfizer a été la cible d'un faux communiqué de presse affirmant que la société n'augmenterait plus les prix de ses médicaments les plus vendus. Cette nouvelle a été publiée la veille du poisson d'avril en utilisant une fausse URL, « pfizerinternational.com », et un communiqué de presse a été envoyé aux médias. Le Washington Post n'a pas tardé à annoncer la nouvelle et à publier un point de vue. L'objectif pour les hackers était de manipuler la valeur de l'action et de faire un profit rapide en «shortant» l'action. Grâce à des alertes des sociétés d'analyse de marché et à la réactivité de l'entreprise, l'action de Pfizer n'a « que » trébuché de 2%.

La chute de la valeur de l'un des leaders mondiaux de la pharmacie contraste avec les coûts minimes nécessaires pour orchestrer la fausse information et la rendre crédible : envoyer un faux email est gratuit et une fausse ligne téléphonique peut être mise en place grâce à une carte prépayée pour 5€. En arrondissant le coût probable de l'attaque s'élève à 30€.

Plus récemment, les fausses annonces de collaborations entre des distributeurs et des crypto-monnaies ont pris de l'ampleur.
Les hackers ont une nouvelle fois montré l'impact de la communication et sa faiblesse face aux cybermenaces. De faux communiqués de presse affirmant que la société autoriserait les crypto-monnaies comme nouvelle option de paiement ont été relayés dans les médias en septembre et novembre 2021 par les « fausses » équipes de communication de Walmart et Kroger. L'information a provoqué une envolée des valeurs des crypto-monnaies concernées. Les hackers ont vraisemblablement gagné des millions en quelques minutes et ne seront probablement jamais retrouvés.

Les recours pour les entreprises victimes sont, quant à eux, très limités. Alors que la SEC et d'autres régulateurs financiers du monde entier peuvent lancer des enquêtes, les chances de découvrir l'identité des hackers sont faibles.
Ils publient de nouvelles directives avec de bonnes pratiques préventives qui malheureusement ne permettent que de retarder le prochain hacking.

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 être jugées co-responsables avec le media l'ayant publiée, amplifiée et légitimée. Le Règlement général de l'AMF indique d'ailleurs clairement que les entreprises cotées doivent assurer la fiabilité de l'information qu'elles diffusent.

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.

2021, UNE ANNÉE RECORD POUR LES FAKE NEWS

Les premiers cas documentés de fake news remontent au début des années 2000 avec l'affaire Emulex. Pendant les quinze années suivantes, ces cas sont restés sporadiques, avec un impact plus ou moins retentissant.

Depuis 2018, la tendance est à la hausse avec une multiplication significative des cas et des modes opératoires toujours plus sophistiqués de la part des hackers. Les retombées sont d'autant plus importantes du fait de l'effet amplificateur des réseaux sociaux et de la digitalisation de la communication. 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.

2022

TESLA

Le 12 avril 2022 un faux communiqué de presse est relayé massivement par les fans de Tesla sur les réseaux sociaux, notamment Twitter. La marque annonce le rachat de Lithium Corporation, un spécialiste de l'extraction de ce précieux métal. L'info crédibilisée par une annonce faite peu de temps auparavant par Elon Musk sur l'intérêt de Tesla pour un rachat dans le secteur. Conséquence: l'action de Lithium Corporation bondit de 250%. Peu après, Lithium Corporation publie un «vrai» communiqué démentant l'information de rachat.

STARBUCKS

Un faux communiqué de presse a annoncé - puis démenti maladroitement - que Starbucks supprimait son supplément sur les laits végétaux sur fonds de racisme alimentaire. Plusieurs médias ont relayé à la fois l'annonce et le démenti.

Le faux communiqué de presse (usurpant l'identité de Blaine Stevenson, directeur des innovations en matière d'égalité chez Starbucks) faisait partie d'un canular très sophistiqué, comprenant : une vidéo diffusée sur un faux site Web Starbucks Cares ; un faux communiqué de démenti émis par un faux Starbucks, et une vidéo de révélation de la campagne finale. Ils sont même allés jusqu'à produire des bons de réduction réalistes pour supprimer le surcoût.

Cette action, perpétrée par les activistes The Fixers, visait à dénoncer le racisme alimentaire et la cause environnementale.

VANGUARD

Un premier faux communiqué de presse a été envoyé à Earther par un hacker. Ce communiqué de presse vantait un nouveau fonds excluant l'investissement dans le secteur des énergies fossiles et dénommé «Vanguardians of the Galaxy». Quelques heures plus tard, un faux démenti est diffusé « Marvel ». Les faux communiqués de presse proposaient un contact (numéro de téléphone et e-mail) et un site Web créé quelques jours auparavant (investor-vanguard.com et marvel.com). Par la suite, les deux communiqués de presse ont circulé sur Twitter avec un public impatient de voir les deux titans faire du greenwashing. En parallèle, le groupe militant Fixers a envoyé des acteurs déguisés en Gardiens de la Galaxie pour distribuer des flyers.

WALMART

Un faux communiqué de presse est diffusé usurpant l'identité de Walmart, mentionnant que le premier distributeur mondial allait accepter la crypto-monnaie Litecoin comme mode de paiement. Le faux communiqué de presse faisait probablement partie d'un système de pump-and-dump destiné à manipuler le prix du Litecoin à des fins de spéculation. La nouvelle du prétendu partenariat a fait bondir le Litecoin de 32% en seulement 25 minutes. La SEC Security & Exchange Commission a ouvert une enquête.

GALP

Un faux communiqué de presse est envoyé par des militants portugais affirmant que Galp Energia abandonnait son implication dans l'exploitation pétrolière dans le nord du Mozambique pour poursuivre un « avenir 100% renouvelable ». L'identité du directeur de la communication a été usurpée et les fake news ont été diffusées à l'aide d'une fausse adresse e-mail similaire à celle de l'entreprise. Le canular a été commis un 1er avril et a été rapidement réfuté par Galp. Mais entre-temps, les principaux médias portugais avaient relayé la fausse information.

2021

DENBURY RESOURCES

Denbury Resources a été victime d'un communiqué frauduleux via le service de communiqués de presse Accesswire, concernant une offre de rachat d'actions à 1,20 $ par action pour la société en difficulté, un prix très au-dessus du cours. Les actions de la société bondissent avant l'ouverture. Le prix de l'action avait triplé juste avant la suspension du cours.

AP7

Le fonds public suédoie Sjunde AP-fonden, est victime d'une manipulation du groupe Extinction Rebellion (XR). Le groupe activiste a diffusé un faux communiqué de presse à plusieurs médias internationaux, pointant vers un faux site internet, copie conforme du site de AP7. Le faux communiqué annonçait que AP7 renonçait à ses investissements dans les énergies fossiles et avait pour ambition de gérer un portefeuille neutre en émissions de CO2 d'ici 2030. Un des militants, joint par l'Agence France Presse, à un faux numéro de téléphone, s'est même fait passer pour le vrai porte-parole du fonds AP7, apportant des précisions crédibles aux journalistes.

2020

SOFTBANK

Softbank a été la victime d'un faux communiqué de presse annonçant le lancement d'une nouvelle carte de crédit utilisant la Blockchain avec son propre système de cryptage. Alors que les nouvelles semblaient légitimes, un grand nombre de médias ont repris le communiqué, tels que Yahoo Finance, AP News, Block Crypto, Coin Telegraph, Business Telegraph et plus encore. Malgé un démenti, l'information est toujours facile à trouver en ligne. À ce jour, l'enquête se poursuit.

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 de Blackrock. Le leader mondial de la gestion d'actifs, 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.

2019

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 par société d'investissement chinoise dénommée ABM Capital. Se faisant passer pour un employé d'ABM, le hacker 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.

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 connu pour ses campagnes decommunication contrariantes. Un communiqué de presse annonce que la compagnie aérienne transportera 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 »

G4S

G4S, groupe britannique leader 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.

2014

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 a même répondu au téléphone pour confirmer l'information.

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.

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.

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 avait déclaré : « 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.

2012

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. La valeur de l'action ICOA (une penny stock) 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.

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.

2011

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.

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 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 ou un media crédible publient une information, ils la « valident » et lui confèrent une crédibilité telle qu'il n'est plus besoin pour le lecteur ou pour d'autres médias de la vérifier.

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

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 ou qu'il est indisponible.

6. 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 ?

Afin d'assurer la fiabilité de l'information et préserver l'image et les intérêts des entreprises exposées, il faut favoriser une vérification facile et rapide de l'information émise. Cette fiabilité repose d'une part sur la capacité de vérification de l'information que portent les médias mais aussi sur l'entreprise émettrice qui est censée prévenir le corporate news hacking. Ce sont ces dernières et leurs actionnaires qui, in fine, en subissent les 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, l'émetteur offre au destinataire une manière simple et rapide pour vérifier l'information. C'est ce que les entreprises font avec Wiztrust en ancrant leurs communiqués de presse ou autres contenus 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 d'un canal à l'autre. 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'un ou deux 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 dans l'information corporate et financière devient la priorité n°1 pour les professionnels, 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

Wiztopic et Wiztrust sont des solutions commercialisées en Europe par Euronext.

SUIVEZ-NOUS !

wiztrust

Certifié avec
wiztrust