Détection automatisée de fausses données utilisées dans les attaques de type HoaxCrash et Fovi (Faux ordres de virement, arnaques au Président).

Thierry Berthier
Chaire de cyberdéfense & cybersécurité Saint-Cyr
Chercheur associé CREC Saint-Cyr

La Calomnie d'Apelle – 1495 – Sandro BOTTICELLI

représente les déesses mineures de la cybersécurité

Sandro Botticelli représente les déesses mineures :

Agnoia (l'ignorance)
AletheIA (la vérité)
Apaté (la ruse)
Diabole (la calomnie)
Epiboule (la roublardise)
Hypolepsis (la méfiance)
Métanoia (le regret)
Ptéropode (l'envie)

Héra, apprenant que Sémélé était enceinte de Zeus (du dieu Dionysos), part à la recherche d'Apaté.
Héra est bien sûr, comme à chaque fois, furieuse d'apprendre que Zeus l'a une nouvelle fois trompée et qu'une nouvelle fois, il va avoir un enfant de son infidélité, mais cette fois-ci, Héra a peur que Sémélé devienne la nouvelle reine des cieux à sa place.
Elle veut donc qu'Apaté lui prête sa ceinture de ruse pour faire revenir son mari mais aussi son fils d'Arès.
On dit que celui qui porte cette ceinture peut faire faire n'importe quoi à la personne qu'il désire.
Bien sûr, Apaté a obéi à Héra. Elle fait partie des maux contenus dans la boîte de Pandore.

- Dans un environnement hyperconnecté, la véracité de l'information devient centrale.

- La sécurité du cyberespace repose sur la véracité des données qui le composent.

- La diffusion de fausses informations économiques peut avoir un impact immédiat et violent sur les marchés financiers.

- Les HoaxCrash et les Fovi (Faux ordres de virement, arnaques au Président)) coûtent très cher aux entreprises.

I
Les attaques par HoaxCrash

Les mécanismes d'un HoaxCrash

- Diffusion d'une fausse information de nature financière ou économique sur une entreprise cotée via une usurpation d'identité pour provoquer un Flash Crash sur le titre ciblé.

- Spéculation sur le cours de l'action par l'attaquant, durant la période de turbulence (à la hausse comme à la baisse).

-L'exemple du HoaxCrash VINCI du 22 novembre 2016.

Qui débute avec le mail suivant que reçoit Bloomberg :

mar. 22/11/2016 16:04

contact.abonnement@vinci.group

VINCI lance une révision de ses comptes consolidés pour l'année 2015 et le 1er semestre 2016

À [redacted]

Nous avons supprimé les sauts de ligne en surnombre dans ce message.

Nouveau communiqué de presse VINCI

Rueil Malmaison, 22 Novembre 2016

VINCI lance une révision de ses comptes consolidés pour l'année 2015 et le 1er semestre 2016

Vinci a annoncé aujourd'hui son intention de réviser ses comptes consolidés pour l'exercice 2015 ainsi que pour le premier semestre 2016. Les résultats d'un audit interne mené par le groupe Vinci ont en effet révélé que certains transferts irréguliers avaient été effectués des dépenses d'exploitation vers le bilan, en dehors de tous principes comptables reconnus. Le montant de ces transferts s'élèverait à 2.490 millions d'euros pour l'exercice comptable 2015 et 1.065 millions d'euros pour le premier semestre 2016. Selon l'audit interne les résultats opérationnels réels seraient de 1.225 millions pour 2015 et de 641 millions pour le premier semestre 2016. Le groupe reporterait donc une perte nette pour 2015 ainsi que pour le premier semestre 2016.

Vinci a rapidement informé ses auditeurs externes (KPMG Audit et Deloitte & Associés) de la découverte de ces transferts. Le 21 Novembre, KPMG a informé Vinci qu'au vu de ces irrégularités, son audit des comptes consolidés de l'année 2015 et du premier semestre 2016 ne sauraient être valides.

Vinci publiera des comptes non audités pour l'exercice 2015 ainsi que pour le premier semestre 2016 dès que possible. Une fois que le nouvel audit sera achevé, Vinci publiera de nouveaux comptes audités pour les deux périodes. Le groupe a par ailleurs lancé une révision complète des règles internes au sein de sa direction financière.

La compagnie a licencié Christian Labeyrie, directeur général adjoint et directeur financier de Vinci.

Vinci a informé l'Autorité des Marchés Financiers (AMF) de ces événements.

La révision des résultats opérationnels pour 2015 et 2016 devrait rester sans conséquence sur la trésorerie du groupe et n'affectera ni les clients ni les prestations du groupe Vinci.

« Notre équipe de direction est très choquée par ces découvertes », a dit Xavier Huillard, Président-Directeur Général de Vinci. « Nous nous engageons à ce que Vinci respecte les plus hauts standards éthiques dans la conduite des affaires du groupe ».

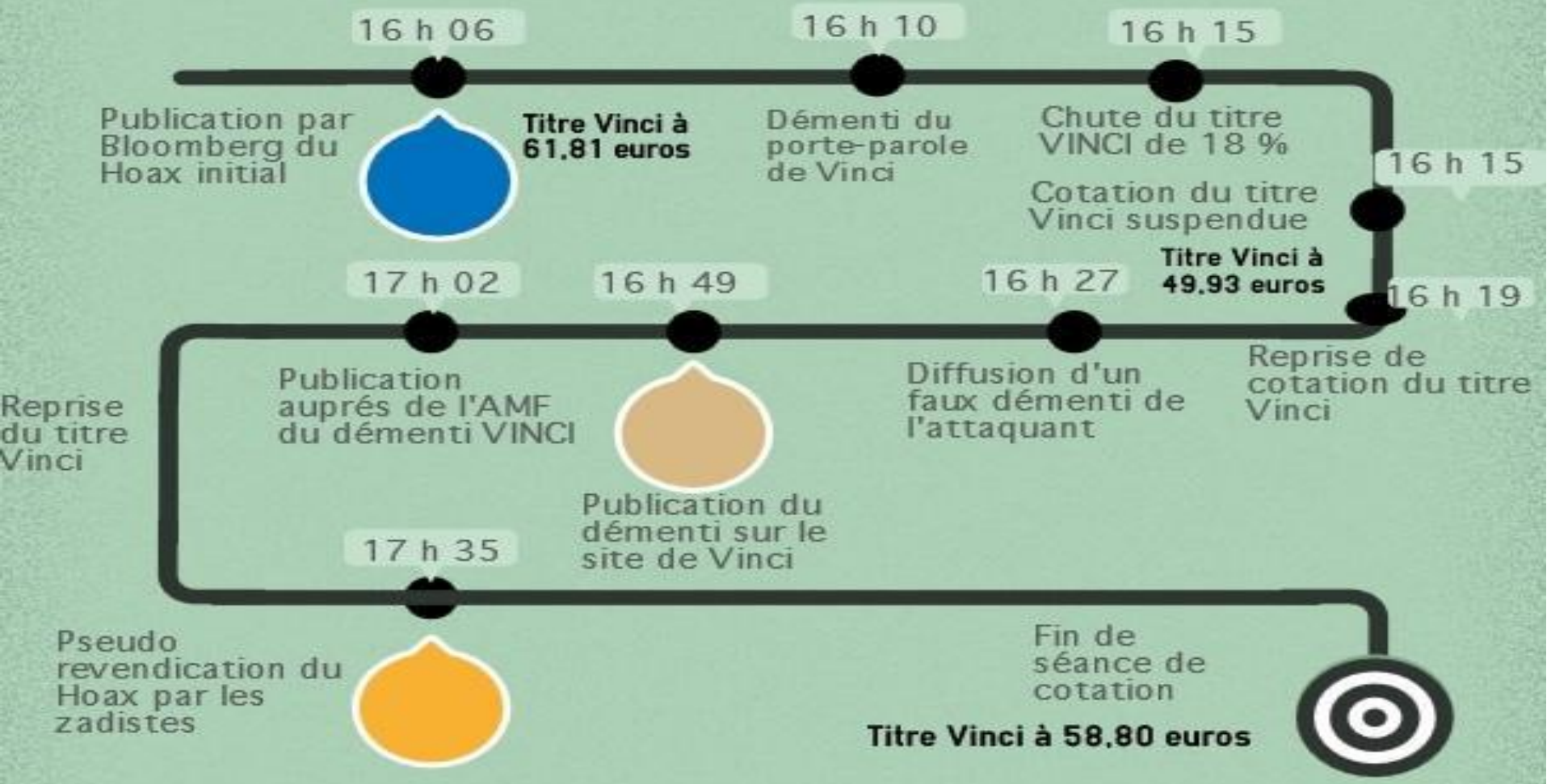
« Nos clients ainsi que nos employés doivent garder confiance en la viabilité du groupe Vinci et en son engagement sur le long terme. Nos services ne sont en aucun cas affectés par ces événements et notre engagement à satisfaire les besoins de nos clients reste une priorité. Les rumeurs qui circulent sur une procédure d'insolvabilité sont totalement fausses » a ajouté le Président Directeur Général de Vinci. « Nous nous engageons à mettre en place les changements nécessaires au sein du Groupe ».

Le groupe Vinci tiendra une conference de presse demain.

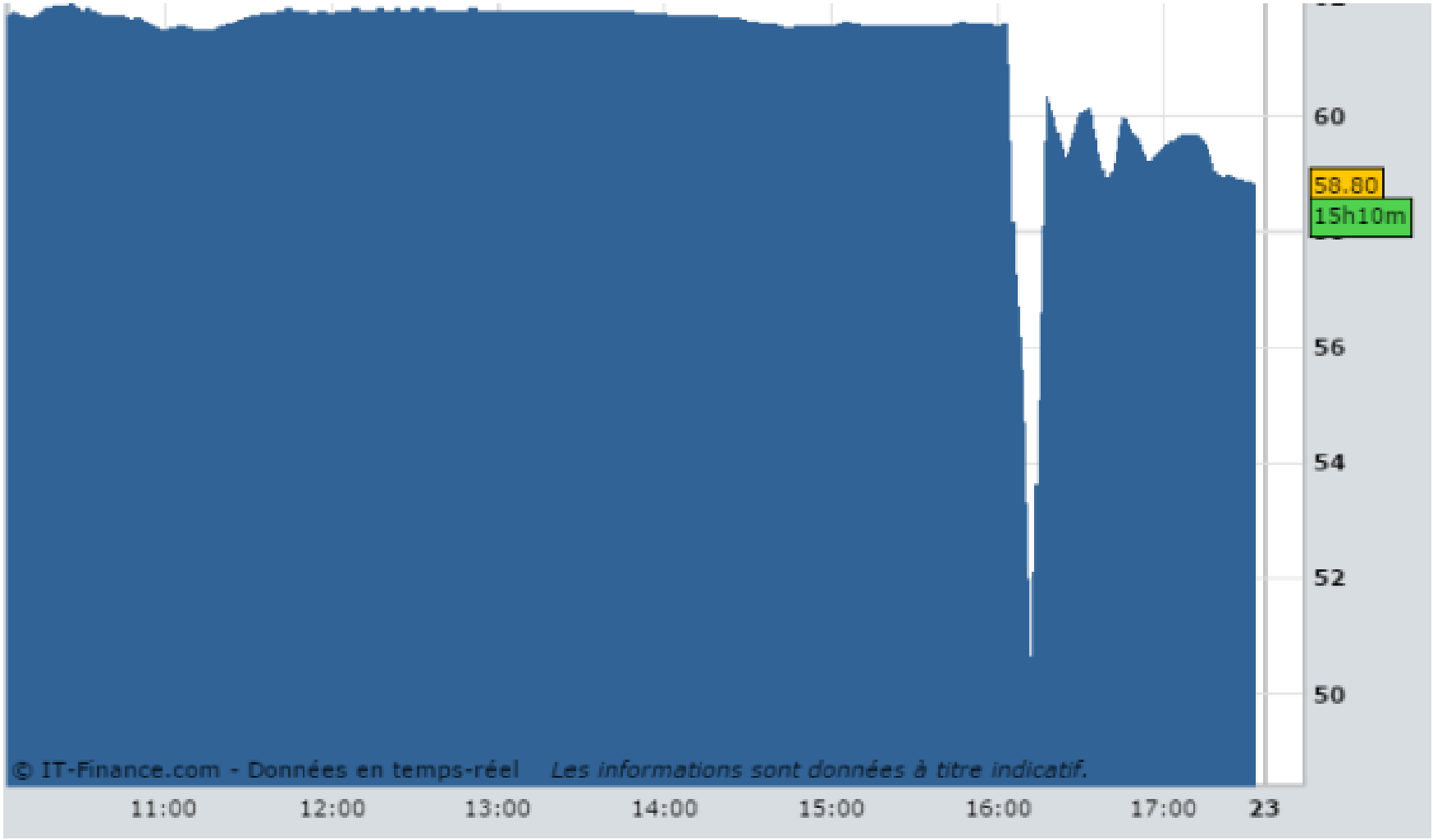
Contact médias
Paul-Alexis Bouquet
Tél. : +33 (0)7 51 93 47 48

http://www.vinci.group/vinci.nsf/fr/communiques/pages/20161122-1557.htm

HoaxCrash VINCI
22 novembre 2016



Flash crash sur le titre Vinci- 22 novembre 2016 - Source IT-Finance.com



Autres attaques efficaces par HoaxCrash

(Les motivations des auteurs de HoaxCrash sont variées)

HoaxCrash	Motivation(s) de l'attaquant
SEA - AP (2013)	Politique - Hacktivisme (conflit syrien)
Whitehaven Coal (2013)	Politique - activisme d'un groupe d'écologistes
G4S (2014)	Politique - activisme
AVON (2015)	Economique - (dégradation d'image - spéculation)
FITBIT (2016)	Economique et activisme
VINCI (2016)	Economique (volatilité - spéculation)

Les recommandations de l'AMF après le HoaxCrash VINCI

Des bonnes pratiques à renforcer

Concernant les sociétés cotées

L'AMF souhaite en premier lieu rappeler aux sociétés cotées que les dispositions relatives à la diffusion effective et intégrale telle que définie par la directive Transparence et ses règlements d'exécution précisent que « les informations réglementées sont communiquées aux médias d'une manière qui garantisse la sécurité de la communication, qui minimise le risque de corruption des données et d'accès non autorisé et qui apporte toute certitude quant à leur source ». Par ailleurs, le texte du règlement européen sur les abus de marché précise que « les informations privilégiées sont communiquées, directement ou par l'intermédiaire d'un tiers,

Les recommandations de l'AMF après le HoaxCrash VINCI

L'AMF recommande également aux émetteurs de renforcer leurs bonnes pratiques, comme certains l'ont déjà fait. En particulier, ils devraient :

- sensibiliser en interne les équipes impliquées dans le processus de gestion de la diffusion de l'information réglementée à l'éventualité d'un cas similaire ;
- envoyer simultanément aux diffuseurs professionnels tout communiqué adressé aux agences de presse ;
- communiquer autant que possible en dehors des périodes de cotation sans pour autant exclure toute communication en séance qui pourrait être indispensable au regard du règlement abus de marché ;
- mettre en place des procédures fiables qui garantissent une transmission et un accès sécurisés en passant notamment par un diffuseur (sous réserve d'une gestion rigoureuse des codes d'accès permettant l'envoi des communiqués de presse à ce même diffuseur) et renforcer la sécurité des transmissions électroniques pour les émetteurs qui souhaitent conserver un canal de diffusion complémentaire à destination de certains acteurs (analystes, investisseurs, medias, journalistes…) ;
- mettre en place un dispositif de veille : identification des noms de domaines proches de celui de l'émetteur, détection de faux sites internet, dispositif pour que le site ne soit pas dupliqué, etc. ;
- prévoir et tenir à jour une procédure d'urgence permettant de réagir au plus vite (personnes impliquées, chaine de décision, communiqué de démenti « type », connaissance de ses interlocuteurs à l'AMF et chez Euronext, etc.) ;
- se tenir informé des nouveaux modes de piratage, d'usurpation d'identité, etc. ; et adapter les dispositifs en conséquence.

Les recommandations de l'AMF après le HoaxCrash VINCI

Concernant les agences de presse et les journalistes

L'AMF encourage par ailleurs les agences de presse à compléter leurs procédures opérationnelles en :

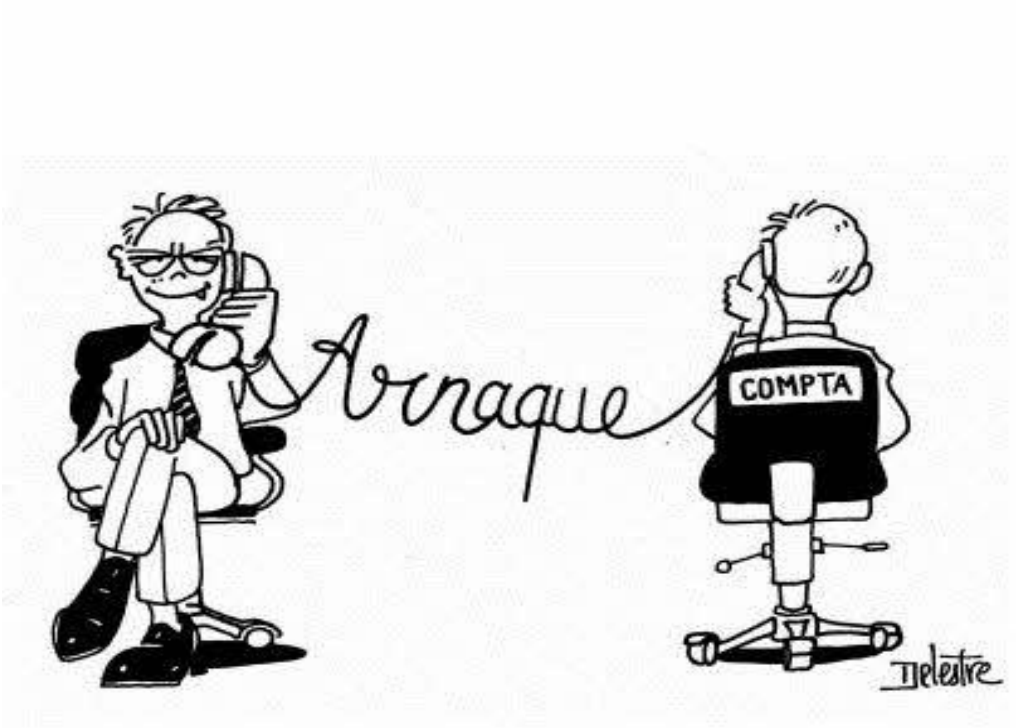
- se tenant informées de toutes les nouvelles possibilités d'usurpation d'identité, de piratage et en adaptant leur organisation en conséquence ;
- vérifiant le nom de domaine et la syntaxe de l'adresse mail source de l'information ;
- s'assurant de la présence d'une certification de l'e-mail de l'émetteur, lorsque ce procédé a été mis en place chez l'émetteur ;
- vérifiant l'information auprès du canal des diffuseurs agréés par l'AMF.

A cet effet et en vue de faciliter la vérification par les journalistes, l'AMF a l'intention de publier sur son site internet une liste indiquant le nom du diffuseur correspondant à chaque émetteur coté sur Euronext, pour les très nombreux émetteurs qui ont recours à un diffuseur.

Une attaque par HoaxCrash se réalise en 5 à 7 minutes.

Compte-tenu de la vitesse de réaction des marchés, la réponse aux attaques par HoaxCrash ne peut être qu'algorithmique.

II
Les attaques FOVI et arnaques au Président



TOP 5 DES TENTATIVES DE FRAUDES

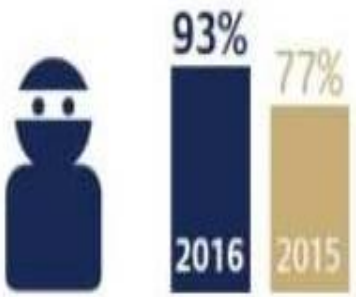
1. 
   Fraudes au président
   55%

2. 
   Faux fournisseurs
   47%

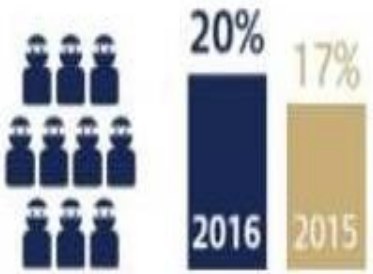
3. 
   Autres usurpations d'identité
   (type banques, avocats…)
   35%

4. 
   Cyber-fraudes
   (intrusions dans les systèmes informatiques)
   32%

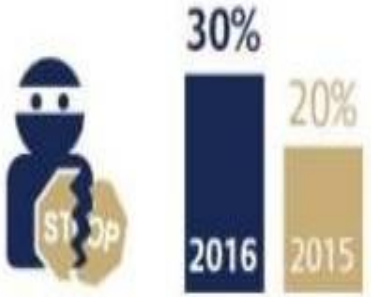
5. 
   Faux clients
   28%



des entreprises ont été victimes (d'au moins) une tentative de fraude dans l'année écoulée



ont connu plus de 10 tentatives de fraude sur cette même période !



répondent qu'ils n'ont pas réussi à déjouer toutes les tentatives de fraude

Fraude aux Faux Ordres de VIrement #FOVI

1

L'escroc collecte des informations pour connaître l'entreprise et ses dirigeants (réseaux sociaux, organigramme)

2

Se faisant passer pour le dirigeant de l'entreprise, l'escroc prétexte une opération financière urgente et confidentielle

3

Sous la pression ou en confiance, l'entreprise exécute la transaction

4

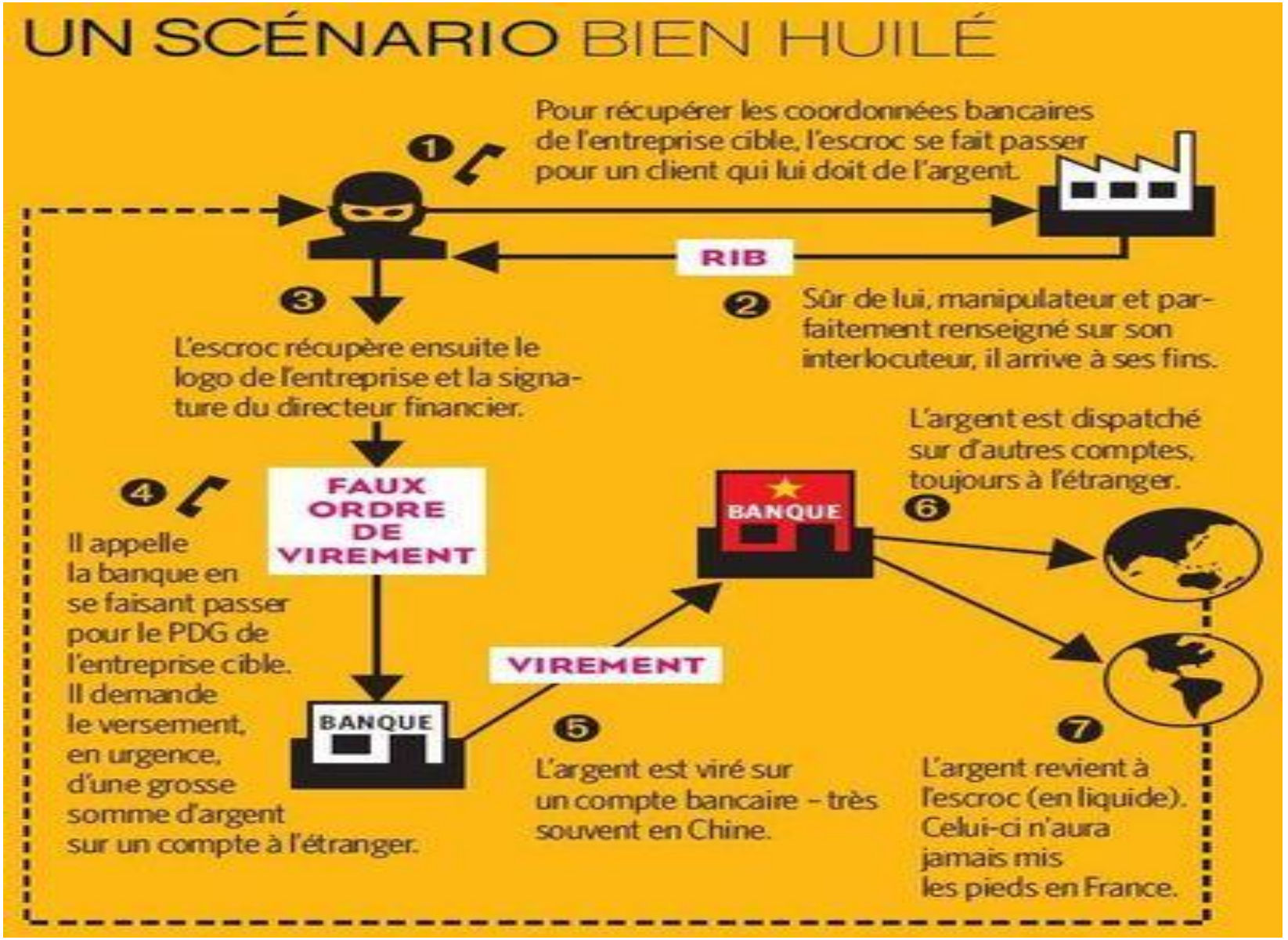
L'escroc transfère l'argent vers des comptes basés à l'étranger

POLICE NATIONALE

NOTRE VOCATION, C'EST VOUS !

@PNationale / Police Nationale

UN SCÉNARIO BIEN HUILÉ



Etape 1

- Etude du rôle des employés de la société ciblée (exploitation des réseaux sociaux, site web de l'entreprise, ...)

Etape 2

- Montage d'un scénario crédible (rachat d'une entreprise, demande du Directeur financier, d'un fournisseur,...)

Etape 3

- Prise de contact avec la cible (par mail puis par téléphone, en usurpant l'identité d'un client, d'un fournisseur, d'un avocat,...)

Etape 4

- Exploitation de la cible & Social Engineering (signature d'une clause de confidentialité, pouvoir hiérarchique, autorité extérieure, dissuasion, installation de la confiance...)

Suite a notre entretien téléphonique concernant la déclaration C1 incomplète, a ce jour et dans le cadre d une vérification de toutes transactions financières en France.

Veuillez nous faire parvenir les éléments suivants :

-La liste de vos clients Français actuels
(uniquement les réglements par virement bancaire)
- Adresses postales ainsi que numéro SIREN
-Coordonnées téléphoniques

EULER HERMES
Our knowledge serving your success

DFCG
ASSOCIATION NATIONALE
DES DIRECTEURS FINANCIERS
ET DE CONTRÔLE DE GESTION

Communiqué de presse

Etude Euler Hermes / DFCG 2017

De la cybercriminalité à la fraude : une menace en pleine mutation

57% des entreprises françaises ont été victimes d'une cyberattaque en 2016

- 8 entreprises sur 10 ont subi au moins une tentative de fraude en 2016
- 25% des entreprises ont subi plus de 10 tentatives de fraude en 2016
- La fraude au « faux président » est la plus citée (59%), suivi par la cyberattaque (57%)

De l'usurpation d'identité au risque cyber : la fraude, une menace protéiforme

Parmi les tentatives de fraude les plus courantes, celle au « faux président » est la plus citée par les répondants (59%). Elle est suivie par d'autres typologies de fraudes reposant sur l'usurpation d'identité : les « faux fournisseurs » (56%), les « faux clients » (25%), ou encore les « faux banquiers, avocats ou commissaires au compte » (29%). Mais le phénomène marquant de cette édition est l'explosion de la cybercriminalité : 57% des entreprises déclarent avoir subi une cyberattaque en 2016 (32% en 2015).

« Nous faisons face à une véritable explosion de ce type de fraude, qui se manifeste sous diverses formes. La plus répandue reste le ransomware, qui a touché 22% des entreprises répondantes l'année dernière. Le panorama des cyberfraudes évolue constamment, à l'image de ses auteurs, habitués à évoluer dans un univers technologique en pleine mutation. Les fraudeurs disposent plus facilement d'outils développés et puissants, permettant l'industrialisation de certaines attaques, d'où une menace croissante et protéiforme », expose Sébastien Hager, Expert Fraude chez Euler Hermes France.

L'étude souligne néanmoins que 63% des entreprises n'ont pas mis en place de plan d'urgence à activer en cas de fraude. Un chiffre inquiétant, la réactivité étant primordiale pour limiter le préjudice subi.

« Pour répondre à ce besoin d'information et de formation sur la fraude, la DFCG a mis en place une formation dédiée », souligne Sophie Macieira-Coelho. « Elle édite également des articles ou des dossiers consacrés à ce sujet dans la revue Finance&Gestion. De manière plus globale, la lutte contre la fraude s'inscrit dans une démarche de gestion des risques, sur lesquelles les entreprises gagnent à s'engager davantage. L'étude montre que seules 22% des entreprises ont réalisé une cartographie des risques, pourtant essentielle. Or la gestion des risques, notamment dans les PME, est prioritaire si l'on veut anticiper et prévenir plutôt que de subir les dommages. »

« 87% des entreprises interrogées redoutent que la fraude affecte lourdement leur trésorerie. S'assurer contre la fraude, c'est le moyen le plus efficace de se protéger d'un tel risque. Afin d'aider les entreprises à protéger proactivement leurs actifs, nous avons lancé en France en 2015 une solution d'assurance fraude qui couvre les pertes consécutives aux fraudes internes, externes et cyberfraudes, ainsi que certains frais induits. Puisque la réactivité est la clé d'une protection efficiente, nous proposons également un accompagnement personnalisé dès la découverte du sinistre, et une indemnisation dans les 30 jours après accord sur son montant », conclut Eric Lenoir.

Attaque FOVI létale pour une PME : Le cas BRM

L'attaque BRM Mobilier (2015 – 2016)

Etape 1 - début 2015 --> juillet 2015
Les attaquants collectent des informations sur l'entreprise, sur ses dirigeants et sur le rôle des employés (44 salariés). Ils ont également probablement piraté certains comptes d'employés et ont eu accès à la messagerie interne.

Etape 2 - début 2015 --> juillet 2015
Les attaquants construisent un scénario plausible, crédible et cohérent avec les informations récoltées : Ils se font passer pour un cabinet d'avocats.

L'attaque BRM Mobilier (2015 – 2016)

Etape 3 - 21 juillet 2015
Les attaquants contactent la Directrice administrative et financière par mail puis par téléphone. Ils obtiennent un premier virement vers la Thaïlande sur une requête de paiement d'une facture à fournisseurs non réglée.

Etape 4 - 21 juillet 2015 --> septembre 2015
Les attaquants maintiennent leur échanges avec la Directrice Financière de BRM et obtiennent de nouveaux virements cette fois vers la Chine. La "facture" est fractionnée en plusieurs petits virements.
27 janvier 2016 : BRM Mobilier est placée en liquidation judiciaire. le montant total détourné par l'attaquant s'élève à 1,6 Millions d'Euros.

BRM escroquée

L'arnaque de 1,6 million d'euros menace de couler BRM

08/09/2015 11:06

Le cauchemar que vivent les 44 salariés de BRM (Bressuire) semble irréel. Victime d'une arnaque au président que l'on croit habituellement réservée aux grosses entreprises et aux magazines à sensation, ils sont pourtant menacés de chômage suite à la disparition de près de 1,6 millions d'euros des caisses de l'entreprise de fabrication de meubles.

L'escroquerie a été découverte le 1er septembre dernier par la direction. A quelques heures d'un comité d'entreprise de rentrée habituel, Jean Brossier, son PDG, a découvert que les comptes avaient été vidés de leur contenu dans l'été. *"Lors de ce comité d'entreprise, la direction ne savait pas encore ce qui s'était passé"*, racontent les représentants du personnel. *"Ils nous ont demandé de leur laisser le temps de déterminer ce qui s'était passé. Mais la situation a été officialisée deux jours plus tard, le 3 septembre, lors d'un comité d'entreprise extraordinaire."*

Une arnaque à 1,6 millions d'euros

Le scénario reconstitué par la direction est classique. Entre le 21 juillet et le 14 août, un escroc a usurpé le compte mail de Jean Brossier puis contacté par téléphone l'entreprise sous le sceau de la confidentialité. Il prétendait être le représentant d'un cabinet d'expertise comptable et d'un avocat et agir dans le cadre d'une stratégie de rachat d'une entreprise par BRM. Il a ainsi obtenu plusieurs versements d'un montant total de près de 1,6 million d'euros. *"Nous pensons qu'on espionnait nos comptes mails parce que cette escroquerie est survenue au moment où nous avions reçu les règlements de plusieurs grosses commandes"*, supposent les représentants du

Crédit BRM Bibliothéques

Placée en redressement judiciaire depuis mi-septembre, l'entreprise BRM Mobilier à Bressuire (Deux-Sèvres), entreprise du groupe financier belge MecaSeat via la SPCM, a été liquidée le 27 janvier par le tribunal de commerce de Niort. Cette décision entraine la cessation de l'activité d'ici fin mars afin d'honorer les dernières commandes. 42 salariés se retrouvent sans emploi.

"*Nous nous attendions à cette décision, mais ça fait très mal*, constate Sylvie Hérault, représentante CFDT, salariée de l'entreprise depuis 8 ans. *Nous avions encore 2 millions d'euros de commandes dans le carnet. Mais en vain. Pas de repreneur retenu, un délai trop court pour proposer une Scop et pas de plan de sauvegarde, nous sommes livrés à nous-même et dans un territoire comme le nôtre, il va être difficile pour certains de se retourner.*"

Le fabriquant de mobilier pour bibliothèques et médiathèques, qui jouissait d'une notoriété de plus de 60 ans, a été victime d'une "fraude au président" (escroquerie qui consiste à exiger d'une entreprise un virement en se faisant passer pour l'un de ses dirigeants) qui a privé la trésorerie de l'entreprise de 1,6 million d'euros. L'enquête est désormais sous l'autorité du tribunal de grande instance de Rennes (Ille-et-Vilaine).

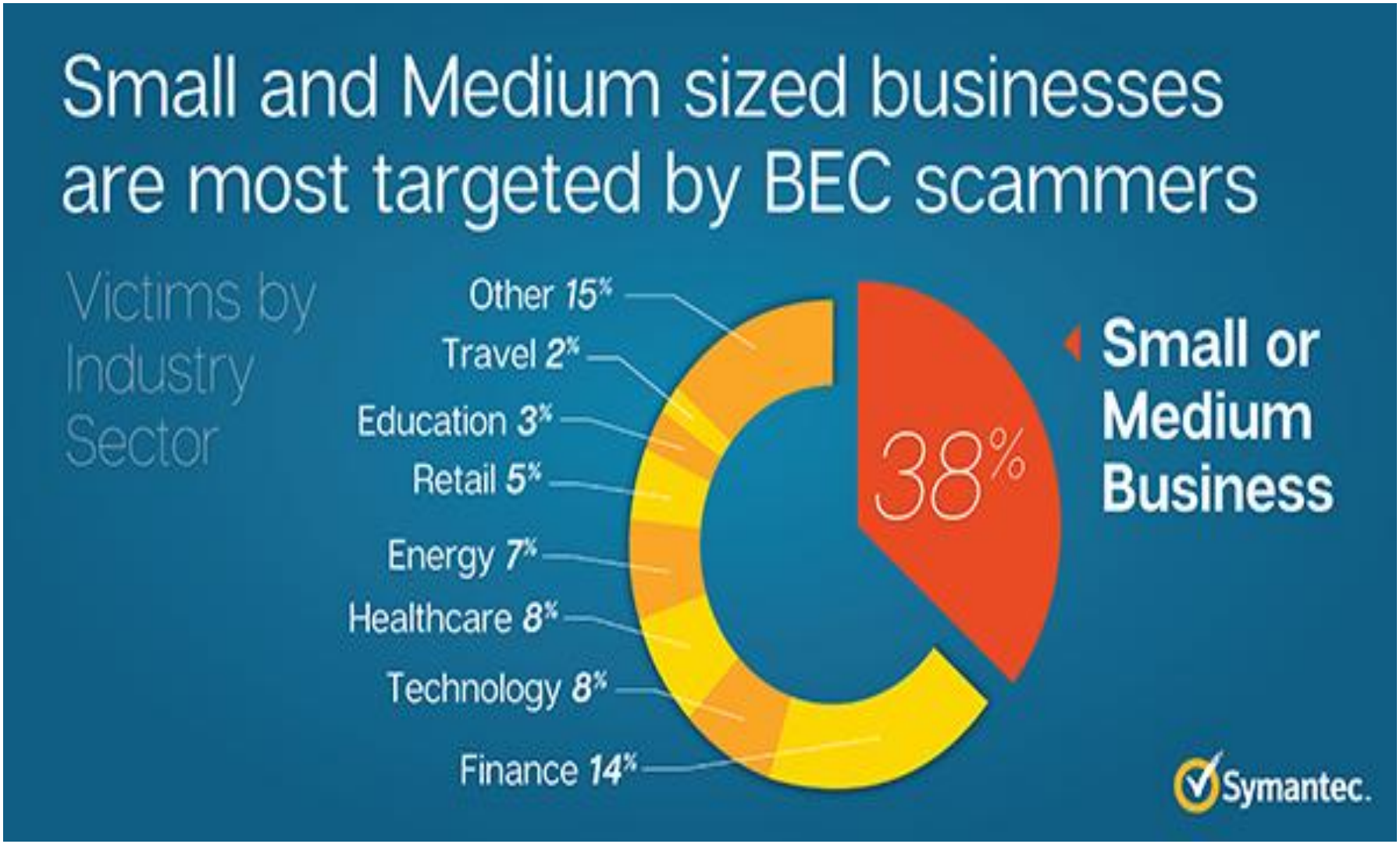
Lydia de Abreu

Au niveau mondial…

L’étude SYMANTEC (juillet 2016)
BEC Fraud - Billion-dollars scams

https://www.symantec.com/connect/blogs/billion-dollar-scams-numbers-behind-bec-fraud

Etude SYMANTEC BEC Scammers – juillet 2016

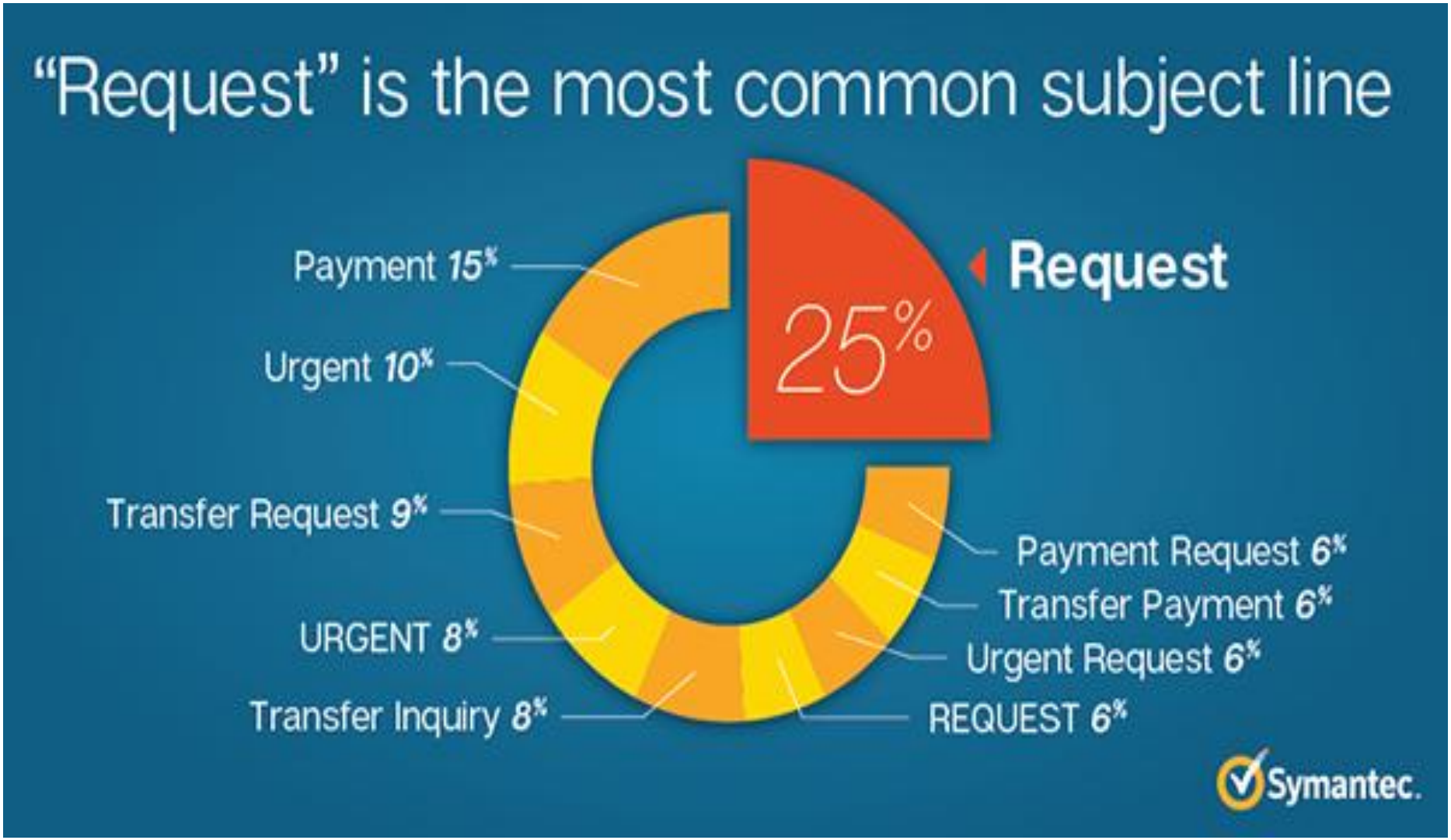


Etude SYMANTEC BEC Scammers – juillet 2016

Etude SYMANTEC BEC Scammers – juillet 2016

Etude SYMANTEC BEC Scammers – juillet 2016

Etude SYMANTEC BEC Scammers – juillet 2016



III
La plateforme ALETHEIA

Détecter le faux, sécuriser le vrai

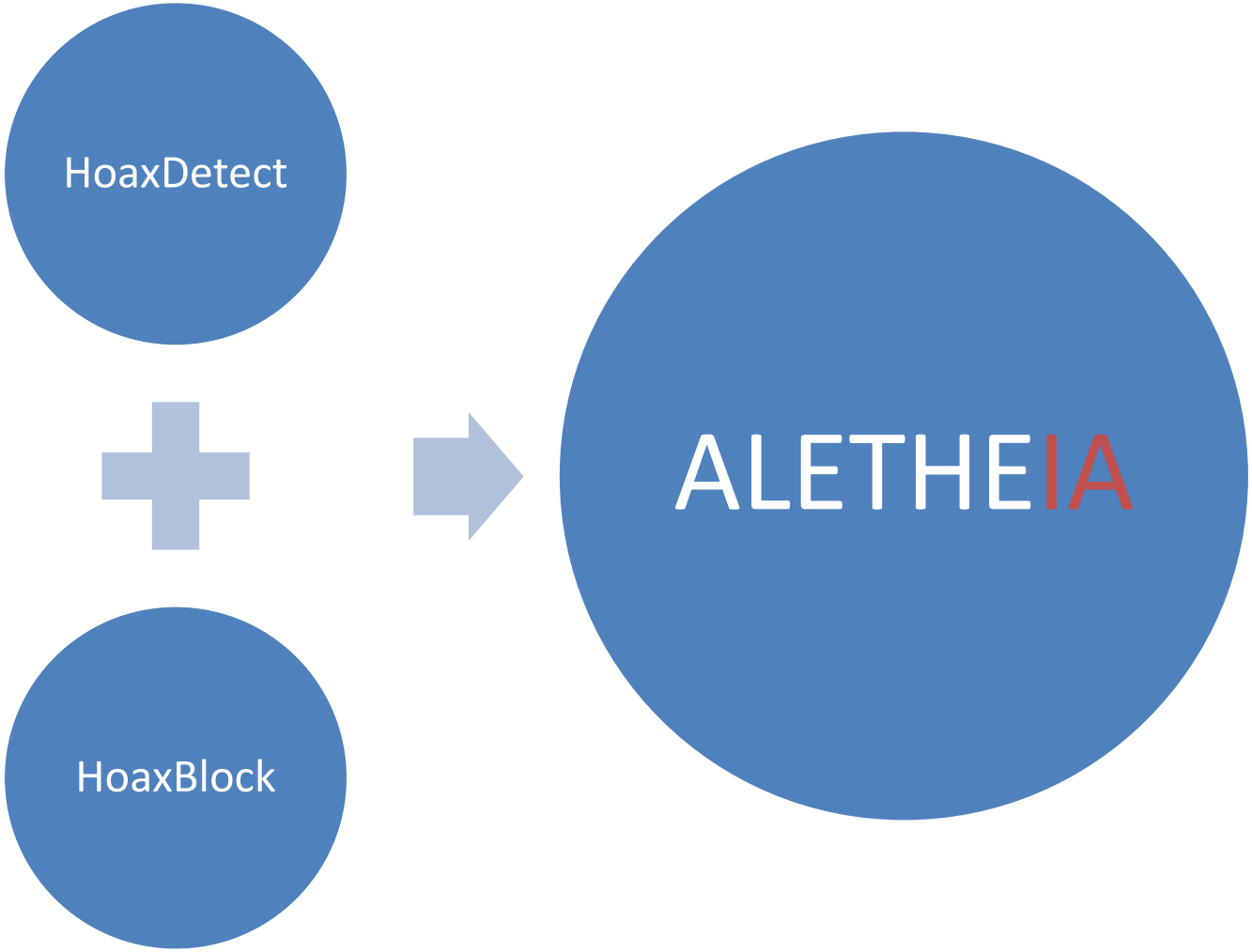
Nous développons trois solutions de cybersécurité

1 HoaxDetect

2 HoaxBlock

3 FOVIDetect

Plateforme de lutte contre les HoaxCrash



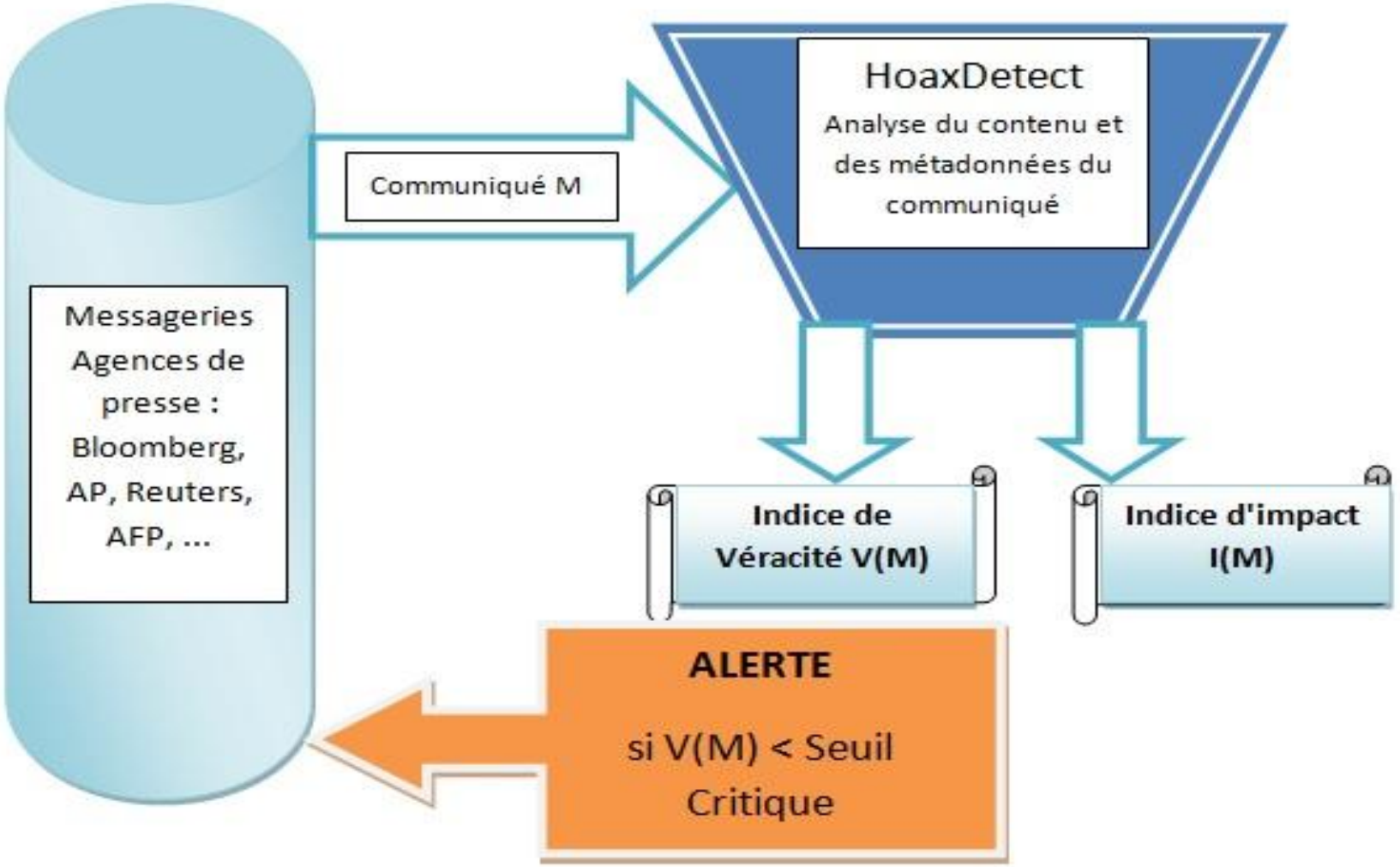
1 - HoaxDetect

HoaxDetect est destiné aux agences de presse spécialisées (Bloomberg, Reuters, Associated Press, AFP, ….) qui diffusent des informations financières. Son noyau s'appuie sur un moteur de règles associé à des technologies classiques de NLP et à une métrique sémantique spécifique.

HoaxDetect analyse les messages et communiqués (contenu et métadonnées associées, mail, pdf, word). Il calcule un indice de véracité et une hauteur d'impact du message par rapport à une base de scénarios de Hoax, de contextes et d'acteurs.

Lorsque l'indice de véracité atteint un niveau critique, HoaxDetect produit automatiquement des alertes « Hoax probable ».

HoaxDetect


Messageries
Agences de presse : Bloomberg, AP, Reuters, AFP, ...
Communiqué M
HoaxDetect
Analyse du contenu et des métadonnées du communiqué
Indice de Véracité V(M)
Indice d'impact I(M)
ALERTE
si V(M) < Seuil Critique

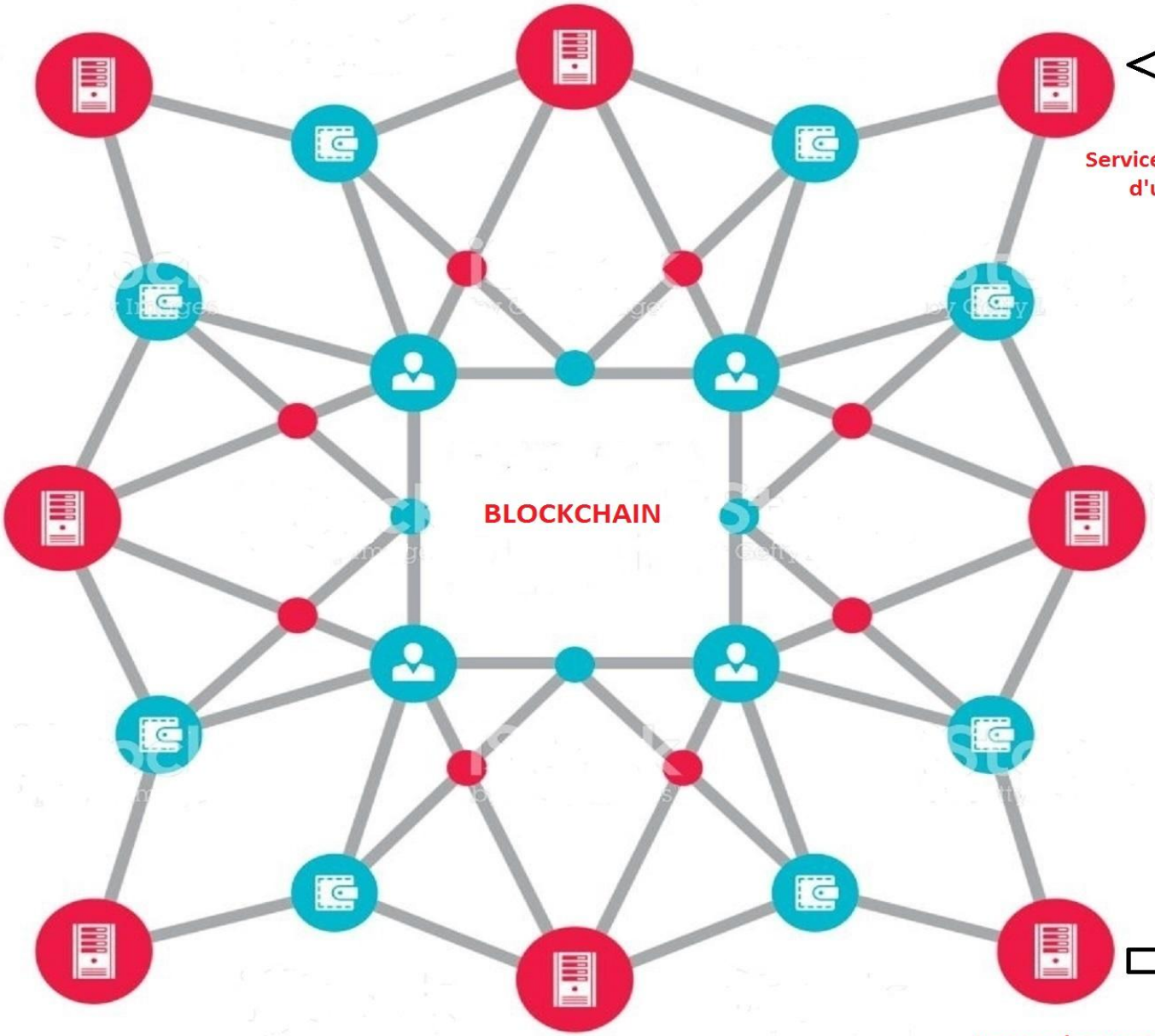
2 - HoaxBlock

Destiné aux directions de la communication des groupes cotés en bourse et aux agences de presses, HoaxBlock s'appuie sur une architecture Blockchain.

Cette architecture permet à ces services de diffuser des communiqués de presse de manière sécurisée et offre aux agences la garantie d'une information certifiée.

L'entrée du diffuseur légitime dans la chaîne de blocs s'effectue via une authentification forte (biométrie), garantissant l'intégrité du message.

HoaxBlock



Communiqué de presse

Service de communication d'une société cotée

Communiqué de presse

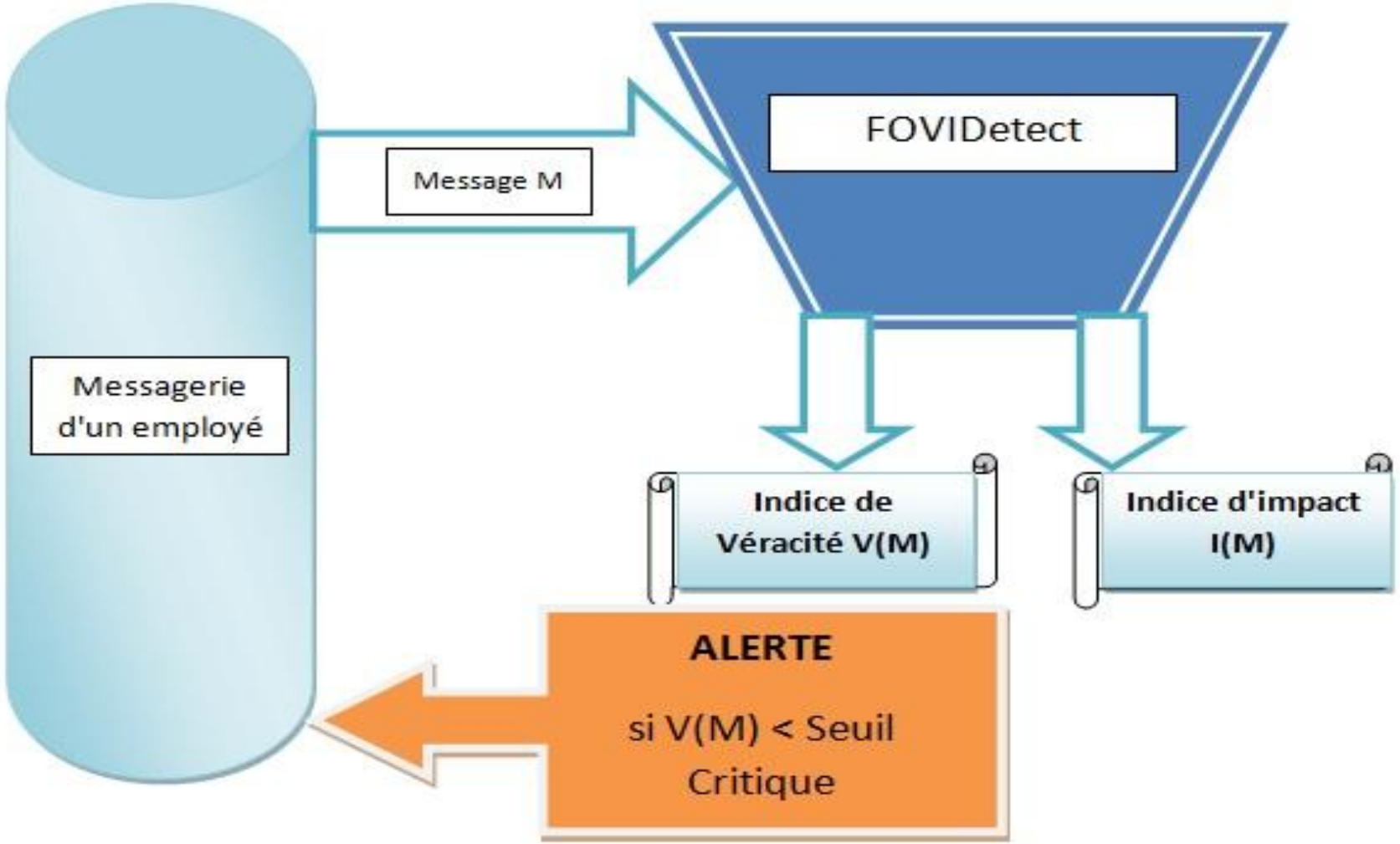
Agence de presse (Bloomberg, Associated Press, Reuters, AFP, ...)

3 - FOVIDetect

FOVIDetect est un détecteur de fraudes FOVI dont la technologie est dérivée de celle de HoaxDetect. Il est destiné à toutes les PME-PMI et grands groupes potentiellement victimes de tentatives d'attaques FOVI (Faux Ordre de Virement), Changement de RIB, Arnaques au Président (2300 plaintes d'entreprises françaises depuis 2013 et plus de 500 Millions d'euros de préjudice en France).

FOVIDetect agit de manière transparente, au dessus de la messagerie des personnels du service de comptabilité de la PME cliente. Il analyse en temps réel les messages reçus (NLP) et détermine un indice de véracité et une hauteur d'impact du message. Lorsque cet indice est inférieur à un seuil critique, FOVIDetect produit des alertes et sollicite des confirmations avant tout virement frauduleux.

FOVIDetect


FOVIDetect
Message M
Messagerie d'un employé
Indice de Véracité V(M)
Indice d'impact I(M)
ALERTE
si V(M) < Seuil Critique

Perspectives

Les structures de données fictives utilisées comme leurres cognitifs au cours d'une cyberattaque doivent faire l'objet d'une détection généralisée. Il faut étendre les détecteurs de faux aux autres types de données, en particulier aux images et aux vidéos.

La détection automatique (par procédés hybrides) des structures de données massives va devenir prioritaire pour les Etats, avec des enjeux de sécurité importants (cf. le programme lancé par la DARPA fin 2016 sur la détection des fausses images et des fausses vidéos et le démonstrateur d'une vidéo d'un discours fictif de Barack Obama créé via une plateforme de deep learning).

MERCI

http://cyberland.centerblog.net/

CYBERLAND

https://fr.slideshare.net/OPcyberland/presentations

http://www.chaire-cyber.fr/