Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

# INGERENCE ECONOMIQUE

Flash n° 22 - Mars 2016

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Vous comprendrez que, par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à : securite-economique@interieur.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°22 Mars 2016

# Les escroqueries aux faux ordres de virement internationaux, une menace protéiforme

Fondées sur les techniques d'ingénierie sociale, les escroqueries aux faux ordres de virement internationaux (FOVI) se sont considérablement développées ces dernières années, recouvrant des modes opératoires toujours plus divers et sophistiqués.

Incontournables aujourd'hui, la numérisation massive des données au sein de l'entreprise et l'utilisation des réseaux sociaux offrent en contrepoint aux escrocs un vaste champ d'opération, facilitant la mise en œuvre de ce type d'escroqueries aux conséquences financières et réputationnelles souvent critiques pour les entités ciblées.

La menace repose principalement sur l'exploitation de vulnérabilités d'origines humaine, technologique et organisationnelle. Parmi les méthodes d'escroqueries FOVI les plus communément utilisées, on relèvera :

- **La fraude dite « au président » et ses diverses variantes** consiste à usurper l'identité d'un chef d'entreprise, d'un haut dirigeant ou d'un sous-traitant de l'entreprise ciblée. Le modus operandi consiste à exiger du service financier ou comptable de procéder, dans l'urgence, à un virement bancaire sur un compte situé en France où à l'étranger, au titre d'une opération nécessitant la plus grande confidentialité. La fraude peut s'effectuer par téléphone, courriel ou fax. Elle intervient fréquemment juste avant un week-end.

- **La fraude dite « au loyer »**, autre variante de la fraude au président, consiste à usurper l'identité du bailleur qui loue les locaux de l'entreprise ciblée. L'objectif est de communiquer au service comptable ou financier de l'entreprise un changement de références bancaires sur lesquelles les virements devront désormais être effectués. La fraude peut également s'effectuer par téléphone, courriel ou fax.

Au cours de l'année 2015, un nombre croissant de ces escroqueries a été constaté. Les trois exemples exposés ci-après ont pour but de rappeler aux entreprises et à leurs salariés la permanence de la menace, la diversité des méthodes d'attaque, la variété des profils ciblés et enfin leurs conséquences pour les sociétés victimes.

**1er exemple**

Le service comptable d'un hôtel a reçu un appel téléphonique d'une personne se présentant comme le gérant d'un établissement prestataire habituel de l'hôtel, afin qu'il procède à un changement de coordonnées bancaires pour les paiements à venir.

La prise en compte de cette modification, sans contrôle préalable du service comptable, a permis de procéder au virement de plus de 27 000 euros sur un compte domicilié en métropole. L'escroquerie n'a été **découverte que trois mois plus tard**, à la suite d'une relance, pour services impayés, de la société prestataire légitime.

**2ème exemple**

En usurpant l'adresse email professionnelle du président d'une PME puis en se faisant passer respectivement pour l'avocat et l'expert-comptable en charge de négociations, des escrocs ont réussi à convaincre le comptable de ladite PME de procéder, en quelques jours, à des virements bancaires vers des établissements financiers situés dans des pays asiatiques, prétextant le rachat imminent d'une entreprise.

Compte tenu du montant de l'escroquerie (plus d'un million d'euros) et faute de trésorerie pour absorber la perte, **la PME a été placée en liquidation judiciaire quelques mois plus tard**.

**3ème exemple**

Le service financier d'un groupe industriel français a été victime d'une tentative de fraude « au président », déjouée *in extremis*.

Dans le cas d'espèce, la formulation des échanges correspondait en tous points au style de communication écrite du dirigeant. Outre l'usurpation de son adresse email personnelle, l'utilisation d'acronymes se rapportant à la société et la fine connaissance des noms et prénoms des interlocuteurs à contacter pour ce dossier ont particulièrement pris en défaut les personnels sollicités.

Pour autant, des éléments ont permis à l'entreprise de déjouer la tentative d'escroquerie : l'absence de justification du virement et le souhait de transférer les fonds de l'entreprise tout juste fusionnée vers le compte personnel du dirigeant.

## Commentaires

Les motivations des auteurs d'escroqueries aux faux ordres de virement sont principalement crapuleuses. La connaissance générale de l'environnement de l'entreprise, la maîtrise technique des attaques informatiques et l'essor des réseaux sociaux conjugué au développement du numérique au sein des entreprises, contribuent à la recrudescence et à la réussite de ces délits.

La collecte d'un maximum de renseignements sur l'entreprise visée et son écosystème (personnels, organisation, présence sur les réseaux sociaux) constitue un préalable à la technique d'ingénierie sociale, permettant d'identifier à la fois les cibles et les leviers d'attaque et de parfaire la crédibilité de l'auteur.

L'usage d'un courriel piégé visant à infiltrer le ou les ordinateurs des personnes ciblées sert aussi fréquemment de levier, discret et peu coûteux, pour procéder à la captation d'informations.

## Préconisations de la DGSI

Compte tenu des évolutions et de la recrudescence de ces escroqueries, sont préconisées les mesures suivantes :

- Sensibiliser et informer l'ensemble des salariés sur les modes opératoires de ces tentatives d'escroqueries, les moments où elles sont susceptibles de se produire (veille de week-end, période de congés du dirigeant, etc...) et les procédures de vérification permettant de les déjouer.

- Identifier et cartographier les personnes-clés en charge du risque financier dans l'entreprise afin de sécuriser les procédures de virements bancaires, en France où à l'international (mise en place d'une chaîne de vérification et de validation fiable, désignation d'un interlocuteur habituel avec des coordonnées téléphoniques connues, etc…).

- Responsabiliser les salariés au strict respect des procédures mises en place par l'entreprise, mais aussi aux informations qu'ils sont amenés à laisser sur les réseaux sociaux professionnels (LinkedIn, Viadeo, Xing, etc…) et non professionnels (Facebook, Twitter, etc...), qui constituent une source privilégiée de renseignements précieux pour des escrocs soucieux de parfaire leur connaissance de la cible, voire d'en identifier une.

- Sécuriser de manière efficace les systèmes d'information (mise à jour des anti-virus, Firewalls, etc…) et sensibiliser les utilisateurs finaux aux risques liés aux outils numériques.