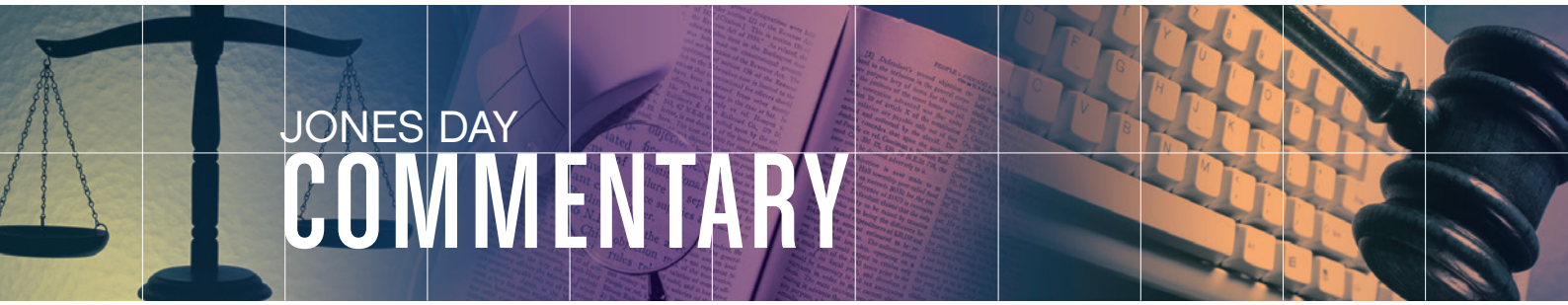
AOÛT 2013



LES ENTREPRISES VICTIMES D'ESCROQUERIES AUX FAUX ORDRES DE VIREMENT INTERNATIONAUX, UNE MENACE CROISSANTE

Les escroqueries massives d'ampleur internationale appelées « escroqueries aux faux ordres de virement internationaux » (« FOVI ») ciblent, depuis environ 2 ans, les filiales de grandes entreprises françaises situées au sein de l'Union Européenne ou les filiales étrangères d'entreprises installées en France.

Sur le plan national, ce phénomène représente, sur cette même période, plus de 400 infractions tentées ou commises, dont le préjudice est estimé à plus de 200 millions d'euros.

Les auteurs de ces infractions opèrent tous par téléphone selon l'Office Central pour la Répression de la Grande Délinquance Financière (« OCRGDF ») de la Direction Centrale de la Police Judiciaire qui a parfaitement identifié le mode opératoire de ces escrocs. Le traçage des virements frauduleux a notamment permis de déterminer que les fonds avaient pour destination finale la Chine et plus particulièrement les banques de la province du Zhejiang.

Pour organiser leurs « escroqueries aux faux ordres de virement internationaux », les groupes criminels organisent leurs actions en plusieurs étapes :

LES ACTES PRÉPARATOIRES AUX ESCROQUERIES

Tout d'abord, le groupe criminel constitue le « social engineering » des entreprises cibles. A cet effet, le groupe criminel achète via Internet, auprès d'organismes tels que « Infogreffe », les informations pertinentes sur l'entreprise, à savoir l'extrait du Registre du commerce et des sociétés (« Extraits K-bis »), l'état d'endettement, les derniers statuts mis à jour, les statuts constitutifs, les derniers actes déposés, les procès-verbaux d'assemblée générale, les comptes annuels, l'historique des modifications, etc. Le dossier complet de l'entreprise, portant les noms de tous les dirigeants, leurs fonctions, leurs numéros de téléphone, leurs signatures… ne coûte qu'une soixantaine d'euros !

Une simple recherche sur internet permet à ces groupes de compléter le dossier de «social engineering» : codes de l'entreprise, logos, effectifs, parfois même « le mot du directeur » ... et de leur donner une vision complète de l'entreprise, de son langage, de ses marques.

Le groupe criminel acquiert ensuite les adresses mail, les numéros de fax et de téléphone pour pouvoir communiquer avec la future victime sans que cette dernière ne puisse se rendre compte du lieu d'établissement des escrocs.

Tous les éléments nécessaires à une attaque ciblée sur une entreprise sont alors entre les mains du groupe criminel. Il est en outre indéniable que l'obtention du « social engineering » a été facilitée par les nouvelles technologies.

LE DANGER DES NOUVELLES TECHNOLOGIES

L'utilisation de cartes de paiement prépayées rechargeables pour les achats d'informations auprès d'Infogreffe a été identifiée par les enquêteurs. Ce type de carte présente l'avantage pour son titulaire d'être anonyme et intraçable. Cependant, le subterfuge ayant été découvert, les escrocs subtilisent désormais fréquemment des numéros de cartes bancaires pirates sur Internet pour effectuer leurs achats sur Infogreffe.

La téléphonie utilisée repose sur le même principe : l'achat de numéros de téléphone auprès de plateformes dématérialisées au moyen de cartes de paiement prépayées rechargeables ou de cartes bancaires piratées.

Ce procédé simple repose sur l'acquisition de numéros de téléphone, pour une somme modique (une dizaine d'euros par mois) qui aura l'indicatif du pays demandé. Si l'entreprise cible est une filiale d'une entreprise française à l'étranger, les numéros de téléphone et de fax achetés commenceront par l'indicatif français, ce qui évitera d'éveiller les soupçons de l'interlocuteur.

LE MODE OPÉRATOIRE

Muni des informations essentielles sur la société cible et utilisant un numéro de téléphone français en apparence, l'escroc va appeler, à titre d'exemple, une filiale à l'étranger de la société cible. Il se fait alors passer pour le dirigeant de l'entreprise et tente de persuader son interlocuteur (généralement le directeur financier de la filiale) d'effectuer un virement sur un compte à l'étranger. L'escroc justifie cette demande inhabituelle et urgente par l'imminence d'un contrôle fiscal, la réalisation d'une opération boursière ou autre, selon son imagination. Usant de stratagèmes psychologiques divers et variés tels que les menaces ou les flatteries, l'escroc va convaincre le salarié ayant pouvoir de signature de procéder au virement.

L'argent sera ensuite compensé, grâce à un système financier élaboré, entre les différents groupes criminels agissant en Israël, en Chine et en France. Ces trois pays ont été identifiés dans cette escroquerie selon le schéma suivant :

- Israël en tant que base arrière d'où les escrocs opèrent par téléphone,
- la France en tant que pays dans lequel se trouvent les entreprises cibles,
- la Chine (Pékin, Wenzhou (province du Zhejiang) et Hong Kong) comme lieu de destination des virements.

Deux groupes de malfaiteurs opérant selon ce modus operandi ont d'ores et déjà été interpellés en France en 2011 et 2012 grâce à l'intervention de l'OCRGDF. Cependant, le phénomène perdure. D'ailleurs, ces réseaux criminels ont désormais compris qu'il fallait former leurs équipes en langue anglaise afin d'étendre l'escroquerie à un plus grand nombre de pays.

La lutte contre cette criminalité organisée nécessite un déploiement d'actions de prévention auprès des entreprises françaises, des banques et de la presse économique spécialisée pour toucher le plus grand nombre de responsables.

Ainsi, face a ce modus operandi très efficace et particulièrement préjudiciable à l'économie nationale, une vigilance renforcée de toutes les entreprises est nécessaire à tous les échelons de leur hiérarchie.

Dans ce domaine, la coopération « public-privé » nationale et internationale est fondamentale pour agir au plus vite sur les blocages de comptes, l'argent pouvant circuler à travers plus de trois pays en moins de 24h. L'Office Central pour la Répression de la Grande Délinquance Financière est chargé de centraliser l'ensemble des informations au plan national pour ce type de fraude.

Il existe plusieurs outils permettant aux entreprises de faire face à ce type de fraude :

Sensibiliser régulièrement en interne sur la fraude. Tous les collaborateurs de l'entreprises doivent être prévenus et en particulier les services comptables et financiers, ainsi qu'au sein des filiales installées à l'étranger, afin de renforcer le niveau de vigilance.

Informer les salariés sur les dangers des nouvelles technologies. Les escrocs peuvent facilement se procurer des données très précises sur le fonctionnement des sociétés victimes via notamment les réseaux sociaux. Il est ici recommandé de rappeler aux salariés de l'entreprise l'importance de ne pas livrer sur les réseaux sociaux des informations qui pourraient être utilisées aux dépens de l'entreprise (telles que certaines données personnelles, les coordonnées ou encore le planning des dirigeants, tout acte présentant la signature d'un membre de la direction, le cachet de l'entreprise…).

Faire réaliser un audit des procédures internes de virement bancaire. Il est également recommandé de déceler en amont les failles éventuelles des procédures internes d'autorisation et d'exécution des virements bancaires ainsi que leur application par les services comptables et financiers.

Instaurer des procédures internes efficaces afin de sécuriser l'autorisation et l'exécution des virements bancaires. Peuvent notamment être envisagés : un système de signatures multiples strict pour tous les virements internationaux (certains logiciels permettent de bloquer toute opération qui n'aurait pas reçue une contre-validation), un système de signature par code ou électronique modifiée régulièrement, une procédure de vérification intragroupe permettant de recouper toute demande de paiement ou encore l'utilisation du réseau intranet de l'entreprise. Il est important d'exclure de ces procédures toute demande orale.

Mettre en place un partenariat avec les banques. Instaurer des procédures de sécurisation des virements bancaires avec les banques de l'entreprise peut être particulièrement efficace.

L'entreprise victime d'une escroquerie aux faux ordres de virement internationaux doit en urgence et en priorité :

- Faire opposition aux virements au sein de l'établissement bancaire concerné afin de bloquer le transfert des fonds. Le temps de réaction est en effet décisif dans ce type de fraude.
- Mandater en urgence un cabinet d'avocats sur le lieu de destination des virements bancaires obtenus frauduleusement (généralement la Chine) pour faire opposition au transfert des fonds sur le compte bancaire destinataire des transferts, au moyen d'une procédure de saisie conservatoire du compte bancaire concerné.
- Déposer plainte auprès du Procureur de la République du lieu de commission de l'infraction, d'informer l'OCRGDF et de procéder à une enquête interne afin de constituer un dossier complet sur la fraude permettant de comprendre son déroulement.

CONTACT

Bénédicte Graulle
Paris
+33.1.56.59.46.75
bgraulle@jonesday.com