CAISSE D'EPARGNE ILE-DE-FRANCE

LES ESCROQUERIES AUX FAUX ORDRES DE VIREMENTS INTERNATIONAUX[1]

Depuis environ trois ans, les filiales de grandes entreprises françaises situées au sein de l'Union Européenne, ou des filiales étrangères d'entreprises installées en France sont victimes de vagues d'escroqueries très importantes, appelées escroqueries aux faux ordres de virements internationaux(FOVI).
Sur le plan national, ce phénomène représente, sur cette même période, environ un millier de faits tentés ou commis. Le préjudice se chiffre en centaines de millions d'euros.
Le mode opératoire traditionnel de ces escrocs qui opèrent généralement par téléphone depuis Israël a été parfaitement défini. Les fonds tracés ont pour destination finale la Chine[2], et plus particulièrement les banques de la province du Zhejiang.
Plus récemment des variantes ont vu le jour, les escroqueries aux loyers, les escroqueries aux nouvelles coordonnées bancaires fournisseurs et les escroqueries aux virements SEPA avec un recours croissant à l'informatique.

1. Le mode opératoire traditionnel

Un groupe criminel va tout d'abord constituer, ce qu'il est convenu d'appeler, le «social engineering» des entreprises cibles. Cela passe par l'achat, à partir d'Internet, auprès d'organisme comme «Infogreffe», des extraits du Registre du commerce et des sociétés (K-bis), de l'état d'endettement de l'entreprise, de ses derniers statuts mis à jour, des statuts constitutifs, des derniers actes déposés, des procès-verbaux d'assemblée générale, des comptes annuels, de l'historique des modifications, etc. Ce dossier complet de l'entreprise, portant les noms de tous les dirigeants, leur fonction, numéros de téléphone, signatures, etc. ne coûte qu'une soixantaine d'euros…
De même, une recherche en source ouverte (Internet) permet de compléter le dossier de «social engineering». Logo de l'entreprise, effectifs, adresses mail, «le mot du directeur» donnent une vision complète de l'entreprise, de son langage, de ses marques, etc.
L'étape suivante passe par l'acquisition d'adresses mail, de numéros defax, et de téléphonie.
Tous les éléments permettant de lancer des attaques ciblées sur des entreprises sont entre les mains du groupe criminel. L'obtention du «social engineering» a été facilitée par les nouvelles technologies.

Les nouvelles technologies, une aide indéniable aux groupes criminels

Il a été mis en évidence l'utilisation de cartes de paiement prépayées rechargeables pour les achats d'informations auprès d'Infogreffe. Il s'agit, pour l'essentiel, de cartes de la marque ICC (Israël Credit Cards). Ce type de carte, présente l'avantage pour son titulaire, d'être anonyme et intraçable. Les escrocs récupèrent également des numéros de cartes bancaires piratés sur Internet pour effectuer des achats sur Infogreffe.

Par ailleurs, la téléphonie utilisée repose sur le même principe: l'achat de numéros de téléphones, auprès de plateformes de dématérialisation, au moyen de cartes de paiement prépayées rechargeables.
Ce procédé simple repose sur l'acquisition de numéros de téléphone, pour une somme modique (une dizaine d'euros par mois). 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 mettra en confiance l'interlocuteur qui recevra l'appel.

Les recours à des virus informatiques

S'adaptant aux nouvelles technologies, les escrocs utilisent sans cesse de nouveaux modes opératoires consistant à contacter les sociétés pour des motifs divers (migration SEPA, fausses factures, audit, etc.) afin qu'elles réceptionnent un fichier envoyé par mail contenant un virus ou « cheval de Troie ». Conçu pour exécuter des actions à l'insu de l'utilisateur, le programme malveillant ou malware peut ainsi ouvrir une «porte dérobée» lui permettant d'accéder secrètement à l'ensemble des fonctionnalités du logiciel et de prendre, à distance, le contrôle de l'ordinateur. Grâce à ce malware, les escrocs recueillent toutes les informations (codes administrateurs des responsables autorisés à conduire des transactions, noms d'utilisateurs, mots de passe, identifiants des emails) leur permettant d'émettre des faux ordres de virements.

Le déclenchement de l'attaque

Muni des informations sur la société cible, et utilisant un numéro de téléphone apparaissant comme français, l'escroc appelle, par exemple, une filiale à l'étranger de la société française. Il se fait passer pour le dirigeant de l'entreprise et va persuader le directeur financier de la filiale d'effectuer un virement sur un compte à l'étranger. L'escroc donne comme justification l'imminence d'un contrôle fiscal, ou pour répondre à une concurrence déloyale etc. Il usera également de flatteries ou de menaces, pour convaincre le cadre 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 mis en évidence dans ce type d'attaques :

- Israël au départ, pays d'où les escrocs opèrent par téléphone,
- la France comme cible,
- la Chine (Pékin, Wenzhou (province du Zhejiang), Hong Kong) comme lieu de destination finale des virements après une première destination dans un pays européen (Grande Bretagne, Chypre, Roumanie, Slovaquie, Pologne, Autriche, Hongrie, Pays-Bas etc…).

1 Source FBF – Mise en garde du 16/04/2014
2 Se reporter au § « Déclenchement de l'attaque »

2. L'apparition de nouvelles formes de faux ordres de virements internationaux

L'escroquerie aux loyers

Lors de la commission de cette infraction le groupe criminel cible les organismes HLM, un escroc se présentant comme étant un responsable du bailleur de la société visée. Il contacte par téléphone un employé de l'entreprise et demande à joindre la personne chargée de valider les quittances de loyer. Il indique alors au service de la comptabilité qu'un changement de domiciliation bancaire va avoir lieu et précise que désormais le loyer devra être viré sur le compte d'une société domiciliée à l'étranger. Il communique les nouvelles coordonnées bancaires à la victime à l'aide d'un mail dont l'adresse est proche de celle du véritable bailleur et qui présente un logo identique à celui de la société dont l'identité a été usurpée. Pour rassurer la victime, l'auteur des faits précise que la gestion du bien immobilier et la perception du loyer ont été cédées à cette société étrangère et communique de faux justificatifs dans ce sens.

L'escroquerie aux nouvelles coordonnées bancaires fournisseurs

L'attaque est similaire à celle perpétrée dans le cadre de l'escroquerie aux loyers.
Le mode opératoire est alors le suivant : l'escroc se faisant passer pour le fournisseur s'adresse à une entreprise cliente par courrier ou mail, indique avoir modifié ses coordonnées bancaires et demande à ce que les prochains règlements soient effectués sur ces nouvelles coordonnées.

L'escroquerie aux virements SEPA

Ce mode opératoire est apparu suite à la mise en place par le secteur bancaire, les entreprises et l'administration de la norme européenne SEPA. Les escrocs, usurpant les identités des employés des banques des victimes, contactent les comptables des sociétés visées et prétextant le passage obligatoire à la norme SEPA pour les virements internationaux les informent que des «techniciens» vont prendre attache avec eux afin d'effectuer des tests. Conformément aux instructions des auteurs des faits, les comptables se connectent sur un site internet où ils procèdent au téléchargement d'une application de prise de contrôle à distance. Par la suite, les escrocs leur expliquent toutes les démarches à entreprendre en vue de la création d'un compte client en indiquant des coordonnées bancaires (domiciliées à l'étranger) et les montants correspondant aux virements tests, les banques étrangères devant leur faire parvenir des rapports concernant la conformité du nouveau protocole des virements bancaires. Toujours dans le cadre de ce type d'escroquerie, une autre variante consiste à demander aux victimes d'installer un lien qui se révélera être un logiciel «espion» puis à les inviter à se connecter sur les portails de leurs banques respectives (consultation en ligne) et à composer leurs identifiants et leurs codes d'accès avant de solliciter l'envoi de modèles d'ordres de virement. En possession des codes d'accès internet et des exemplaires portant tampons et signatures, les auteurs confectionnent des faux ordres de virement, les transmettent à leurs banques et dans le même temps modifient les mots de passes d'accès aux services en ligne empêchant les comptables de vérifier l'état de la trésorerie.

D'ores et déjà, plusieurs groupes de ces malfaiteurs opérant de la sorte ont été interpellés en France, en 2011, 2012 et 2013. Mais, le phénomène continue !
La lutte contre cette forme de criminalité passe par le 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 à ce modus operandi aussi efficace que préjudiciable à l'économie nationale, la vigilance de chaque entité est nécessaire chacune à son propre niveau d'autant que les modes opératoires utilisés par les escrocs ne sont pas figés et sont sans cesse adaptés en fonction des réactions des victimes et des messages de prévention qui sont diffusés. L'Office Central pour la Répression de la Grande Délinquance Financière de la Direction Centrale de la Police Judiciaire centralise l'ensemble des informations au plan national pour ce type de fraude.