

Exclusif : 47 grandes entreprises françaises ciblées par une tentative d'escroquerie à grande échelle | Le Net Expert Informatique



47 grandes entreprises françaises ciblées par une tentative d'escroquerie à grande échelle

Selon nos informations, une cinquantaine de grandes entreprises sont actuellement – ou ont été au cours des derniers jours – la cible d'un réseau criminel spécialisé dans l'escroquerie aux faux ordres de virement (FOVI), encore appelée « Arnaque au président ». La technique n'est pas nouvelle. Ce qui interpelle, dans le cas présent, c'est l'ampleur de l'offensive mise à jour.

« L'arnaque au président » n'est pas vraiment d'un genre nouveau. D'ailleurs son pionnier, Gilbert Chikli, poursuivi par 33 banques et aujourd'hui réfugié en Israël, vient d'être condamné par contumace à 7 ans de prison et à 1 millions d'euros d'amende.

En cause : des escroqueries jugées « hors-norme », dont l'essaimage est devenu en quelques mois la bête noire des grandes directions financières, à commencer par celles que l'on pensait être les plus aguerries. Ainsi en 2012, c'est KPMG qui en a fait les frais : le géant mondial de l'audit et du conseil en fiscalité a laissé s'envoler à son insu pas moins de 7,6 millions d'euros.

Ces tentatives d'escroquerie n'épargnent personne : pas plus Michelin ou le Palais de l'Elysée, que nos PME régionales. Si Gilbert Chikli promet aujourd'hui avoir tiré sa révérence, il n'est en revanche pas improbable qu'il ait, directement ou non, inspiré quelques disciples.

47 entreprises sous la menace imminente de la criminalité financière

C'est une longue liste de cibles que s'est procuré la rédaction du JDE, par l'intermédiaire d'un cabinet privé spécialisé dans l'investigation et la lutte anti-fraude. Pour des raisons évidentes de sécurité, les consultants qui nous ont transmis cette information préfèrent rester anonymes.

Ils témoignent : « la spécificité de cette affaire réside dans l'ampleur de l'attaque. A ce jour, nous ne pouvons confirmer son état de progression ou son éventuel aboutissement. Nous avons contacté chacune des entreprises ciblées pour tenter d'être mis en relation avec les directions générales ou financières afin de de les en avertir. Malheureusement, le personnel n'étant pas toujours sensibilisé à ce type de risque, certains de nos appels sont restés sans suite. »

Une situation qui n'étonne guère ces analystes rompus à la gestion des affaires réservées des dirigeants : «Malheureusement, ces escroqueries aboutissent la plupart du temps à cause de défaillances dans la sûreté et les procédures internes de l'entreprise. La formation des collaborateurs, la circulation intelligente de l'information et l'instauration de procédures de vérification restent les meilleurs remparts contre ces attaques. »

Parmi les entreprises ciblées ou déjà attaquées, recensées par les enquêteurs, on retrouve de grands noms de l'économie française, des groupes familiaux plus discrets, et des enseignes bien connues des Français. « Des attaques qui sont en préparation depuis fin avril », précisent nos interlocuteurs, qui nous livrent ci-après le nom des entreprises ou organismes concernés :

Direction Finance, Ludendo, Système U, Abbott, 3 Suisses, GE Capital, Sonepar, Joué Club, Monoprix, BHR Béton, La Redoute, Eurofactor, Sephora, Picard, Imerys, Groupe Flo, GSF, DB Apparel, Optic 2000, Marionnaud, Groupe Pigeon, Invacare, Franck Provost, Auchan, Continental Corporation, Pronatura, Finifac, Provalliance, Carrefour, Vivendi, Korian, Accor, Servair, Bricorama, SKF, SNEF, SNCF, Rexel, Ecolab, Soprasteria, Chausson Matériaux, Faurecia, Immocho, Eiffage, Clemessy.

Comment réagir en cas d'attaque ?

« Nous avons pris des mesures directes pour tenter d'endiguer la marge de manœuvre des 'assaillants' et prévenir le risque d'escroquerie, et travaillons en étroite relation avec nos partenaires depuis plus d'un mois, expliquent les analystes. Surtout, nous accompagnons nos clients dans la mise en place d'une procédure judiciaire à l'encontre des auteurs de la tentative d'escroquerie, en sachant pertinemment qu'elle sera longue et complexe. »

D'après le cabinet, en effet, les quelques traces électroniques analysées laissent apparaître un mode opératoire assez classique, probablement piloté depuis Israël ou un territoire voisin comme l'indiquent les paquets de données qui ont été analysés.

« Dans certains pays, les moyens de paiement prépayés sont très répandus et peu régulés, donc difficilement traçables. Ils peuvent être ensuite utilisés en France, pour acquérir de l'information légale sur les sociétés ou à l'étranger, pour recourir anonymement aux services d'une plateforme téléphonique ». Ce sont également ces cartes prépayées qui, en toute vraisemblance, auront permis aux escrocs de réserver des noms de domaine pour peaufiner leur déguisement électronique.

Un déguisement qui va, selon les experts, jusqu'à l'usurpation d'identité de personnes vivantes ou décédées : « Pour brouiller les pistes, ces brigands 2.0 utilisent vos adresses, numéros de téléphone, dates de naissance pour réserver des noms de domaine et procéder à certaines formalités en ligne. C'est probablement supposé divertir les enquêteurs », ironise l'un de nos experts.

Piqûre de rappel : Le mode opératoire

Une opération couronnée de succès est une opération bien préparée. Les escrocs commencent par une phase de renseignement en « zone grise », en collectant un maximum d'informations sur leur cible. C'est ce qu'on appelle le « social engineering », dont le but est de recueillir suffisamment de données quant à l'environnement humain (personnes clés, numéros de téléphone, adresse email) et économique (contrats, fournisseurs, bilans, etc.) de l'entreprise.

C'est bien moins compliqué qu'il n'y paraît : munis d'une carte prépayée, il leur suffit de se rendre sur une base de données de type Infogreffe et de télécharger les documents les plus riches en information : derniers statuts et actes déposés, PV d'assemblées générales, ou comptes annuels par exemple. L'identification, sur les réseaux sociaux, des « personnes clés » dans l'organigramme de la cible permet parfois de se familiariser avec leurs futurs interlocuteurs.

Depuis une plateforme téléphonique située à l'étranger, mais avec un numéro français d'apparence, l'escroc appelle un directeur financier, un service comptable, ou tout individu ayant compétence à agir sur les comptes de l'entreprise.

Se faisant généralement passer pour le dirigeant de l'entreprise, il déploie alors des trésors de créativité et/ou de séduction. Tantôt flatteur, tantôt menaçant, il prétexte une situation d'urgence (opération boursière sensible, ou imminence d'un contrôle fiscal par exemple) et exige le virement immédiat d'une importante somme sur un compte habituellement hébergé en Chine.

Nos interlocuteurs invitent donc les entreprises à la plus grande vigilance : « ces offensives sont généralement fulgurantes et, le temps de réagir, nos escrocs sont déjà loin... »

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

http://www.journaldeleconomie.fr/Exclusif-47-grandes-entreprises-francaises-ciblees-par-une-tentative-d-escroquerie-a-grande-echelle_a2456.html