Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 21 – Février 2016

Ce « flash » de l'ingérence économique évoque des actions 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° 21 Février 2016

Les dangers des faux profils sur les réseaux sociaux professionnels

Depuis plusieurs années, la diffusion de faux profils, bien réalisés et crédibles à première vue, se multiplie sur les réseaux sociaux professionnels tels que LinkedIn ou Viadeo.

Ces faux profils se présentent généralement comme des professionnels du recrutement travaillant pour des cabinets spécialisés (fictifs ou dont l'identité a été usurpée) ou des groupes internationaux de tous secteurs d'activités. Certains d'entre eux se font également passer pour des cadres supérieurs de grandes entreprises.

Ces profils sont souvent très détaillés et intègrent des informations dupliquées depuis des comptes légitimes et accompagnés d'une photo de jeune femme ou de jeune homme que l'on peut facilement retrouver sur Internet. Ils affichent généralement un grand nombre de contacts.

Pourquoi créer de faux profils ?

Il s'agit d'initiatives d'acteurs malveillants cherchant à entrer en contact avec des personnels travaillant dans des entreprises ciblées, première étape d'une démarche potentielle d'ingérence, émanant notamment de l'étranger.
Les salariés ciblés reçoivent des demandes de mise en contact émanant de ces faux profils. Dès l'établissement de la relation sur les réseaux sociaux professionnels, les auteurs de la démarche sont en mesure de cartographier les cercles de relations professionnelles et obtenir de nombreuses informations à finalité opérationnelle (coordonnées téléphoniques, adresses de messagerie électronique, etc…).

Après avoir gagné la confiance de leur nouveau contact, les faussaires pourront exploiter les informations recueillies afin de conduire plusieurs types d'actions, notamment des attaques informatiques : usurpation d'identité, envoi de spams, phishing/spearphishing ou courriel accompagné d'une pièce jointe piégée avec un logiciel malveillant (virus, cheval de Troie…).

Commentaire

Ce mode opératoire repose, une fois encore, essentiellement sur des techniques d'ingénierie sociale visant à abuser de la confiance des victimes et obtenir des informations de façon déloyale.

Si une demande d'ajout, par un(e) inconnu(e), à son relationnel sur les réseaux sociaux professionnels paraît anodin de prime abord, il peut également s'agir d'un signal faible, annonciateur d'une prochaine attaque informatique ou d'une approche à des fins malveillantes. Les conséquences peuvent alors être importantes pour l'entreprise : intrusion dans ses réseaux informatiques, installation d'un logiciel malveillant, vol de données confidentielles, sabotage des systèmes informatiques, tentative de débauchage, captation d'informations, etc…

Préconisations de la DGSI

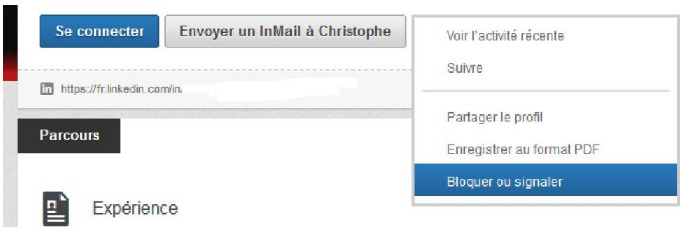
Afin de détecter un faux profil sur un réseau social professionnel, la DGSI recommande d'appliquer les bonnes pratiques suivantes :

- Rester vigilant et ne pas accepter les demandes de contact provenant d'inconnu(e)s ou de profils suspects ;
- Vérifier si la photo de profil n'a pas été copiée-collée depuis Internet, en utilisant les fonctions de recherche inversée par image de Google Images ou TinEye ;
- Vérifier si la description du profil n'a pas été dupliquée depuis un autre compte en effectuant une recherche partielle sur un moteur de recherche ;
- Vérifier si la personne existe vraiment en recoupant les informations disponibles avec des recherches sur Internet avec ses nom, prénom et entreprise ;
- Vérifier si le parcours étudiant et professionnel du profil suspect semble cohérent (dates, fonctions exercées, villes…).

En cas de doute après avoir accepté une mise en contact, il est conseillé de :

- Supprimer le contact en utilisant les options proposées par les différentes plates-formes de réseaux sociaux ;

- Signaler le profil suspect à l'éditeur du réseau social ;



Procédure pour signaler un faux profil sur LinkedIn

- Faire preuve d'une grande vigilance à l'égard des courriels inhabituels reçus.