Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 54 – Juin 2019

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°54 Juin 2019

Les *Massive Open Online Courses* (MOOC), potentiels vecteurs d'ingérence

Les *Massive Open Online Courses* (MOOC) permettent un accès libre à des cours en ligne interactifs, présentés sous la forme de vidéos, d'exercices et de quizz, dispensés par des professeurs d'universités ou des professionnels. Si certaines de ces formations sont diplômantes, d'autres sont simplement validées par une attestation de suivi de cours.

Les MOOC sont toutefois susceptibles d'être utilisées par des acteurs étrangers à des fins d'intelligence économique, comme vecteur d'approche et de recrutement de profils à fort potentiel ou de captation informationnelle.

PREMIER EXEMPLE

Une plateforme extra-européenne propose différentes formations diplômantes touchant à des thématiques de défense et de sécurité. Ces cours sont très prisés des salariés travaillant dans ces domaines stratégiques.

Or, cette plateforme sous-traite ses examens en ligne à une société étrangère tierce. Cette dernière se voit autorisée, dès lors que l'utilisateur accepte les conditions générales d'utilisation, à installer un logiciel de prise de contrôle à distance de l'ordinateur lors du passage de l'examen, permettant ainsi entre autres une prise de contrôle à distance du clavier et de la souris, une visualisation de l'écran ou l'activation de la caméra et du microphone de l'ordinateur.

Une telle pratique, menée à des fins malveillantes, pourrait permettre de réaliser une empreinte numérique du poste cible afin de mener, par la suite, des opérations cyber de plus grande ampleur.

DEUXIEME EXEMPLE

Une employée française s'est vue proposer un contrat de thèse, très attractif, par une université étrangère après avoir suivi différents cours en ligne sur un même sujet.

L'université, qui propose plusieurs formations en ligne, indiquait dans son courriel avoir été impressionnée par la rapidité et la justesse de ses réponses.

Grâce aux indications renseignées lors de l'inscription à la plateforme de formation, l'université semblait connaître beaucoup de détails sur le métier, les fonctions exactes et l'entreprise au sein de laquelle travaille la salariée tricolore.

COMMENTAIRES

Dispensés sur des plateformes internet dédiées, les MOOC, généralement gratuits, sont accessibles par une simple connexion internet et constituent un grand espoir de développement et d'expansion du savoir académique. Il convient néanmoins de conserver à l'esprit que ces plateformes comportent des vulnérabilités intrinsèques.

En effet, afin d'améliorer leurs services, les serveurs des plateformes sont automatiquement rendus destinataires de « données profondes » [1] permettant, après analyse, d'obtenir un profil psychologique et cognitif détaillé des utilisateurs. Au-delà des seuls éléments d'identité, ces données permettent d'obtenir des informations sur la vélocité intellectuelle des apprenants, les durées de connexions, les sujets abordés ou encore les préférences en termes de modes d'apprentissage.

Le référencement des profils offre ainsi l'opportunité aux hébergeurs étrangers de certaines plateformes de cours en ligne de disposer **d'une cartographie précise de compétences humaines à l'échelle mondiale**. Ils sont ainsi capables, à des fins d'intelligence économique, de détecter les profils à très hauts potentiels, qu'ils s'agissent d'étudiants spécialisés ou de salariés d'entreprises stratégiques désireux d'approfondir leurs connaissances. En outre, l'exploitation de ces données profondes par des acteurs étrangers peut leur permettre d'effectuer une analyse globale des faiblesses et atouts des employés d'une société concurrente.

A ce titre, l'on rappellera que la confidentialité des données hébergées sur des serveurs à l'étranger doit être fortement relativisée, et que les informations personnelles et professionnelles transmises dans le cadre de MOOC sont donc potentiellement accessibles à des entités étatiques étrangères.

Par ailleurs, les services web proposés par certains MOOC pourraient être utilisés à des fins malveillantes. Ainsi, un attaquant pourrait mener des opérations de reconnaissance (prise d'empreinte numérique) en vue de compromettre le(s) poste(s) de(s) l'utilisateur(s) du service web (transmission de pièces jointes malveillantes). Cette technique ouvrirait la porte à une éventuelle opération cyber de plus grande ampleur (élévation des privilèges, latéralisation sur le système d'information,...).

[1] *Les « données profondes » sont constituées principalement d'informations recueillies automatiquement par les serveurs des plateformes de cours en ligne.*

PRECONISATIONS DE LA DGSI

Afin de réduire ces risques, la DGSI recommande d'appliquer les bonnes pratiques suivantes :

→ Sensibiliser et informer l'ensemble des salariés sur le sujet.

→ Si possible, dans le cadre d'une formation non diplômante, mettre à disposition les cours sur le réseau interne de la société après vérification de l'innocuité du contenu. Créer, le cas échéant, des profils « entreprise » pour s'inscrire sur les plateformes.

→ Utiliser des postes dédiés ou suivre ces formations en ligne sur un poste déconnecté du réseau interne de l'entreprise.

→ Lors d'une inscription à titre personnel, rester discret, ne pas communiquer des informations professionnelles et personnelles trop précises.

→ Encourager les professeurs français d'université à mettre en ligne leurs cours sur des plateformes françaises ou, à défaut, européennes. De la même manière, pour les entreprises, préférer des prestataires français ou européens (comme la plateforme française *France Université Numérique* [FUN]).

→ Accorder une attention particulière aux conditions générales d'utilisation et à la localisation géographique des serveurs où sont stockées les données hébergées par la plateforme.

→ Prévenir, le plus rapidement possible, le Responsable Sécurité de son entreprise et la DGSI en cas de tentative d'approche ou de suspicion d'un cas d'ingérence étrangère.