MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #118

Février 2026

LES SÉJOURS À L'ÉTRANGER, PROPICES AUX MANŒUVRES DE CAPTATION ÉTRANGÈRES

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.

Il est également disponible sur le site internet : **www.dgsi.interieur.gouv.fr**

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**

LES SÉJOURS À L'ÉTRANGER, PROPICES AUX MANŒUVRES DE CAPTATION ÉTRANGÈRES

Les déplacements à l'étranger peuvent constituer une opportunité pour des acteurs privés ou étatiques d'opérer des approches ciblées de certains profils sensibles à des fins de captation d'informations.

Cadres d'entreprises, experts techniques ou chercheurs peuvent ainsi, lors de leur séjour, être victimes de piégeages de leurs outils numériques, de vols matériels ou de documents, ou encore être directement approchés ou mis en relation avec des personnes inconnues. À ce titre, les lieux publics, tels que les aéroports, les gares, les hôtels ou les bars/restaurants sont des lieux privilégiés par les acteurs étrangers dans le cadre de leurs approches et nécessitent donc une vigilance renforcée.

Ce « Flash ingérence » présente trois cas d'approches intrusives ayant ciblé des profils français à l'occasion de leurs déplacements à l'étranger.

1 CAPTATION D'INFORMATION ET TENTATIVE DE CORRUPTION CIBLANT UN CHERCHEUR FRANÇAIS À L'OCCASION D'UN DÉPLACEMENT À L'ÉTRANGER

Un chercheur français, expert particulièrement cité dans son domaine, a été sollicité par l'un de ses anciens doctorants étrangers, désormais enseignant dans son pays d'origine, afin de réaliser une mission d'une semaine dans son université locale. Ayant l'habitude de collaborer avec ce pays et cette université, le chercheur français a accepté cette offre.

Cependant, durant ce séjour, plusieurs réunions non programmées lui ont été imposées avec cinq experts étrangers dont le chercheur français n'a pu recueillir ni les identités, ni les fonctions. Lors de ces réunions, il a été interrogé de manière détaillée sur ses travaux de recherche et s'est vu proposer avec insistance une collaboration dans son domaine d'excellence, qu'il a déclinée avec fermeté. Le chercheur français s'est ensuite vu proposer une somme de plusieurs milliers d'euros en espèces pour le convaincre d'accepter. Ce dernier n'a pas cédé et a maintenu son refus de toute collaboration.

Plusieurs incidents ont également eu lieu le jour du départ du chercheur. En effet, à son arrivée à l'aéroport, il lui a été demandé de régler, ce qu'il a refusé, sa chambre d'hôtel et ses billets d'avion, pour un montant de plusieurs milliers d'euros, alors qu'il avait été initialement convenu que tous les frais du voyage seraient assurés par l'université accueillante. En outre, durant le trajet de retour, l'intéressé a constaté que son ordinateur ne se trouvait plus dans ses bagages à main. Conscient d'avoir subi une approche à des fins de captation technologique ainsi qu'une tentative de corruption sur le territoire étranger, le chercheur français envisage de mettre un terme à sa collaboration avec ce pays et cette université étrangère.

2 CONTRÔLE DOUANIER INTRUSIF CIBLANT UN CHERCHEUR FRANÇAIS

À son arrivée dans un aéroport étranger, un chercheur français a été soumis à un contrôle douanier intrusif lors de son passage au point de contrôle des visas. Le chercheur s'est vu confisquer son passeport et a été conduit dans une pièce annexe où il a été longuement interrogé. Avant de commencer l'entretien, il a dû laisser son téléphone portable déverrouillé à l'extérieur de la pièce.

À sa sortie, le chercheur a constaté que plusieurs actions avaient été effectuées sur son téléphone, comme la désactivation de la procédure de double authentification et la connexion d'appareils inconnus en bluetooth. De plus, un téléphone inconnu s'est connecté à l'un de ses comptes de messagerie instantanée.

Face à ce constat, le chercheur a réinitialisé son téléphone sur les paramètres d'usine et changé ses mots de passe. Les autorités fonctionnelles de son université ont été averties de l'incident.

3 MULTIPLES INCIDENTS CIBLANT LE DIRIGEANT D'UNE START-UP FRANÇAISE À L'OCCASION D'UN VOYAGE D'AFFAIRES

Le dirigeant d'une start-up française, lauréate d'un concours organisé à l'étranger, a été invité à un voyage d'affaires dans le pays d'origine du concours afin d'y rencontrer des entreprises sur place et éventuellement signer des partenariats.

Le séjour a néanmoins été entaché de plusieurs incidents et notamment des tentatives de captations d'informations. Ainsi, outre les contrôles d'identité répétés, les valises et la chambre d'hôtel du dirigeant ont fait l'objet de fouilles sans que l'intéressé ne constate la disparition d'effets personnels. Il a également déploré le fait d'avoir été constamment filmé et photographié sans son consentement. Enfin, à l'occasion d'une soirée, un individu se présentant comme le directeur d'une société de conseil l'a approché et a brièvement manipulé le téléphone du dirigeant sans son consentement.

L'ensemble de ces démarches se sont néanmoins révélées infructueuses dans la mesure où le dirigeant français avait été sensibilisé par la DGSI avant son départ. Ainsi, celui-ci avait pris soin de n'emporter aucun document sensible en lien avec sa société et de ne prendre avec lui qu'un téléphone vierge de toute donnée.

Commentaires

Tout voyage à l'étranger peut être instrumentalisé par un acteur étranger, privé ou étatique. Les cadres d'entreprise, experts techniques et chercheurs français, constituent donc des cibles potentielles et sont ainsi exposés à différents risques dans le cadre de leurs déplacements.

Les contrôles aéroportuaires, justifiés par des motifs d'ordre sécuritaire, peuvent ainsi être détournés et exploités à des fins de captation de données ou de piégeage informatique. De plus, les supports numériques (ordinateurs, tablettes, téléphones portables), susceptibles de contenir des données sensibles ou confidentielles (listes de contacts, informations financières et commerciales, travaux de recherche, etc.) doivent faire l'objet d'une vigilance renforcée et continue lors des déplacements.

Les approches humaines constituent également un mode opératoire privilégié par des acteurs étrangers pour obtenir, par exemple, des informations stratégiques à moindre coût. À ce titre, il convient de maintenir une posture de vigilance lors des échanges avec des interlocuteurs étrangers, même dans le cadre d'une relation de confiance établie de longue date avec un collaborateur.

Enfin, les séjours personnels et touristiques, au cours desquels la vigilance individuelle peut être moins soutenue, sont également susceptibles de faire l'objet de manœuvres d'ingérence étrangère et nécessitent la mise en place de mesures de précaution.

PRÉCONISATIONS DE LA DGSI

◆ En amont d'un voyage à l'étranger

- **Privilégier l'utilisation de matériels informatiques (téléphones, ordinateurs) dédiés exclusivement à la mission et limiter le stockage d'informations et de documents sensibles aux seuls besoins du déplacement.**
  Cette mesure permet de réduire les risques de perte, de vol ou de captation de données. Il est fortement déconseillé de se déplacer avec l'intégralité de ses documents commerciaux ou travaux de recherche.

- **Concernant les données nécessaires au voyage, il est conseillé de :**
  - **Effectuer une sauvegarde de données avant le départ.**
    Cette mesure permet, en cas d'incident lors d'un déplacement, de récupérer de manière intacte ses données.
  - **Recourir à des solutions sécurisées pour protéger les données sensibles.**
    Lorsque les dispositifs numériques et applications le permettent, privilégier une authentification forte. Il est également conseillé de diversifier ses mots de passe et d'en créer un différent pour chaque appareil et application. Concernant les dispositifs de chiffrement, vérifier que l'utilisation de ces moyens ne nécessite pas une autorisation préalable à leur introduction sur le territoire étranger dont le défaut constituerait le motif à un contrôle renforcé. Certaines pratiques sont en effet légales en France mais interdites à l'étranger.

- **Répondre le plus sincèrement possible aux questionnaires destinés à établir un visa d'entrée dans un pays, tout en évitant d'entrer dans les détails.** Il est conseillé d'éviter de chercher à dissimuler certains déplacements antérieurs (qui ne figureraient pas dans un nouveau passeport par exemple). En effet, une fausse déclaration ou une omission peuvent être lourdes de conséquences, compte tenu des capacités très importantes de recoupement et de croisement de données de certaines administrations étrangères.

- **Être conscient de son exposition sur les réseaux sociaux et les plateformes d'échange de services en ligne.** À la recherche de profils spécifiques, des acteurs malveillants mettent en place des veilles actives et régulières, notamment sur les réseaux sociaux professionnels, mais aussi sur des plateformes d'échanges de biens ou de services. Plus un individu dévoile d'informations personnelles et professionnelles, plus il sera facile à identifier et à approcher dans un déplacement, notamment privé, en s'appuyant sur des éléments trouvés en ligne.

- **S'il y en a, prendre connaissance des règles de sécurité, notamment numériques, mises en place par son entreprise, son université ou son centre de recherches dans le cadre des déplacements à l'étranger.** Il peut être utile de se rapprocher de son responsable de la sécurité des systèmes d'information (RSSI) afin de prendre connaissance des règles élémentaires d'hygiène numérique. **Dans certains pays considérés comme étant à risque, utiliser du matériel dédié, ordinateur et téléphone, vierge de toutes données à caractère professionnel ou privé. Une fois à l'intérieur du pays, ces données pourront être récupérées via un canal sécurisé. Au retour de la mission, le matériel sera confié au service informatique qui le réinitialisera.**

- **Consulter les guides de l'Agence nationale de la sécurité des systèmes d'information (www.ssi.gouv.fr) relatifs aux bonnes pratiques à l'usage des professionnels en déplacement.**

- **Sensibiliser en amont les employés ou chercheurs aux différentes menaces et approches étrangères auxquelles ils peuvent être exposés.** La DGSI, notamment à travers ses conférences de sensibilisation, peut accompagner les entreprises et les établissements de recherche sensibles dans ces démarches.

PRÉCONISATIONS DE LA DGSI

◆ Lors du passage à l'aéroport

- **Garder un contact physique avec ses appareils électroniques :** par exemple, dans son bagage à main ou s'ils doivent être déposés physiquement, les placer, si possible, dans une enveloppe sécurisée afin de les protéger et d'être en mesure de vérifier si quelqu'un a cherché à y accéder.

- **En cas de contrôle, ne pas chercher à s'y opposer mais à l'accompagner.** Dans la mesure du possible, demander à son interlocuteur de préciser son identité ou de justifier sa fonction avant de répondre à des questions jugées intrusives. Essayer de garder son matériel électronique avec soi ou demander à être présent lors du contrôle des appareils.

- **À l'issue du contrôle, être attentif au comportement de ses appareils** (icônes déplacées, consommation excessive ou rechargement injustifié de batterie).

◆ Pendant le séjour

- **Dans les lieux publics (transports en commun, hôtels, restaurants, etc.) :**
  - **Ne pas recharger ses appareils sur les bornes de recharge USB en libre-service.** Toujours utiliser son propre matériel de recharge et le brancher sur des prises électriques.
  - **Éviter de se connecter aux réseaux Wi-Fi publics.** Le cas échéant, il est important d'utiliser les outils professionnels sécurisés fournis par son organisme d'origine, ou un réseau privé virtuel (VPN). Après avoir eu recours à un réseau Wi-Fi public, il est préférable de modifier les mots de passe des applications utilisées régulièrement sur ses appareils.
  - **Faire preuve de discrétion.** Il est conseillé de limiter l'utilisation des dispositifs numériques contenant des données sensibles en public et les équiper de filtres de confidentialité. Il est également préférable d'éviter de s'entretenir de sujets confidentiels au téléphone en public.

- **Maintenir une posture de vigilance lors des échanges avec des interlocuteurs étrangers.** Il est conseillé de faire preuve de prudence lors des échanges ou à l'occasion de nouvelles rencontres, particulièrement lorsqu'elles se déroulent dans un cadre informel. Il est recommandé de ne pas détailler la nature exacte de ses missions et travaux lorsqu'elles portent sur des thématiques sensibles.

- **En cas d'approche inhabituelle ou suspecte.** Si un acteur étranger se démarque par des questions récurrentes et intrusives, il est conseillé de mettre un terme aux échanges sans attendre afin de limiter toute exposition aux risques de captation.

- **Ne pas accepter de cadeaux dont la valeur semble disproportionnée.** Si les cadeaux protocolaires sont courants lors des voyages d'affaires, il est essentiel de ne pas accepter de dons dont la valeur semble excessive au regard du contexte. Accepter pareils cadeaux peut placer le récipiendaire dans une position de dépendance, voire ouvrir la voie à des tentatives de chantage.

PRÉCONISATIONS DE LA DGSI

◆ Bonnes pratiques à mettre en œuvre lors du retour en France

- **Renouveler les mots de passe de tous les appareils électroniques et des applications utilisés lors du déplacement.**

- **Décontaminer les appareils électroniques par son service informatique et avant de les connecter aux réseaux internes de son organisation.** Cette étape est essentielle pour éviter une possible contamination du système informatique de son organisation et afin de détecter si des données ont été captées, volées ou détruites par un acteur tiers.

- **Informer sans délai le service informatique de son employeur en cas de problème avec ses appareils électroniques à l'issue d'un déplacement, notamment s'ils ont été manipulés par des autorités lors d'un contrôle.**
  Des mesures pourront ainsi être mises en œuvre pour limiter la perte de données et protéger l'entité, notamment en cas de perte, de vol ou de fonctionnement anormal des équipements.

- **De même, signaler les approches jugées inhabituelles ou suspectes à sa hiérarchie, à sa direction sûreté ou au fonctionnaire de sécurité-défense (FSD) de sa structure de tutelle.**
  Tout fait inhabituel, même anecdotique au premier abord, ou approche singulière doivent être signalés à son employeur ou structure d'encadrement. Ce dernier est susceptible d'avoir recueilli d'autres signalements qui permettraient par exemple de recouper l'approche d'un acteur étranger.

- **En cas de suspicion de captation d'information ou de technologie, d'approches inhabituelles d'acteurs étrangers ou d'incidents survenus lors de contrôles aéroportuaires, contacter la DGSI à :**
  securite-economique@interieur.gouv.fr

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité