MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH DGSI #72

FÉVRIER 2021

INGÉRENCE ÉCONOMIQUE

EXEMPLE D'UNE APPROCHE ÉTRANGÈRE CIBLÉE À DES FINS DE CAPTATION DE TECHNOLOGIES

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.

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

TENTATIVE D'ESPIONNAGE ÉCONOMIQUE ORGANISÉE PAR UN SERVICE DE RENSEIGNEMENT ÉTRANGER À L'ENCONTRE D'UNE SALARIÉE FRANCAISE

Dans le cadre de sa mission de protection économique, le Service détecte et analyse les menaces et ingérences étrangères auxquelles sont confrontés les sociétés, les administrations ou encore les établissements de recherche français.

Les acteurs français qui concourent à enrichir le patrimoine économique et scientifique national ne sont pas uniquement confrontés aux actions menées par un concurrent malveillant, aux manœuvres d'un investisseur peu scrupuleux ou aux attaques d'un pirate informatique motivé par l'appât du gain. En effet, particulièrement dans des secteurs stratégiques où les entreprises développent les technologies les plus innovantes, les acteurs économiques étrangers peuvent parfois bénéficier d'un soutien, explicite ou tacite, de la part d'un État qui met au service d'intérêts privés la puissance publique et ses outils afin de capter des savoir-faire et des technologies.

Dans ce cadre, des agents appartenant à des services de renseignement étrangers peuvent être mobilisés par des États dans le but d'approcher des entités françaises. S'ils mettent en œuvre des techniques connues, voire éculées, leurs cibles (jeunes chercheurs, cadres de PME ou de grands groupes, dirigeants de start-up, etc.) peinent souvent à les identifier, loin d'imaginer qu'ils ont pu, à leur niveau, retenir l'attention d'un service de renseignement étranger.

PREMIÈRE PHASE

Une scientifique française, après avoir obtenu un doctorat dans un domaine de pointe, a été recrutée par une PME française, sous-traitante de grands groupes dans un secteur stratégique, pour laquelle elle avait déjà travaillé au cours de ses études. Présente sur les réseaux sociaux et utilisatrice régulière des plateformes d'échange de services, la scientifique partageait de nombreuses informations personnelles et professionnelles sur des réseaux non-professionnels, notamment à travers les informations de son profil.

Dans le cadre d'activités annexes à celles de sa société, la Française a ainsi été contactée sur Internet par une ressortissante étrangère qui s'est présentée comme consultante pour un cabinet de conseil. Cette dernière a indiqué à sa cible être à la recherche de profils susceptibles de l'aider, contre rémunération, dans son travail de prospection économique en France, consistant notamment à rassembler des informations publiques. Ces premiers échanges ont donné lieu à l'organisation d'un premier rendez-vous.

DEUXIÈME PHASE

Lors de leur première rencontre, la consultante étrangère s'est exprimée en français et a précisé ses attentes à la salariée française. Cette dernière a ainsi été invitée à effectuer des recherches à partir de sources publiques d'information, à rassembler les éléments collectés sur un support de stockage informatique et à remettre le support à la consultante, contre une rémunération en espèces, à l'occasion d'un prochain rendez-vous.

Les rencontres se sont ainsi multipliées entre la consultante étrangère et la salariée française. Chaque rendez-vous s'effectuait autour d'un dîner payé par la ressortissante étrangère, dans une ambiance conviviale. Si lors des premiers rendez-vous, la consultante a d'abord parlé d'elle et tenté d'inspirer confiance à sa cible, elle a orienté la discussion, au fil des entretiens, vers la Française et lui a posé de nombreuses questions, tant personnelles que professionnelles, tout en entretenant un climat très chaleureux.

TROISIÈME PHASE

Après plusieurs rendez-vous, la consultante a précisé ses questions et les sujets de recherche soumis à la scientifique française. Sans ambiguïté, la ressortissante étrangère a également fini par demander à son interlocutrice des informations précises sur son activité et si elle pouvait lui transmettre des documents internes de la PME pour laquelle elle travaillait. De plus, lors de ce rendez-vous et contrairement aux précédents, la consultante a porté une attention particulière à un appareil électronique qu'elle avait posé sur le bord de la table du restaurant, suscitant l'inquiétude de la salariée française, qui a eu l'impression d'être filmée ou enregistrée.

Mal à l'aise, la salariée française a alors décidé de ne plus revoir la consultante étrangère et de ne plus répondre à ses sollicitations. Celle-ci s'est alors montrée insistante et a tenté de contacter à plusieurs reprises la Française, qui a finalement décidé de rapporter ces faits à la direction sûreté de son entreprise.

La société a alors averti la DGSI, qui a pu établir que la consultante étrangère était en réalité un officier expérimenté appartenant à un service de renseignement étranger et dont la mission était de récolter des informations sensibles sur des entreprises stratégiques françaises.

COMMENTAIRES

En se faisant passer pour une consultante, un officier de renseignement étranger est entré en contact avec une ressortissante française afin, non pas d'obtenir des informations stratégiques concernant les affaires militaires ou diplomatiques de la France, mais pour récolter des informations techniques et précises à des fins économiques.

Dans un premier temps, grâce aux informations disponibles sur Internet, l'officier de renseignement étranger a été en mesure d'identifier sa cible et les failles sur lesquelles il allait pouvoir s'appuyer. Dans un second temps, au fil des entretiens qui se sont tenus sur plusieurs mois, l'officier de renseignement a pris le temps de créer une relation de confiance avec sa cible. Enfin, après plusieurs rendez-vous et après plusieurs missions rémunérées sans conséquences, qui lui ont permis de bâtir la relation mais aussi d'apprécier la qualité de travail de la salariée française, l'officier de renseignement a tenté d'obtenir de la part de sa cible des informations sensibles relatives à la PME qui l'employait, par ailleurs sous-traitante de plusieurs grands groupes dans un secteur stratégique.

À travers cette opération, un État a ainsi tenté de capter des informations technologiques sensibles portant sur une PME française, probablement pour en faire bénéficier ses propres entreprises qui évoluent dans le même secteur et qui sont des concurrentes directes de la société française pour laquelle travaille la salariée française ciblée.

PRÉCONISATIONS DE LA DGSI

RECOMMANDATIONS AUX SALARIÉS FACE AU RISQUE D'APPROCHE CIBLÉE

- **Rester discret sur les réseaux sociaux et les plateformes d'échange de services en ligne.** À la recherche de profils spécifiques, les acteurs étrangers, entreprises ou services de renseignement mettent en place des veilles actives et régulières, notamment sur les réseaux sociaux professionnels, mais aussi sur des plateformes qui, à première vue, apparaissent très éloignées des préoccupations professionnelles. Plus un salarié dévoile d'informations personnelles et professionnelles, plus il sera facile pour un acteur malveillant de l'identifier et de le cibler.
- **Être conscient que travailler pour une entreprise d'un secteur stratégique, indépendamment de la taille de l'entreprise ou du poste occupé, fait de chaque salarié une cible potentielle.** Les vrais coïncidences ou hasards de rencontre sont rares. Si certaines préconisations relèvent du bon sens, il est parfois difficile à l'échelle individuelle, et face à des faits *a priori* anecdotiques, d'envisager que la situation résulte d'une organisation et de la mise en œuvre d'une stratégie complexe. Tout fait inhabituel ou approche singulière doivent ainsi être rapportés à la direction sûreté de l'entreprise.

- **Connaître les quatre leviers qui peuvent inciter un individu à fournir des renseignements à un acteur étranger malveillant.** L'argent, l'idéologie, la coercition et l'ego (MICE : *money, ideology, compromission, ego*) sont les quatre grandes familles de leviers qui peuvent être utilisés par un individu pour arriver à ses fins. Les services de renseignement étrangers, mais aussi des acteurs privés, utilisent ces vulnérabilités pour obtenir des informations sensibles. Connaître ses faiblesses, c'est aussi apprendre à s'en protéger.
- **La rémunération en espèces, l'offre de cadeaux ou encore les invitations régulières dans des restaurants sont des méthodes classiques d'approche qui doivent alerter le salarié.** Ces situations doivent être signalées au plus vite, au risque d'être pris au piège dans une relation compromettante, voire illégale dans certains cas, avec l'individu qui n'hésite pas à dépenser d'importantes sommes d'argent pour gagner la confiance de sa cible.
- **Participer aux conférences de sensibilisation de la DGSI organisées par l'entreprise.** Les conférences de la DGSI permettent aux salariés de prendre conscience des menaces auxquelles ils sont exposés et des actions d'espionnage économique dans lesquels ils peuvent, malgré eux, être entraînés.

RECOMMANDATIONS AUX ENTREPRISES FACE AU RISQUE DE CAPTATION DE SAVOIR-FAIRE À TRAVERS UN DE LEURS EMPLOYÉS

- **S'assurer que chaque salarié a accès uniquement aux informations et aux documents dont l'accès lui est autorisé.** Il s'agit notamment de limiter l'accès au réseau interne de l'entreprise en fonction des besoins et des fonctions de chaque salarié.
- **Être capable, à travers une cartographie des risques, d'évaluer les conséquences en cas de fuite d'informations sensibles.** Si, malgré les précautions et les mises en garde, un salarié transmet des documents stratégiques ou sensibles à un tiers non-autorisé, il est important d'être capable d'évaluer le risque pour l'activité de l'entreprise, pour ses clients et pour ses partenaires (privés et publics).
- **Encourager ses salariés à faire remonter toute sollicitation inhabituelle.** Désigner et faire connaître au sein de l'entreprise un point de contact, notamment au sein de la direction sûreté, qui permet aux salariés de rapporter tout fait inhabituel, notamment des approches d'individus, français ou étrangers. Le point de contact informera la DGSI et les services compétents.
- **Organiser régulièrement des conférences de sensibilisation à destination des salariés.** L'employeur a un rôle clé dans la sensibilisation de ses salariés aux différentes menaces et approches étrangères auxquelles ils peuvent être confrontés. La DGSI, notamment à travers ses conférences de sensibilisation, peut aider les entreprises, les administrations et les établissements de recherche dans ces démarches.