



Protéger >>>>> NOS SECRETS

Les services du renseignement militaire de la Chine se servent des plateformes occidentales de recherche d'emploi en ligne pour attirer des ressortissants des pays membres du Groupe des cinq qui ont accès à des informations sensibles

MENACE



Les services du renseignement militaire chinois utilisent un éventail de plus en plus large de **sites de réseautage professionnel et de plateformes de recherche d'emploi en ligne** afin de viser le personnel du gouvernement et militaire des pays membres du Groupe des cinq et quiconque ayant accès à des informations classifiées ou privilégiées.

Ces auteurs de menace utilisent une stratégie agressive de recrutement en ligne au cours de laquelle des agents du renseignement ou leurs collaborateurs se font passer pour des employés de sociétés privées d'experts-conseils, de recrutement ou de groupes de réflexion et publient des offres d'emploi en ligne pour des postes d'analystes en politique étrangère et en défense (ou des postes semblables).

Les personnes retenues subissent des pressions pour fournir des informations non publiques à des clients non précisés qui sont associés au gouvernement chinois. **L'objectif ultime des services du renseignement militaire chinois est d'acquérir du renseignement militaire, politique et économique pouvant procurer à la Chine un avantage stratégique et tactique sur les pays membres du Groupe des cinq.**

Qui est à RISQUE?



Les agents du renseignement chinois tentent de recruter et d'entretenir des relations à long terme des individus aux profils suivants en échange d'informations classifiées ou privilégiées :

- Les titulaires de cotes de sécurité, particulièrement dans les domaines de la défense, des affaires étrangères et de la sécurité et du renseignement.
- Le personnel militaire, notamment celui affecté à l'Indo-Pacifique qui possède des connaissances sur les capacités régionales et les activités générales.
- Les personnes qui ont un accès direct ou indirect aux informations du gouvernement, p. ex. les universitaires, les journalistes, les auteurs pigistes, les membres de groupes de réflexion ou quiconque a des liens avec les secteurs de la défense, de la sécurité, des politiques et de l'économie.

RECRUTEMENT

Les agents du renseignement chinois se font passer pour des agents de recrutement des ressources humaines ou des consultants qui représentent de fausses sociétés de couverture, qui semblent toutefois légitimes, et qui prétendent être situées dans des pays autres que la Chine.



- 1 | Premier contact.** Les agents de recrutement publient des offres d'emploi sur des plateformes de réseautage professionnel et sur des sites de contrats à la pige comme LinkedIn, Indeed et Upwork. Les curriculum vitæ (CV) sont classés en fonction de la probabilité d'accès à des informations sensibles, puis les agents de recrutement débutent leurs stratégies de prise de contact.
- 2 | Entrevue.** Les entrevues se déroulent de façon virtuelle, le cas échéant. Les agents de recrutement dissimulent leur identité et peuvent commencer par sonder les candidats et candidates au sujet de leur accès à des contacts au gouvernement. Il est possible que des membres du personnel militaire soient interrogés au sujet de leur rôle et des activités de leur unité, de leur point d'attache ou de leur navire.
- 3 | Test initial.** Les candidates et les candidats sont priés de rédiger un rapport de test sur un sujet comme les relations bilatérales de la Chine, l'Indo-Pacifique et des questions connexes sur la défense, ou les relations internationales.
- 4 | Demandes subséquentes et changement de plateforme.** On avise les personnes que pour les autres rapports, le client désire recevoir davantage d'informations privilégiées. Au cours du processus de recrutement, les agents de renseignement déplacent habituellement la conversation vers une plateforme « plus sûre », comme une application de messagerie chiffrée.
- 5 | Paiement.** Les personnes reçoivent un montant se situant entre quelques centaines et plusieurs milliers de dollars par rapport et peuvent se voir offrir une somme plus importante en échange d'informations plus sensibles. Les méthodes de paiement utilisées incluent des plateformes de paiement tierces, telles que PayPal, Payoneer, Zelle, Skrill et Wise ainsi que Western Union, les virements électroniques et la cryptomonnaie. La rémunération versée aux personnes proviendra souvent d'un compte appartenant à une personne qu'elles n'ont pas rencontrée dans le cadre du processus de recrutement.



Pourquoi c'est IMPORTANT?

Bien que souvent, les personnes approchées n'ont pas un accès direct aux informations classifiées, **même des informations non classifiées** sur les politiques gouvernementales, ou sur la stratégie, les moyens et les installations militaires peuvent être recueillies et mises en commun avec des informations plus sensibles afin de dresser un tableau exhaustif des activités opérationnelles.

Certains types de données peuvent mettre la vie du personnel militaire de première ligne ou autre en danger, affaiblir notre prospérité économique et permettre l'ingérence dans nos processus démocratiques.

La protection de la vie privée des personnes qui fournissent leur CV et d'autres données personnelles pourrait être compromise.

Les personnes qui communiquent sans autorisation des informations sensibles ou classifiées pourraient subir diverses conséquences, notamment une poursuite en vertu des lois nationales, notamment celles sur l'espionnage.

Les organismes des pays membres du Groupe des cinq ont identifié des individus qui ont pris part à de telles activités, ce qui a mené à des poursuites criminelles, à des pertes d'emploi et à la révocation de la cote de sécurité.

SIGNALEMENT d'incidents

Si vous êtes visé par l'un des moyens de recrutement énumérés ci-dessus ou si c'est le cas d'une personne que vous connaissez, veuillez communiquer avec le bureau de la sécurité interne de votre organisation ou ministère pour obtenir des conseils et des instructions. Nos organismes respectifs assurent la liaison avec les bureaux de sécurité interne concernant cette menace.

CANADA

Pour signaler une menace non-immédiate concernant la sécurité nationale,

SCRS //

Par téléphone : 613-993-9620

Web : www.canada.ca/fr/service-renseignement-securite/organisation/signaler-des-informations-relatives-a-la-securite-nationale.html

La mention d'un produit, d'un processus ou d'un service commercial précis ou l'utilisation de tout nom de société dans la présente alerte est à titre informatif uniquement. Il ne saurait être considéré que l'appareil du renseignement du Groupe des cinq approuve, recommande ou dénigre ce produit, ce processus, ce service ou cette société.

