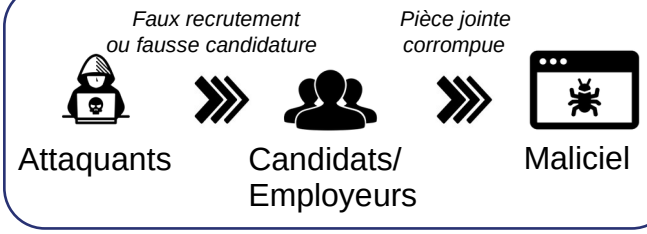
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

COMCYBER-MI

FICHE CYBER

Phénomènes cybercriminels associés aux processus de recrutement

Confiance : **Bonne**
Statut : **En cours**
Secteurs affectés : **Tous**
Zones géographiques touchées : **Monde**
Objectif : **Lucratif, espionnage**



SYNTHÈSE

Les processus de recrutement représentent une aubaine pour les cybercriminels. Les recruteurs et les candidats sont naturellement prompts à ouvrir des documents moins prudemment que dans la vie courante. Ils peuvent aussi se montrer moins vigilants face à des risques d'escroquerie ou d'utilisation malveillante des données fournies.

I. Contexte : fausses offres d'emploi et fausses candidatures

Le marché de l'emploi constitue une porte d'entrée des cyberattaquants parfois sous-estimée. Souvent, et pour des raisons ayant notamment trait à des biais psychologiques ou à la possible vulnérabilité économique des postulants, les échanges numériques entre recruteurs et candidats ne bénéficient **pas du même degré de méfiance** que dans d'autres circonstances.

Du côté des **candidats,** les fausses annonces sont généralement alléchantes : travail flexible, rémunération élevée et avantages divers. Elles peuvent être appuyées par un site *web* imitant celui d'une véritable entreprise afin de rendre la démarche frauduleuse plus crédible.
Des individus mal intentionnés peuvent aussi se faire passer pour des recruteurs légitimes et propager des maliciels dans les documents qu'ils envoient aux candidats, souvent peu méfiants dans ces circonstances.

Du côté **des recruteurs**, le personnel des ressources humaines est amené à constamment ouvrir des pièces jointes transmises de sources inconnues par les candidats, derrière lesquels peuvent se cacher des attaquants.

II. Principaux objectifs des cybercriminels

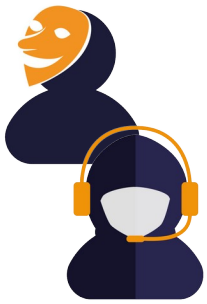
Recherche de points d'entrée, ou *initial accesses*, sur des systèmes informatiques de particuliers ou d'organisations.

Vol de données personnelles (adresses courriel, téléphone, carnets d'adresses, RIB, scans de documents d'identité) permettant de **récupérer des fonds** auprès des proches, d'obtenir frauduleusement des crédits, d'ouvrir des comptes bancaires, etc.

Escroqueries :
- Nécessité de payer une somme d'argent pour accéder à l'offre d'emploi ;
- Demande au candidat d'avancer des frais préalables au démarrage de son activité.

Espionnage
- Introduction et maintien discrets dans le système de la victime ;
- Récupération de **données sensibles** d'organisations ou d'entreprises.

III. Modes opératoires



Ressorts classiques

Que l'attaquant se présente comme candidat ou comme recruteur, les ressorts employés sont similaires.

L'objectif est d'amener la victime à ouvrir un document qui exécutera du code malveillant. Un pseudo-candidat peut intégrer un **maliciel au sein d'un curriculum vitae** présenté dans un format de type traitement de texte par exemple. Il peut ainsi potentiellement **infecter** le système d'une organisation au travers de son service des ressources humaines.

Un attaquant peut aussi **usurper l'identité** et la société d'appartenance d'un recruteur légitime et approcher ses victimes par le biais d'annonces sur des plateformes bien connues de mises en relation professionnelles.

Des techniques d'**hameçonnage ciblé** peuvent également être observées dans cette phase d'approche. Une fois le contact établi et le candidat-victime mis en confiance, ce dernier est incité à **télécharger un fichier malveillant d'apparence légitime** (par exemple un test de programmation informatique). Si le candidat ouvre ce fichier depuis son lieu de travail, le système d'information de son employeur est susceptible d'être infecté.

Techniques nouvelles

Aux États-Unis, le FBI a constaté plusieurs cas de candidatures par visioconférence impliquant des « ***deepfakes*** » reposant sur de l'**intelligence artificielle**.

De faux candidats à des emplois en télétravail exclusif ont postulé à distance en utilisant des dispositifs permettant de diffuser des vidéos et de l'audio sur lesquels ils n'apparaissaient pas réellement. Ils ont ainsi pu infiltrer des entreprises potentiellement sensibles en masquant leur identité.

Exemple d'attaque par fausses offres d'emploi

En octobre 2023, un acteur de la menace cyber d'attribution vietnamienne a créé de fausses offres d'emploi sur LinkedIn qui ciblaient des employés de sociétés administrant des comptes Facebook Business. L'objectif des attaquants était de leur proposer un emploi auprès d'une société fabriquant des périphériques informatiques.

Les candidats trompés téléchargeaient le maliciel DarkGate dissimulé dans un fichier nommé *Job Description*, ou *Salary and new products.txt* ou *Salary and Products.pdf*. Le but des cybercriminels était d'accéder aux comptes Facebook Business et d'y dérober des données personnelles et financières, puis de les détourner à leur profit.

Quelques mesures de précaution	**Recruteurs**	**Candidats**
Mettre antivirus et pare-feu à jour	●	●
Désactiver l'exécution des macros par défaut	●	●
Sensibiliser le personnel des ressources humaines	●	
Ne jamais envoyer d'argent à un employeur potentiel		●
Ne jamais transmettre des données personnelles à un recruteur suspect		●

SOURCES

https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs-threat-assessment-hr-departments.pdf
https://www.eset.com/fr/about/newsroom/press-releases/recherche/attaque-lazarus-linkedin-espionnage-aero/
https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/
https://www.ic3.gov/Media/Y2022/PSA220628
https://dev.to/ikemhood/the-fake-job-listings-that-was-just-a-front-for-pushing-malware-my-story-38f6
https://money.com/common-jobs-scams/
https://osintcorp.net/phony-job-vacancy-targets-linkedin-users-with-darkgate-malware/