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

Gendarmerie nationale

LA LETTRE CYBER *en région Grand Est*

MARS 2024

LA THEMATIQUE DU MOIS:
Le Processus de Recrutement: Existe-t-il un risque Cyber?

Social engineering, phishing, deepfakes, ransomwares etc…
Vous en avez forcément entendu parler mais ce n'est pas concret?
En quoi le recrutement peut-il nous amener à ces risques??
Nous allons voir que le recrutement comme beaucoup de choses peut être un vecteur d'attaque:

RAPPEL:

SOCIAL ENGINEERING (ingénierie sociale): Il s'agit du fait de manipuler une ou plusieurs personnes aux fins de réaliser une escroquerie.

PHISHING (Hameçonnage): Il s'agit de récupérer des données personnelles par de la tromperie (mail, SMS, QR code nous faisant croire à une connexion vers une plateforme légitime et sur laquelle nous entrons nos données personnelles sans nous douter qu'il s'agit d'une interface créée par des escrocs pour les récupérer)

RANSOMWARE (Rançongiciel): logiciel que nous exécutons malgré nous et qui a pour effet de chiffrer nos données, les rendant illisibles. Comme prises en otages, une rançon est demandée pour les rendre à nouveau lisibles. Ces données sont parfois volées par la même occasion.

DEEPFAKES: Technique de synthèse Multimédia permettant de simuler une image, un visage, une scène grâce à l'intelligence artificielle.

Mais quel rapport avec le recrutement?

1/ Vous cherchez un emploi, et consultez journalièrement les sites d'offres d'emploi et les réseaux sociaux. Vous postulez à certaines offres et conversez par mail etc… Un jour vous recevez un mail, ou découvrez une offre sur les réseaux sociaux qui correspond parfaitement à ce que vous vouliez (paye, week-end, proximité etc…) Ce mail ou publication sur les réseaux sociaux est une forme de PHISHING. Du fait de votre situation particulière vous êtes déjà une cible plus faible qu'une personne ayant déjà un emploi le travail de SOCIAL ENGINEERING a déjà commencé… Vous êtes appâté par cette offre d'emploi et le voulez vraiment, vous cliquez sur le lien ou vous êtes redirigé vers une page qui vous met en confiance. Vous remplissez les formulaires demandés sans même vous soucier du « pourquoi on me demande mon numéro de sécurité sociale ? ce doit être pour l'assurance de la boîte tant pis je le donne je veux vraiment ce job ». En réalité vous venez d'offrir à un escroc toutes vos données personnelles…

2/ Vous êtes le recruteur, vous suivez consciencieusement le protocole de recrutement mais il y a fort à parier qu'à un moment ou un autre vous deviez prendre connaissance de documents transmis par un candidat. La pièce jointe est elle réellement le scan de la pièce d'identité du candidat? Pourquoi ne serait ce pas un RANSOMWARE. Lorsque nous traitons 30,50, 100 candidatures il est normale de baisser sa garde mais attention cela peut avoir des conséquences graves pour l'entreprise. L'évolution constante de la technologie peu même amener les escrocs à utiliser la technologie comme le DEEPFAKE afin de se rendre à un entretien visio et se faire passer pour un candidat identifié ou un recruteur.

Les principaux objectifs des cybercriminels

Ce ne sont que quelques exemples de ce qui est imaginé par les escrocs et leur imagination n'a aucune limite afin d'arriver à leur objectifs mais quels sont ils?

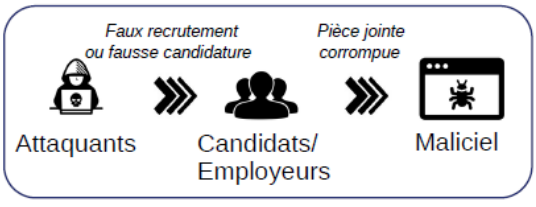
Recherche de points d'entrée, ou *initial accesses*, sur des systèmes informatiques de particuliers ou d'organisations.

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.

Exemple réel



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.

POUR CONCLURE:

Le processus du recrutement est un processus pendant lequel, l'humain est fragilisé, moins sur ses gardes car il est déterminé à recruter son employé ou à décrocher son job. Les escrocs en ont conscience et c'est pour cette raison que cette façon de faire se répend. Il est indispensable, lors de recrutement comme dans la vie de tous les jours de faire attention à nos cybers interlocuteurs et ne jamais baisser la garde, peu importe la raison.
ON NE CLIQUE PAS SUR UN LIEN / UNE PIECE JOINTE sans vérifications.

+ D'INFOS

CYBER MALVEILLANCE .GOUV.FR

PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

e-Enfance 3018

CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

ANSSI Agence nationale de la sécurité des systèmes d'information

Région de gendarmerie du Grand Est
LA LETTRE CYBER en région Grand Est
Directeur de la publication : GCA O.KIM
Responsable éditorial : COL L. GRAU
Rédacteurs : ADJ M. KNOBLOCH – ADJ E. DUBOIS

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
laurent.grau@gendarmerie.interieur.gouv.fr
mathieu.knobloch@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie :