PLAYBOOK DE RÉPONSE À INCIDENT

Voici un playbook de réponse à incident élaboré sur la base de la simulation d'attaque par cheval de Troie décrite dans le rapport, en se concentrant sur les phases de l'attaque simulée (Initial Access et Post Compromise)

1. Préparation

Cette phase est continue et vise à minimiser l'impact d'un futur incident

- **Inventaire et Classification :** Maintenir un inventaire à jour des actifs critiques (serveurs, postes RH, bases de données sensibles) et des utilisateurs à haut privilège (administrateurs, RH)
- **Renforcement des Défenses :**
    - Mettre en œuvre un système de **filtrage des fichiers entrants** (documents, CV, PDF) utilisant des sandboxes pour l'analyse dynamique avant l'ouverture.
    - Déployer des solutions de détection des comportements anormaux (EDR) pour identifier les techniques avancées comme le *Process Hollowing* ou l'exécution de *shellcode*
    - S'assurer que l'antivirus natif (ex. Windows Defender) ou la solution EDR est configurée pour la détection heuristique avancée, et pas seulement basée sur les signatures
- **Sensibilisation et Formation :** Former le personnel, en particulier les RH, aux risques d'hameçonnage ciblé (*Spear Phishing*) et à la manipulation de pièces jointes provenant d'expéditeurs externes.

2. Détection et Analyse

Cette phase vise à identifier la compromission et à déterminer l'étendue de l'attaque.

Étape	Action	Réponse Spécifique au Cheval de Troie
Alerte	Déclenchement d'une alerte (utilisateur ou système).	Un utilisateur (ex: RH) signale un comportement inattendu après l'ouverture d'un CV
Vérification	Isoler le poste de travail (déconnexion du réseau).	Identifier le processus suspect qui pourrait se cacher dans un processus légitime comme svchost.exe (*Process Hollowing*)
Collecte d'Indice	Examiner les logs système, antivirus et réseau.	Rechercher la tentative de connexion du *meterpreter* à l'adresse IP/Port spécifiés. Examiner les fichiers récemment ouverts (CV infecté)
Scope de l'Attaque	Déterminer la date, l'heure et l'étendue de l'accès.	Vérifier si l'attaquant a réussi l'escalade des privilèges et l'installation d'outils (Incognito, Kiwi)

3. Endiguement, Éradication et Récupération (Containment, Eradication & Recovery)

Cette phase met fin à l'attaque et restaure le système à un état sain.

3.1. Endiguement (Containment)

- **Isolation :** Isoler immédiatement le poste de travail du RH et tous les systèmes avec lesquels l'attaquant a interagi (serveurs, autres postes).
- **Blocage C2 :** Bloquer les communications du canal *Command and Control* (C2) au niveau du pare-feu, en utilisant l'adresse IP et le port du serveur de l'attaquant (si identifiés)
- **Changement d'Identifiants :** Changer immédiatement tous les mots de passe compromis, en particulier le mot de passe administrateur et les mots de passe des comptes RH. Utiliser des mots de passe complexes et uniques.

3.2. Éradication (Eradication)

- **Nettoyage du Malware :** Supprimer l'exécutable malveillant (*XCODER.exe*) et tout fichier persistant installé par le cheval de Troie.
- **Vérification des Processus :** Forcer l'arrêt et inspecter tous les processus légitimes ayant fait l'objet d'un *Process Hollowing* (ex: svchost.exe).
- **Analyse Complète :** Effectuer une analyse antivirus/EDR complète sur tous les systèmes potentiellement touchés pour garantir l'absence d'autres malwares ou portes dérobées.

3.3. Récupération (Recovery)

- **Restauration :** Restaurer les systèmes à partir de sauvegardes saines, antérieures à la date de compromission.
- **Mise en Production :** Une fois la sécurité vérifiée, reconnecter les systèmes au réseau et remettre les services en production.

4. Bilan Post-Incident (Post-Incident Review)

- **Analyse des Causes Racines :** Identifier la cause initiale (ex. manque de filtrage des fichiers entrants, profil RH ciblé)
- **Rapport d'Incident :** Documenter l'incident (chronologie, actions, impact, données exfiltrées). Confirmer quelles données sensibles ont été accédées (ex: informations sur les employés).
- **Amélioration du Playbook :** Mettre à jour les procédures et les défenses en fonction des leçons apprises (ex. renforcer la sensibilisation du service RH).