Rapport : Développement des Scripts pour l'Identification et la Neutralisation des Fichiers Malveillants.

Enjeux et Objectifs de la Mission :

Enjeux :

- *Sécurité des Clients : Assurer que les sites web des clients ne sont pas compromis par des fichiers malveillants permettant un contrôle à distance non autorisé.*
- *Réputation de l'Entreprise : Maintenir la confiance des clients en démontrant une réponse rapide et efficace aux incidents de sécurité.*
- *Prévention des Pertes de Données : Éviter la perte ou le vol de données sensibles via des fichiers malveillants.*
- *Conformité Réglementaire : Assurer que les pratiques de sécurité respectent les normes et régulations en vigueur.*

Objectifs :

- *Identification : Développer un script capable d'identifier les fichiers malveillants selon des critères définis (nom du fichier et contenu spécifique).*
- *Neutralisation : Créer un script pour neutraliser les fichiers malveillants en les renommant, empêchant ainsi leur exécution.*
- *Documentation : Documenter tout le processus et les résultats pour permettre une transparence totale vis-à-vis des clients et des supérieurs.*

Fonctionnement des Scripts :

Script+1.py : Liste des Fichiers.

Boucle os.walk : *Ce script parcourt les sous-répertoires du dossier "sites_clients" pour lister tous les fichiers présents.*

Construction du Chemin Complet : *Pour chaque fichier trouvé, le chemin complet est construit et affiché, fournissant une vue d'ensemble de tous les fichiers présents dans les sous-répertoires.*

Script+2.py : Identification des Fichiers par Préfixe .

Condition startswith : *Ce script identifie les fichiers malveillants en vérifiant si le nom du fichier commence par le préfixe "xmc6_" et si le fichier n'est pas déjà neutralisé (n'a pas l'extension ".disabled").*

Stockage et Affichage des Fichiers Malveillants : *Les fichiers identifiés comme malveillants sont stockés dans une liste et affichés. Cela permet de repérer rapidement les fichiers suspects basés sur leur nom.*

Script+3.py : Identification des Fichiers par Adresse IP .

Fonction fichier_contient_ip : *Ce script lit le contenu des fichiers pour vérifier la présence de l'adresse IP "8.13.193.9".*

Deux Listes de Fichiers Malveillants : *Les fichiers sont séparés en deux listes : ceux trouvés par leur nom (préfixe) et ceux trouvés par leur contenu (adresse IP), permettant une distinction claire des méthodes de détection.*

Script+4.py : Neutralisation des Fichiers Malveillants .

Vérification des Conditions : *Utilise les mêmes vérifications que les scripts précédents (préfixe et adresse IP) pour identifier les fichiers malveillants.*

Renommage des Fichiers : *Si un fichier est identifié comme malveillant, il est renommé en ajoutant ".txt" à la fin de son nom, ce qui le neutralise sans supprimer l'extension ".php". Le renommage est ensuite confirmé par un message affiché à l'écran.*

Résultats Obtenus :

Les scripts ont permis d'identifier et de neutraliser efficacement les fichiers malveillants. Les fichiers malveillants identifiés et renommés sont les suivants :

Identifiés par Préfixe "xmc6_" :

- **D:\Cours_cybersecu\Projet3\P4\sites_clients\site_cite_musique\includes\xmc6_cetna919.php**
- **D:\Cours_cybersecu\Projet3\P4\sites_clients\site_photographes_paris\composer\semver\src\Constraint\xmc6_rulu987.php**

Identifiés par Adresse IP "8.13.193.9" :

- **D:\Cours_cybersecu\Projet3\P4\sites_clients\site_cite_musique\network\9c4433c53ca82b115a7a189b6b134646a2a6045f.php**
- **D:\Cours_cybersecu\Projet3\P4\sites_clients\site_photographes_paris\drupal\core-vendor-hardening\7717be8de2ebc42393ba6b5ac3bd19a51678e390.php**

Tous ces fichiers ont été renommés avec succès pour empêcher leur exécution.

Conclusion :

Les scripts développés ont permis d'identifier et de neutraliser efficacement les fichiers malveillants. Tous les fichiers malveillants ont été renommés pour empêcher leur exécution, et la vérification a confirmé qu'il n'y a plus de fichiers malveillants actifs.

Recommandations :

Il est recommandé de continuer à surveiller les sites clients pour détecter d'éventuelles futures infections et d'appliquer des mesures de sécurité supplémentaires pour prévenir de nouvelles attaques.