Rapport de Projet : Nettoyage de Fichiers Malveillants

Objectif du Projet :

L'objectif de ce projet est d'identifier et de neutraliser les fichiers malveillants déposés sur les sites web clients. Ces fichiers permettent de prendre le contrôle à distance des machines.

Étapes du Projet :

Script+1.py : Lister les fichiers :

Un script Python (Script1.py) a été développé pour lister tous les fichiers dans les sous-répertoires du dossier sites_clients.

Script+2.py : Identification des fichiers par préfixe :

Un second script Python (Script2.py) a été créé pour identifier les fichiers malveillants ayant le préfixe xmc6_.

2 fichiers malveillants portant le préfixe xmc6_ ont été trouvés :

- **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**

Script+3.py : Identification des fichiers par adresse IP :

Un troisième script Python (Script3.py) a été développé pour identifier les fichiers contenant l'adresse IP 8.13.193.9.

2 fichiers malveillants trouvés par contenu (adresse IP) :

- **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**

2 fichiers malveillants trouvés par nom (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**

Neutralisation des Fichiers Malveillants :

Script+4.py : Renommer les fichiers malveillants :

Le dernier script Python (Script4.py) a été conçu pour neutraliser les fichiers malveillants en ajoutant l'extension .txt à leur nom.

4 fichiers malveillants ont été renommés avec l'extension .txt :

- **D:\Cours_cybersecu\Projet3\P4\sites_clients\site_cite_musique\includes\xmc6_cetna919.php -> D:\Cours_cybersecu\Projet3\P4\sites_clients\site_cite_musique\includes\xmc6_cetna919.php.txt**
- **D:\Cours_cybersecu\Projet3\P4\sites_clients\site_cite_musique\network\9c4433c53ca82b115a7a189b6b134646a2a6045f.php -> D:\Cours_cybersecu\Projet3\P4\sites_clients\site_cite_musique\network\9c4433c53ca82b115a7a189b6b134646a2a6045f.php.txt**
- **D:\Cours_cybersecu\Projet3\P4\sites_clients\site_photographes_paris\composer\semver\src\Constraint\xmc6_rulu987.php -> D:\Cours_cybersecu\Projet3\P4\sites_clients\site_photographes_paris\composer\semver\src\Constraint\xmc6_rulu987.php.txt**
- **D:\Cours_cybersecu\Projet3\P4\sites_clients\site_photographes_paris\drupal\core-vendor-hardening\7717be8de2ebc42393ba6b5ac3bd19a51678e390.php -> D:\Cours_cybersecu\Projet3\P4\sites_clients\site_photographes_paris\drupal\core-vendor-hardening\7717be8de2ebc42393ba6b5ac3bd19a51678e390.php.txt**

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.