Cybersécurité : Projet fishing

EOZINOU Antoine
DANMANVILLE Arnaud
BIED Tom
LAUMOND Victor

Sommaire

Stratégie

Notre stratégie consiste à utiliser un mail à première vue de confiance pour guider les victimes vers une page de connexion frauduleuse.

Il est important que l'attaque fonctionne aussi bien sur les étudiants que sur le personnel de l'ESTA, afin de toucher un maximum de monde. L'attaque est plus grave si des adresses e-mail de l'administration sont piratées, permettant l'accès à des données confidentielles par exemple.

Nous utiliserons le portail de connexion Moodle pour l'attaque. Ce portail est utilisé par les élèves pour consulter leurs cours et documents, et par les professeurs et administrateurs de l'école.

Nous créons donc un mail d'apparence inoffensive mais qui pousse à ouvrir le lien. (Voir Contenu du mail)

De cette manière, le personnel comme les étudiants auront tendance à cliquer sur le lien et donc donner leurs identifiants sur le portail de connexion frauduleux.

Page web

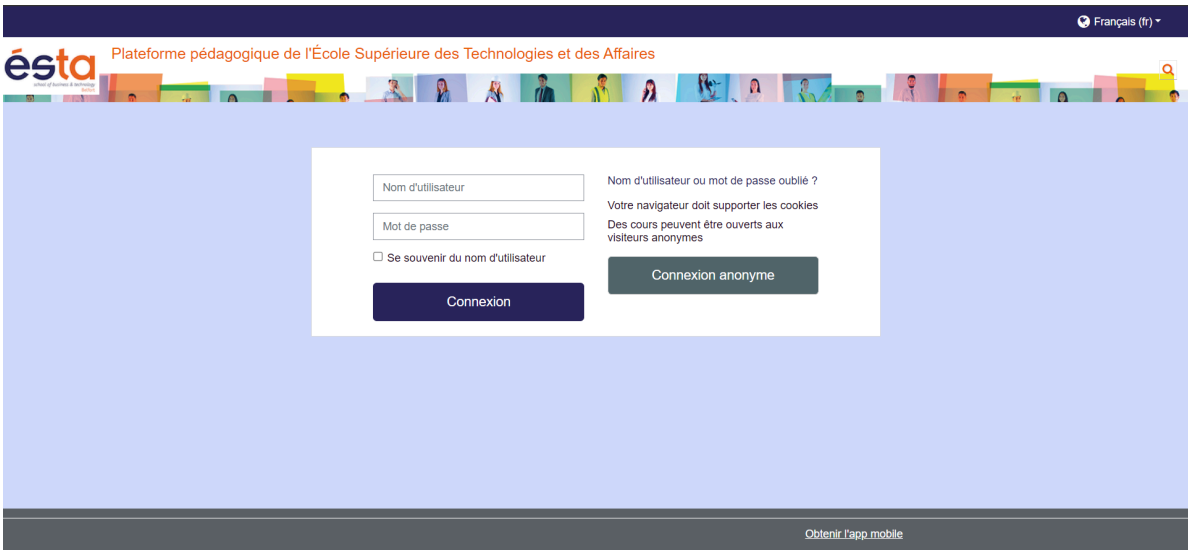
Il est important de choisir un nom de domaine très similaire à celui de la page que l'on souhaite répliquer, afin que l'oeil non-averti ne s'en rende pas compte.

Le nom de domaine du portail de connexion : https://moodle.esta-groupe.fr/login/index.php

Nous utiliserons donc le nom de domaine : https://moodle.esta.groupe.fr/login/index.php

Le nom de domaine est très proche de l'original, disponible, et facilement passable en https.

Le portail de connexion frauduleux utilise le code source html du portail original et ressemble à cela :



Adresse de l’envoyeur

Afin de tromper le plus de monde et récolter le maximum de données sensibles, nous avons choisi d’utiliser l’adresse mail de Constance Voisin.

Les étudiants et le personnel accordent pour la majorité une grande confiance à Constance, nous augmentons donc notre crédibilité en optant pour son adresse.

De plus, les étudiants reçoivent quasi quotidiennement des mails de sa part, réduisant les chances de détection de l’attaque.

L’adresse utilisée sera donc cvoisin@esta-groupe.fr.

Contenu du mail

Le contenu du mail a pour objectif d'être sommaire et crédible.
Pour cela, nous utiliserons le prétexte d'une mise à jour de la confidentialité du site ESTA Campus. Tous les utilisateurs doivent se connecter et prendre connaissances de la nouvelle réglementation. Ils doivent faire cette action avant le lendemain 18h. Ce dernier élément ajoute une notion d'urgence.

Ce n'est pas la première fois que l'administration nous demande de réaliser des actions dans un temps court sur certain site, cette demande ne paraitra donc pas louche.

Voici le mail à envoyer :

Objet: Politique de confidentialité de Moodle

Bonjour à toutes et à tous,

J'espère que vous allez bien !

Je vous informe d'une mise à jour importante de la politique de confidentialité de Moodle.

Pour accepter la nouvelle politique de confidentialité de Moodle, vous devez vous connecter en **cliquant ici**, puis aller dans la section **Politique de Confidentialité → Accepter la Politique de Confidentialité**.
Vous y trouverez aussi le détail de la nouvelle Politique de Confidentialité de Moodle.

Nous vous prions de bien vouloir effectuer cette action **avant demain 23h59 !!!**

Je compte sur vous pour le faire ! 🙂

Belle journée
Cordialement,

Timing

Le moment où les mails sont le plus souvent regardés est le mardi matin aux alentours de 9h, 9h30.

Les étudiants comme le personnel sont connectés et consultent leur boîte mail. Ainsi, il sera possible d’obtenir un meilleur taux de clic que pendant la pause de midi ou l’après-midi par exemple.