Projet campagne de phishing

Sommaire

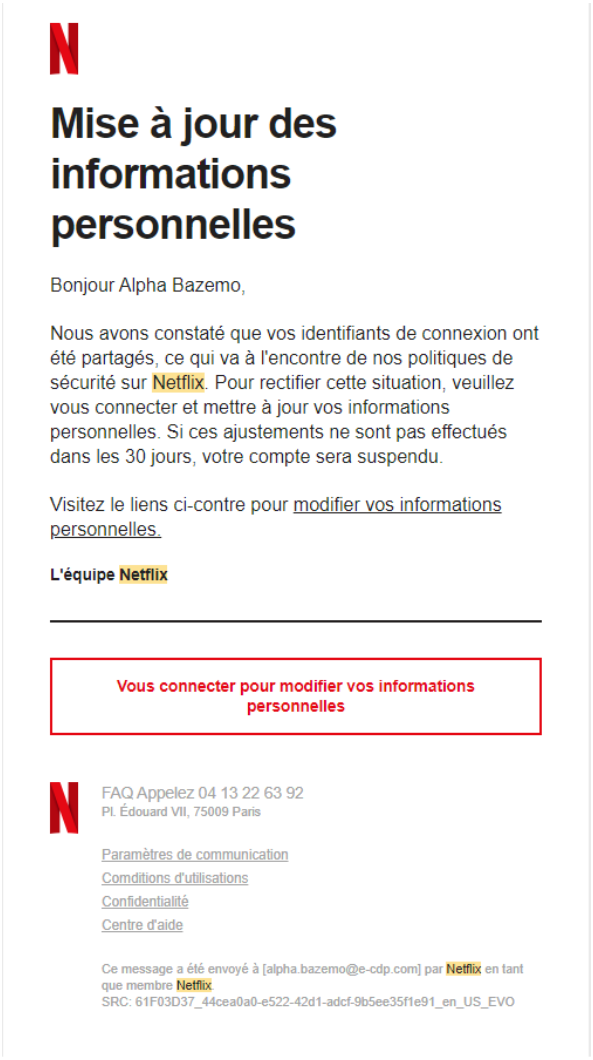
Contexte du projet et objectifs :

Nous faisons partie de l'équipe informatique d'une entreprise, et avons décidé de créer une campagne de phishing fictive afin de sensibiliser nos utilisateurs sur les dangers des messages reçus par mail, sms ou autres types de communication.

Méthodes utilisées :

Pour notre campagne de phishing, pour une question de rapidité et de commodité, nous sommes partis sur la solution GoPhish utilisant docker. Cette dernière nous fournit une interface nous permettant de choisir parmi des templates connues de site Web à usurper (ex : Facebook, Instagram, Twitter, Netflix…). Cette solution nous permet aussi de récupérer les informations rentrées dans les champs et ainsi récupérer de manière simple les données (Mots de passe, code de carte bancaire, adresse mail, login…)

Nous avons décidé de partir sur la copie d'un mail de Netflix, personnalisable selon la cible pour assurer le succès de la campagne. La cible étant notre professeur d'informatique. Voici le mail en question :



Mise à jour des informations personnelles

Bonjour Alpha Bazemo,

Nous avons constaté que vos identifiants de connexion ont été partagés, ce qui va à l'encontre de nos politiques de sécurité sur Netflix. Pour rectifier cette situation, veuillez vous connecter et mettre à jour vos informations personnelles. Si ces ajustements ne sont pas effectués dans les 30 jours, votre compte sera suspendu.

Visitez le liens ci-contre pour modifier vos informations personnelles.

L'équipe Netflix

Vous connecter pour modifier vos informations personnelles

FAQ Appelez 04 13 22 63 92
Pl. Édouard VII, 75009 Paris

Paramètres de communication
Comditions d'utilisations
Confidentialité
Centre d'aide

Ce message a été envoyé à [alpha.bazemo@e-cdp.com] par Netflix en tant que membre Netflix.
SRC: 61F03D37_44cea0a0-e522-42d1-adcf-9b5ee35f1e91_en_US_EVO

Lorsque l'utilisateur cible clique sur le bouton pour changer ses informations, il est redirigé sur une page identique à celle présente sur le site officielle de Netflix, la seule différence étant l'URL du site qui est différente. L'utilisateur se doit alors d'être vigilant pour ne pas se faire piéger.

On prend un nom de domaine similaire a netflix pour tromper l'utilisateur (exemple : netflux.fr), ce nom de domaine sera lié grâce a un reverse proxy a l'ip de la Vm hôte de la fausse page de connexion Netflix.

Nous récupérons ensuite les données de l'utilisateurs sous cette forme :

Recent Campaigns

View All

Show 10 entries

Search:

Name	Created Date						Status	
test	February 26th 2018, 11:45:54 am	2	2	0	0	2	In progress	
Copy of Copy of Copy of 1	February 23rd 2018, 2:06:07 pm	2	2	0	0	1	In progress	
Copy of Copy of 1	February 23rd 2018, 9:35:28 am	0	0	0	0	2	In progress	
2	February 21st 2018, 10:52:37 am	0	0	0	0	1	In progress	
Copy of 1	February 20th 2018, 11:44:55	0	0	0	0	1	In progress	