Rapport d’Incident :
Analyse et plan d’action

Remplissez ce document avec les informations demandées, pour chaque alerte qui représente une menace. N’oubliez pas d’inclure des captures d’écran dans toutes les instances indiquées.

NB: Un seul gabarit est fourni par section. Copiez et collez le gabarit autant de fois que nécessaire pour représenter le nombre d’alertes et/ou dossiers concernés.

I. Investigation

Alerte : **Malicious Email Detected :** Un email suspect signalé par un utilisateur.
L'email ne contient pas de pièce jointe ou de lien, cela semble être un simple spam basic
Risque: Faible

Détails d’investigation

Reportez ici toutes les informations que vous avez pu recueillir sur l’alerte. Ajoutez ou enlevez des points au besoin.

Date de l'Alerte : 19 février 2023 à 15h00
Source de l'Alerte : Signalée par un utilisateur
Tags : Spam
Expéditeur : julie@closedclassrooms.com
Destinataire : romeo.hernandez@carochan.com
Sujet : Webinaire ClosedClassrooms
Corps de l'Email : Contient des tactiques de manipulation basées sur des promesses de bénéfices financiers.

Indicateurs de compromission

Détaillez ici les éléments qui permettent d’identifier cette menace dans l'avenir. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

Domaine de l'expéditeur (closedclassrooms.com) (Domaine non enregistré)
Absence de liens ou de pièces jointes, contenu potentiellement utilisé pour des techniques d'ingénierie sociale.

Actifs impactés

Détaillez ici les machines, applications et utilisateurs impactés par cette alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

romeo.hernandez@carochan.com

Remplissez le tableau avec les informations indiquées.

Source et raison de levée de l'alerte	Qualification de l'alerte *(faux positif ou incident vérifié)*	Justification de la qualification
Email signalé par un utilisateur suspectant un contenu frauduleux.	faux positif	Domaine de l'expéditeur non enregistré et contenu manipulatif, cependant l'email ne contient pas de lien ou de pièce jointe

II. Analyse

Dossier :

Alertes :

Listez ici les alertes regroupées dans ce dossier. Ajoutez ou enlevez des points au besoin.

Caractéristiques

Détaillez ici les éléments communs qui réunissent ces alertes. Ajoutez ou enlevez des points au besoin.

Commentaires/observations

Si vous avez des observations à signaler par rapport à ce dossier, notez-les ici. Ajoutez ou enlevez des points au besoin.

L'email pourrait être une première approche avant une attaque plus ciblée mais pour le moment il ne semble représenter aucune menace.

Scénario : *résumez brièvement le scénario d'attaque que vous concevez pour ce dossier. Ajoutez ou enlevez des points au besoin.*

L'email semble être une tentative de social engineering, utilisant des promesses de bénéfices pour inciter l'utilisateur à une future action. L'absence de pièces jointes ou de liens pourrait être une stratégie pour établir la crédibilité et préparer un futur phishing plus sophistiqué.
Cependant il ne représente actuellement aucune menace.

III. Plans d'action

Dossier : Malicious_Email_ALE-7

Plan d'action : *résumez brièvement le plan d'action que vous concevez pour ce dossier, en fonction du scénario associé. Ajoutez ou enlevez des points au besoin.*

Sensibilisation des Employés : Organiser des sessions de formation pour aider les employés à identifier ce type de menace.
Mise en Place de Règles de Blocage : Configurer des règles pour bloquer les emails provenant de domaines non enregistrés.
Surveillance Renforcée : Surveiller les communications futures provenant de ce domaine et toute autre activité suspecte.