1/

Pour commencer l’enquête je suis allé chercher le document leak

J’ai utilisé Purview sur le Sharepoint site afin de découvrir où se trouve le fichier

J’avais comme information que c’était Amari qui avait enregistré ça

Je savais que c’était un Excel donc le bon fichier était celui terminant par « .xlsx »

2/

Ensuite j’ai utilisé Sentinel pour avoir des informations sur ce qui a pu se produire

Mon premier reflexe ici a été de regarder dans les logs

Une image contenant texte, logiciel, Page web, capture d’écran

Description générée automatiquement

En affinant ma recherche avec SecurityAlert j’ai pu trouver une ligne intrigante ainsi que 3 autres lignes importantes :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Mon second reflexe a été d’aller voir dans la catégorie Incident

Une image contenant texte, nombre, logiciel, capture d’écran

Description générée automatiquement

Je suis ensuite allé voir dans les détails de l’alerte avec l’ID 12 et j’ai pu trouver plusieurs choses

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Ensuite, en cherchant un peu j’ai fini par aller sur Defender, ici j’ai pu aller voir en détail l’alerte de menace et tomber directement sur les détails du PC de Amari

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

J’ai été dans les détails d’incident et suis tombé sur un processus « Patch.exe » qui semblait suspect

Une image contenant texte, capture d’écran, logiciel, Système d’exploitation

Description générée automatiquement

3/

La troisième étape était d’aller voir dans la partie Identity Protection

La première chose a été de regarder dans l’onglet « Risky Users » afin d’avoir des détails sur notre cible

Une image contenant texte, capture d’écran, nombre

Description générée automatiquement

Ensuite l’onglet « Risk Detections » permet d’avoir plus de détail sur la connexion sur cet utilisateur, on a pu y découvrir pleins de détails permettant de mieux cibler la personne s’était connecté

Une image contenant texte, logiciel, nombre, Icône d’ordinateur

Description générée automatiquement

4/

La quatrième chose à faire est d’appliquer des risk policy pour protéger les cartes de crédits

J’ai établi tout une risk policy permettant d’éviter une fuite du numéro de carte des victimes

5/

L’étape suivante est d’appliquer des Compliances Policies

Une image contenant texte, logiciel, Icône d’ordinateur, Page web

Description générée automatiquement

6/

L’étape suivante est d’inspecter en détail ce qui a pu se passer sur l’ordinateur d’Amari via Defender

La première étape est de récolter les informations

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Ensuite on répète l’opération pour tout les Events

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

J’ai ensuite été me connecté en SSH sur la machine afin de vérifier les fichiers suspects

Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement

7/

On fait ensuite une recherche sur l’IP utilisé pour nous attaquer, afin d’avoir tout les détails de communications sur elle

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Tout ceci nous mène à un échange mail via Exchange

Une image contenant capture d’écran, texte, logiciel, Page web

Description générée automatiquement

8/

Suite a ça j’ai pu vérifier dans les logs que seul la session d’Amari a été comprise

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

J’ai donc créé une rule dans Analytics afin d’avoir des informations lorsqu’une connexion est établi avec cette IP

9/

L’étape suivante est d’établir une Baseline

10/

L’étape suivante est de mettre en place l’Identity protection policies

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

11/

Après ça on part vérifier les informations de connexion de Angel pour vérifier les messages envoyé à Amari mais cela n’a rien donné

12/

Afin d’avoir d’avantage d’informations sur Angel on a été voir Sentinel

Une image contenant texte, logiciel, Page web, capture d’écran

Description générée automatiquement

En cherchant un peu on a fini par trouver l’IP avec laquelle la personne s’est connectée

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

13/

On fait désormais la même recherche d’échange mais sur Angel

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

On se rend compte d’un échange à cette date précise et qu’elle a accepté

Une image contenant texte, capture d’écran, ligne, Police

Description générée automatiquement

14/

On a ensuite vu que Tomo a établi une connexion sur l’ip d’Angel

Grâce à tout ceci on a pu établir qu’Angel a effectuer une connexion RDP pour pouvoir télécharger les données

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant habits, Visage humain, personne, sourire

Description générée automatiquement