# |Morning investigation

A computer screen shot of a computer screen

Description automatically generatedA screenshot of a computer

Description automatically generatedAvant de débuter l'enquête, j'ai examiné les preuves disponibles, notamment les propriétés du fichier qui a fuité, révélant qu'il s'agissait d'un document Excel. Sur base de ces données, j'ai initié une recherche avec Purview Content Search pour localiser le fichier.

En examinant les alertes de Sentinel, j’ai remarqué 10 incidents de sécurité. J’ai vu qu'un fichier patch.exe a été exécuté sur le pc105 à partir du compte d'Amari Rivera. Ce fichier a été téléchargé à l'aide de la commande "curl". Peu après, patch.exe a établi une connexion avec l'adresse IP 20.108.242.184:443, suivi de l'utilisation de l'outil Meterpreter pour obtenir un shell et lire le contenu du fichier zip "ShoppingList.zip". Nous retrouvons sur le pc105 le processus patch.exe (ID 8836).

A screenshot of a computer

Description automatically generated

Depuis l'AD, j'ai remarqué que le niveau de risque du compte d'Amari Rivera est "high". J’ai marqué son compte comme compromis, puis j’ai réinitialisé le mot de passe. J’ai reçu également des informations sur l'attaque utilisée pour compromettre le compte. La méthode "Password Spray" a été utilisée, ce qui signifie que quelqu'un connaissait déjà le mot de passe.

A screenshot of a phone

Description automatically generated

Bonus : Dans l'onglet "Risky Sign-ins", j’ai détecté également des anomalies pour Nestor Wilke et Emily Braun.

J'ai déployé une politique de gestion des risques spécifiquement pour l'équipe en charge de l'application e-commerce (ECommerceApp@bestforyourorganic.onmicrosoft.com), axée sur la protection des informations sensibles, en mettant l'accent sur les cartes de crédit stockées sur SharePoint. Voici les étapes :

Microsoft Purview -> Insider Risk Management -> Policies -> Generate Data leaks -> [ECommerceApp@bestforyourorganic.onmicrosoft.com](mailto:ECommerceApp@bestforyourorganic.onmicrosoft.com) -> Cocher SharePoint Sites & Sensitive Info types -> Sélectionner :

* Priority Content: SharePoint sites : …/ECommerceApp
* Priority Content: Sensitive info types : Credit card number
* Triggering Event : User performs an exfiltration activity

-> Policy indicators : cocher toutes les options ensuite « Submit »

# | Afternoon Investigation

J'ai établi une politique visant à chiffrer les fichiers et les e-mails contenant des informations sur les cartes de crédit.

Etapes : Purview Microsoft -> Information Protection -> Labels -> Create a Label ->

New sensitivity label :

* Scope : Fiiles & Emails
* Protection settings : Encrypt
* Permissions : assign now

Assign permissions now :

* User access to content expires: Never
* Allow offline access: Never
* Assign permissions to specific users and groups: eCommerce app team

Next jusqu’à ce qu’on tombe sur la page d’accueil, ensuite cliquer sur « Auto-labeling ».

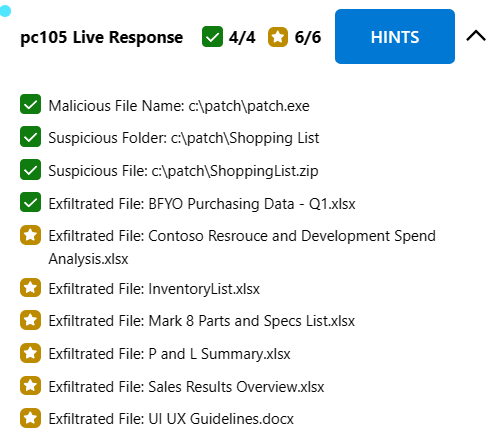
* Use A default policy template
* Financial
* Policy Name : eCommerce PCI DSS auto-labeling policy : tout cocher
* Choose a label to auto-apply : Confidential eCommerce App Team
* Test the policy : tout cocher sauf « Speed up deployment of the policy »

En utilisant Microsoft Defender (Advanced Hunting), j'ai analysé les logs pour mieux comprendre l'attaque. Dans Device Inventory, j'ai examiné les logs du pc105 (-> Threat analytics -> pc 105 -> Alerts).

A screenshot of a computer

Description automatically generated

J'ai ensuite effectué une vérification sur l'ordinateur compromis, identifiant les fichiers présents sur le système et les fichiers exfiltrés.



Pour le moment, nous savons comment l'attaque a eu lieu et quels fichiers ont été exfiltrés.

J'ai effectué une recherche approfondie dans les courriels, les documents et les communications Teams afin d'identifier toute information liée à l'adresse IP externe utilisée dans la récente attaque, en la considérant comme un indicateur de compromission (IoC).

Une fois que j’ai exporté le contenu des mails, on peut voir un message Teams de la part d’Angel Brown.

A screenshot of a computer

Description automatically generated

Angel Brown est désormais soupçonné d'être la personne à l'origine de cette attaque, mais nous devons poursuivre notre enquête. J’ai aussi regardé pour voir si un autre ordinateur de l’infrastructure s’est connecté à l’ip externe mais aucun résultat.

J’ai ajouté une baseline de sécurité afin de mieux protéger les systèmes. Voici les étapes :

EndPoint -> EndPoint security -> Next …

How do you reduce vulnerabilities, or attack surfaces, in your applications with intelligent rules that help stop malware?: Attack less reduce

* Select the configuraiton setting you would choose to protect against this phishing scenario.
  + Block office communication apps from creating child processes
  + Block all office applications from creating child processes
  + Block exécution of potentially ofuscated scripts (js/vbs/ps)
  + Block win32API calls from office macro

# | Evening Investigation :

J'ai configuré des politiques de protection de l'identité dans Azure AD Identity Protection, qui n'étaient pas initialement en place.

A screenshot of a computer screen

Description automatically generatedA screenshot of a sign in policy

Description automatically generated

Angel Brown étant notre suspecte, j'ai enquêté sur son compte pour vérifier toute compromission potentielle. Aucune alerte de sécurité n'a été déclenchée, et son ordinateur n'a pas été compromis, indiquant qu'elle était probablement l'auteure de l'attaque.

Lors de l'accusation, Angel a reconnu sa culpabilité. Cependant, ses intentions restent à déterminer

A screenshot of a computer screen

Description automatically generated