TP Découverte « Analyse » - Bloc 3 – JOBARD Guillaume – 2023/2024 – Mewo

Objectifs : analyser une demande client, en tirer des conclusions, se documenter et expérimenter une solution dans un environnement dédié. Rien que ça.

magatte seye
Campus Mewo
21 août 2024

Introduction générale

On a été contactés par un client confronté à plusieurs problèmes sur son réseau informatique, notamment des ralentissements inhabituels, des conflits d'adresses IP et des redirections vers des sites web inconnus. Ces incidents perturbent sérieusement l'activité quotidienne de l'entreprise, en particulier dans des services critiques comme la comptabilité. On vas lui répondre directement par mail pour le dire notre avis face à ces problèmes.

Rendu Professionnel

Objet : Incident Réseau - Rapport de Diagnostic et Actions Correctives

De : magatte seye
À : Josiane
Date : 21 Août 2024

Objet : Diagnostic des ralentissements réseau et actions correctives en cours

Chère Josiane,

Suite à votre demande et à la situation décrite concernant les ralentissements réseau, les conflits d'IP, et les redirections vers des sites inconnus, j'ai mené une analyse approfondie pour identifier la cause du problème et les mesures à prendre pour y remédier. Vous trouverez ci-dessous un résumé de mes conclusions ainsi que les actions en cours pour résoudre ce problème.

1. Diagnostic : Nature du problème

Après analyse, il est apparu que le réseau a été victime d'une **attaque malveillante**, de type **Man-in-the-Middle**

(MITM). Voici les éléments principaux qui m'ont conduit à cette conclusion :

Conflit d’adresses IP **:** Plusieurs utilisateurs, y compris vous-même, ont signalé des messages indiquant des conflits d’IP. Cela peut être causé par une machine non autorisée qui essaie de s'attribuer une adresse IP déjà en usage.

Redirections non désirées : Vous avez mentionné être redirigée vers des sites inconnus de manière aléatoire. Ceci est un signe classique d'une attaque où un attaquant manipule les requêtes DNS pour rediriger le trafic.

Propagation : Le fait que plusieurs utilisateurs rencontrent des problèmes similaires suggère que l’attaque s’est propagée à travers le réseau, touchant potentiellement plusieurs machines.

2. Explication du processus du pirate

1. **Accès initial au réseau** : L'attaquant peut avoir exploité une machine vulnérable (par exemple, celle liée à la récente intervention technique non surveillée) pour accéder le réseau.
2. **Interception du trafic** : Une fois à l'intérieur, le pirate a pu mettre en place une attaque MITM, intercepter les communications réseau, et modifier les requêtes DNS pour rediriger les utilisateurs vers des sites malveillants.
3. **Manipulation DNS** : En modifiant les paramètres DNS, le pirate redirige les utilisateurs vers des sites de phishing ou des pages contenant du malware, compromettant ainsi la sécurité des données.

3. Actions correctives en cours

Pour résoudre ce problème, les actions suivantes sont en cours :

1. **Isolation des machines infectées :** Les machines soupçonnées d'être compromises ont été isolées du réseau pour éviter une propagation supplémentaire.

2. **Analyse réseau :** Une analyse détaillée du trafic réseau est en cours pour identifier les appareils suspects et les comportements anormaux.
3. **Mise à jour et patching :** Nous vérifions que toutes les machines ont les dernières mises à jour de sécurité pour éliminer les vulnérabilités potentielles.
4. **Réinitialisation des paramètres DNS :** Les paramètres DNS des machines impactées sont en train d'être réinitialisés pour s'assurer qu'ils pointent vers des serveurs fiables.
5. **Analyse antivirus :** Toutes les machines du réseau seront scannées pour détecter et supprimer tout logiciel malveillant.

4. Conclusion

Nous On vas continuer à surveiller de près la situation et vous tiendrons informés de toute évolution. Soyez assurée qu'on vas prendre toutes les mesures nécessaires pour sécuriser le réseau et éviter que cela ne se reproduise.

Si vous avez des questions ou des préoccupations supplémentaires, n'hésitez pas à me contacter directement.

Cordialement,

Magatte seye

Étudiante Campus mewo

Conclusion générale

Ce TP nous a permis de mettre en évidence les difficultés des menaces qui regardent sur les infrastructures réseau modernes et l'importance d'une approche polyvalente pour les contre. En intégrant la détection, la réponse aux incidents, et la prévention, on peut renforcer la force de nos systèmes face aux attaques malveillantes. Cette expérience souligne également la nécessité de maintenir une veille technologique et une sensibilisation continue pour protéger efficacement les actifs numériques d'une organisation.