Rapport d’incident de sécurité - appliquer les techniques de renforcement des systèmes d’exploitation

Google Cybersecurity Certificate

Section 1 : Identifier le protocole réseau impliqué dans l’incident

Le protocole réseau impliqué dans cet incident est le protocole de transfert hypertexte (HTTP), qui opère au niveau de la couche application du modèle TCP/IP. Ce protocole est essentiel pour le transfert de pages web et des données entre le serveur et le navigateur de l’utilisateur.
Il est utilisé conjointement avec le protocole TCP pour établir une connexion fiable et sécurisée. De plus, le système de noms de domaines (DNS) est utilisé pour traduire les noms de domaines (comme yummyrecipesforme.com) en adresse IP, ce qui permet aux navigateurs de localiser les serveurs web.

Section 2 : Documenter l’incident

Suite à des plaintes de clients concernant une mise à jour de navigateur suspecte lors de la visite de yummyrecipesforme.com, entraînant un ralentissement notable de leurs ordinateurs, une enquête a été menée.

En utilisant un environnement sandbox pour isoler l’analyse, l’outil tcpdump a capturé le processus par lequel les utilisateurs étaient incités à télécharger un logiciel malveillant. Ce fichier a redirigé les utilisateurs vers un site clone, greatrecipesform.com, affichant gratuitement les recettes auparavant vendues. L’examen des logs tcpdump a montré une demande initiale de résolutions DNS pour yummyrecipesforme.com, suivie d’une redirection vers greatrecipesforme.com après l’exécution du fichier malveillant.

Il est apparu que l’accès non autorisé au panneau d’administration et la modification du code source ont été réalisés via une attaque par force brute, exploitant le mot de passe par défaut du compte administrateur. Le script malveillant ajouté au site original a facilité le téléchargement et l'exécution du fichier nuisible par les visiteurs, compromettant ainsi leur sécurité. Ce script a également servi à rediriger les visiteurs vers le site clone greatrecipesforme.com. Le script malveillant a été injecté dans le code source du site web original via une attaque par force brute.

Section 3 : Recommandations de mesures correctives pour les attaques par force brute.

Pour renforcer la sécurité contre les attaques par force brute, l’implémentation de l’authentification à deux facteurs (2FA) est fortement recommandée. Cette méthode exige que les utilisateurs fournissent un mot de passe à usage unique (OTP), en plus de leurs identifiants habituels, pour accéder au système. L’OTP peut être envoyé par e-mail ou SMS, ajoutant une couche de sécurité qui empêche efficacement l’accès non autorisé, même si le mot de passe initial est compromis. Cette stratégie réduit significativement le risque d’attaques réussies par force brute, en demandant une vérification d’identité par un moyen que seul l’utilisateur légitime peut fournir.

Pour aller un peu plus loin, pour éviter d’autres attaques par force brute, on pourrait recommander d’implémenter une politique de verrouillage après un certain nombre de tentatives de connexions échouées. Par exemple, après 5 tentatives de connexion infructueuses, le compte peut être bloqué temporairement, ce qui empêche les attaquants de continuer à deviner les mots de passe. Cette mesure doit être accompagnée par l’exigence de mots de passe forts pour tous les utilisateurs, en particulier les comptes administrateurs. Les mots de passe forts doivent contenir au moins 12 caractères, combinant des lettres majuscules et minuscules, des chiffres et des symboles.

Enfin, la mise en place d’un système d’alerte en cas de multiple tentatives de connexions échouées peut alerter les administrateurs d’une éventuelle attaque en cours, permettant une réaction plus rapide. Cela peut inclure des notifications par e-mail ou SMS aux administrateurs, signalant les tentatives de connexion suspectes.