Rapport d'incident de sécurité

| Section 1 : identifier le protocole réseau impliqué dans l'incident |
| --- |
| Le protocole concerné par l'incident est le protocole de transfert hypertexte (HTTP). L'exécution de tcpdump et l'accès au site Web yummyrecipesforme.com pour détecter le problème, capturer le protocole et l'activité du trafic dans un fichier journal du trafic DNS et HTTP ont fourni les preuves nécessaires pour parvenir à cette conclusion. Le fichier malveillant est transporté vers les ordinateurs des utilisateurs à l'aide du protocole HTTP au niveau de la couche application. |

|  |
| --- |
| Section 2 : documenter l'incident |
| Plusieurs clients ont contacté le propriétaire du site Web en indiquant que lorsqu'ils visitaient le site, ils étaient invités à télécharger et à exécuter un fichier qui leur demandait de mettre à jour leur navigateur. Depuis, leurs ordinateurs personnels fonctionnent lentement. Le propriétaire du site Web a essayé de se connecter au serveur Web, mais a constaté que son compte était bloqué.  L'analyste cybersécurité a utilisé un environnement sandbox pour tester le site Web sans affecter le réseau de l'entreprise. Ensuite, il a exécuté tcpdump pour capturer les paquets de trafic du réseau et de protocole produit par l'interaction avec le site Web. L'analyste a été invité à télécharger un fichier prétendant mettre à jour le navigateur de l'utilisateur, a accepté le téléchargement et l'a exécuté. Le navigateur a ensuite redirigé l'analyste vers un faux site Web (greatrecipesforme.com) qui semblait identique au site original (yummyrecipesforme.com).  L'analyste cybersécurité a inspecté le journal tcpdump et a observé que le navigateur a d'abord demandé l'adresse IP du site Web yummyrecipesforme.com. Une fois la connexion avec le site Web établie via le protocole HTTP, l'analyste s'est souvenu avoir téléchargé et exécuté le fichier. Les journaux ont montré un changement soudain dans le trafic réseau lorsque le navigateur a demandé une nouvelle résolution IP pour l'URL greatrecipesforme.com. Le trafic réseau a ensuite été redirigé vers la nouvelle adresse IP du site Web greatrecipesforme.com.  Le professionnel de la cybersécurité a analysé le code source des sites Web et le fichier téléchargé. Il a découvert qu'un pirate informatique avait manipulé le site Web pour y ajouter un code qui incitait les utilisateurs à télécharger un fichier malveillant déguisé en mise à jour de navigateur. Étant donné que le propriétaire du site Web a déclaré que son compte administrateur avait été verrouillé, l'équipe pense que le pirate informatique a utilisé une attaque par force brute pour accéder au compte et modifier le mot de passe de l'administrateur. L'exécution du fichier malveillant a compromis les ordinateurs des utilisateurs finaux. |

| Section 3 : recommander une mesure corrective pour les attaques par force brute |
| --- |
| L'une des mesures de sécurité que l'équipe prévoit de mettre en œuvre pour se protéger contre les attaques par force brute est l'authentification à deux facteurs (2FA). Ce plan d'accès 2FA comprendra une obligation supplémentaire pour les utilisateurs de confirmer leur identification en saisissant un mot de passe à usage unique (OTP) envoyé soit à leur e-mail, soit à leur téléphone. Une fois que l'utilisateur a confirmé son identité à l'aide de ses identifiants de connexion et de l'OTP, il peut accéder au système. Tout acteur malveillant qui tente une attaque par force brute n'obtiendra probablement pas l'accès au système parce qu'il nécessite une autorisation supplémentaire. |