20.06.2024

Attaque de phishing de type «reply-chain»

Tout le monde connaît les chaînes de réponse par e-mail. Le concept est simple: un utilisateur reçoit dans sa messagerie un mail collectif auquel différentes personnes répondent. Mais il n'imagine pas que la conversation puisse être détournée et qu'un message de phishing puisse apparaître comme une réponse au premier mail ou comme une continuation du fil de discussion. En effet, la plupart des gens s'attendent à ce qu'un e-mail de phishing leur parvienne comme un nouveau message, et non comme une réponse à un message précédent.

Lors d'une attaque par chaîne de réponses, les cybercriminels commencent par prendre le contrôle d'un compte de messagerie électronique pour envoyer une réponse contenant un lien ou un code QR malveillant. À partir du moment où l'adresse e-mail de ce compte fait partie de la liste de diffusion, le cyberpirate peut envoyer des messages frauduleux que les autres participants à la discussion percevront comme provenant d'un destinataire connu et fiable. De plus, comme il a accès à tous les messages du fil de discussion, le malfaiteur peut confectionner une réponse tout à fait pertinente, ce qui qui va renforcer encore davantage la crédibilité de l'e-mail frauduleux. Convaincue que la réponse provient d'un expéditeur de confiance, la victime de ce type d'attaque sera moins méfiante et plus encline à cliquer sur un lien piraté ou à ouvrir une pièce jointe malveillante.

Voici ce que vous pouvez faire pour réduire le risque de tomber dans le piège des attaques par chaîne de réponses:

- Utilisez des mots de passe forts et enregistrez-les dans un endroit sûr (p. ex. dans un gestionnaire de mots de passe). Vous compliquerez ainsi fortement la tâche des hackers qui souhaiteraient prendre le contrôle de votre boîte de messagerie.
- Soyez extrêmement prudent lorsque vous recevez un lien par email, SMS ou autre système de messagerie courte, ou après lecture d'un code QR.
- Ne communiquez jamais vos identifiants de connexion à vos appareils, comptes de messagerie, etc.

Pour tout complément d'informations sur le phishing, cliquez ici (https://www.ebas.ch/fr/le-phishing/) .