OUCH! | Décembre 2015

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

L'hameçonnage / Phishing

Vue d'ensemble

Le courrier électronique est l'un des principaux moyens par lequel nous communiquons. Nous l'utilisons non seulement tous les jours au travail, mais aussi pour rester en contact avec nos amis et notre famille. De plus, l'email est maintenant utilisé également par la plupart des entreprises offrant des services en ligne, tels que pour la confirmation de votre achat en ligne ou la disponibilité de vos relevés bancaires. Puisque tant de personnes dans le monde dépendent du courriel, ce dernier est devenu l'une des méthodes d'attaques principales utilisées par les cybercriminels. Dans ce numéro, nous expliquons ce qu'est le phishing, une méthode d'attaque électronique commune, et les mesures que vous pouvez prendre pour utiliser le courrier électronique en toute sécurité.

Editeur invité

Le Dr. Lance Hayden est le directeur général de Berkeley Research Group. Expert dans la culture et dans le comportement à la sécurité, il est l'auteur de People-Centric Security: Transforming Your Enterprise Security Culture de Crawl-Hill. Vous pouvez le trouver via **www.linkedin.com/in/drhayden**.

Le phishing (ou l'hameçonnage)

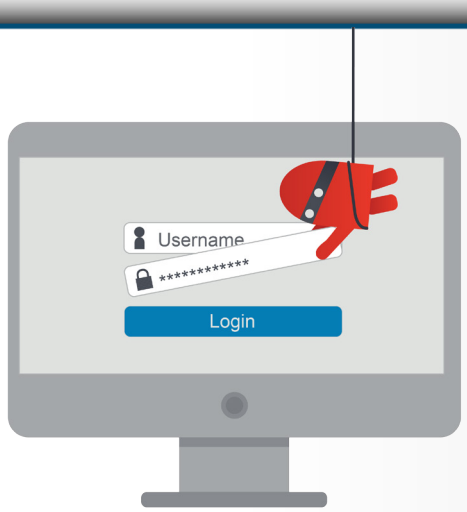
Le phishing se réfère à une attaque qui utilise le courrier électronique ou un service de messagerie tels que sur les sites de médias sociaux qui peuvent vous jouer des tours ou vous prendre pour un idiot en vous faisant fare une action à votre insu, comme par exemple cliquer sur un lien ou ouvrir une pièce jointe. En tant que victime d'une telle attaque, vous risquez d'avoir vos informations hautement sensibles volées et / ou votre ordinateur infecté. Les attaquants travaillent dur pour concevoir des e-mails de phishing convaincants. Par exemple, ils feront en sorte que leur email ressemble au mieux à quelque chose que vous connaissez ou semble provenir de quelqu'un que vous connaissez, comme d'un ami ou d'une société de confiance auprès de laquelle vous avez vos habitudes. Ils vont même jusqu'à ajouter des logos de votre banque ou encore falsifier l'adresse e-mail afin que le message paraisse le plus légitime possible. Puis les assaillants envoient ces e-mails par phishing à des millions de personnes. Ils ne savent pas qui va être victime, tout ce qu'ils savent c'est que plus d'e-mails ils envoient, plus ils augmentent leurs chances de réussite. Le phishing est similaire à l''utilisation d'un filet pour attraper du poisson, vous ne savez pas ce que vous allez attraper mais plus gros sera le filet, plus de poissons vous aurez. Il y'a plusieurs façons d'utiliser le phishing pour que les attaquants obtiennent ce qu'ils veulent.

- **Récolte d'informations** : Le but de l'attaquant est de récolter vos informations personnelles, telles que vos mots de passe, numéros de carte de crédit ou coordonnées bancaires. Pour ce faire, ils vous enverront un lien qui vous mènera à

L'hameçonnage / Phishing

un site Web qui vous semblera légitime. Ce site vous demande de fournir des informations de votre compte ou vos données personnelles. Toutefois, le site est faux et toutes les informations que vous entrez parviennent directement à l'attaquant.

- **Liens malveillants**: Le but de l'attaquant est de prendre le contrôle de votre appareil. Pour ce faire, ils vous envoient un e-mail avec un lien. Si vous cliquez sur le lien, il vous emmène sur un site Web qui lance une attaque sur votre dispositif et qui, en cas de succès, infecte votre système.
- **Pièces jointes malveillantes**: Le but de l'attaquant est le même, infecter et prendre le contrôle de votre appareil. Cependant, à la place d'un lien, l'attaquant vous envoie cette fois-ci un fichier infecté, comme un document Word. Ouvrir la pièce jointe déclenche l'attaque, donnant potentiellement le contrôle à l'attaquant de votre système.
- **Escroqueries**: Certains courriels de phishing ne sont rien de plus que des escroqueries numériques. Ils essaient de vous tromper en disant que vous avez gagné à la loterie, faisant semblant d'être un organisme de bienfaisance ou encore de vous demander votre aide pour déplacer des millions de dollars. Si vous répondez à toutes ces choses, ils vont dire qu'ils ont d'abord besoin que vous payez leurs services ou l'accès à votre compte bancaire, pour ainsi vous escroquez de l'argent.



Votre meilleure défense est votre bon sens. Si un e-mail ou un message vous semble bizarre, suspect, ou trop beau pour être vrai, il peut s'agir d'une attaque par phishing.

Se protéger

Dans presque tous les cas, l'ouverture et la lecture d'un courriel ou d'un message se passe sans encombres. Pour une attaque par phishing, le but des cybercriminels est de vous inciter à faire quelque chose. Heureusement, il existe des indices vous permettant de déceler qu'un message est une attaque, voici les plus courants:

- L'email crée un sentiment d'urgence, exigeant une "action immédiate" avant que quelque chose de mauvais arrive, comme la fermeture de votre compte. L'attaquant veut vous précipiter à la faute sans que vous puissiez prendre le temps de réfléchir.
- Vous recevez un email avec une pièce jointe que vous n'attendiez pas ou l'e-mail vous incite à ouvrir la pièce jointe. Les exemples incluent un courriel disant qu'il a une pièce jointe avec les détails de licenciements sans préavis, les informations de salaire de l'employé ou une lettre des impôts vous stipulant que vous êtes poursuivi.
- Au lieu d'utiliser votre nom, l'email utilise une salutation générique comme "Cher client". La plupart des entreprises ou des amis qui vous contactent connaissent votre nom.

L'hameçonnage / Phishing

- Les demandes par email d'informations hautement sensibles, tels que votre numéro ou mot de passe de carte de crédit.
- Le courriel dit qu'il vient d'une organisation officielle, mais a une mauvaise grammaire ou orthographe, ou utilise une adresse de courriel personnelle comme @ gmail.com, @ yahoo.com, hotmail.com ou @.
- Le lien semble étrange ou non officiel. Une astuce consiste à passer votre souris sur le lien jusqu'à ce qu'une fenêtre pop-up vous montre la destination du lien. Si le lien dans l'e-mail ne correspond pas à la destination de pop-up, ne cliquez pas dessus. On obtient le même pop-up sur les appareils mobiles en maintenant votre doigt sur un lien. Une étape encore plus sûre consiste à copier puis coller l'URL de l'email dans votre navigateur ou de taper le lien correct.
- Vous recevez un message de quelqu'un que vous connaissez, mais le libellé sonne faux et ne ressemble pas au style de cette personne. Si vous avez des doutes, appelez l'expéditeur afin de vérifier qu'il vous l'a bien envoyé. Il est facile pour un attaquant de créer un courriel qui semble provenir d'un ami ou d'un collègue.

Si vous soupçonnez qu'un email ou un message est une attaque par phishing, il suffit de le supprimer. En fin de compte votre bon sens est votre meilleure défense.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients. Pour en savoir plus, veuillez vous référer aux liens suivants : http://www.answer.ch et http://answersecurity.com/

Sources

Ingénierie sociale :	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_fr.pdf
Cinq étapes pour rester sécurisé :	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201410_fr.pdf
J'ai été hacké, que dois-je faire maintenant? :	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-2014-05_fr.pdf
OnGuard Online :	https://www.onguardonline.gov/phishing
Conseil du jour par du SANS sécurité :	https://www.sans.org/tip_of_the_day.php

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet