Votre publication mensuelle de conscientisation à propos de la Sécurité

Repérer et arrêter les attaques de messagerie

Que sont les attaques par messagerie?

Le smishing (un mot-valise combinant SMS et phishing) est une attaque qui se produit lorsque des cyber-attaquants utilisent des SMS, message texte ou des technologies de messagerie similaires pour vous inciter à prendre une action que vous ne devriez pas entreprendre. Peut-être qu'ils vous trompent en fournissant les détails de votre carte de crédit, vous obligent à appeler un numéro de téléphone pour obtenir vos informations bancaires ou vous convainquent de remplir un sondage en ligne pour recueillir vos informations personnelles. Tout comme dans les attaques d'hameçonnage par courriel, les cybercriminels jouent souvent sur vos émotions pour vous amener à agir en créant un sentiment d'urgence ou de curiosité, par exemple. Cependant, ce qui rend les attaques par messagerie si dangereuses, c'est qu'il y a beaucoup moins d'informations et moins d'indices dans un texte que dans un courriel, ce qui rend beaucoup plus difficile pour vous de détecter que quelque chose ne va pas.

Une arnaque courante est un message vous informant que vous avez gagné un iPhone, et il vous suffit de cliquer sur un lien et de remplir un sondage pour le réclamer. En réalité, il n'y a pas de téléphone et l'enquête est conçue pour récolter vos informations personnelles. Un autre exemple serait un message indiquant qu'un colis n'a pas pu être livré avec un lien vers un site Web où vous êtes invité à fournir les informations nécessaires pour terminer la livraison, y compris les détails de votre carte de crédit pour couvrir les « frais de service ». Dans certains cas, ces sites peuvent même vous demander d'installer une application mobile non autorisée qui infecte et prend le contrôle de votre appareil.

Parfois, les cybercriminels combinent même des attaques par téléphone et par messagerie. Par exemple, vous pouvez recevoir un SMS urgent de votre banque vous demandant si vous avez autorisé un paiement inhabituel. Le message vous demande de répondre OUI ou NON pour confirmer le paiement. Si vous répondez, le cybercriminel sait maintenant que vous êtes prêt à vous engager et vous appellera en prétendant être le service des fraudes de la banque. Ils essaieront ensuite de vous parler de vos informations financières et de carte de crédit, ou même de l'identifiant et du mot de passe de votre compte bancaire.

Détecter et arrêter les attaques de messagerie

Voici quelques questions à vous poser pour repérer les indices les plus courants d'une attaque par messagerie:

© SANS Institute 2021

- Le message crée-t-il un énorme sentiment d'urgence en tentant de vous précipiter ou de vous forcer à prendre des mesures?
- Le message vous amène-t-il vers des sites Web qui vous demandent vos informations personnelles, votre carte de crédit, vos mots de passe ou d'autres informations sensibles auxquelles ils ne devraient pas avoir accès?
- Le message semble-t-il trop beau pour être vrai? Non, vous n'avez pas vraiment gagné un nouvel iPhone gratuitement.
- Le site Web ou le service lié vous oblige-t-il à payer en utilisant des méthodes non standard telles que Bitcoin, des cartes-cadeaux ou des virements Western Union?
- Le message vous demande-t-il le code d'authentification multi-facteur qui a été envoyé sur votre téléphone ou généré par votre application bancaire?
- Le message ressemble-t-il à un « mauvais numéro ? » Si tel est le cas, n'y répondez pas et n'essayez pas de contacter l'expéditeur; il suffit de le supprimer.

Si vous recevez un message d'une organisation officielle qui vous alerte, rappelez directement l'organisation. N'utilisez pas le numéro de téléphone inclus dans le message, utilisez plutôt un numéro de téléphone de confiance. Par exemple, si vous recevez un SMS de votre banque indiquant qu'il y a un problème avec votre compte ou votre carte de crédit, obtenez un numéro de téléphone de confiance sur le site Web de votre banque, un relevé de facturation ou au dos de votre banque ou carte de crédit. N'oubliez pas non plus que la plupart des agences gouvernementales, telles que les agences fiscales ou les forces de l'ordre, ne vous contacteront jamais par SMS, elles ne vous contacteront que par courrier à l'ancienne.

Lorsqu'il s'agit d'attaques par messagerie, vous êtes votre meilleure défense.

Rédacteur invité

Jeff Lomas est détective pour le département d'investigation cyber de la police métropolitaine de Las Vegas et enseigne le cours SANS SEC487 Open-Source Intelligence Gathering and Analysis (OSINT). Jeff enquête sur les crimes financiers de haute technologie, notamment les compromissions de messagerie professionnelle, le smishing, les ransomwares et les cas complexes de vol de crypto-monnaie et de blanchiment d'argent.

Ressources

Arrêtez ce hameçonnage: https://www.sans.org/newsletters/ouch/stop-that-phish/
Attaques d'ingénierie sociale: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Vishing - Attaques et escroqueries par appel téléphonique: https://www.sans.org/newsletters/ouch/vishing/

Traduit pour la communauté par: Jérôme Boutin et Sebastien Kierszka

OUCH! Publié par SANS Security Awareness et distribué sous Creative Commons BY-NC-ND 4.0 license. Vous êtes libre de partager ou de distribuer cette lettre de nouvelles tant que vous ne la vendez pas ou ne la modifiez pas. Équipe d'éditeur: Walter Scrivens, Phil Hoffman, Alan Waggoner, Les Ridout, Princess Young.