Les bases de l'hameçonnage

Devolutions

CE QU'ILS SAVENT QUI EST DANGEREUX, C'EST CE QU'ILS IGNORENT!

Je sais que les professionnels de l'informatique qui fréquentent notre blogue connaissent les dangers de l'hameçonnage. Il y a toutefois bien des chances que certains de vos collègues moins technos ne les connaissent pas. Ils sont au fait de certaines notions, mais ce n'est pas ce qu'ils savent qui est dangereux, c'est ce qu'ils ignorent!

L'hameçonnage existe depuis longtemps et il ne disparaîtra pas de sitôt. Voici quelques statistiques assez effrayantes tirées du Rapport d'enquête sur les violations de données de Verizon (DBIR):

- 94% des logiciels malveillants sont envoyés par courriel.
- 90% des attaques et des violations comptent un élément d'hameçonnage.
- 28% des tentatives d'hameçonnage sont ciblées.
- 21% des rançongiciels impliquent des actions sociales comme l'hameçonnage.

De plus, des sondages et études menés par CSOOnline.com ont révélé que 56% des décideurs informatiques estiment que la prévention des attaques d'hameçonnage est leur priorité numéro un.

J'ai donc pensé rédiger un billet sur les bases de l'hameçonnage. Si vous êtes un professionnel de l'informatique, en plus de vous rafraîchir la mémoire (une petite révision de temps en temps ne fait jamais de mal, non?), ce texte pourra vous servir pour sensibiliser vos collègues à cette problématique. Il faut s'assurer qu'ils font partie de la solution en matière de cybersécurité et non (involontairement) du problème.

Qu'est-ce que l'hameçonnage?

Essentiellement, l'hameçonnage est une tentative de pirates informatiques de se déguiser en individus légitimes (par exemple, en collègues/amis) ou en organisations, pour inciter leurs victimes à partager des informations sensibles telles que des mots de passe, des numéros de carte de crédit, etc.

Comment se produit l'hameçonnage?

À l'heure actuelle, il est fort probable – en fait c'est pas mal certain à 100% - que vous ayez été la cible de nombreuses attaques d'hameçonnage. La grande majorité d'entre elles ont été captées par les filtres antipourriel de votre service de messagerie, mais certains d'entre eux passent parfois entre les mailles du filet et peuvent se retrouver dans votre boîte de réception.

Beaucoup de ces courriels d'hameçonnage sont des tentatives d'escroquerie évidentes que vous pouvez facilement repérer. Ce serait toutefois une grave erreur de penser que toutes les tentatives sont facilement décelables. Par exemple, dans notre sondage de septembre dernier, nous vous avons demandé de partager les cyberarnaques les plus réalistes dont avez été témoins. De nombreux répondants ont souligné les courriels d'hameçonnage qui semblaient provenir d'expéditeurs légitimes tels qu'Amazon, Microsoft, eBay, Apple, des compagnies de cartes de crédit et même leurs propres collègues.

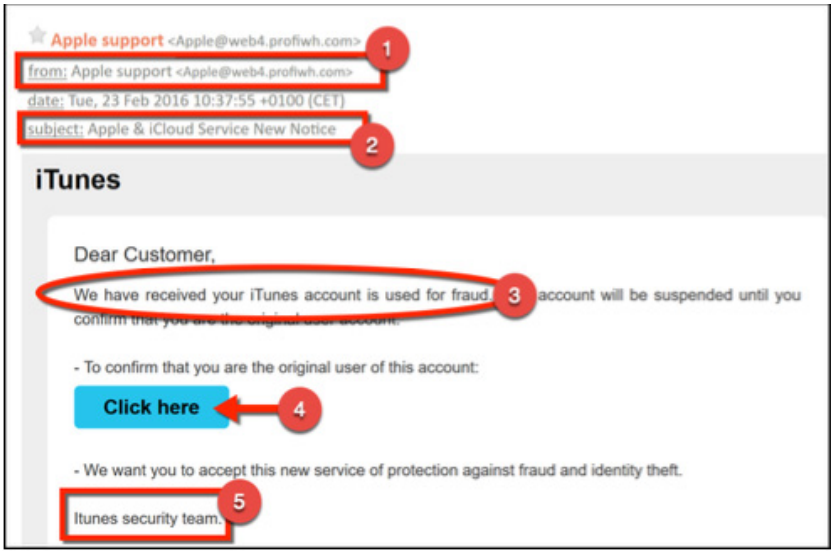
Règle générale, les attaques d'hameçonnage qui utilisent de faux sites Web suivent cette démarche :

Étape 1 – Ciblage

Les pirates déterminent une organisation qu'ils souhaitent spoofer (c'est-à-dire faussement représenter). Souvent, ils choisissent une organisation réputée et de confiance avec une large base de clients comme des institutions financières, des sites d'enchères en ligne, des créateurs de logiciels et des grandes chaînes de vente au détail. Ensuite, ils créent une copie du site Web de l'organisation en utilisant le même texte, les mêmes logos et les mêmes images que sur le site d'origine. Tout comme les courriels, certains de ces faux sites Web peuvent sembler très vrais.

Étape 2 – Envoi par courriel

Les pirates envoient un courriel à un grand nombre de destinataires ou à des individus spécifiques (c'est ce qu'on appelle le harponnage). Les destinataires sont invités à cliquer sur un lien qui les amène au faux site Web décrit précédemment. Voici un exemple :



1. **De** (*From*) : Vous remarquerez que l'adresse courriel de l'expéditeur est la suivante : apple@web4.profiwh.com. À première vue, ça semble légitime, car l'adresse contient le mot « Apple ». Et encore là, de nombreuses personnes ne prennent même pas la peine de regarder l'adresse courriel de l'expéditeur. Ils regardent simplement son nom qui est « Apple Support » dans cet exemple.
2. **Objet** (*Subject*) : C'est souvent quelque chose qui vise à créer un sentiment d'urgence. Dans cet exemple, les pirates utilisent deux mots qui augmentent les taux d'ouverture des courriels : « Avis » (Notice) et « Nouveau » (New).
3. **Contenu** (*Content*) : Habituellement, la première ligne du courriel d'hameçonnage vise à faire augmenter vos pulsations cardiaques, ce qui nuit à votre jugement. Dans cet exemple, la première

ligne est en effet assez épeurante : « Nous avons reçu que votre compte iTunes est utilisé pour fraude ». Les gens sont tellement stressés qu'ils ont tendance à ne pas remarquer que la phrase est mal écrite. La seule chose qui leur traverse l'esprit est : « Oh non, mon compte a été piraté! »

Les pirates utilisent généralement un titre générique plutôt qu'un nom spécifique. Par exemple, dans ce courriel, ils utilisent « Cher client ». C'est simplement parce qu'ils envoient le même courriel à des milliers de victimes potentielles. Les courriels de harponnage utilisent généralement le prénom de la personne ciblée (et éventuellement son nom de famille). Mon dossier pourriels est rempli de faux courriels qui commencent par « Chère Jenny ».

4. **Bouton d'action** : De nombreux courriels d'hameçonnage n'ont pas d'hyperliens au look traditionnel. Ils ont souvent un bouton, ce qui est le cas dans l'exemple ci-dessus. Le bouton est utilisé de manière stratégique, car les gens sont plus susceptibles de cliquer sur des boutons que sur des liens (en passant, c'est aussi la raison pour laquelle vous voyez des boutons sur les pages destinées à vous vendre des choses).
5. **Signature** : Il s'agit souvent d'une « équipe » ou d'un « service », bien que parfois ce soit le nom d'un (faux) employé. Dans cet exemple, le faux courriel provient de « l'équipe de sécurité ITunes ». Encore une fois, le fait que « ITunes » soit mal écrit (ça devrait plutôt être « iTunes ») devrait mettre les victimes sur leurs gardes. Elles sont parfois tellement paniquées qu'elles oublient ce genre de détails.

Étape 3 – Collecte d'informations et vol d'identité

Une fois qu'ils ont réussi à capturer une victime, les pirates informatiques collectent des informations personnelles et confidentielles telles que les numéros de carte de crédit, les mots de passe, les NIP, les numéros d'assurance sociale, les dates de naissance, etc. Ces informations sont ensuite utilisées pour commettre un vol d'identité, vider des comptes bancaires, effectuer des achats frauduleux par carte de crédit, contracter des prêts et des hypothèques, etc.

L'hameçonnage par téléphone

Parfois, les pirates tentent d'attirer les victimes par téléphone. C'est ce qu'on appelle l'hameçonnage par téléphone (ou l'hameçonnage vocal). Les pirates peuvent par exemple prétendre être des représentants d'une compagnie de carte de crédit qui a détecté une utilisation abusive d'une carte et, par conséquent, ils demandent à la victime de confirmer son numéro de carte de crédit ou son numéro d'assurance sociale.

Les pirates peuvent combiner des tactiques téléphoniques et par courriel dans la même attaque. Par exemple, les pirates vont appeler une victime qui travaille dans le service des comptes payables d'une

entreprise et se font passer pour un fournisseur qui a récemment changé de banque. Le pirate informatique dit alors à la victime qu'il lui enverra par courriel les nouvelles informations de compte bancaire. Parce que la victime voit immédiatement le courriel au moment où l'appel se termine (ou parfois même pendant l'appel), elle croit qu'il est légitime. La victime modifie ensuite les détails du paiement en conséquence. L'escroquerie n'est révélée que lorsque le vrai fournisseur se plaint de ne pas avoir été payé!

Que devez-vous faire si vous avez cliqué sur un hyperlien frauduleux

Évidemment, personne ne veut cliquer sur un hyperlien frauduleux et se faire prendre dans le filet d'un pirate. Mais que se passe-t-il si ça vous arrive? Dans la plupart des cas, suivez les sages paroles de Douglas Adams dans Le guide du voyageur galactique : NE PANIQUEZ PAS.

Tant que vous ne vous êtes pas connecté au faux site Web ou que vous n'avez pas fourni d'autres informations confidentielles, voici ce que vous devez faire : fermez votre navigateur, effacez votre cache et vos cookies, et lancez une analyse anti-logiciels malveillants, une analyse antivirus et une analyse anti-logiciel espion.

Trucs pour rester en sécurité

Voici quelques conseils supplémentaires pour éviter d'être victime d'attaques d'hameçonnage :

- Vérifiez toujours l'URL! Même si l'adresse semble correcte, vous n'êtes pas forcément sur un site légitime. Souvent, si vous regardez attentivement, vous remarquerez quelques petits changements, comme le remplacement de la lettre « l » par le chiffre « 1 » (par exemple, www.1inkedin.com au lieu de www.linkedin.com). Vérifiez également si l'URL commence par http:// au lieu de https://. Un site Web sécurisé commencera toujours par https://. Le petit « s » supplémentaire est vraiment important! Enfin, recherchez le petit cadenas à côté de l'adresse du site Web.
- Soyez toujours méfiant lorsque vous recevez un courriel qui :

1. Semble urgent et vous invite à cliquer immédiatement sur un lien ou un bouton.
2. Vous demande des informations personnelles ou financières.
3. Vous demande de changer de mot de passe.
4. Vous offre une récompense en échange d'informations.

- Ne cliquez pas sur les liens ou les boutons dans un courriel. Si vous pensez que le courriel est légitime, accédez directement au site Web de l'entreprise.
- Ne téléchargez pas de pièces jointes provenant d'une source inconnue. Celles-ci sont souvent utilisées pour propager des virus et des logiciels malveillants.

- Si vous pensez qu'un courriel est suspect ou si vous vous trouvez sur un site Web qui semble douteux, communiquez directement avec l'organisation qui a fait l'envoi. Important : ne téléphonez pas à l'entreprise en utilisant le numéro qui apparaît dans le courriel! Croyez-le ou non, la personne à l'autre bout du fil pourrait faire partie de l'arnaque. Recherchez le numéro de l'organisation dans un bottin ou une source fiable.

En plus de l'hameçonnage, d'autres escroqueries en ligne peuvent être très dangereuses si vos utilisateurs finaux n'en sont pas conscients. Par exemple, lisez notre article, en anglais, intitulé 7 escroqueries en ligne célèbres.

En gros, le plus important est d'être vigilant. Restez vigilant, ne présumez rien et suivez votre instinct. Comme dirait Obi-Wan : « Que la Force soit avec vous! »