Club informatique Mont-Bruno

Séances du 24 février et du 14 mars 2012
Présentateur : André Charest

L'hameçonnage et le harponnage

L'hameçonnage et le harponnage sont des techniques utilisées par des fraudeurs pour nous piéger.

L'hameçonnage (phishing, en anglais) consiste à envoyer massivement des courriels demandant des renseignements personnels précis et en prétendant faussement qu'ils proviennent d'une entreprise réputée et de confiance, tels une banque, le gouvernement ou une compagnie reconnue.
Note : le mot anglais phishing est un mot inventé par des pirates (hackers) à partir de fishing.

Le harponnage (spear-phishing, en anglais) est une variante sophistiquée de l'hameçonnage. Il consiste à obtenir d'abord des renseignements de compagnies, d'institutions, de gouvernements ou de réseaux sociaux. Les fraudeurs se servent ensuite de ces renseignements pour tendre des pièges ciblés.

L'hameçonnage

Les fraudeurs construisent toutes sortes de scénarios pour hameçonner leurs victimes. Typiquement, les messages ainsi envoyés semblent émaner d'une société digne de confiance et sont formulés de manière à alarmer le destinataire afin qu'il effectue une action.

Une approche souvent utilisée est d'indiquer à la victime potentielle qu'à cause d'un problème de serveur son compte a été désactivé, ou que toutes ses informations ont été perdues, et que la réactivation ne sera possible que par suite d'une action de sa part. Le message fournit un hyperlien qui dirige l'utilisateur vers une page Web qui ressemble à s'y méprendre à la vraie page d'accueil du site de la société digne de confiance. Arrivé sur cette page falsifiée, l'utilisateur est invité à saisir, en plus de son nom et de son adresse, des informations confidentielles (comme son numéro d'assurance sociale, son numéro de compte de banque ou son NIP) qui sont alors enregistrées par le criminel. Il ne faut pas se fier pas au « s » après le http dans la barre d'adresse de la page Web et à la présence de l'icône  . L'utilisateur qui tombe dans le panneau devient victime d'un vol d'identité.

Ce qu'il faut savoir, et c'est très important, c'est que jamais une banque, caisse, compagnie de crédit ou institution financière ne demande de valider des informations personnelles par téléphone ou par courriel. Dans le doute, cherchez vous-même le numéro de téléphone de votre succursale et contactez-la directement.

Voici d'autres exemples d'hameçonnage qui ne se limite pas au vol d'identité. On vous invite à

- acheter des actions en bourse sous prétexte qu'elles sont sous-évaluées [hameçonnage de type **Pump and dump** (présentations de J-P Jacquet les 27 janvier et 15 février derniers)] ;
- coopérer avec quelqu'un pour faire une action comme sortir de l'argent d'un autre pays ;
- fournir des renseignements personnels pour devenir employé d'une entreprise qui propose un salaire de 30 $ l'heure pour faire des sondages téléphoniques ;
- payer des frais ou des taxes pour recevoir un prix alléchant que l'on a supposément gagné (par exemple un ordinateur, un iPad ou une console de jeux) ;
- faire une action qui permet à un fraudeur d'installer un ou plusieurs logiciels malveillants dans votre ordinateur ;
- etc.

Ne répondez jamais à ce type de courriel, ne cliquez pas sur les liens proposés et ne donnez jamais d'information personnelle. Aucune entreprise légitime ne fait de telle demande par courriel (ou par téléphone). Gardez vos **logiciels antipourriel** et **antivirus** à jour, ainsi que votre système d'exploitation. Si vous devez faire des **transactions électroniques**, assurez-vous que le site est fiable et de bonne réputation en utilisant le **filtre antihameçonnage** de votre navigateur Web.

Voici un exemple de courriel tiré de Wikipédia après traduction libre. Notez que deux lettres composant le sigle de la banque dans l'hyperlien sont inversées.

BDC Banque du coin

Cher client,

On nous a avisés que vous avez récemment tenté de retirer 215,00 $ de votre compte de chèque alors que vous étiez en voyage à l'étranger.

Si cette information est fausse, il pourrait s'avérer qu'un inconnu a accès à votre compte. Pour plus de sécurité, visitez notre site Web en cliquant sur le lien ci-dessous pour vérifier vos informations personnelles.

http://www.bcd.com/general/verificateur.asp

Aussitôt que ce sera fait, notre service des fraudes s'emploiera à prévenir tout retrait frauduleux de votre compte.

Nous vous remercions de votre confiance.

Banque du Coin

Si la banque **BDC** n'est pas votre banque, il s'agit d'hameçonnage. Si la banque **BDC** est votre banque, il pourrait quand même s'agir d'hameçonnage. Le fraudeur peut savoir que, dans votre région la banque, **BDC** est une institution populaire. Il envoie le courriel à une série de personnes de votre région dont il a obtenu les adresses courriel. Sur ces personnes, certaines seront clientes de la banque **BDC**. Que quelques personnes mordent à l'hameçon et la pêche sera rentable pour le fraudeur.

Le fraudeur pourrait avoir acheté sur Internet une liste de clients de la banque **BDC**. Seuls alors les clients de **BDC** recevront alors le courriel frauduleux. La partie de pêche pourrait être bien meilleure. Dans ce cas, il s'agit plutôt de harponnage.

Voici un autre exemple tiré tel quel cette fois de Wikipédia.

From: Webmaster Admin <in-foweb@live.co.uk>
To: undisclosed-recipients: ;
Reply-to: in-foweb@live.co.uk
Subject: Attention !! Re-activer le service e-mail
Date: Wed, 19 Jan 2011 15:54:21 +0100 (CET)
User-Agent: SquirrelMail/1.4.8-5.el5.centos.10

Votre quota a dépassé l'ensemble quota/limite est de 20 Go Vous êtes en cours d'exécution sur 23FR de fichiers et parce que les fichiers cachés sur votre e-mail.

S'il vous plaît cliquer sur le lien ci-dessous pour confirmer votre boîte de réception lettres et d'augmenter votre quota.

http://www.knaus-camping-hennesee.de/phpform/use/webform/form1.html

S'il vous plaît Cliquez sur le lien et confirmez votre quota Si non, peut entraîner une perte de des informations importantes dans votre boîte aux lettres.

Cet avertissement est du service de chef de département. S'il vous plaît mettez à jour votre compte dans le lien fourni pour éviter la perte de votre e-mail.

Je vous remercie
Service Web comptes

Attention (mise en garde très importante) : ne fournissez pas votre mot de passe de messagerie sur une page qui ressemble à la page d'accueil de votre messagerie Web (Hotmail, Gmail, Yahoo) si vous avez obtenu cette page en cliquant sur un lien contenu dans un courriel. Vous n'êtes probablement pas sur la page d'accueil de votre messagerie Web, mais bien sur la page d'un pirate informatique qui tente de vous voler votre mot de passe. Cette mise en garde est valable même si le courriel semble provenir d'une personne que vous connaissez.

Le harponnage

Depuis des années, les courriels frauduleux et les logiciels malveillants se propagent sur l'internet. Grâce à de l'information tirée de sites comme Facebook et LinkedIn, la menace est plus ciblée que jamais : courriels personnalisés, coordonnées financières précises et sollicitations apparemment légitimes provenant de personnes ou d'institutions connues. Exemples.

- Un internaute pris à l'étranger se dit prêt à vous vendre son véhicule remisé à Montréal si vous acceptez de le payer en ligne.
- Une collègue en voyage en Afrique vous demande de faire un virement bancaire de toute urgence pour la dépanner.
- La banque vous envoie un courriel contenant votre numéro de carte de crédit et vous exhorte à changer votre mot de passe par suite d'une fraude au Moyen-Orient. Ça semble normal? Ce ne l'est pas. C'est la plus récente vague de fraudes en ligne, plus raffinée que jamais.

Où les pirates prennent-ils leurs informations pour vous cibler? Ils n'hésitent pas à voler les listes d'envoi des grandes entreprises. Ils écument les réseaux sociaux. Les pirates se spécialisent. Il y en a qui se spécialisent dans la recherche d'informations partout où ils peuvent les trouver. Ils les vendent ensuite sur Internet à d'autres pirates qui eux tendent les pièges.

Grâce aux données accumulées, même s'ils sont établis en Europe de l'Est, aux États-Unis ou en Amérique du Sud, les pirates nous connaissent comme s'ils étaient nos voisins immédiats.

Par le harponnage, les pirates ne se contentent pas de mettre leurs lignes à l'eau en espérant que ça morde. Ils lancent des attaques ciblées sur des victimes bien précises.

Actions pour diminuer votre exposition à l'hameçonnage et au harponnage (les conseils ci-dessous dépassent le strict domaine de l'hameçonnage et du harponnage)

- Lorsque vous envoyez des courriels à un grand nombre de destinataires, placez les adresses dans la liste des cci (copies conformes invisibles).
- Quand il s'agit de courriels que les destinataires sont susceptibles de renvoyer à d'autres (pps, wmv, etc.) demandez qu'on efface votre adresse courriel avant de réacheminer le courriel, ex. : ***Merci d'effacer mon adresse avant de réacheminer ce courriel.***
  (Thank you for deleting my e-mail address before forwarding.).
- Si vous réacheminez vous-même un courriel qui vous a été transféré, effacez toutes les adresses précédentes qui ne seraient pas pertinentes pour les nouveaux destinataires.
- Évitez d'entrer dans les chaînes pyramidales de courriels qui vous demandent de transférer le courriel reçu à x autres destinataires en vous promettant une grâce

quelconque si vous le faites ou un malheur si vous ne faites pas. Ces courriels servent souvent à accumuler des informations sur vous et vos destinataires.

- N'entrez pas dans les chaînes de courriels à contenu idéologique surtout si vous n'avez pas les connaissances requises pour juger de la véracité des faits ou allégations rapportés; ex, les courriels contre les OGM ou un vaccin, etc.
- Ne répondez pas à un courriel d'une institution qui n'est pas sensée connaître votre adresse courriel.
- Méfiez-vous si vous êtes francophone et que le courriel que vous recevez est en anglais, et surtout en mauvais anglais ou que le courriel en français est mal rédigé.
- Évitez de cliquer sur des liens dans un courriel quand vous n'êtes pas absolument sûr de la source du courriel.
- Ne demandez jamais à votre messagerie Web de se souvenir de votre mot de passe.
- Quand vous ouvrez la page Web de votre banque, de votre courtier ou de toute autre institution chez laquelle vous faites des transactions ou encore celle d'une messagerie Web (Hotmail, Gmail ou Yahoo), tapez vous-même l'adresse dans la barre d'adresse pour éviter d'ouvrir une page bidon dont le lien a été installé dans votre navigateur par un pirate. Vous serez certain ainsi de ne pas donner votre mot de passe à un pirate.
- Quand vous tapez un mot de passe important, ajoutez des caractères au mot de passe en les tapant dans un autre champ (la barre d'adresse par exemple). Le mot de passe enregistré par un enregistreur de frappes (keylogger) sera faux.
- Faites attention aux jeux multijoueurs en ligne; le site qui vous permet de jouer pourrait être mal protégé.

Sources

- ISIQ : http://monidentite.isiq.ca/decouvrez_menaces/hameconnage.html
- Denis Talbot, Vigilance sur le Net : http://www.vigilancesurlenet.com/tournee/html/section-multimedia/capsules-denis-talbot/hameconnage.php
- Alain McKenna, La Presse : http://technaute.cyberpresse.ca/nouvelles/internet/201101/24/01-4363327-fini-lhameconnage-place-au-harponnage.php
- Branchez-vous.com : http://www.branchez-vous.com/actu/05-12/09-352505.html
- Wikipédia
- Michel Gagné