Focus

Le Phishing

Claude Chaloux 

Degré de difficulté

Grâce à l'Internet, de nouveaux services financiers et transactionnels sont maintenant à la disposition d'utilisateurs amateurs. Des adaptations dans les techniques qu'utilisent les cyber-pirates étaient prévisibles. Quelles sont ces nouvelles techniques ? L'identité des victimes est-elle connue à l'avance ? Pouvons-nous protéger nos clients face à de telles attaques ?

L'hameçonnage consiste en un envoi massif de courriels contrefaits, communément appelés courriels hameçon, utilisant l'identité d'une institution financière ou d'un site commercial connu de façon apparemment authentique.

Dans ces courriels contrefaits, on demande aux destinataires de mettre à jour leurs coordonnées bancaires ou personnelles en cliquant sur un lien menant vers un site Web illégitime qui est habituellement une copie conforme du site de l'institution ou de l'entreprise. Le pirate, ou criminel informatique qui a envoyé le courriel hameçon peut alors récupérer ces renseignements afin de les utiliser à son avantage.

Le terme anglais *phishing* est issu de l'anglais *fishing* (pêche) écrit avec un *ph*, comme c'est souvent le cas dans le jargon des pirates informatiques. Il fait allusion à la pêche à la ligne et à l'océan des utilisateurs d'Internet, dans lequel le pirate essaie de piéger quelques poissons.

En guise d'hameçon (d'où la proposition du terme français *hameçonnage*), un courriel est lancé sur l'Internet jusqu'au moment où un internaute, moins soupçonneux qu'un autre, s'y accroche.

Historique : d'où ça provient ?

Le terme *phishing* s'inspire du terme *phreaking*, qui est un diminutif de *phone* et *freak*. *Originellement*, le phreaking était un type d'arnaque utilisé afin de profiter de services téléphoniques

Cet article explique ...

- Ce qu'est l'hameçonnage, les scénarios d'attaques possibles, les faiblesses exploitées dans ce type d'attaque ainsi que les techniques les plus fréquemment utilisées. De plus, il mentionne certains des mécanismes de prévention et de défense présents et futurs pour enfin conclure avec des statistiques sur les attaques de ce genre.

Ce qu'il faut savoir ...

- Le lecteur doit être un utilisateur d'Internet ayant des connaissances de base envers son fonctionnement et ses principes. De plus, le lecteur doit avoir un minimum d'intérêt vis-à-vis la sécurité de l'information sur Internet ainsi qu'aux technologies de sécurité qui s'y rattachent.

gratuits surtout présents à l'époque des appareils analogiques (années '70).

Le terme phishing aurait été inventé par les pirates informatiques qui essayaient de voler des comptes AOL. Il serait construit sur l'expression anglaise *password harvesting fishing*, soit *pêche aux mots de passe*. Un attaquant se faisait passer pour un membre de l'équipe AOL et envoyait un message instantané à une victime potentielle. Ce message demandait à la victime d'indiquer son mot de passe afin de vérifier son compte AOL ou confirmer ses informations bancaires. Après que la victime ait révélé son mot de passe, l'attaquant pouvait accéder au compte et l'utiliser à des fins malveillantes, comme pour effectuer des envois de pourriel, c'est-à-dire des communications massives, sous forme de courriels électroniques, non sollicités par les destinataires servant à des fins publicitaires ou malhonnêtes.

Les criminels informatiques utilisent généralement l'hameçonnage pour voler de l'argent. Les cibles les plus populaires sont les services bancaires et de cartes de crédit en ligne ainsi que les sites de ventes aux enchères tels que eBay. Les adeptes de l'hameçonnage envoient habituellement des courriels au plus grand nombre d'utilisateurs possibles afin de rejoindre le plus grand nombre de victimes potentielles.

Typiquement, les messages ainsi envoyés semblent émaner d'une société digne de confiance et sont formulés de manière à ne pas alarmer le destinataire afin qu'il effectue une action en conséquence.

Une approche souvent utilisée est d'indiquer à la victime que son compte a été désactivé due à un problème et que la réactivation ne sera possible que lorsque l'usager suivra certaines instructions.

Le message fournit alors un lien qui dirige l'utilisateur vers une page Web qui est une copie conforme du vrai site de la société de confiance. Arrivé sur cette page trompeuse, l'utilisateur est invité à entrer des informations confidentielles qui sont alors capturées et enregistrées par le criminel.

L'hameçonnage est donc une forme de vol d'identité électronique, aussi appelée usurpation d'identité, qui emploie l'ingénierie sociale ainsi que le *pharming*.

L'ingénierie sociale est la discipline consistant à obtenir de l'information personnelle et confidentielle en exploitant la confiance, mais parfois aussi l'ignorance ou la crédulité de tierces personnes. Il s'agira pour les personnes usant de ces méthodes d'exploiter le facteur humain, qui peut être considéré comme le maillon faible de tout système de sécurité.

Ce terme est surtout utilisé en jargon informatique pour définir les méthodes des pirates informatiques qui usent d'ingénierie sociale pour obtenir respectivement un accès à un système informatique ou pour satisfaire leur curiosité.

Le *pharming* de son côté est une technique de piratage informatique exploitant des vulnérabilités DNS pour récupérer les données d'une victime. Ce type d'hameçonnage permet de voler des informations après avoir attiré la victime sur un site web maquillé même si le nom de domaine est correctement saisi ou affiché.

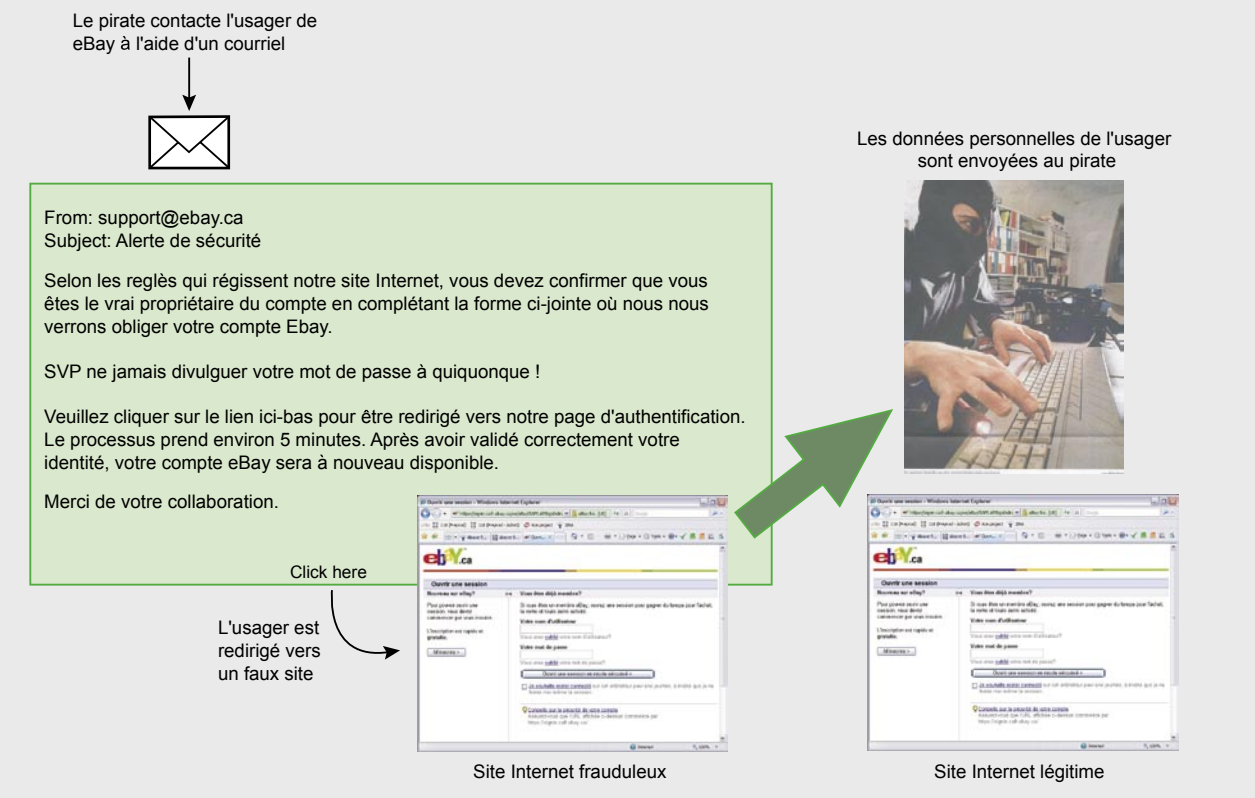

Figure 1. *Schéma d'une attaque typique*

Ainsi, l'adresse d'une banque, par exemple, ne pointera plus vers l'adresse IP du serveur de ladite banque, mais plutôt vers un serveur frauduleux.

Certaines techniques d'hameçonnage plus récentes, consistent en des logiciels malveillants, ou maliciels, qui sont développés dans le but de nuire à des systèmes informatiques. Dans le cas d'une attaque d'hameçonnage, les logiciels malveillants peuvent varier d'un capteur de touches aux corrupteurs de données stockées.

Tandis qu'un capteur de touches est utilisé pour intercepter les touches frappées à l'aide du clavier et ainsi capter des mots de passe et autres informations personnelles, les corrupteurs de données de leur côté servent plutôt à corrompre les données des infrastructures de navigation afin de réorienter de façon automatique les utilisateurs vers des sites Web frauduleux à l'aide d'aiguilleurs (*proxy*) contrôlés par des pirates informatiques.

Comment ça fonctionne, pourquoi et pour qui ?

Les premières attaques utilisant l'hameçonnage visaient essentiell-ement à gagner l'accès aux comptes AOL pour obtenir des renseignements de cartes de crédit dans le but de commettre des fraudes. Les messages hameçon exploitaient la naïveté des usagers qui croyaient recevoir un message automatisé de l'entreprise de messagerie électronique.

Comme démontré dans la Figure 1, on demande à l'utilisateur de cliquer sur le lien pour être redirigé vers un site de la compagnie afin d'y entrer ses informations personnelles, nom d'utilisateur et mot de passe.

Une autre méthode qui était très répandue consistait à envoyer un message faisant croire à une corruption de bases de données ou à une défaillance au niveau du matériel qu'utilise la compagnie fraudée. Cette défaillance avait supposément engendré une erreur et une corruption dans les données personnelles ou confidentielles des utilisateurs contactés.

Ces utilisateurs voyant un message apparemment officiel se résignaient facilement à la volonté des pirates puisque le message en question avait un ton sérieux et qu'il semblait offrir de l'assistance. De plus, les utilisateurs étaient priés de répondre rapidement afin d'éviter un problème sérieux, comme l'annulation de leur compte par exemple.

Les données de cette époque pas si lointaine mentionnent que les pirates exerçaient leurs actes de fraude seuls ou en petits groupes peu sophistiqués. D'autres rubriques et documents de littérature de cette époque mentionnent aussi que les premiers pirates utilisant l'hameçonnage étaient des adolescents qui désiraient récupérer de l'information de comptes personnels afin de causer du vandalisme électronique et pour faire des appels interurbains, sans pour autant faire partie d'organisations criminelles.

Aujourd'hui, la stratégie préférée des pirates utilisant l'hameçonnage est d'envoyer des courriels truqués (courriels semblant provenir de compagnies de confiance) au plus grand nombre d'utilisateurs possible, en espérant que les utilisateurs qui ont déjà confiance à cesdites compagnies agiront rapidement et sans réfléchir. L'attaquant espère donc que les victimes seront fourvoyées et enverront les données sensibles au site illégitime, qui est une réplique exacte de celui de la compagnie digne de confiance mais qui est gouverné par les pirates eux-mêmes.

Des exemples de compagnies de confiance que les pirates utilisent sont les banques populaires, les compagnies de cartes de crédit ainsi que des marchands électroniques bien connus sur Internet. Les courriels hameçons affichent un très haut degré de ressemblance avec les originaux, ce qui ne fait qu'accroître les chances de piéger les utilisateurs ciblés. Les attaques d'hameçonnage dépendent généralement de certains outils et techniques de base afin de tromper les utilisateurs crédules.

La structure de base requise pour commettre des attaques d'hame-çonnage peut être, dans le plus simple des cas, une copie du code HTML du site d'une compagnie que les pirates veulent utiliser comme appât, vers un site Web compromis; copie conforme de celle de la compagnie. De plus, le serveur qui est l'hôte du site compromis doit avoir un script, ou un processus, dont le but est de capturer et d'enregistrer les données que les utilisateurs crédules envoient. Dans d'autres cas, les pirates peuvent aussi utiliser des sites compromis plus complexes avec de la redirection de trafic.

Cependant, le but est le même, créer une fausse présence sur Internet d'une compagnie digne de confiance avec une assistance automatisée qui capture les données des utilisateurs et qui les met à la disposition de l'attaquant. De nos jours, il est très facile, à l'aide d'outils d'édition de code HTML, de créer un site Web qui imite le site d'une organisation, société ou d'une compagnie légitime. Les sites Web, les serveurs généraux et autres ordinateurs qui affichent un faible niveau de sécurité et qui peuvent être retracés facilement sur Internet sont ceux qui sont choisis dans la majorité des cas par les pirates.

De plus, les attaquants emploient souvent des balayeurs Internet afin de trouver des sites hôtes vulnérables dans des sections entières d'Internet. Une fois compromis, même les ordinateurs personnels situés dans des résidences privées peuvent être utilisés de façon très efficace comme hôte pour les sites hameçons, mais les sites corporatifs bien connus ain-

Figure 2. *Des internautes peu méfiants se voient voler leur identité …*

si que les institutions académiques sont les plus souvent attaqués. Les pirates se soucient rarement de l'endroit où se situe l'ordinateur à piéger puisqu'ils incluent, dans leur projet d'hameçonnage, tous les ordinateurs ayant rapporté une vulnérabilité lors du balayage d'Internet.

Lorsque le pirate a établi un site Web illégitime de façon convaincante et réaliste, son principal problème est désormais de trouver la meilleure façon de détourner les utilisateurs du site réel vers l'illégitime. À moins que le pirate ait la capacité d'altérer les données DNS d'un site Web légitime (technique communément appelée empoisonnement DNS) ou de rediriger le trafic réseau du site légitime, le pirate doit alors se fier sur un appât relativement fiable de façon à attirer les utilisateurs malchanceux vers le site illégitime. Meilleur est l'appât et plus le nombre d'utilisateurs visés est grand, plus il y a de chance pour qu'un grand nombre de ceux-ci accèdent au site frauduleux et fournissent leurs données personnelles. Les pirates, qui contrefont l'image d'une compagnie en particulier (comme une banque ou un marchand connu) n'ont souvent aucune information sur qui sont les clients faisant affaire avec elle et donc, qui pourrait être plus réceptifs à un appât particulier. Même si les pirates pouvaient envoyer des messages présentant des hyperliens pointant au site illégitime dans des sessions de clavardage et autres forums électroniques reliés à la compagnie visée, celle-ci se rendrait compte ou serait avisée très rapidement du lien fautif et pourrait l'effacer ou le désactiver avant qu'il n'y ait un trop grand nombre de victimes.

De plus, il y a de fortes chances pour que la compagnie visée prenne des mesures drastiques afin de mettre fin au site illégitime à l'aide de lois et des agences du maintien de l'ordre qui les régit. Les pirates n'ont alors d'autres choix que d'utiliser une façon de rejoindre le plus de victimes potentielles ayant un très faible taux de risque via l'envoi massif de courriels contrefaits. Les pirates utilisant l'hameçonnage possèdent des bases de données contenant plusieurs millions d'adresses de courriel valides et actives.

La technique d'envoi massif est souvent préconisée par ces pirates pour envoyer des courriels au plus grand nombre de destinataires possibles avec un taux de risque pratiquement nul. Un utilisateur recevant un courriel à l'effigie de sa banque utilisera malheureusement les hyperliens qui lui sont offerts vers le site pour y entrer des données personnelles. Les chances de réussite dans ce dernier cas sont en effet plus grandes que si le courriel n'affiche rien de connu et mène vers un site affichant une image avec lequel l'utilisateur n'est pas familier.

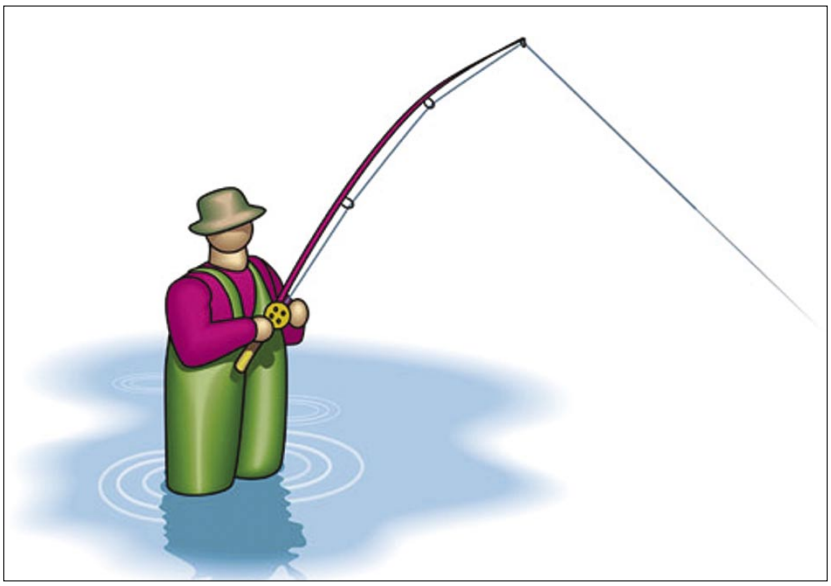

Figure 3. *Les cyber-pirates s'adapteront constamment pour trouver les techniques les plus efficaces*

Afin d'améliorer les chances que les utilisateurs puissent croire que le courriel envoyé est légitime, les pirates peuvent utiliser un nombre de techniques connexes afin d'améliorer la qualité de leur arnaque :

- en utilisant une adresse IP au lieu d'un nom de domaine dans les hyperliens qui dirigent les utilisateurs vers le site illégitime. Plusieurs victimes innocentes ne vérifieront pas (ou ne savent comment vérifier) qu'une adresse IP est enregistrée et assignée à la compagnie visée et dont le site illégitime dit représenter,
- en enregistrant des noms de domaines DNS similaires ou s'approchant de très près de celui du nom utilisé par la compagnie visée en espérant que les utilisateurs se méprendront entre le vrai nom de domaine de la compagnie de celle vers laquelle ils se font malicieusement diriger,
- en encapsulant les hyperliens dans du code HTML dont consiste le courriel contrefait afin que le navigateur Internet des utilisateurs puisse faire la plupart des connexions HTTP au vrai site Web de la compagnie avec un minimum de connections au site Web illégitime. Si dans ce cas le navigateur de l'utilisateur supporte l'interprétation automatique du contenu du courriel, l'utilisateur en question sera alors contraint d'être dirigé vers le site Web illégitime dès l'ouverture du courriel,
- en encodant ou en rendant la fausse adresse URL obscure. Dépendamment de la méthode utilisée, plusieurs utilisateurs ne se rendront pas compte ou ne comprendront tout simplement pas que les hyperliens ont été altérés et assumeront alors qu'ils sont légitimes. Une variante de cette technique est l'utilisation d'hyperliens dans le format Unicode, qui

se voit dans le navigateur comme l'adresse ori-ginale du site de la compagnie visée, mais qui dirige les utilisateurs vers le site Web illégitime à l'aide d'une tout autre adresse,

- en tentant d'exploiter une faiblesse quelconque dans le navigateur Internet de l'utilisateur afin de masquer la vraie nature du contenu du message. Le navigateur de Microsoft (Internet Explorer) ainsi que les applications d'Outlook ont été particulièrement vulnérables à cette technique, nous y reviendrons plus tard dans cet article,
- en configurant le site Web illégitime pour capturer et enregistrer les données entrées par l'utilisateur puis en redirigeant celui-ci, subtilement, vers le vrai site Web. Cette action occasionnera sûrement un message d'erreur (mot de passe non valide, S. V. P. essayer de nouveau) ou être totalement transparente. Dans ces deux cas, le pirate aura obtenu ce qu'il voulait,
- en configurant le site Web illégitime pour qu'il puisse agir en tant que proxy (ou d'aiguilleur) pour le vrai site Web, qui pourra donc capturer et enregistrer les données sensibles des utilisateurs piégés qui ne sont pas chiffrés (utilisant SSL), ou parfois même en les décryptant en utilisant un certificat SSL valide pour le domaine illégitime,
- en redirigeant les victimes vers un site illégitime en se servant avant tout de logiciels malveillants qui installent des objets d'aide malveillants au navigateur Internet directement sur l'ordinateur personnel des victimes. Les objets d'aide malveillants sont des ajouts type *plugiciel* aux navigateurs Internet qui permettent certains changements personnalisés qui, si bien utilisés par les pirates, pourront faire en sorte de rediriger les utilisateurs de façon parfaitement transparente vers les sites illégitimes,
- en utilisant des logiciels malveillants préalablement installés sur les ordinateurs des victimes dans le but de manipuler le fichier hôte qui est utilisé afin de maintenir les liens entre les noms de domaine et les adresses IP associées. En insérant une fausse entrée DNS dans le fichier hôte d'une victime, la victime sera automatiquement redirigée vers le site illégitime, mais verra l'adresse de la compagnie légitime alors qu'il navigue sur le site illégitime.

Pourquoi et pour qui ça fonctionne ?

La motivation première qui fait en sorte que l'hameçonnage existe depuis un certain temps est sans contredit la fraude, c'est-à-dire le gain d'argent pour les pirates en utilisant les techniques les plus simples et les moins risquées pour eux

Avec la croissance exponentielle des transactions financières qui se déroulent sur Internet, l'hameçonnage est ainsi devenu une option lucrative pour les pirates. De nos jours, presque toutes les banques et compagnies de crédit offrent des services en ligne. Les clients de ces banques en ligne peuvent devenir des proies faciles pour les pirates utilisant l'hameçonnage comme arme de prédilection. En utilisant de l'information volée, les pirates informatiques peuvent exercer un nombre d'activités criminelles telles que :

- exécuter des transactions non autorisées en utilisant des numéros de carte de crédit ou de débit,
- en accédant à des applications bancaires et/ou financières en utilisant un nom d'utilisateur et un mot de passe volé, les pirates peuvent avoir accès aux détails financiers des utilisateurs et effectuer des transactions financières au dépend des victimes,
- vendre les données sensibles des victimes tels numéros de téléphone, adresses civiques et numéros de compte à d'autres groupes de pirates pour différentes activités malicieuses,
- causer un refus ou une suspension de service pour les utilisateurs légitimes en modifiant les mots de passe et autres détails des fiches de contacts,
- détruire la confiance qu'a une victime face à une compagnie quelconque afin de salir la réputation de cette dernière.

Moyens de détection et de prévention

La vérification de l'adresse Web dans la barre d'adresse du navigateur Web peut ne pas être suffisante pour détecter la supercherie, car certains navigateurs n'empêchent pas l'adresse affichée à cet endroit d'être contrefaite. Il est toutefois possible

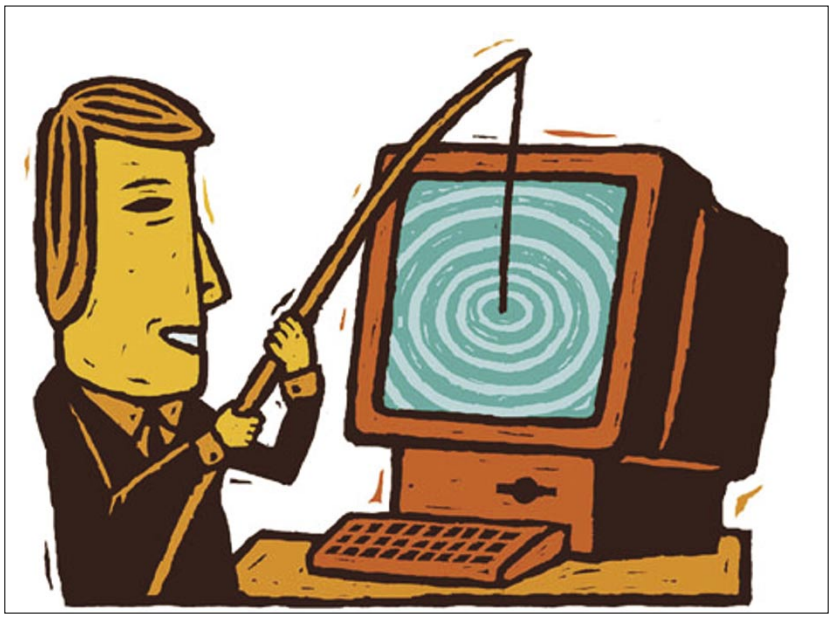

Figure 4. *Vos clients morderont-ils à l'hameçon ?*

d'utiliser la boîte de dialogue *propriétés de la page* fournie par le navigateur pour découvrir la véritable adresse de la page illégitime.

Une personne contactée au sujet d'un compte devant être vérifié doit chercher à régler le problème directement avec la société concernée ou se rendre sur le site Web en tapant manuellement l'adresse dans son navigateur. Il est important de savoir que les sociétés bancaires n'utilisent jamais le courriel pour corriger un problème de sécurité avec leurs clients. En règle générale, il est recommandé de faire suivre le message suspect à *usurpation* (par exemple, si l'hameçonnage concerne *societe.com*, ce sera *usurpation@societe.com*), ce qui permettra à la société de faire une enquête.

Il faut être particulièrement vigilant lorsque l'on rencontre une adresse contenant le symbole @, par exemple *http://www.mabanque.com @members.onsite.com/.* Ce genre d'adresse tentera de connecter l'internaute en tant qu'utilisateur *www.mabanque.com* sur le serveur *members.onsite.com*. Il y a de fortes chances que cela se réalise même si l'utilisateur indiqué n'existe pas réellement sur le serveur, mais par cette méthode la première partie de l'adresse semble être tout à fait innocente.

Des navigateurs récents, tels que Firefox et Internet Explorer 7, possèdent un système permettant d'avertir l'utilisateur du danger et de lui demander s'il veut vraiment naviguer sur de telles adresses douteuses. Netscape 8 intègre quant à lui des technologies permettant de tenir à jour une liste noire de sites dangereux de ce type.

Les filtres anti-pourriels aident aussi à protéger l'utilisateur contre des criminels informatiques en réduisant le nombre de courriels que les utilisateurs reçoivent et qui peuvent être de l'hameçonnage.

Le logiciel client de messagerie Mozilla Thunderbird comporte un filtre bayésien très performant (filtre anti-pourriels auto-adaptatif). Tel que mentionné plus tôt dans cet article, les fraudes concernant les banques en ligne visent à obtenir l'identifiant (nom d'utilisateur) et le mot de passe du titulaire d'un compte. Il est alors possible pour le fraudeur de se connecter sur le site Web de la banque et d'effectuer des virements de fonds vers son propre compte. Pour parer à ce type de fraude, la plupart des sites bancaires en ligne n'autorisent plus l'internaute à saisir lui-même le compte destinataire du virement. En règle générale, il faut téléphoner à la banque afin d'utiliser un service qui reste le seul moyen de saisir le compte destinataire dans une liste de comptes. La conversation téléphonique est souvent enregistrée et peut alors servir de preuve. D'autres banques utilisent une identification renforcée, qui verrouille l'accès aux virements si l'utilisateur n'indique pas la bonne clé à quatre chiffres demandée aléatoirement, parmi les soixante-quatre qu'il possède.

Si la clé est la bonne, l'internaute peut effectuer des virements en ligne. Due à la nature relativement complexe de plusieurs applications Web de transactions financières et autres transactions électroniques en ligne, qui souvent emploient des cadres (frames) et sous-cadres HTML ou autres structures de pagination Web complexes, il pourrait s'avérer être difficile pour un utilisateur quelconque de déterminer si le contenu et même l'adresse d'un de ces cadres est légitime ou non. L'utilisation d'une combinaison des techniques énumérées préalablement dans cet article peut faire en sorte de masquer la source légitime de la page (et de ses cadres HTML) visionnée par l'utilisateur, qui trompe ce dernier et l'incite à entrer ses informations personnelles, faisant de lui une autre victime d'une attaque d'hameçonnage.

Pourquoi tant de poissons mordent-ils à l'hameçon ?

Essayons à présent de creuser un peu plus afin de découvrir ce qui fait qu'une attaque d'hameçonnage soit souvent malheureusement couronnée de succès…

L'utilisateur n'est pas familier avec l'Internet et ses pièges

Le fait que les utilisateurs de l'Internet soient peu familiers avec ce type d'attaque est probablement le plus gros facteur de succès de l'hameçonnage. Puisque les utilisateurs ne peuvent différencier le site Web ou courriel légitime des contrefaits, ceux-ci deviennent des victimes en divulguant leurs informations personnelles.

Banque d'adresses de courriels facilement accessible

Un autre facteur est la facilité avec laquelle les pirates peuvent avoir accès aux adresses de courriel. Les pirates d'aujourd'hui possèdent d'immenses banques de données contenant plusieurs millions d'adresses de courriel. Ceci leur permet d'être en mesure de contacter le plus de proies possible. Ces adresses de courriel peuvent aussi bien appartenir à des utilisateurs quel conques qu'à des utilisateurs de banques et autres firmes de crédits en ligne.

Une technologie maintenant facile à utiliser

La facilité d'utilisation de la technologie offerte aux pirates contribue aussi au bon succès de l'hameçonnage. En utilisant la technologie qu'offre l'Internet et le Web, les pirates peuvent ainsi construire, configurer et déployer rapidement de sites illégitimes. Si on compare avec la création de virus, de vers et autres techniques d'exploitation, l'hameçonnage est relativement simple.

Vulnérabilités dans les protocoles de courriels

L'existence de faiblesses et de vulnérabilités dans les protocoles de courriels qu'utilisent les systèmes de courriers électroniques aide d'autant plus les pirates. Par exemple, un pirate peut très facilement modifier l'adresse d'origine du courriel (*From*) pour paraître légitime. De plus, il existe de simples fonctionnalités rendues

disponibles par les langages de programmation Web qui permettent de tromper les utilisateurs. Si on considère le code HTML suivant :

```
<a href=http://www.site-illegitime.com>
   https://www. site-legitime. com
</a>
```

Ce code est utilisé pour afficher un hyperlien dans une page Web ou dans un courriel par exemple. L'utilisateur voit le lien comme étant *http://www.site-legitime.com* mais lorsqu'il clique dessus, il est dirigé vers la page Web dont l'adresse est *http://www. site-illegitime.com*.

En plus de ce cas spécifique, plusieurs autres techniques avancées peuvent être utilisées afin de rendre obscure la destination finale qui est affichée dans la barre d'adresse du navigateur.

Vulnérabilités dans les navigateurs browsers

L'une de ces techniques consiste à exploiter certaines vulnérabilités que possèdent les navigateurs Internet qui aident ainsi à tromper les utilisateurs. Un exemple de ce phénomène était la vulnérabilité reliée à la fonctionnalité de la barre d'adresse d'Internet Explorer lorsqu'elle analysait le contenu qui lui était passé en paramètre.

Cette vulnérabilité permettait à l'attaquant de modifier l'adresse de la barre d'adresse du navigateur pendant que la page du site Web illégitime était ouverte et accédé. Considérons l'adresse *http://www.site-legitime.com%01%00@www.site-illegitime.com*.

Lorsque l'adresse était visitée, le résultat était que la barre d'adresse du navigateur affichait seulement la partie *http://www.site-legitime.com* alors que l'utilisateur était dirigé vers *http:// www.site-illegitime.com*.

Cette vulnérabilité était causée par une mauvaise interprétation des caractères spéciaux tels que *%01* et *%00*. La solution était alors d'appliquer *un patch* que fournissait le vendeur, dans le cas présent Microsoft, qui mettait à jour le navigateur et enraillait complètement la vulnérabilité.

L'anonymat qu'offre le Web et l'Internet en général, dans certaines situations, fait en sorte de rendre encore plus difficile la tâche de localiser les attaquants. En effet, les pirates peuvent très rapidement lancer leurs attaques et effacer toutes traces de leurs actes de façon tout aussi rapide.

Les logiciels d'anti-pourriels et de filtration de contenu ne sont pas très efficaces pour détecter et arrêter les courriels hameçons. De plus, la plupart des navigateurs Internet n'offrent pas de mesures de détection ou autres outils anti-hameçonnage efficaces. Toutes ces raisons regroupées font en sorte de contribuer à la grande croissance dans le monde des attaques utilisant l'hameçonnage.

Ce que les firmes peuvent faire pour aider à contrer l'hameçonnage

Un adage bien connu sur la sécurité dit : *La bonne gestion de la sécurité est directement dépendante des gens, du processus et de la technologie qui la gouverne.*

Cette approche est aussi vraie en ce qui concerne la défense contre l'hameçonnage. Même si les solutions contre l'hameçonnage sont encore au stage de développement, plusieurs combinaisons de mécanismes de défense peuvent être jumelées pour prévenir et dissuader l'hameçonnage. La section suivante décrit certains de ces mécanismes qui peuvent être implémentés par les banques ou autres organisations pour se protéger contre l'hameçonnage.

Il existe une variété de techniques de contrôle qui aident à prévenir les attaques que les firmes, les banques et autres organisations ou institutions cibles devraient mettre en pratique pour contrer l'hameçonnage lors de la construction de leurs applications Web. Un simple nom d'utilisateur et un mot de passe ne sont pas suffisants pour les sites Web offrant des services aussi cruciaux que celui du domaine de la finance en ligne. En effet, le processus d'authentification devrait être agrémenté en introduisant des certificats sécurisés ou des clés matérielles sécurisées (*hardware tokens*).

Les clés matérielles (ou jetons) sécurisées introduisent un deuxième niveau d'authentification dans les applications Web. Ces dispositifs de clés matérielles sont généralement de deux types : celles qui utilisent la méthode du challenge – réponse; et ceux qui utilisent le dispositif *SecureID* de RSA. Dans le cas des dispositifs qui utilisent la méthode du challenge – réponse, l'application Web envoie un challenge lorsque l'utilisateur se connecte à l'aide de son nom d'utilisateur et son mot de passe. Le challenge qui est en fait un nombre généré au hasard est envoyé dans le dispositif de sécurité afin de générer un nouveau nombre au hasard, qui est la réponse.

Cette réponse est ainsi envoyée à l'application pour une seconde authentification. Puisque la réponse générée est toujours différente et dépendante du dispositif, les pirates utilisant l'hameçonnage ne peuvent avoir accès au site visé, même s'il a réussi au préalable à obtenir le nom d'utilisateur et son mot de passe. Dans le cas du dispositif *SecureID* de RSA, le serveur d'authentification est parfaitement synchronisé avec le dispositif de sécurité où un code de six chiffres affiché sur ce dernier est modifié toutes les trente ou soixante secondes. Il est alors possible de jumeler ce code avec un mot de passe qui devient alors impossible à déchiffrer puisque le délai de rotation des codes est trop court. Dans les deux cas, le pirate doit nécessairement avoir en main le dispositif de l'utilisateur visé.

Les certificats clients peuvent eux aussi introduire un processus d'authentification plus fort dans les applications Web. Une option est d'utiliser des certificats clients à travers des cartes intelligentes (*smart card*) utilisant les capacités cryptographiques d'infrastructures à clé publique. Les cartes intelligentes introduisent une

plateforme mobile et sécuritaire pour l'authentification. Dans les applications Web qui se servent de cartes intelligentes, seulement les utilisateurs qui ont les bonnes cartes peuvent avoir accès à l'application Web. Puisque le pirate n'aurait pas en sa possession une carte intelligente valide, celui-ci ne pourrait donc pas avoir accès à l'application Web, même si encore une fois, il a préalablement réussi à obtenir d'autres informations tels le nom d'utilisateur, le mot de passe ou le numéro de compte de l'utilisateur visé. Le problème avec les cartes intelligentes cependant est l'infrastructure qui doit être mise en place afin de supporter cette solution. Si l'on compare avec les dispositifs matériels sécurisés, l'infrastructure requise pour traiter avec des cartes intelligentes est beaucoup plus rigoureuse que celle requise pour traiter avec des dispositifs matériels sécurisés.

Comme vous pouvez le constater, l'utilisation de dispositifs matériels sécurisés ou de certificats clients transmit par cartes intelligentes présente bon nombre de problèmes et de changements qui doivent être apportés aux applications Web existantes. C'est pourquoi l'utilisation de ces derniers est propice lors du développement et la création de nouvelles applications Web.

Il existe cependant une autre solution simple qui permet de réduire considérablement le risque d'hameçonnage. La solution qui peut être implémentée est celle où l'on fait en sorte de rendre la tâche d'usurpation d'identité d'un site plus difficile, voir même impossible dans certains cas. Une façon de réaliser ceci est de personnaliser l'application Web pour les utilisateurs. En effet, l'application Web peut utiliser deux pages lors de l'authentification d'un utilisateur. La première page peut demander à l'utilisateur d'entrer seulement le nom de l'utilisateur. Lorsque l'application reçoit un nom valide d'utilisateur, celle-ci afficherait alors une seconde page qui serait personnalisée et dans laquelle l'utilisateur entrerait son mot de passe.

Cette seconde page pourrait être personnalisée selon une phrase que l'utilisateur a préalablement choisit lors de son inscription ou grâce à une image ou autre moyen pourvu qu'il soit personnalisé. Il serait alors extrêmement difficile pour un site illégitime, utilisé pour l'hameçonnage, de fournir la deuxième page avec succès. La personnalisation de pages Web peut aussi être accomplie en utilisant d'autres moyens. Des biscuits (*cookie*) persistants du côté de l'utilisateur (stockés sur son ordinateur) peuvent être utilisés par l'application Web afin de présenter une page personnalisée d'authentification.

En effet, lorsque l'utilisateur se connecte pour la toute première fois sur le site, l'application Web pourrait enregistrer un biscuit persistant sur l'ordinateur de l'utilisateur contenant une phrase clé non confidentielle, comme le nom de cet utilisateur par exemple. Lorsque l'utilisateur retournera sur le site afin d'être authentifié à nouveau, l'application Web pourra alors souhaiter la bienvenue à l'utilisateur en utilisant son nom tel que stocké dans le biscuit avant qu'il entre ses informations personnelles.

Un site illégitime utilisant l'hameçonnage ne pourrait en aucun cas lire le contenu de ce biscuit puisqu'il est limité à son propre domaine. L'utilisateur qui naviguerait sur le site illégitime ne verrait pas le mot de bienvenue comme l'application Web légitime afficherait et serait ainsi en mesure de conclure qu'il n'est pas sur le bon site ou du moins, permettre d'annuler sa visite. Encore une fois cependant, ces méthodes de personnalisation de pages n'auront de succès que si les utilisateurs restent constamment vigilants et alertes.

La majorité des attaques ayant du succès dépendent de la réaction et des réponses de la part des utilisateurs visés. Il doit donc y avoir certaines mesures de sécurité qui doivent être implémentées aussi du côté des utilisateurs. Bon nombre d'attaques peuvent être évitées si les utilisateurs sont alertes et en connaissances des menaces auxquels ils font face. Les banques et autres organisations ciblées devraient mieux informer leur clientèle et leurs employés sur les pratiques de sécurité de base.

En effet, la mise à disposition d'information sur les façons de détecter les sites et courriels illégitimes devrait être établie par les banques et autres organisations qui sont visées par l'hameçonnage. Des guides de base simples devraient être distribués aux utilisateurs afin de les informer sur la procédure qui est suivie lorsqu'une banque contacte ses utilisateurs. Cette séance d'information devrait être présentée non seulement de façon périodique, mais aussi de façon sécuritaire et facilement comprise par tous les types d'utilisateurs, des incrédules aux crédules. Ces guides pourraient être offerts sous forme de documents remis aux utilisateurs lors de leur inscription. Ces guides pourraient aussi être affichés à même le site Web avant que les utilisateurs puissent s'y authentifier.

Bref, cette pratique servirait non seulement à informer les utilisateurs du site des méthodologies de sécurité encourue par les banques et autres organisations, mais aussi pour les informer à propos d'alertes concernant des attaques frauduleuses qui peuvent ou sont en train de survenir. Voici les propos sur lesquels les banques, les organisations et autres institutions devraient informer leurs utilisateurs :

- la banque ou l'organisation ne demandera jamais aux utilisateurs de fournir leur nom d'utilisateur, leur mot de passe, leur numéro de carte de crédit, leur numéro de compte (etc.) par courriel,
- que les courriels envoyés aux utilisateurs, s'il y a, ne con-tiendraient j amais d'hyperlien et ne demanderait jamais d'entrer de l'information à l'aide d'un formulaire contenu dans le courriel,
- les courriels ne demanderaient jamais aux utilisateurs de télé-charger des logiciels provenant d'autres sites et ne leur demanderait jamais

d'aller visiter d'autres sites à part ceux d'organisations connexes bien connues,
- les utilisateurs devraient toujours accéder au site de la banque, par exemple, en tapant directement l'adresse du site dans la barre d'adresse du navigateur et de regarder pour les indications de sécurité affichées sur la page et/ou dans le navigateur,
- finalement, les utilisateurs devraient être suspicieux vis-à-vis les courriels contenant des requêtes urgentes de confirmation ou de modification d'entrée d'information personnelle.

De plus, les utilisateurs devraient être mis au courant des meilleures pratiques en matière de sécurité, incluant :

- mettre à jour régulièrement le navigateur Internet utilisé afin d'y appliquer les derniers correctifs,
- avoir un filtre anti-pourriels ainsi qu'un logiciel d'anti-virus installé et configuré correctement,
- utiliser un simple stoppeur de page pop-up pour arrêter l'exécution de code malicieux,
- et utiliser des outils de détection de logiciels malveillants (*maliciels*) pour détecter et effacer ce type de programmes nuisibles.

Finalement, l'utilisation de signatures numériques est une autre bonne solution pour différencier les courriels contrefaits des légitimes.

Les organisations, les banques et autres institutions devraient du mieux qu'elles le peuvent signer numériquement chacune des communications avec les utilisateurs via courriel et les informer sur la façon d'identifier une signature valide. La clé publique requise pour vérifier la signature de l'organisation ou l'institution concernée pourra alors être distribuée sous forme de CD-ROM lorsque requis.

Tendances et évolution

Quelques technologies futures pourront aider à ralentir la menace qu'impose l'hameçonnage. Un tel effort est conduit par le *Sender ID* Framework proposé par Microsoft.

Une autre approche est celle proposée par Cisco Systems qui s'appelle l'*Identified Internet Mail*. Dans les deux cas, ce qui est proposé est l'arrêt de courriels contrefaits avant même qu'ils ne rejoignent la boîte postale des destinataires. Le Sender *ID Framework* essaie de prévenir l'usurpation d'identité de domaines. Il vérifie les messages des courriels pour assurer qu'ils proviennent bel et bien des domaines desquels ils disent provenir. L'adresse IP d'origine du courriel est utilisée pour cette vérification. Le serveur qui reçoit le courriel contrefait peut alors valider et distribuer seulement ceux qui sont valides. L'approche que Cisco propose de son côté est un mécanisme basé sur l'authentification signée pour assurer la validité d'un courriel. En utilisant la méthode cryptographique à clé publique, le serveur de courriers électroniques qui envoie un courriel signe numériquement celui-ci et il est vérifié lors de la réception par le serveur sur le domaine le recevant.

Cette vérification peut autant se faire au niveau du domaine qu'au niveau de l'utilisateur. Une politique de sécurité peut être définie afin de savoir quoi faire dans le cas ou la vérification de l'authenticité d'un courriel échouerait.

Dans ce cas, les courriels ayant aucune ou une mauvaise signature numérique pourront être considérés comme étant de courriels contrefaits destinés à causer une attaque d'hameçonnage. Enfin, de nouveaux consortiums comme le FSTC (*Financial Services Technology Consortium*) et l'APWG (*Anti-Phishing Working Group*) travaillent actuellement à de nouvelles solutions. Ces groupes ont rassemblé leurs ressources afin de développer un modèle de travail qui pourra être utilisé par les banques et autres institutions financières pour détecter et contrer les attaques d'hameçonnage.

Pour conclure, quelques statistiques de L'APWG

L'APWG (*anti-phishing working group – http://www. antiphishing. org/*) est un groupe formé de professionnels en sécurité informatique qui se concentre exclusivement sur les crimes commis sur Internet provenant de l'hameçonnage et dont le but est d'enrailler ce genre d'attaque.

Ce groupe possède un système de traçage et d'enregistrement d'alertes causées par des attaques utilisant l'hameçonnage ainsi que des sites illégitimes dont les pirates se servent. Ils ont tout récemment amélioré leur système de traçage de rapport de courriels hameçons uniques en plus des sites utilisés afin de commettre des attaques d'hameçonnage. Nous entendons par *rapports de courriels hameçons uniques*, un courriel unique qui est envoyé à plusieurs utilisateurs cibles, qui les dirigent vers un site illégitime servant à l'hameçonnage. L'APWG compte chacun de ces rapports de courriels uniques comme ceux qui dans un mois donné possèdent la même ligne de sujet dans le courriel. L'APWG répertorie et compte le nombre de sites servant à des buts d'hameçonnage.

Ceci est maintenant déterminé à l'aide des adresses uniques des sites illégitimes identifiées. Finalement, l'APWG répertorie aussi les logiciels malveillants en calculant un hachage MD5. Selon l'APWG, le nombre de sites illégitimes servant à l'hameçonnage détectés par le groupe a augmenté à 55,643 en avril dernier, un bond majestueux par rapport au mois de mars qui affichait 35,000 sites illégitimes.

Cette augmentation drastique est le résultat de tactiques agressives d'hameçonnage par sous-domaine, où les attaquants regroupent un grand nombre d'adresses de sites illégitimes sous le même domaine. Cette tactique ressemble étrangement à la tactique utilisée vers la fin de 2006, où les pirates rassemblaient des milliers d'adresses sous le seul et même domaine.

En avril 2007, le groupe a enregistré une augmentation des marques et des compagnies attaquées à plus de 174 et il a aussi remarqué que de plus en plus de marques n'étant pas reliées

aux finances étaient attaquées, telles les compagnies de réseaux sociaux et les larges compagnies qui offrent des services de courriers électroniques.

Malgré ce fait, le groupe note que ce sont les services d'institutions financières qui sont le plus visés, ce qui représente plus de 92. 5% des attaques perpétrées et que les banques des États-Unis sont les plus visées.

Un grand nombre de banques européennes sont aussi visées puisque sept des vingt marques les plus visées sont européennes, alors qu'une seule des vingt marques attaquées appartient à une institution financière canadienne. Le groupe a aussi déterminé que 98. 83% des sites illégitimes redirigeaient le trafic vers un serveur Web qui écoute sur la porte logicielle HTTP 80 ou 8080.

Éventuellement, les filtres antipourriels et les autres méthodes de détection d'attaques basées sur l'hameçonnage vont s'améliorer. Le nombre et la qualité des courriels augumentera malheureusement au même rythme que les techniques de détection.

Cependant, même avec toutes les technologies disponibles, demeurer vigilant face aux messages que nous recevons et traitons semble être la solution la plus efficace contre l'hameçonnage présentement. ●

À propos de l'auteur

L'auteur a travaillé plus de 10 années au Centre de Sécurité des Télécommunications du gouvernement fédéral du Canada exclusivement dans le domaine de la sécurité informatique.

Il détient un baccalauréat universitaire de l'Université de Sherbrooke en Informatique. Il travaille actuellement chez Above Sécurité à la division de Montréal (province de Québec) dans un poste de recherche et de développement visant à améliorer sans cesse les produits et services offerts par cette compagnie.