FR

SAC 028
Rapport consultatif du SSAC sur l'usurpation d'identité des bureaux d'enregistrement lors d'attaques d'hameçonnage

REMARQUE SUR LES DOCUMENTS TRADUITS

La version originale du présent document est rédigée en anglais. Elle est disponible sur la page Web http://www.icann.org/committees/security/sac028.pdf. En cas de différence d'interprétation entre le présent document et le texte original, ce dernier prévaut.

Rapport consultatif du conseil consultatif
sur lasécurité et la stabilité
(SSAC, Security and Stability Advisory Committee)
de l'ICANN
Mai 2008

Introduction

Ce rapport consultatif décrit une forme d'attaque d'hameçonnage qui vise les bureaux d'enregistrement de noms de domaine. Un pirate usurpe l'identité d'un bureau d'enregistrement de noms de domaine et envoie à un client de ce bureau (un registrant) un message attendu ou prévisible au sujet d'un nom de domaine. Il peut s'agir, par exemple, d'un avis d'expiration de l'enregistrement d'un nom de domaine, d'un e-mail promotionnel, d'un avis informant le registrant d'un problème de gestion de son compte ou, plus généralement, de tout message qui requiert l'attention immédiate d'un client. Cependant, ce message est un faux : l'hameçonneur crée un site Web frauduleux, similaire à celui du bureau d'enregistrement, pour inciter le client à accéder à son compte de gestion du domaine concerné et à révéler involontairement ses informations d'identification à l'hameçonneur. Ce dernier utilise les informations d'identification du client ainsi obtenues pour accéder au portefeuille de noms de domaine du client, modifier les informations DNS des noms de domaine de ce compte et utiliser les domaines pour lancer d'autres attaques.

Dans ce rapport consultatif, le SSAC décrit les formes génériques de ce type d'attaque. Les types et formats d'informations pris en compte sont ceux inclus dans les messages électroniques légitimes que divers bureaux d'enregistrement envoient à leurs clients. Il est question de la manière dont les hameçonneurs manipulent ces types et formats d'informations afin de créer des messages frauduleux destinés à inciter les clients des bureaux d'enregistrement, par *ingénierie sociale*[1], à consulter des sites Web usurpant l'identité de ces bureaux. Les pirates conçoivent ces sites Web usurpés dans le but d'inciter les clients à divulguer par erreur les noms et les informations d'identification de leurs comptes de gestion de domaine. Ce rapport aborde certaines des pratiques actuellement recommandées pour limiter ou prévenir les attaques d'hameçonnage envers des cibles courantes, telles que les institutions financières et les grandes entreprises. Il suggère aux bureaux d'enregistrement des mesures à prendre pour que leurs communications avec les registrants soient moins susceptibles de faire l'objet d'attaques d'hameçonnage, et pour que les registrants puissent détecter et éviter cette forme d'hameçonnage.

[1] Voir « Why Phishing Works », http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, pour plus d'informations sur l'ingénierie sociale.

Contexte : fonctionnement d'une attaque

Les hameçonneurs utilisent divers types de messages électroniques que marchands ou établissements financiers envoient à leurs clients[2]. Les bureaux d'enregistrement utilisent également le courrier électronique pour envoyer de nombreux messages relatifs à l'enregistrement des noms de domaine, y compris :

- des avis de renouvellement de noms de domaine ;
- des confirmations de noms de domaine ;
- des confirmations de demandes d'enregistrement ;
- des confirmations de modification des informations d'un domaine ;
- des rappels relatifs à l'exactitude des données du WHOIS ;
- des avis d'expiration ou d'annulation de noms de domaine ;
- des promotions ou des réclames pour des services et fonctionnalités (nouveautés).

Les hameçonneurs profitent du fait que les bureaux d'enregistrement utilisent uniquement l'e-mail pour leurs communications. En usurpant l'identité d'un bureau d'enregistrement lors d'une attaque d'hameçonnage, le pirate est capable d'attirer le client d'un bureau d'enregistrement vers une copie frauduleuse de la page de connexion du client, où ce dernier peut révéler involontairement ses informations d'identification au pirate. Ces informations permettent à l'hameçonneur d'accéder de manière non autorisée à un compte de gestion de noms de domaine. Le compte contient diverses informations de valeur pour le pirate :

- les enregistrements de domaines du client, qui peuvent être modifiés à des fins malveillantes (voir le panorama des risques) ;
- les traces (potentielles), dans les fichiers du bureau d'enregistrement, de l'utilisation de cartes de crédit ou d'autres moyens de paiement, qui pourraient être utilisées pour acquérir des domaines supplémentaires pouvant ensuite être exploités à des fins malveillantes.

Les hameçonneurs collectent les informations de sources diverses pour perpétrer une attaque d'usurpation d'identité de bureau d'enregistrement. Ils copient des pages, des images, des logos et des fichiers nécessaires à la production d'une copie frauduleuse mais crédible de la page de connexion du bureau d'enregistrement à partir du site Web « authentique » du bureau. Ces informations sont hébergées sur un serveur Web géré par les pirates et sont utilisées pour imiter la page de connexion du bureau d'enregistrement. L'hameçonneur utilise également des informations glanées dans les messages courants envoyés par le bureau d'enregistrement à ses clients afin de « personnaliser » le message qu'il inclut dans l'e-mail d'hameçonnage. Pour connaître ces messages, il suffit de devenir l'un des registrants du bureau d'enregistrement visé. Le pirate utilise les informations du WHOIS pour personnaliser davantage ses messages d'hameçonnage ; surtout, il est capable d'utiliser les informations du WHOIS pour dresser une liste de destinataires qui sont des registrants du bureau d'enregistrement visé.

[2] Des exemples d'hameçonnage et de scams peuvent être consultés dans les archives de l'Anti-Phishing Working Group (http://www.apwg.org/phishing_archive/phishing_archive.html) et de MillersMiles.co.uk (http://www.millersmiles.co.uk/archives.php).

Exploitation des informations tirées des messages des bureaux d'enregistrement

Dans leurs messages les plus courants, les bureaux d'enregistrement peuvent inclure des informations provenant des enregistrements de noms de domaine. Il peut s'agir de l'identifiant du client, du numéro de compte du client, ou encore des numéros de transaction ou de reçu. Certains bureaux d'enregistrement peuvent également inclure leurs coordonnées de contact ou d'assistance à l'usage des clients : numéros de téléphone, adresses e-mail et URL (liens hypertexte), par exemple. Les bureaux d'enregistrement qui rédigent des e-mails au format HTML peuvent également insérer des logos, des bannières de publicité et des graphismes illustrant leur « marque ».

Les pirates peuvent exploiter cette profusion d'informations pour rédiger des e-mails frauduleux à l'attention des clients de ces bureaux d'enregistrement. Par exemple, un pirate peut inclure les numéros de compte et de transaction du client afin de *personnaliser* le message, comme le montre l'exemple de message suivant, qui correspond au corps d'un e-mail d'hameçonnage potentiel en texte brut :

```
MERCI POUR VOTRE COMMANDE
Mercredi 19 octobre 2005, 05 h 18 m 34 s

Cher client,

Merci pour votre commande chez <bureau>. Voici le détail de cette
transaction. Veuillez conserver ces informations pour référence
ultérieure.

NUMERO CLIENT : 123456789
IDENTIFIANT : machintruc
NUMERO DE RECU : 298884-3340
TOTAL COMMANDE : $19.99
SERVICE CLIENT : 800-555-1234

Vous devez vous connecter à votre compte pour valider cette
transaction. Cliquez sur le lien de confirmation suivant pour
accéder au site http://www.<bureau>.tld/login
```

Dans cet exemple d'attaque, l'URL `http://www.registrar.tld/login` est en fait un lien hypertexte dans l'e-mail qui redirige la victime vers un hôte différent, c'est-à-dire que la balise HTML intégrée dans l'e-mail autour de `http://www.bureau.tld/login` pourrait ressembler à

```
<a
href="http://stealyourdomaininthisway.tld">http://www.registrar.tld/login</a>
```

Cliquer sur ce lien amène le client sur le site `stealyourdomainthisway.tld` via un navigateur. L'inclusion des informations du client n'est pas absolument nécessaire, et ces informations ne doivent pas nécessairement être exactes. Toutefois, le simple fait de mentionner un numéro de compte ou de transaction, même incorrect, renforce la supercherie : le message *a l'air* légitime, et même si certains clients conservent le détail des transactions et sont capables de reconnaître leur numéro de client, ce n'est pas le cas de tous, et certains clients peuvent accepter ces informations sans se poser de question. À l'inverse, des informations inexactes peuvent induire une réaction d'un registrant qui, sinon, ignorerait le message. Prenons l'exemple d'un registrant fictif, Jean Dupont, qui accorde beaucoup de valeur au nom de domaine `smith.tld`. Il reçoit un rappel relatif à l'exactitude des données du WHOIS pour un autre individu portant le même nom, et contenant les coordonnées de ce dernier, comme dans l'exemple ci-dessous :

```
Expéditeur : whoisreminders@whoisupdate.com
Envoyé : Mercredi 12 décembre 2007, 11 h 57
Destinataire : John Smith
Objet : Rappel des données du WHOIS

Très cher client,

Conformément à la résolution 03.41 de la politique de rappel des
données du Whois (WDRP) de la Société pour l'attribution des noms
de domaines et des numéros sur Internet (ICANN), nous vous rappelons
que vous devez tenir à jour les coordonnées associées à votre
enregistrement de nom de domaine. Nos archives contiennent les
informations suivantes, en date du 15/11/2007 :

Nom de domaine : smith.tld
Date d'enregistrement : 09/08/2006
Date d'expiration : 09/08/2008
Coordonnées du registrant
Nom : Peter Smith
Adresse : 11 Smith Street
Adresse : (vide)
Ville : Smithville
État/Province : S/O
Code postal :
Pays : USA
Coordonnées du contact administratif
Nom : Peter Smith
E-mail : psmith@iamtherealsmith.tld
Adresse : 11 Smith Street
Adresse :
Ville : Smithville
État/Province : S/O
Code postal :
Pays : USA
Téléphone : 0123456789
Nom du bureau d'enregistrement : <bureau>
Détails du serveur de noms
```

```
Si l'une des informations ci-dessus est incorrecte, vous devez la
corriger en vous rendant sur le site
http://correctmywhoisinfo.tld/login[3]. N'oubliez pas que selon les
termes de votre accord d'enregistrement, la communication
d'informations WHOIS erronées peut entraîner l'annulation de votre
enregistrement de nom de domaine.
```

Craignant le piratage de son nom de domaine, Jean réagit rapidement pour corriger le problème. Dans sa précipitation, il clique sur le lien intégré, accède au site d'hameçonnage et divulgue ses informations d'identification au pirate.

[3] Dans cet exemple, la balise HTML intégrée dans l'e-mail d'hameçonnage contient une adresse IP et non un nom de domaine, p.ex. <a "href=http://206.197.43.103/login/"> http://correctmywhoisinfo.tld/login .

Exploitation des informations obtenues des services WHOIS

La chronologie des événements dans une attaque par usurpation d'identité d'un bureau d'enregistrement donné est la suivante :

1. L'hameçonneur met en ligne un portail client frauduleux imitant celui du bureau d'enregistrement (site de connexion).
2. L'hameçonneur rédige un message électronique qui semble provenir du bureau d'enregistrement.
3. L'hameçonneur envoie ce message aux adresses de contact du nom de domaine (de manière sélective, c'est-à-dire en ciblant ce registrant en particulier, ou de manière globale en attaquant une liste de clients d'un bureau d'enregistrement).
4. Certains des clients du bureau d'enregistrement tombent dans le piège, accèdent au portail frauduleux et révèlent leurs identifiants de connexion.
5. L'hameçonneur collecte les informations d'identification du registrant pour les utiliser ultérieurement à des fins abusives.

D'après cette chronologie des événements, il est évident que les hameçonneurs ont besoin d'établir une corrélation entre un client, un nom de domaine et le bureau d'enregistrement sponsor du nom de domaine pour lancer une attaque d'usurpation d'identité de bureau d'enregistrement. Les services WHOIS fournissent des informations d'enregistrement de nom de domaine, y compris les coordonnées du registrant et son adresse postale, les adresses électroniques des contacts administratifs et techniques, et celles du bureau d'enregistrement sponsor. Voici un exemple de résultat d'une requête WHOIS :

```
Domain ID:D2347548-LROR
Domain Name:ICANN.ORG
Created On:14-Sep-1998 04:00:00 UTC
Last Updated On:16-Nov-2007 20:24:23 UTC
Expiration Date:07-Dec-2011 17:04:26 UTC
Sponsoring Registrar:Register.com Inc. (R71-LROR)
Status:DELETE PROHIBITED
Status:RENEW PROHIBITED
Status:TRANSFER PROHIBITED
Status:UPDATE PROHIBITED
Registrant ID:C4128112-RCOM
Registrant Name:(ICANN) Internet Corporation for Assigned Names and Numbers
Registrant Organization: Internet Corporation for Assigned Names and Numbers
Registrant Street1:4676 Admiralty Way, Suite 330
Registrant City:Marina del Rey
Registrant State/Province:CA
Registrant Postal Code:90292
Registrant Country:US
Registrant Phone:+1.3108239358
Registrant FAX:+1.3108238649
Registrant Email:icann@icann.org
Admin ID:C4128112-RCOM
Admin Name:(ICANN) Internet Corporation for Assigned Names and Numbers
Admin Organization:Internet Corporation for Assigned Names and Numbers
(ICANN)
Admin Street1:4676 Admiralty Way, Suite 330
Admin City:Marina del Rey
Admin State/Province:CA
Admin Postal Code:90292
Admin Country:US
Admin Phone:+1.3108239358
Admin FAX:+1.3108238649
Admin Email:icann@icann.org
```

```
Tech ID:C1-RCOM
Tech Name:Domain Registrar
Tech Organization:Register.Com
Tech Street1:575 8th Avenue
Tech Street2:11th Floor
Tech City:New York
Tech State/Province:NY
Tech Postal Code:10018
Tech Country:US
Tech Phone:+1.9027492701
Tech FAX:+1.9027495429
Tech Email:domain-registrar@register.com
Name Server:NS.ICANN.ORG
Name Server:A.IANA-SERVERS.NET
Name Server:C.IANA-SERVERS.NET
Name Server:B.IANA-SERVERS.ORG
```

Dans de nombreux cas, un service WHOIS de bureau d'enregistrement ou de tiers fournit des informations supplémentaires sur le domaine, y compris :

- l'état de sécurité (si le site est accessible via le protocole SSL ou HTTP) ;
- les dates de création et de dernière modification du domaine (dans certains cas, il est possible d'obtenir un historique partiel ou complet du domaine) ;
- la date d'expiration du domaine ;
- l'état du registre (le code d'état EPP[4] que le registre a donné au nom de domaine : clientTransferProhibited, RedemptionPeriod, etc.) ;
- les données du serveur, c.-à-d. le type de serveur Web (p.ex. Apache, Microsoft IIS), l'état du site Web (p.ex. actif), l'adresse IP, l'état de la liste noire ;
- les informations DNS (noms et adresses IP des serveurs de noms) ;
- la recherche par registrant (c.-à-d. les autres domaines enregistrés par un registrant) ;
- les mots-clés META que le registrant du nom de domaine utilise pour affiner les recherches ;
- la publicité.

Les pirates peuvent utiliser les informations contenues dans les résultats du WHOIS pour hameçonner des registrants en masse ou à titre individuel à partir de messages prévisibles, par exemple pour signaler l'expiration d'un nom de domaine. Certaines informations WHOIS identifient des contacts électroniques pour le nom de domaine, et donc des destinataires cibles, ainsi que le bureau d'enregistrement sponsor dont l'hameçonneur va usurper l'identité (l'expéditeur). D'autres informations peuvent être utilisées pour renforcer la crédibilité du message : par exemple, les dates de création, de dernière modification et d'expiration du domaine peuvent servir à créer une notification frauduleuse de renouvellement, l'état de sécurité peut servir à créer une notification frauduleuse relative à un certificat SSL, etc.

[4] Extensible Provisioning Protocol (EPP), voir RFC 3731.
http://www.rfc-archive.org/getrfc.php?rfc=3731

Panorama des risques

Le piratage de nom de domaine par hameçonnage est possible, mais c'est rarement le principal objectif visé. Une fois que le pirate a accès au compte du registrant, il peut modifier les enregistrements DNS par le biais du bureau d'enregistrement, de manière à les faire pointer vers des serveurs de noms sous son contrôle.[5] C'est bien souvent l'objectif des activités criminelles et malveillantes qui exploitent les services de noms dans les attaques de type fast-flux ; avec des adresses qui pointent vers des systèmes qu'il contrôle, le pirate peut manipuler les valeurs de durée de vie (TTL, time-to-live) et modifier les enregistrements DNS des données de la zone de domaines sur les serveurs de noms qu'il gère à ces adresses.

Le pirate peut faire plus qu'exploiter le DNS pour lancer des attaques de type fast-flux. Par exemple, il peut ajouter ou modifier les enregistrements suivants dans les données de la zone de domaines qu'il contrôle :

- **MX**, pour pointer vers des hôtes de messagerie sous son contrôle et les utiliser pour envoyer du spam. Il est préférable pour le pirate d'utiliser le domaine d'un registrant plutôt qu'un domaine qu'il pourrait enregistrer directement car dans la plupart des cas, le domaine du registrant est déclaré comme « fiable » par les autres systèmes de messagerie, c'est-à-dire qu'il n'est pas réputé émettre ou relayer du spam et n'est pas sur liste noire ou bloqué d'une autre manière pour le transfert d'e-mails.

- **A** ou **AAAA**, pour pointer vers des systèmes qui hébergent des sites Web usurpés que le pirate contrôle également (vise surtout le Web, mais il est également possible de modifier de la même manière les adresses IP pour le transfert FTP ou d'autres services d'hébergement de contenu). Le pirate peut alors héberger le contenu de son choix sur le site frauduleux ; par exemple, il peut choisir de dénaturer le site Web pour mettre le registrant dans l'embarras.

  Les hameçonneurs peuvent également remplacer les informations du site par des informations incorrectes afin de perturber les activités du registrant. Cette forme d'attaque peut se manifester par des annonces de réductions importantes sur le prix des produits, des rappels de produits, etc. Le pirate peut également inclure des liens hypertexte qui semblent inoffensifs mais qui redirigent le destinataire vers des sites qui hébergent du contenu nuisible en téléchargement, ou qui remplacent des applets et fichiers exécutables à télécharger par du contenu malveillant.

[5] Voir le rapport SAC022, *Fast Flux Attacks and DNS*, http://www.icann.org/committees/security/sac025.pdf

- **A** ou **AAAA**, pour pointer vers des systèmes qui hébergent des sites Web internes ou client usurpés également sous le contrôle du pirate. Le pirate peut cibler une entreprise qui fournit un accès en ligne à des informations sensibles par le biais d'une page d'authentification. En faisant pointer des enregistrements DNS vers une page d'authentification frauduleuse à un intranet qu'il contrôle, le pirate s'attend à tromper les employés peu soupçonneux afin qu'ils lui révèlent leurs identifiants et mots de passe, qu'il pourra alors vendre ou utiliser ultérieurement pour attaquer « en profondeur » cette société. Les institutions financières sont des cibles de choix pour ce genre d'attaques, car les clients divulguent des informations sur leur compte qui peuvent être utilisées pour réaliser des transactions frauduleuses et des vols de fonds. Toutefois, les entreprises et les organisations qui donnent accès à des informations sensibles, exclusives ou personnelles protégées par les lois sur la vie privée courent également le risque de subir de telles attaques.

Cette liste n'est pas exhaustive : elle donne simplement un aperçu des types d'enregistrements DNS que les hameçonneurs cherchent à ajouter ou à modifier.

Ajout ou modification d'enregistrements DNS

Les hameçonneurs semblent préférer l'ajout au remplacement d'enregistrements DNS car le registrant peut continuer à ignorer l'attaque plus longtemps si certains ou tous les noms de son domaine sont toujours résolus comme prévu. De plus, en utilisant de manière abusive un nom de domaine détenu par un registrant de bonne réputation, le pirate espère semer le doute lorsque des plaintes pour utilisation abusive sont déposées par des organismes anti-hameçonnage et de protection des marques. Les bureaux d'enregistrement peuvent hésiter, voire se refuser, à prendre des mesures à l'encontre d'un client fiable ou à demander une injonction, etc., ce qui peut retarder la suspension des activités illégales éventuellement menées en rapport avec ce nom de domaine.

Le pirate peut également utiliser les outils d'administration du domaine fournis par le bureau d'enregistrement pour activer la redirection ou modifier un domaine, de manière à ce que les enregistrements DNS pointent vers un autre emplacement (lien). Si le client hameçonné fait appel au bureau d'enregistrement pour l'hébergement de son site Web ou de sa messagerie, le pirate peut charger du contenu sur le site Web du client ou le modifier, créer des comptes de messagerie (pour l'envoi de spam), ou accéder aux comptes de messagerie existants de ce domaine et les modifier ou les transférer.

Comment les bureaux d'enregistrement peuvent limiter les risques d'hameçonnage

Les hameçonneurs ont élargi leur domaine de chasse, autrefois limité aux institutions marchandes et financières, aux fournisseurs de services d'enregistrement de domaines. Les bureaux d'enregistrement et les revendeurs doivent à leur tour prendre conscience de la menace de l'hameçonnage. Le SSAC recommande aux bureaux d'enregistrement (et aux revendeurs) de faire preuve de prudence et de suivre les meilleures pratiques anti-hameçonnage en matière de rédaction de messages à l'attention de leurs clients. Les pratiques suivantes sont fortement recommandées :

1. Inclure uniquement les informations nécessaires à la compréhension du message destiné au client. N'inclure aucun numéro de compte, aucune coordonnée et (de manière générale) aucune information d'enregistrement du client. Ces informations peuvent être utilisées par les pirates pour personnaliser leurs e-mails.

2. Éviter l'utilisation de liens hypertexte dans les messages destinés aux clients. Les hameçonneurs modifient fréquemment les liens afin de rediriger les utilisateurs d'une page légitime vers une page frauduleuse.

3. Inviter les clients à ne pas cliquer sur les liens hypertexte inclus dans un message, qu'il s'agisse de texte ou d'une image. Inclure des avertissements dans le corps des messages envoyés, tels que « Pour lutter contre l'hameçonnage, nous vous invitions à saisir l'adresse Internet suivante dans la barre d'adresse de votre navigateur » ou « Ne faites pas confiance aux liens présents dans les e-mails. Saisissez toujours les adresses Internet dans la barre d'adresse de votre navigateur ». Les clients apprécieront cette marque d'attention portée à leur sécurité et à leur vie privée, même si taper une adresse plutôt que de cliquer dessus est un inconvénient.

4. Faire savoir que les bureaux d'enregistrement sont la cible d'attaques d'hameçonnage. Proposer (ou développer) des FAQ pour attirer l'attention sur l'usurpation d'identité des bureaux d'enregistrement, les menaces posées par ces attaques d'hameçonnage, les mesures prises pour lutter contre l'hameçonnage et les mesures que les clients peuvent prendre pour éviter d'en être les victimes. Expliquer le type d'informations qui seront incluses dans vos messages et, en particulier, identifier les informations que vous n'inclurez *jamais* dans vos messages, afin que vos clients puissent savoir si un message reçu est légitime ou suspect.

5. Donner aux clients le moyen de signaler les attaques d'hameçonnage potentielles, soit directement, soit en coopération avec une organisation qui encourage le signalement des e-mails suspects (scams) ou frauduleux et tient des archives d'e-mails d'hameçonnage[6].

6. Envisager de mettre en place un moyen de vérification de l'origine des messages destinés aux clients, comme une signature numérique.

[6] Page de signalement dédiée à l'hameçonnage de l'APWG, à l'adresse http://www.antiphishing.org/report_phishing.html

Comment les registrants peuvent éviter de devenir les victimes de l'usurpation d'identité d'un bureau d'enregistrement

Les registrants ont la responsabilité de protéger leurs investissements en noms de domaine. Cette responsabilité n'est pas moins importante dans les contextes de la présence, du fonctionnement et du commerce sur Internet que celle de protéger son identité contre le vol et l'utilisation abusive. Les organismes de protection des consommateurs, les institutions financières et les sociétés de carte de crédit alertent les consommateurs au sujet de la fraude en ligne et des scams, et leur expliquent comment détecter et éviter les attaques d'hameçonnage. Leurs conseils sont applicables à la prévention de l'usurpation d'identité des bureaux d'enregistrement lors d'attaques d'hameçonnage. Certains des conseils les plus pertinents sont repris ci-dessous :

1. Ne cliquez pas sur les liens hypertexte présents dans les messages électroniques que vous recevez. À la place, saisissez manuellement l'adresse de la page Web dans la barre d'adresse de votre navigateur.

2. Utilisez un client de messagerie qui offre des fonctionnalités anti-spam et anti-hameçonnage, ou installez un complément ou plugin réputé fiable qui dotera votre client de messagerie de telles fonctionnalités.

3. Utilisez un client de messagerie capable de révéler les liens hypertexte associés aux textes ou images affichés inclus dans une adresse e-mail, ou apprenez à afficher et déchiffrer le texte « source » ou brut (ASCII) des messages électroniques. Apprenez à déchiffrer les balises des liens hypertexte, telles que HREF, pour détecter rapidement la redirection frauduleuse, comme un lien `www.example.com` qui vous redirige vers le domaine d'un pirate :

   ```
   <A HREF="http://iwillscamu.tld">www.example.com</a>
   ```

   ou son adresse IP :

   ```
   <A HREF="http://192.168.2.3">www.example.com</a>.
   ```

4. Méfiez-vous des messages électroniques qui exigent une réponse urgente, et auxquels il est uniquement possible de répondre en visitant un site Web. La plupart des sociétés en ligne réputées fiables, bureaux d'enregistrement compris, prévoient d'autres méthodes comme le téléphone, l'e-mail ou le fax, pour contacter leur service client. En cas de doute, répondez à votre bureau d'enregistrement en utilisant l'une de ces méthodes, en particulier une directement référencée sur le site de votre bureau.

5. Lisez attentivement le corps du message électronique. Une grammaire et une ponctuation incorrectes sont souvent le signe d'un message frauduleux.

6. Ne faites pas confiance à un message électronique simplement parce qu'il est personnalisé.

7. Ne divulguez aucune information personnelle ou relative à votre compte par l'intermédiaire d'un formulaire en ligne sans avoir vérifié la légitimité de la page.

8. Vérifiez que les formulaires en ligne ou les pages de connexion que vous visitez sont sécurisés à l'aide du protocole SSL. Mais ne faites pas confiance à un lien hypertexte simplement parce qu'il semble vous amener sur une page sécurisée. Vérifiez l'authenticité du certificat numérique associé aux pages SSL[7].

9. Si vous avez l'intention de souscrire des services de noms de domaine à l'aide d'une carte de crédit, choisissez un bureau d'enregistrement qui exige de ses clients l'envoi du code de vérification de la carte (CVV, Card Verification Value) au moment de la transaction. Le CVV est une mesure de sécurité utilisée par les sociétés de carte de crédit pour vérifier que vous possédez réellement la carte avec laquelle vous effectuez l'achat.

10. Signalez la réception de messages d'hameçonnage potentiels à votre bureau d'enregistrement ou à des organismes anti-hameçonnage comme l'APWG, le Phish Report Network[8], PhishTank[9] ou votre CERT local[10].

Pour plus d'informations sur la manière de déjouer les pièges des hameçonneurs, lisez les pages de conseils de l'Anti-Phishing Working Group[11], de PhishTank et du SpamHaus Project[12].

Conclusions

Les noms de domaine sont devenus des biens de grande valeur, et ceux qui sont réputés pour leur fiabilité sont des cibles de choix pour les pirates. L'usurpation de l'identité d'un bureau d'enregistrement afin d'obtenir les informations d'identification d'un client, et accéder ainsi aux enregistrements de noms de domaine, est une menace sérieuse. Le SSAC encourage les bureaux d'enregistrement et les revendeurs à prendre conscience de la menace de l'hameçonnage et à prendre des mesures pour éviter tout abus.

Le SSAC reconnaît que l'hameçonnage repose sur la tromperie et l'ingénierie sociale. Les hameçonneurs essayeront de contourner les mesures mises en place par les bureaux d'enregistrement. Au final, il incombe au consommateur d'éviter de tomber dans le piège des scams et de la fraude. Par conséquent, bien que de nombreuses mesures soient à la disposition des bureaux d'enregistrement pour lutter contre l'hameçonnage, l'essentiel est de sensibiliser les consommateurs et de leur conseiller la prudence envers les messages reçus de la part des bureaux d'enregistrement.

---

[7] Voir SSL.com, Q10068 - FAQ : Comment savoir si une page Web est sécurisée ? (en anglais) http://info.ssl.com/Article.aspx?id=10068.
[8] Phish Report Network, http://www.phishreport.net/
[9] PhishTank : Rejoignez la lutte contre l'hameçonnage (en anglais), http://www.phishtank.org
[10] Inclure ici les adresses e-mail ou les pages Web.
[11] Conseil aux consommateurs : Comment éviter l'hameçonnage (en anglais), http://www.antiphishing.org/consumer_recs.html
[12] Index de la Foire Aux Questions (FAQ) du SpamHaus Project, http://www.spamhaus.org/faq/index.lasso