FR

19 août 2009

SAC 40 : MESURES POUR PROTEGER LES SERVICES D'ENREGISTREMENT DE NOMS DE DOMAINE CONTRE L'EXPLOITATION OU LE MAUVAIS USAGE

Un rapport du
Comité consultatif
pour la sécurité et la stabilité (SSAC)
de l'ICANN

Préface

Ce document est un rapport rédigé par le Comité consultatif pour la sécurité et la stabilité (SSAC), décrivant les mesures visant à protéger les services d'enregistrement contre le mauvais usage. Le SSAC conseille la communauté et le Conseil d'administration de l'ICANN sur les questions liées à la sécurité et à l'intégrité des systèmes d'attribution des noms de domaine et des adresses Internet. Ceci inclut des questions opérationnelles (par ex. des questions se rapportant à l'opération correcte et fiable du système de noms racine), des questions administratives (par ex. des questions se rapportant à l'attribution d'adresses et de numéros sur Internet), et des questions d'enregistrement (par ex. des questions se rapportant aux services de registres et de bureaux d'enregistrement tels que le WHOIS). Le SSAC se livre à une évaluation continue des menaces et à une analyse des risques des services de nommage et d'attribution d'adresses Internet pour localiser les principales menaces à la sécurité et à la stabilité, et conseille la communauté de l'ICANN en conséquence. Le SSAC n'a pas d'autorité officielle pour réglementer, veiller à l'application ou juger. Ces fonctions-là appartiennent à d'autres, et les conseils fournis ici devraient être évalués en fonction de leur valeur.

Les noms des personnes ayant collaboré à ce rapport, les références aux biographies et aux déclarations d'intérêt des membres du comité ainsi qu'aux objections des membres du comité aux résultats ou aux recommandations de ce rapport, se trouvent à la fin de ce rapport.

Introduction

Les attaques contre les comptes d'enregistrement de noms de domaine et la reconfiguration malveillante de registres de systèmes de noms de domaine (DNS) sont des évènements nuisibles liés à la sécurité. Les incidents survenus l'année dernière prouvent que l'accès aux comptes d'enregistrement de noms de domaine et aux DNS continue à être une cible attirante pour les attaquants. Les activités résultant d'une modification non autorisée des informations associées à un enregistrement de nom de domaine, y compris l'altération malveillante des informations de configuration du DNS afin d'utiliser le DNS pour diriger le trafic vers une destination différente que celle de l'hôte visé, *même temporairement*, peuvent perturber le cours des affaires, causer des dommages financiers et constituer une atteinte à la réputation.

Ni le piratage de comptes d'enregistrement de noms de domaine ni celui de services de résolution de noms ne représentent de nouveaux vecteurs d'attaque. Dans des rapports consultatifs et autres précédents, le comité consultatif pour la sécurité et la stabilité de l'ICANN (SSAC) a examiné des problèmes qui touchent les enregistrements de noms de domaine et l'opération de DNS du point de vue de l'utilisateur (client de bureau d'enregistrement, à savoir titulaire de nom de domaine). Nous avons identifié des situations où les titulaires de noms de domaine n'avaient pas agi pour protéger suffisamment leurs noms de domaine (par ex. omission de renouvellement d'enregistrement ou de maintien d'informations de contact précises). Nous avons recommandé des mesures que les titulaires peuvent adopter pour protéger leurs affaires et leurs intérêts opérationnels par rapport aux noms de domaine qu'ils enregistrent et gèrent.

Ce rapport décrit de récents incidents ayant impliqué un accès non autorisé à des comptes d'enregistrement de noms de domaine. La description de tels évènements n'a pas pour but d'embarrasser ou de critiquer les bureaux d'enregistrement, les revendeurs, *ou* les titulaires de noms de domaine. Nous le faisons parce que l'analyse d'évènements liés à la sécurité révèle toujours *quelque chose* que chaque partie aurait pu faire pour éviter la production ou la gravité de l'évènement.

Dans ce rapport, nous attirons l'attention sur certains incidents mettant en jeu des comptes d'enregistrement de noms de domaine, dont on a beaucoup parlé, pour déterminer s'il existe des causes communes aux évènements qui pourraient révéler des mesures visant à réduire ou à limiter certaines menaces et vulnérabilités. Le rapport examine les incidents d'une manière suffisamment détaillée pour identifier comment les comptes ont-ils été compromis, les actions que les attaquants ont mené à partir de la prise de contrôle du compte, et les conséquences. Les descriptions proviennent des nouvelles et des articles publiquement disponibles. Elles ont été complétées par des informations obtenues lors d'entretiens avec les bureaux d'enregistrement ciblés et leurs clients. Nous avons délibérément omis de mentionner des informations qualifiées confidentielles par les parties ciblées.

Le rapport présente des mesures de sécurité utilisées dans d'autres secteurs d'activité sur Internet (par ex. financiers, négociants de biens de consommation durables) pour protéger les clients contre

des vulnérabilités similaires. Le rapport identifie des pratiques que les bureaux d'enregistrement peuvent partager avec les clients afin que le bureau d'enregistrement et le client puissent conjointement protéger les noms de domaine enregistrés contre l'exploitation ou le mauvais usage. Il discute de méthodes visant à sensibiliser les titulaires de noms de domaine par rapport aux risques liés à une perte de contrôle, même temporaire, des noms de domaine et des configurations DNS y liées. Alors que certains bureaux d'enregistrement se différencient effectivement par une prestation de services de haut niveau, ce rapport cherche à encourager un plus grand nombre de bureaux d'enregistrement à examiner les possibilités éventuelles de fournir une protection supplémentaire contre les attaques de comptes d'enregistrement de noms de domaine. Ce rapport cherche à encourager les bureaux d'enregistrement à considérer la mise en valeur des mesures de sécurité relatives à l'enregistrement comme moyen de différencier leurs services sur un marché hautement compétitif.

Qu'est-ce qui a motivé cette étude ?

Plusieurs incidents mettant en jeu un accès non autorisé à des comptes de noms de domaine et dont on a beaucoup parlé, ont eu lieu au cours des douze derniers mois. Cette vague d'attaques partage certains traits avec celles qui ont motivé de précédentes études du SSAC sur le piratage de noms de domaine[1] et les conséquences imprévues liées au non renouvellement de noms de domaine.[2,3] Certains incidents sont des actes malveillants contre le personnel des bureaux d'enregistrement et les services d'enregistrement (par ex. les outils optimisés Web d'administration de comptes de noms de domaine). D'autres usent du piratage psychologique et peuvent avoir exploité la correspondance courante et prévue entre un bureau d'enregistrement et ses clients.[4]

Le SSAC a examiné une série d'incidents survenus entre mai 2008 et avril 2009. De ces incidents, nous avons identifié des vulnérabilités ainsi que les politiques et les pratiques (commerciales et opérationnelles) exploitées, afin d'examiner l'éventualité d'un point commun. Alors que nous examinions ces incidents, nous avons noté ce qui suit :

(1) Plusieurs organisations avaient des comptes d'enregistrement de noms de domaine qui comportaient des noms de haute valeur ou commercialement cruciaux, des noms de domaine qui pourraient être aussi précieux pour l'organisation que tout actif corporel, marque commerciale ou droit de propriété intellectuelle appartenant à l'organisation.

(2) Beaucoup de fournisseurs de services d'enregistrement ont des objectifs de service orientés vers le consommateur ; en d'autres termes, le service d'enregistrement est hautement automatisé et concentré sur le service de très grands nombres de titulaires à un rythme de transaction élevé. L'automatisation est extrêmement importante dans toute entreprise qui essaie de fournir un service de manière opportune et extensible. Notre étude a révélé que les attaquants s'étaient familiarisés avec le comportement des bureaux d'enregistrement et exploitaient certains aspects de l'automatisation ; par exemple, sachant que le courrier électronique est la méthode préférée pour informer les titulaires de noms de domaine de changements de contact et de configuration, de renouvellements, etc., les attaquants tentent souvent de perturber la livraison aux adresses de courrier électronique en modifiant les configurations de DNS.

---

1 SAC007, Rapport sur le piratage de noms de domaine, http://www.icann.org/announcements/hijacking-report-12jul05.pdf

2 SAC011, Problèmes causes par le non renouvellement d'un nom de domaine associé à un serveur de nom DNS, http://www.icann.org/committees/security/renewal-nameserver-07jul06.pdf

3 SAC010, Considérations de renouvellement à l'adresse des titulaires de noms de domaine, http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf

4 SAC028, Rapport consultatif sur les attaques d'hameçonnage et d'usurpation d'identité de bureaux d'enregistrement (26 mai 2008), http://www.icann.org/committees/security/sac028.pdf

(3) Dans les incidents examinés, les victimes étaient fréquemment des clients titulaires de comptes de noms de domaine commercialement cruciaux, gérés par des fournisseurs de services d'enregistrement ayant des objectifs de service orientés vers le consommateur. Dans certains cas, les clients n'avaient pas convenablement estimé le risque lié à une perte de contrôle ou d'accès éventuelle à leur compte d'enregistrement de nom de domaine jusqu'au moment où ils avaient été attaqués ; dans d'autres cas, les politiques et les activités de surveillance internes en place avant l'incident ne suffisaient pas à détecter ou à bloquer l'attaque.

Tenant compte de la taille et de la réputation commerciale, certaines des victimes sembleraient être suffisamment averties en matière d'administration interne de sécurité et de gestion du risque pour reconnaître la valeur de leurs noms de domaine et pourtant, elles ne semblaient pas avoir inclus leurs noms de domaine dans leur estimation des risques. D'autres victimes, notamment des petites et moyennes entreprises ou des particuliers, peuvent ne pas avoir très bien compris l'importance de leurs noms de domaine jusqu'au moment où le problème est apparu. Ceci est en accord avec le comportement concernant d'autres domaines à risque. Dans beaucoup de situations, une organisation peut reconnaître la valeur ou la nature commerciale cruciale d'un élément d'actif, mais peut ne pas adopter les mesures convenables pour protéger cet actif contre les menaces jusqu'à ce qu'un incident survienne.

Du point de vue sécurité, les titulaires de noms de domaine qui estiment que leurs noms de domaine sont des biens cruciaux devraient considérer la sécurité comme un critère de sélection important au moment de choisir un fournisseur de services d'enregistrement. Les incidents que le SSAC a examinés révèlent que les titulaires de noms de domaine soit ne comprennent pas la gamme de services de sécurité disponible auprès des fournisseurs de services d'enregistrement soit n'estiment pas qu'il *existe* une gamme de services de sécurité desquels ils peuvent choisir. Un bureau d'enregistrement a confié au SSAC que les titulaires de noms de domaine estiment que les services d'enregistrement sont plus ou moins les mêmes, et déduisent que puisque tous les bureaux d'enregistrement vendent le même produit provenant des mêmes registres, les mesures de sécurité que les bureaux d'enregistrement fournissent sont sans doute les mêmes. Les incidents que nous décrivons dans la section suivante ont aidé le SSAC à conclure que les différences entre les fournisseurs de services d'enregistrement ne sont pas bien comprises en dehors de la communauté des noms de domaine.

Attaques contre les comptes d'enregistrement de noms de domaine

Une liste exhaustive des évènements liés à ce sujet dépassant le champ de ce rapport, nous présentons des résumés de certaines attaques de comptes d'enregistrement de noms de domaine qui ont fait la une, pour fournir un contexte à la discussion et à l'analyse Alors que les résumés citent libéralement des sources publiques, le SSAC s'est également entretenu avec des bureaux d'enregistrement impliqués dans les incidents ainsi qu'avec des organisations victimes des attaquants et les remercie sincèrement de leur coopération.

Comcast (mai 2008)

Comcast est le plus grand câblo-opérateur, le deuxième plus grand fournisseur de services Internet, et l'un des plus grands fournisseurs de téléphone fixe aux Etats-Unis.[5] A l'époque de l'incident, Comcast avait enregistré environ 200 noms de domaine par le biais de Network Solutions, Inc. [6] Le 28 mai 2008, des attaquants obtinrent un accès au compte d'enregistrement de noms de domaine de Comcast auprès de Network Solutions. Au départ, les attaquants altérèrent méchamment certaines informations de contact, pour la publicité sans doute.[7] Le personnel de Comcast reçut une notification du changement par courrier électronique et rétablit les informations correctes.

Les attaquants prétendent avoir contacté un administrateur de Comcast pour lui décrire la vulnérabilité et leur exploit. Les attaquants prétendent avoir utilisé une combinaison de piratage psychologique et de bidouillage technique pour obtenir l'accès au compte d'enregistrement de noms de domaine. [8]Network Solutions rapporta qu'il n'y avait pas eu de brèche de sécurité ou de piratage psychologique de leur personnel et que les changements du DNS avaient été réalisés par quelqu'un qui possédait les informations d'ouverture de session du client. [9] Dans un article du *Wired Magazine*, les attaquants prétendent qu'un directeur de Comcast « se moqua de leurs affirmations et leur raccrocha le téléphone au nez ».[10] Les attaquants accédèrent au compte une deuxième fois. Cette fois-ci, ils altérèrent la configuration DNS du nom de domaine comcast.net et redirigèrent le trafic vers un site Web de défacement hébergé par des serveurs qu'ils avaient compromis. Toutefois, le personnel de Comcast ne reçut pas de notifications de changement par courrier électronique de la part de Network Solutions. Les contacts technique et administratif enregistrés dans les registres d'enregistrement des noms de domaine utilisaient des adresses de courrier électronique attribuées à partir des noms de domaine enregistrés de Comcast. En altérant la configuration DNS, les attaquants avaient efficacement évité que le personnel de Comcast reçoive des notifications par courrier électronique de l'activité du compte : ces messages ne pouvaient simplement pas être délivrés. L'attaque fut efficace et fit la une des journaux de par le monde. Selon le *Wired Magazine*, « l'attaque commença vers 23 heures (heure de l'Est) et les pirates informatiques avaient pris le contrôle de Comcast.net jusqu'à 4 heures ou 5 heures du matin. Même lorsque Comcast reprit le contrôle, il a fallu des heures pour que le changement se propage entièrement à travers le DNS, laissant ainsi quelques clients sans accès à leur courriel Web jusqu'à 11 heures 30 jeudi matin ». Un article paru le 29 mai 2009 dans *The Register* commente que « l'attaque démontre que les

---

5 Article relatif à Comcast sur en.wikipedia.org/wiki/Comcast

6 Le domaine Comcast.net piraté chez Network Solutions, http://www.domainnamenews.com/featured/comcastnet-domain-hijacked-at-network-solutions/1619

7 Comment Comcast.net a-t-il été piraté ?, http://blogs.zdnet.com/security/?p=1224

8 Le nom Comcast.net piraté, http://www.internetidentity.com/2008/June-2008.html

9 La question de l'accès au compte Comcast – clarification, http://blog.networksolutions.com/2008/comcast-account-access-issue-clarification/

10 Les pirates de Comcast disent avoir d'abord averti la compagnie, http://blog.wired.com/27bstroke6/2008/05/comcast-hijacke.html

compromis vieux jeu d'un compte sont également suffisants pour altérer des quantités importantes de trafic Internet ». [11]

CheckFree (décembre 2008)

CheckFree (aujourd'hui FIServ) est le fournisseur mondial principal de systèmes de gestion de l'information et de commerce électronique au secteur des services financiers.[12] Le 2 décembre 2008, un attaquant prit le contrôle du compte d'enregistrement des noms de domaine de CheckFree auprès de Network Solutions.[13] L'attaquant modifia la configuration DNS de plusieurs noms de domaine, y compris le checkfree.com et le mycheckfree.com. Les clients qui essayaient d'accéder à leurs comptes pour utiliser les services de paiement en ligne étaient redirigés vers un serveur usurpateur localisé en Ukraine qui tentait d'installer un code malveillant en exploitant le lecteur Adobe Reader.[14] CheckFree rétablit la configuration correcte de DNS dans les huit heures suivant l'attaque, mais comme dans le cas d'autres incidents similaires, la propagation des changements à travers l'ensemble de l'infrastructure du DNS nécessita un nombre d'heures beaucoup plus important.[15]

Le blogue « Security Fix » du *Washington Post* notait que l'attaquant avait accédé au compte en utilisant l'information correcte d'ouverture de session. Dans le même article, Network Solutions mit l'accent sur le fait que l'attaquant ne s'était pas infiltré dans ses systèmes pour obtenir les justificatifs d'ouverture de session.[16] Comment l'attaquant a-t-il pu s'emparer du compte utilisateur et des justificatifs reste incertain (ou non divulgué).

ICANN, Photobucket, RedTube (juin 2008)

Le 26 juin 2008, l'ICANN elle-même fut la victime d'un groupe de pirates informatiques qui obtinrent un accès non autorisé au compte d'enregistrement du nom de domaine de l'ICANN auprès de Register.com. Selon un communiqué de presse de l'ICANN, l'attaque était « sophistiquée, alliant des techniques technologiques et psychologiques ». [17] Selon le directeur TI de l'ICANN, les attaquants altérèrent les configurations DNS de plusieurs noms de domaine – icann.net, iana-servers.com, icann.com, internetassignednumberauthority.com et iana.com – de sorte que le trafic intrant était acheminé vers un site Web de défacement publié sur des comptes d'hébergement

---

11 Des pirates informatiques farfelus volent les clés de comcast.net, et vont faire un tour, http://www.theregister.co.uk/2008/05/29/comcast_domain_hijacked/

12 FIServ, http://en.wikipedia.org/wiki/Fiserv

13 Une attaque de DNS pirate un site Web de paiement, http://www.techworld.com/security/news/index.cfm?newsid=107959

14 L'attaque d'hameçonnage contre network Solutions a précédé la prise de contrôle du domaine CheckFree, http://*www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122722*

15 http://www.internetidentity.com/2008/Nov-Dec-2008-FIN.html#cf

16 En creusant plus profondément dans l'attaque contre CheckFree, http://voices.washingtonpost.com/securityfix/2008/12/digging_deeper_into_the_checkf.html

17 La réponse de l'ICANN aux menaces récentes contre la sécurité, http://www.icann.org/en/announcements/announcement-03jul08-en.htm

gratuits opérés par Atspace.com. Les spéculations sur le fait que l'attaque était politique se basaient sur le moment choisi pour créer l'incident (début de la conférence de l'ICANN à Paris avec des débats publics concernant les nouveaux gTLD) et sur le message du défaceur. Le personnel TI de l'ICANN détecta les changements du DNS et Register.com rétablit les informations de configuration correctes peu après avoir été averti par l'ICANN. Cependant, comme dans le cas de l'incident de Comcast, les informations de configuration de DNS malveillantes sont restées dans le DNS global environ 24 à 48 heures[18] alors que les informations corrigées se propageaient à l'échelle mondiale.

Le groupe pirate qui revendiqua la responsabilité de l'attaque contre l'ICANN utilisa des tactiques similaires et le même fournisseur d'hébergement Web gratuit lors d'attaques subséquentes. Photobucket est un site Web d'hébergement d'images, de vidéos, de partage de diaporamas et de photos acheté par Fox Interactive Media en 2007.[19] Le 18 juin 2008, le même groupe pirate revendiqua la responsabilité d'une attaque contre Photobucket qui résulta en l'interruption des services aux utilisateurs de Photobucket.[20] Le groupe perpétra une autre attaque de défacement le 7 février 2009 contre le site Web pour adultes RedTube.[21] ,[22]

DomainZ (avril 2009)

DomainZ (Domainz.net.nz) est la filiale en Nouvelle Zélande d'une société TI et d'un bureau d'enregistrement basés à Melbourne. Le 21 avril 2009, des pirates à la recherche de notoriété utilisèrent une attaque par injection de commandes SQL sur une page de récupération de mots de passe chez DomainZ pour rassembler les justificatifs de comptes de plusieurs titulaires de noms de domaine très en vue, y compris Coca-Cola, Fanta, F-secure, HSBC, Microsoft, Sony et Xerox. Les attaquants modifièrent les registres de configuration DNS des noms de domaine enregistrés sous .CO.NZ pour pointer vers des serveurs de noms enregistrés sous un nom de domaine .INFO (turkguvenligi.info). Ces serveurs hébergeaient des informations de zone non autorisées qui détournaient les noms de domaine piratés vers des sites Web de défacement hébergés par les attaquants. Une partie du trafic intrant se retrouva sur des pages Web malveillantes qui ciblaient la marque (par ex. Microsoft) ; une autre partie du trafic était redirigée vers des pages de protestations politiques.

Que révèlent ces incidents ?

Les similarités des attaques contre Comcast, ICANN, Photobucket et RedTube illustrent le fait que les applications utilisées par les attaquants de comptes d'enregistrement sont de type similaire aux

---

18 Des pirates informatiques criminels turcs s'attaquent aux sites de l'ICANN, http://news.cnet.com/8301-10789_3-9980713-57.html

19 Photobucket, http://en.wikipedia.org/wiki/Photobucket

20 Les registres DNS de Photobucket piratés par un groupe de pirates turcs, http://blogs.zdnet.com/security/?p=1285

21 Site porno populaire attaqué par des bégueules, http://www.securecomputing.net.au/News/102818,popular-porn-site-hacked-by-prudes.aspx

22 Des pirates turcs prennent le contrôle d'un site porno connu, http://www.darkreading.com/security/perimeter/showArticle.jhtml;jsessionid=FV31FLACFRJQYQSNDLPSKH0CJUNN2JVN?articleID=208803672&subSection=Security

applications Web, transferts de fichiers et autres applications sur Internet en ce sens : une fois qu'une vulnérabilité est efficacement exploitée sur le terrain, les attaquants se partagent l'exploit et balayent les cibles à la recherche des mêmes cibles ou de cibles aussi vulnérables.

Des incidents décrits ci-haut, le SSAC note ce qui suit :

Pour certains bureaux d'enregistrement :

1. Tout ce dont un attaquant a besoin pour acquérir le contrôle de la totalité du portefeuille de noms de domaine d'une organisation (et entraver l'accès autorisé à ce portefeuille) est d'un compte utilisateur et d'un mot de passe.

2. Les attaquants ont uniquement besoin de deviner, hameçonner, ou appliquer des techniques de piratage psychologique sur un seul point de contact pour acquérir le contrôle d'un compte d'enregistrement de noms de domaine.

3. Les attaquants balayent les portails d'administration et d'enregistrement de comptes de noms de domaine à la recherche de vulnérabilités des applications Web (par ex. injection de commandes SQL). Une exploitation réussie d'un code d'application vulnérable peut résulter en la divulgation de justificatifs d'identité de plusieurs comptes de noms de domaine.

4. Le courrier électronique est la méthode préférée et souvent la seule méthode que certains bureaux d'enregistrement utilisent pour informer un titulaire de nom de domaine de l'activité du compte. (Nous nous référons à des méthodes de contact supplémentaires dans des sections suivantes).

5. Les attaquants peuvent bloquer la livraison de notifications par courrier électronique de titulaires ciblés en altérant les données de configuration DNS de sorte que les notifications par courrier électronique n'atteignent aucun destinataire pour ce qui est des noms de domaine que l'attaquant contrôle par le biais d'un compte compromis (par ex. les adresses de courrier électronique des contacts administratif et technique identifiés du titulaire hébergés sous le nom de domaine).

6. L'accès aux informations de configuration DNS et de contact et la capacité de modifier ces informations pour tous les noms de domaine dans un compte d'enregistrement sont communément accordés à travers un seul compte utilisateur et mot de passe.

7. Même lorsqu'une modification non autorisée d'informations DNS est rapidement découverte, le processus de rétablissement de ces informations et de correction suite à une configuration malveillante peut être long, est inhérent à la distribution du DNS et lié à des valeurs de durée de vie (TTL).

Les clients ne sont pas familiarisés avec les mesures de protection des enregistrements

Certains bureaux d'enregistrement protègent bien leurs activités et leurs clients. Ils appliquent les meilleures pratiques pour protéger les applications Web, les serveurs de noms et d'hébergement. Ils surveillent les systèmes et les comptes pour détecter les activités suspectes. Le personnel

administratif du bureau d'enregistrement répond de façon efficace aux plaintes pour infraction ou abus. Toutefois, dans un secteur aussi vaste que celui des services d'enregistrement de noms de domaine et comme c'est le cas pour toute classe d'activité cybermarchande ou en ligne, il est inévitable que certains bureaux d'enregistrement s'avèrent vulnérables à des vecteurs d'attaque connus. D'autres, même les meilleurs, peuvent s'avérer vulnérables à des attaques qui n'étaient pas prises en compte dans un audit de sécurité, ou jamais rencontrées auparavant.

Il ressort des incidents décrits dans ce rapport (et d'autres incidents cités dans le SAC012 et survenus depuis sa publication), que les procédés des bureaux d'enregistrement ont été et continuent à être exploités par des attaquants. Étant donné la taille et la diversité du secteur, ceci n'est pas inhabituel. Les bureaux d'enregistrement ont été et continueront à être des cibles d'attaquants. *Tout comme les clients d'institutions financières peuvent être victimes d'attaques menées contre le portail d'un réseau d'informatique bancaire, les titulaires de noms de domaine peuvent de même être les victimes d'attaques menées contre des pages d'administration de noms de domaine d'un bureau d'enregistrement.*

Il incombe finalement au titulaire du nom de domaine d'estimer le risque d'attaque contre le nom de domaine et la configuration DNS et de choisir le service d'enregistrement qui réduit l'exposition du titulaire du nom de domaine aux attaques dans une mesure acceptable. Toutefois, les bureaux d'enregistrement n'attirent pas généralement l'attention sur les mesures de protection qu'ils offrent, et en l'absence de méthodes leur permettant de comparer les services de sécurité des bureaux d'enregistrement, les clients peuvent conclure à tort que tous les bureaux d'enregistrement sont les mêmes en matière de sécurité, et choisir soit mal soit indifféremment.

Les bureaux d'enregistrement ont des marchés-cibles et des modèles de service différents

Ceci pris en compte, le SSAC a considéré la vaste panoplie de services d'enregistrement de noms de domaine et a établi que l'enregistrement de noms de domaine était en grande partie pris en charge à travers deux modèles de service.

Un modèle de service populaire offre des services d'enregistrement de noms de domaines à des prix modiques ou réduits. La prestation du service est principalement automatisée et conçue de sorte à privilégier la rapidité de traitement des transactions, de volume important, d'une manière systématique et répétable qui minimise souvent les possibilités d'erreurs humaines. La correspondance avec les clients est d'habitude réalisée par un envoi de messages électroniques pour communiquer les avis ou transmettre de simples instructions (souvent point par point) pour guider les clients à travers un processus obligatoire (par exemple, une révision annuelle de l'exactitude des données WHOIS). La transmission automatisée de demandes d'assistance par le biais d'un système de suivi de problèmes est d'usage courant. Généralement, l'automatisation semble battre l'implication humaine ; dans la plupart des cas, l'intervention humaine n'est recherchée par les clients que lorsque l'automatisation ne fonctionne pas tel que prévu ou n'est pas comprise, ou encore lorsque le client a un problème que les processus automatisés ne peuvent pas résoudre ou qu'il souhaite signaler un incident. Les mesures de sécurité courantes, observables, pour protéger les comptes de noms de domaine et les configurations DNS contre les abus comportent d'habitude une connexion au compte du nom de domaine et une administration de portefeuille du nom de domaine sécurisées par protocole SSL, une notification par courrier électronique lorsque la

configuration DNS ou les informations de contact liées au compte sont sujettes à des changements, des services de confidentialité (services WHOIS protégés ou délégués tel que décrit dans le SAC023[23]), et une protection du transfert du nom de domaine (verrouillage, confirmation de code d'autorisation entre le bureau d'enregistrement sortant et le nouveau bureau d'enregistrement).[24]

Un deuxième modèle de services d'enregistrement offre des mesures de protection qui répondent aux besoins des clients qui accordent une grande valeur à leurs noms de domaine, qui considèrent que leurs noms de domaine et leur présence en ligne sont cruciaux pour leurs affaires, ou qui reconnaissent que leurs activités ou leurs marques peuvent être souvent les cibles d'abus ou d'activités criminelles. Ces clients reconnaissent les menaces contre les noms de domaine et veulent minimiser ou limiter le risque de perte, d'erreur de configuration, de modification des informations de contact ou de configuration DNS, ou encore un mauvais usage de leurs noms de domaine. Ils ont rassemblé assez d'informations pour prendre une décision avertie en matière de recherche de bureaux d'enregistrement qui puissent satisfaire de telles exigences. Ces bureaux d'enregistrement fournissent des mesures de sécurité pour la protection contre le non renouvellement des noms de domaine du client à cause d'une erreur technique ou d'une omission, pour protéger le client contre le piratage du nom de domaine par le biais d'une modification non autorisée des registres d'enregistrement, et pour éviter une configuration malveillante, non autorisée du DNS. Le modèle d'activité de ces bureaux d'enregistrement se concentre sur le traitement de transactions individuelles avec une probabilité d'erreur très réduite. Le bureau d'enregistrement satisfait des clients qui mettent la protection de leur portefeuille de noms de domaine au premier plan et sont prêts à payer un supplément pour une assistance humaine (notamment, une assistance fournie par un spécialiste de compte chargé du client). Les clients peuvent, par exemple, vouloir la sécurité d'une confirmation orale ou écrite de la part du contact autorisé par le client avant d'exécuter une demande de changement et exiger une surveillance en temps réel des services de configuration du DNS et de résolution des noms de la part des bureaux d'enregistrement.

D'habitude, les mesures mentionnées ci-dessus font partie d'un ensemble plus vaste qui met l'accent sur la protection de la valeur de la marque. Les mesures de protection de la valeur de la marque cherchent à limiter les risques y compris l'abus de marques commerciales (à savoir, l'utilisation non autorisée d'une marque commerciale pour attirer des internautes vers un site autre que celui du détenteur de la marque commerciale), les enregistrements de noms de domaine qui ciblent le détenteur de la marque (domaines « homographes » visuellement similaires utilisés pour l'hameçonnage ou les attaques de fraude informatique), et le détournement de revenus ou de trafic, les « backorders » (tentatives d'enregistrement pour le compte d'un client de noms de domaine déjà enregistrés par d'autres parties au cas où ces noms de domaine seraient de nouveau disponibles), et les enregistrements défensifs (enregistrement d'une marque commerciale ou d'un nom dans tous les noms de domaine de premier niveau).

---

23 SAC023, Le service WHOIS est-il une source d'adresses de courrier électronique pour les polluposteurs ? http://www.icann.org/en/committees/security/sac023.pdf

24 Certains bureaux d'enregistrement mettent en œuvre des mesures anti-abus ou de sécurité pour protéger les systèmes internes (cruciaux pour l'entreprise), les processus et les bases de données. Ceux-ci sont généralement transparents à l'égard des clients d'un bureau d'enregistrement.

Qui a besoin de protection contre le piratage de comptes de noms de domaine et de DNS ?

Les mesures de protection puissantes contre l'altération malveillante de comptes de noms de domaine ou d'informations de configuration de DNS sont d'habitude bien connues et recherchées par les organisations qui ont des investissements importants dans des portefeuilles de noms de domaine ou des préoccupations de valeur de marque et qui ont les moyens et la volonté de payer pour protéger leurs marques. Toutefois, *les titulaires de noms de domaine ne devraient pas conclure que seules les sociétés ayant des marques ou une propriété intellectuelle à protéger, ont besoin de protection contre le piratage de compte de noms de domaine ou l'altération malveillante des paramètres de configuration DNS.* Nombre d'organisations pour lesquelles la présence en ligne est une question de vie ou de mort n'utilisent pas nécessairement des noms de domaine liés à une marque. D'autres pourraient facilement mener leurs activités sous n'importe quel nom de domaine qu'elles pourraient enregistrer. De telles organisations subiraient quand même des dommages ou des pertes financières si les noms qu'elles venaient à attribuer à leurs services Web, de poste électronique ou autres services sur Internet ne trouvaient pas les adresses IP qui leur sont associées (résolution des noms de domaine) là où leurs organisations hébergent ces services.

Étant donné que certaines organisations *gagneraient* à choisir des services d'enregistrement qui réduiraient sensiblement le risque associé à la perte d'un (de) nom(s) de domaine ou à l'altération malveillante des paramètres de configuration DNS, nous avons cherché à identifier de possibles raisons autres que les mesures de sécurité, pour lesquelles de telles organisations pourraient choisir un bureau d'enregistrement. Ci-suivent certaines raisons possibles :

Coût perçu en tant que tel : Dans certains cas, une organisation se trompe en pensant ou en concluant que le coût de l'enregistrement de noms de domaine par le biais d'un bureau d'enregistrement qui offre des mesures de protection rigoureuses contre le piratage de comptes de noms de domaine et de DNS est prohibitif.

Manque d'informations : Certains clients seraient disposés à payer pour des mesures de protection rigoureuses contre le piratage de comptes de noms de domaine et de DNS mais ne sont pas au courant de l'existence de tels services.

Informations erronées : Dans certains cas, l'organisation a conclu selon les informations disponibles limitées que tous les bureaux d'enregistrement offraient des mesures de protection similaires.

« Votre offre de services groupée ne convient pas à mon organisation » : Dans certains cas, une organisation serait disposée à payer pour certaines mesures de protection rigoureuses contre le piratage de comptes de noms de domaine et de DNS, mais n'est pas disposée ou capable de payer les services que certains bureaux d'enregistrement offrent (ou donnent l'impression d'offrir) en groupage, par ex. des mesures rigoureuses plus une protection de la valeur de la marque.

Dans ce contexte, certaines questions supplémentaires méritent d'être considérées :

Les organisations cherchant à protéger leurs marques sont-elles les seules intéressées par des mesures de protection de l'enregistrement plus rigoureuses ?

Non. Beaucoup d'organisations doivent mesurer le désir de protéger aussi bien leurs marques que leur présence en ligne en fonction du coût de protection. Certaines mesures de protection rigoureuses de l'enregistrement sont fréquemment offertes en complément de la protection de la valeur de la marque. Des mesures de protection rigoureuses de l'enregistrement, éventuellement offertes en plus des services d'enregistrement de base – comme service en option ou « contre paiement » ou les deux – pourraient rendre des aspects de sécurité souhaitables accessibles à des organisations motivées à investir dans des mesures de sécurité pour réduire l'éventualité de perte de disponibilité résultant d'une exploitation ou d'un mauvais usage.

Des organisations autres que celles qui ont des préoccupations de marque devraient-elles prendre en compte les noms de domaine lors de l'évaluation des risques et de la gestion des biens ?

Oui. Les rapports du SSAC ont expliqué les conséquences préjudiciables auxquelles les titulaires de noms de domaine sont confrontés lorsque leurs noms de domaine sont piratés, y compris les pertes financières, la gêne et l'atteinte à la réputation. [25] Les rapports du SSAC expliquent également les problèmes liés au non renouvellement des noms de domaine et ceux qui peuvent être causés par le non renouvellement d'un nom de domaine associé à un nom de serveur DNS.[26] En particulier, le SSAC mentionne dans le SAC010 que « les noms de domaine devraient être considérés comme des éléments d'actif ayant une valeur marchande, une valeur d'échange par courtage ou par vente directe, ou comme un moyen de générer des revenus récurrents » et que « les titulaires de noms de domaine qui ne renouvellent pas des noms de domaine enregistrés, de plein gré ou involontairement, devraient être conscients du fait que chaque nom de domaine représente potentiellement une valeur pour certains … et que de nouveaux titulaires pourraient utiliser un nom de domaine ayant expiré de manière pouvant s'avérer nuisible au titulaire précédent ».[27]

Quelles mesures de protection pourraient-elles être offertes à des organisations qui considèrent les noms de domaine comme des éléments d'actif pour les aider à gérer le risque et limiter les menaces contre leurs investissements dans les noms de domaine et leur dépendance vis-à-vis de ces derniers ?

---

[25] SAC007 : Rapport sur le piratage de noms de domaine (12 juillet 2005) http://www.icann.org/announcements/hijacking-report-12jul05.pdf

[26] SAC011 : Problèmes causés par le non renouvellement d'un nom de domaine associé à un nom de serveur DNS (7 juillet 2006) http://www.icann.org/en/committees/security/renewal-nameserver-07jul06.pdf

[27] SAC010 : Considérations de renouvellement à l'adresse des titulaires de noms de domaine (29 juin 2006) http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf

Certaines mesures utilisées dans d'autres secteurs d'activité sur Internet (par ex. financiers, négociants de biens de consommation durables) pourraient être utilement et pratiquement appliquées pour la protection des services d'enregistrement. Avant de considérer des mesures spécifiques, et profitant aux titulaires de noms de domaine en particulier, il est utile de réexaminer d'abord les principes : en particulier, comment les cadres de gestion de l'actif, de l'allocation automatique de ressources et du risque utilisés par les grandes organisations s'appliquent-ils aux enregistrements de noms de domaine ? Pourquoi considérer l'enregistrement d'un nom de domaine comme un élément de l'actif ?

Des rapports précédents du SSAC expliquent qu'un nom de domaine est une identité par laquelle une entité – un négociant, un établissement financier ou éducationnel, une entreprise ou une société à but lucratif ou non lucratif, un particulier ou un produit – est connue ou réalise des activités sur Internet. Ceci peut être le même nom que la société enregistre comme dénomination commerciale (doing business as), le nom d'une célébrité, d'un auteur, d'une personnalité politique ou autre. Aussi bien les particuliers que les organisations gèrent leurs noms (marques, marques de services, marques commerciales) dans le monde physique comme éléments d'actif et prennent des mesures pour les protéger contre le mauvais usage (statuts, brevets, droits d'auteur, etc.). Un nom de domaine est souvent le même que la marque, la marque de services, la marque commerciale. Les titulaires des noms de domaine devraient donc prendre des mesures pour protéger de tels noms non seulement en les enregistrant mais en les protégeant contre l'exploitation ou le mauvais usage.

L'enregistrement de noms de domaine garantit le caractère unique du domaine à l'échelle mondiale et associe le domaine à un titulaire pour autant que le titulaire du nom de domaine continue à payer les frais de renouvellement de l'enregistrement et à respecter ses obligations contractuelles (par ex. usage acceptable, exactitude de l'enregistrement). Ceci est donc équivalent à d'autres disciplines de gestion de réseau, tels que l'actif, le risque et l'allocation automatique de ressources.

Les noms de domaines sont également des identificateurs conviviaux qui peuvent se résoudre en utilisant le DNS pour établir les adresses Internet des hôtes qui fournissent des services à ce domaine (Web, messagerie électronique, réseaux sociaux, voix, etc.). La valeur opérationnelle du domaine – notamment, la garantie que la résolution du nom de domaine est largement disponible et que les noms dans un domaine se résolvent comme prévu – est d'une importance incommensurable pour la plupart des organisations.

Par exemple, dans le contexte d'un programme de gestion de l'actif et du risque, il est possible :

- d'identifier la valeur d'un élément de l'actif (corporel ou incorporel) ;
- d'énumérer les manières selon lesquelles cette valeur est menacée (perte, vol, mauvais usage) ;
- de déterminer comment la menace pourrait-elle être mise à exécution, à savoir ce qui rend le nom de domaine vulnérable à l'attaque ou à l'exploitation ?
- de déterminer la probabilité ou le risque de mise à exécution de chaque menace ;
- de déterminer comment le risque peut-il être atténué ou réduit ;

- de déterminer le coût de l'atténuation ou de la réduction du risque à un niveau de coût et de risque acceptable ; et
- d'établir le budget approprié et de mettre en œuvre l'atténuation ou la réduction du risque.

Si un nom de domaine est un élément de l'actif, il requiert la même rigueur que les autres éléments inventoriés, précieux ou sensibles. Vue sous cet angle, la gestion de l'enregistrement d'un nom de domaine semble partager beaucoup de caractéristiques avec la gestion de l'allocation automatique de ressources dans les réseaux de grande échelle. Par exemple, les opérations essentielles dans l'allocation automatique de ressources et l'enregistrement d'un nom de domaine sont {ajouter, supprimer, modifier}. Les meilleures pratiques appliquées dans la gestion de l'allocation automatique de ressources visent à garantir que ces opérations soient exécutées dans le bon ordre, par des parties autorisés, de manière opportune et vérifiable, impliquant une probabilité réduite d'omission, d'intrusion ou d'erreur. De telles meilleures pratiques devraient s'étendre à la gestion de l'enregistrement de noms de domaine et les services d'enregistrement devraient chercher à appliquer de meilleures pratiques similaires.

Les mesures de sécurité qui protègent les enregistrements de noms de domaine devraient être aussi importantes pour l'organisation que les mesures de sécurité que l'organisation met en place pour l'accès à intranet, à une base de données distante et à d'autres applications que l'organisation considère cruciales pour son activité. Afin de minimiser les chances d'omission, d'intrusion ou d'erreur dans la gestion de l'enregistrement de noms de domaine, les clients qui attribuent une valeur d'actif significative aux enregistrements de noms de domaine, devraient rechercher des services d'authentification, d'autorisation et de vérification qui ressemblent au même service qu'ils mettent en œuvre pour les autres applications cruciales pour leur activité. Certaines de ces mesures peuvent être mises en œuvre par le client. D'autres pourraient être incorporées dans les services d'enregistrement par les bureaux d'enregistrement qui décident que la prestation de mesures de sécurité supplémentaires offre un moyen de se différencier dans un marché hautement compétitif. Nous examinons ces mesures en détail dans les sections suivantes.

Mesures pour éviter le piratage de comptes de noms de domaine et de DNS

Nous décrivons dans cette section les mesures que certains bureaux d'enregistrement offrent aujourd'hui en tant que partie d'un ensemble de services, souvent conjointement avec la protection de la réputation en ligne (valeur de la marque). Ensuite, nous décrivons les mesures que les bureaux d'enregistrement pourraient offrir et que les parties interviewées dans le cadre de l'étude des incidents de 2008 par le SSAC ont identifié comme souhaitables ou essentielles. En dernier lieu, nous considérons les mesures que les grandes entreprises utilisent pour sécuriser l'accès aux applications à distance ainsi que les mesures que les établissements financiers et les cybermarchands fournissent pour protéger les comptes clients. Qu'elles soient offertes séparément en tant que services à sélectionner par le client ou dans le cadre d'une offre de services groupée, ces mesures amélioreraient la sécurité des comptes d'enregistrement de noms de domaine des clients motivés et disposés à investir dans des mesures de protection pour réduire le risque d'exploitation ou de mauvais usage du compte de noms de domaine. Les bureaux d'enregistrement sont encouragés à considérer dans quelle mesure la prestation de ces caractéristiques créerait des opportunités ou serait un moyen de les différencier dans un marché compétitif.

Les clients (titulaires de noms de domaine) jouent un rôle crucial dans la protection des noms de domaine. Dans cette section, nous décrivons brièvement certaines mesures complémentaires que les clients peuvent et devraient adopter pour (a) sécuriser leurs rôles dans la gestion électronique des processus entre titulaire de nom de domaine et bureau d'enregistrement, liée à la création et au renouvellement de l'enregistrement de noms de domaine et (b) sécuriser les processus de changement et de maintenance des paramètres de configuration et des informations de contact. Les bureaux d'enregistrement peuvent recommander de telles mesures aux clients détenteurs de portefeuilles de noms de domaine décisifs à travers des foires aux questions existantes ou nouvelles (FAQ) ou par d'autres moyens. Par exemple, les bureaux d'enregistrement sont encouragés à informer leurs clients de ce rapport et à le mettre à leur disposition, à les encourager à le consulter et à mettre en œuvre les mesures qu'ils considèrent nécessaires pour réduire ou limiter les risques qu'ils estiment menaçant le plus leurs portefeuilles de noms de domaine.

Le SSAC estime qu'une offre de services qui pourvoit à la protection de l'enregistrement d'un nom de domaine a un potentiel d'adoption plus élevé et peut être plus complète que la somme d'initiatives et de mises en œuvre indépendantes des petites et moyennes organisations. Nous basons cette affirmation sur la réussite remarquée des boîtiers de sécurité UTM (traitement unifié de la menace – *unified threat management*) : systèmes de sécurité informatique qui allient de nombreuses fonctionnalités pare-feu, filtrage anti-spam, logiciel anti-virus et autres fonctionnalités supplémentaires. Ils ont réussi une plus grande pénétration du marché auprès des petites et moyennes entreprises (PME) que les meilleures combinaisons de systèmes de sécurité offrant une seule caractéristique de sécurité. Nous estimons que la prestation de services de sécurité supplémentaires peut être déterminante dans l'enregistrement de noms de domaine des PME tout comme les UTM ont prouvé l'être.

Protéger l'accès au portefeuille de noms de domaine

Les mesures décrites dans cette section ont pour objectif de protéger contre l'accès non autorisé au compte de noms de domaine du client via une interface utilisateur (Web) en ligne ou un service d'assistance d'un bureau d'enregistrement ou d'un revendeur ou encore via des services d'assistance à la clientèle par téléphone.

Vérification de l'enregistrement. Un modèle d'enregistrement optimisé pour des volumes de transaction élevés et une allocation rapide de noms de domaine n'est souvent pas optimisé pour vérifier que le titulaire du nom de domaine est bien celui qu'il prétend être et que nulle fraude ou atteinte n'est commise durant le paiement. Des études d'anti-hameçonnage[28,29], l'expérience de la lutte contre les botnets (Srizbi, Conficker), et réseaux d'attaque en 'fast flux' illustrent le fait que les comptes d'enregistrement de noms de domaine sont une ressource clé pour les activités criminelles et continueront à l'être. La vérification des informations du point de contact transmises par le titulaire du nom de domaine lors de l'enregistrement et chaque fois que ces informations sont

---

28 Rapport sur les tendances des activités d'hameçonnage APWG, 2ème semestre 2008, http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf

29 Enquête sur l'hameçonnage au niveau mondial : Utilisation des noms de domaine et tendances au 2ème semestre 2008 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf

modifiées peut limiter l'usurpation d'identité et l'abus des noms de domaine. Les bureaux d'enregistrement sont encouragés à considérer offrir une vérification d'enregistrement par courrier électronique ; l'enregistrement du nom de domaine est complété uniquement lorsque le titulaire du nom de domaine confirme son adresse électronique en visitant un lien hypertexte incorporé dans un message électronique d'activation envoyé par le bureau d'enregistrement. En tant que mesure supplémentaire, certains établissements financiers contacteront le client au numéro de téléphone fourni au lieu d'envoyer un message électronique. L'entreprise fournit un numéro de confirmation par téléphone et le client doit le saisir sur un formulaire Web pour activer un compte ou autoriser une transaction. Le SSAC reconnaît qu'une mesure de cette nature retarde le traitement de l'enregistrement et la livraison du produit (la résolution de l'enregistrement et du nom de domaine enregistré), mais les bureaux d'enregistrement sont encouragés à mettre en balance ce retard et la valeur de la réduction des abus non seulement en ce qui concerne le client mais également la communauté Internet élargie. Un autre avantage consiste en le fait que les bureaux d'enregistrement visiblement dynamiques dans la sécurisation du système de noms de domaine sur Internet se bâtissent une réputation positive et sont d'habitude recommandés plutôt que d'autres par les professionnels de la sécurité et les collègues du secteur.

Améliorer le système d'authentification basé sur mot de passe. La méthode d'authentification prédominante parmi les bureaux d'enregistrement consiste en un simple nom d'utilisateur et mot de passe. Les bureaux d'enregistrement ne sont pas obligés d'imposer des contrôles de longueur, de durée de vie maximale ou de complexité des mots de passe et ne protègent peut-être pas contre les attaques de supposition en force en limitant le nombre de tentatives incorrectes d'ouverture de session. Les meilleures pratiques de sécurité communément acceptées recommandent que ces mesures soient présentes dans tout système d'authentification basé sur mot de passe.

Enregistrement du système. Les cybermarchands et les établissements financiers complètent maintenant les systèmes de mots de passe améliorés en permettant au client d'enregistrer l'ordinateur personnel (PC) ou l'adresse IP de laquelle il va administrer un compte.

Authentification multifactorielle. Les cybermarchands, les établissements financiers et même les opérateurs de jeux en ligne (jeux de rôle), offrent aux clients l'option d'ajouter un jeton d'authentification de matériel en tant que deuxième facteur de vérification de l'identité du client lors de la connexion à un compte. Le jeton ajoute « quelque chose que l'on a » à l'information consistant en « quelque chose que l'on sait » représentée par le mot de passe. Cette authentification bifactorielle rend plus difficile une intrusion de l'attaquant dans un compte de nom de domaine : même si l'attaquant devine ou obtient le nom d'utilisateur et le mot de passe d'un compte, il doit également prendre possession du jeton. Il existe aujourd'hui de nombreuses mises en œuvre de l'authentification bifactorielle, et la technologie s'étend sur de très grandes populations de clients. Le SSAC note que VeriSign a soumis une proposition de service d'authentification bifactorielle entre registres et bureaux d'enregistrement par le biais du processus d'évaluation des services des registres (RSEP) de l'ICANN. La proposition demande que « les noms d'utilisateurs et les mots de passe actuellement utilisés pour le traitement de requêtes d'actualisation, de transfert et/ou de suppression soient accompagnés par des codes de passe dynamiques » en tant que service librement

consenti et facultatif pour les bureaux d'enregistrement. [30] La phase 1 du déploiement proposé par VeriSign ajouterait une authentification bifactorielle entre le registre et le bureau d'enregistrement. Une deuxième phase rendrait ce service disponible aux demandes adressées par un titulaire de nom de domaine à son bureau d'enregistrement et comprenant le mot de passe à usage unique dans la transaction de protocole d'avitaillement extensible (EPP) entre le bureau d'enregistrement et le registre. Le SSAC encourage les bureaux d'enregistrement à examiner cette proposition et à considérer les avantages qu'ils pourraient tirer de leur participation. En plus de la considération de l'authentification bifactorielle telle que décrite ici, le SSAC recommande que les bureaux d'enregistrement prennent également en compte des méthodes et des directives d'authentification telles que la directive d'authentification électronique de l'Institut national des normes et de la technologie (NIST). [31]

Systèmes de défi. Certains établissements financiers recueillent des réponses à une série de questions personnelles d'identification lors de la création d'un compte. L'établissement choisit au hasard un sous-ensemble de ces questions et défie toute personne essayant de se connecter d'y répondre. D'autres demanderont à l'utilisateur une réponse à une paire image-légende secrète. Lorsqu'un client se connecte à son compte pour la première fois, il doit sélectionner une image secrète. Il soumet alors une légende d'image. Lors du processus d'authentification, le client doit mentionner la légende de l'image avant d'être requis de saisir son mot de passe. Les bureaux d'enregistrement sont encouragés à offrir cette mesure de sécurité en tant que service pouvant être sélectionné par les clients qui accepteraient les défis supplémentaires comme faisant partie du coût/dérangement pour la protection des noms de domaine et la prévention d'abus de configuration DNS.

Vérifications de l'accès par nom de domaine. L'accès à un compte d'enregistrement de noms de domaine accorde aux utilisateurs ainsi qu'aux attaquants un accès illimité à tous les noms de domaine enregistrés sous ce compte. Dans le monde réel, un modèle analogue au modèle communément rencontré de vérification d'accès à un compte d'enregistrement, serait un coffre-fort de banque sous forme de placard : une fois ce type de coffre-fort ouvert, vous pouvez en faire ce que vous voulez. Comparez-le à une chambre forte comprenant des coffres : dans ce cas, le client ou l'intrus doit non seulement obtenir l'accès à la chambre forte mais également la(les) clé(s) de chaque coffre séparé. Les bureaux d'enregistrement sont encouragés à considérer la prestation d'un modèle d'accès similaire aux clients qui sont à la recherche d'une plus grande protection ; par ex. une caractéristique sélectionnable pourrait accorder aux clients la possibilité de contrôler quels points de contact peuvent procéder à des changements d'informations de contact et de configuration DNS, démarrer ou autoriser un transfert de nom de domaine, etc.

Points de contact uniques multiples. Les organisations ont intérêt à maintenir des informations de points de contact précises dans les registres d'enregistrement des noms de domaine. Certaines

---

[30] Service d'authentification bifactorielle registre-bureau d'enregistrement http://www.icann.org/en/registries/rsep/

[31] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

organisations ont également intérêt à faire correspondre à chaque point de contact requis, une personne ou une position unique dans l'organisation : ceci répartit le risque au cas où un initié revendiquerait la propriété ou tenterait de pirater un nom de domaine de son employeur ou du client de son employeur. Le SSAC recommande ces mesures aux titulaires de noms de domaine qui veulent protéger leurs noms de domaine contre les abus d'initiés. Ces mesures offrent également des perspectives aux bureaux d'enregistrement qui gèreraient les informations de contact pour le compte des titulaires de noms de domaine. Par exemple, un bureau d'enregistrement pourrait vérifier et demander des coordonnées de points de contact uniques, notamment concernant le mode de correspondance préféré (adresse de courrier électronique) en tant que caractéristique de service sélectionnable. Le titulaire du nom de domaine et le bureau d'enregistrement peuvent utiliser des points de contact uniques pour créer un modèle accordant des privilèges de manière granulaire. Par exemple, certaines organisations peuvent vouloir s'assurer que seul le point de contact du titulaire du nom de domaine peut transférer un nom de domaine, ou que seul le point de contact technique peut modifier une configuration DNS (d'autres modèles existent, et ceux-ci sont présentés ici uniquement à titre d'illustration). Les bureaux d'enregistrement peuvent encourager les titulaires de noms de domaine à choisir ces mesures en les combinant avec d'autres, telles qu'une confirmation interactive ou des processus de notification de plusieurs destinataires.

Confirmations ou notifications de changements. Certaines organisations se protègent contre des changements non autorisés ou erronés en créant une gestion électronique des travaux dans le cadre de laquelle certaines actions requièrent la confirmation de plusieurs parties. Les confirmations multiples améliorent les défenses d'une organisation contre l'usurpation d'identité : un attaquant doit psychologiquement pirater ou usurper l'identité de deux parties et non pas d'une seule. Certaines organisations peuvent être intéressées par la sélection d'un service où les bureaux d'enregistrement vérifient et requièrent de multiples points de contact uniques. Ainsi, de telles organisations peuvent élargir la gestion électronique qu'elles utilisent en interne pour englober les changements de points de contact, les transferts de noms de domaine, ou la configuration DNS. Pour les organisations qui ne disposent pas de gestion électronique des travaux, les bureaux d'enregistrement pourraient offrir un service facultatif permettant cette gestion pour le compte du client. Par exemple, lors de l'enregistrement initial, un service de confirmation de changement du bureau d'enregistrement pourrait vérifier que le client a bien soumis un point de contact unique pour chaque contact requis et lié au nom de domaine. Ceci pourrait également permettre au client de choisir les points de contact qui doivent être notifiés lors d'une requête de changement de configuration DNS, ou d'exiger que les contacts technique et administratif répondent par téléphone ou par courrier électronique avant de procéder à un changement requis par une partie. De plus, la confirmation du changement peut aider à éviter un transfert de nom de domaine vindicatif ou opportuniste. Considérez, par exemple, une situation dans laquelle un employé désigné comme point de contact a quitté l'organisation et l'organisation a omis de remplacer les coordonnées de cet employé par celles de son remplaçant. Si l'employé est parti mécontent, il pourrait tenter de revendiquer le nom de domaine à travers un transfert de nom de domaine. Dans le scénario de confirmation des changements, les autres contacts sont requis de confirmer le transfert et la tentative de transfert pourrait être bloquée.

Notifications de destinataires multiples. Pour correspondre avec les clients, les bureaux d'enregistrement utilisent systématiquement le courrier électronique. Le SAC028 « Usurpation d'identité des bureaux d'enregistrement lors d'attaques d'hameçonnage », mentionne plusieurs correspondances communes y compris :

- Les avis de renouvellement de noms de domaine ;
- Les confirmations de commande de noms de domaine ;
- Les confirmations de demande d'enregistrement ;
- Les changements des coordonnées de contact du nom de domaine et des paramètres DNS ;
- Les rappels d'exactitude des données WHOIS ;
- Les avis d'expiration ou d'annulation de noms de domaine ; et
- Les offres, la publicité de (nouveaux) services et caractéristiques.

Offrir l'option d'envoi d'une telle correspondance à des destinataires multiples aide le client de plusieurs manières. Par exemple, le client pourrait éviter d'être la victime d'une usurpation d'identité du bureau d'enregistrement lors d'une attaque d'hameçonnage : un des destinataires du client pourrait être dupé par le courriel hameçon mais un autre pourrait reconnaître le message fantôme et alerter le bureau d'enregistrement et les autres contacts au sein de son organisation. De même, si le bureau d'enregistrement devait délivrer des avis de renouvellement de noms de domaine à des destinataires multiples, ceci protègerait contre une situation dans laquelle une erreur ou une omission du client pourrait dans le cas contraire conduire à la déchéance de l'enregistrement. Par exemple, un renouvellement pourrait prendre fin si le seul destinataire d'un avis de renouvellement était en congé prolongé et loin de sa messagerie électronique. Dans un scénario de destinataires multiples, cette expiration de l'enregistrement pourrait être évitée si d'autres destinataires recevaient également les avis de renouvellement. Les bureaux d'enregistrement peuvent également considérer les méthodes que certains établissements financiers utilisent pour aider leurs clients à identifier des accès aux comptes non autorisés. Le bureau d'enregistrement peut tenter de délivrer des notifications ou des confirmations en utilisant la version originale et la version modifiée des coordonnées de contact, pour améliorer la probabilité que le message soit délivré à la destination correcte indépendamment du fait que le changement soit voulu ou frauduleusement soumis, et indépendamment du fait que le message ait été transmis avant ou après que le changement ne soit entré en vigueur.

Méthodes de livraison multiples pour la correspondance essentielle. Plutôt que de se fier totalement au courrier électronique pour correspondre avec les clients, les bureaux d'enregistrement pourraient offrir une transmission des notifications essentielles par téléphone, télécopie, poste ou coursier aux clients qui recherchent une protection supplémentaire. De tels services pourraient rendre les transferts non autorisés très difficiles pour un attaquant. Les clients qui prévoient renouveler « pour toujours » des noms de domaines d'une importance cruciale, accueilleraient cette protection (laquelle n'a aucun impact dans le cours normal des affaires). Les clients qui exécutent des transferts de noms de domaine d'une importance cruciale peuvent également, après avoir réalisé une analyse des risques/bénéfices, considérer que le retard dans la « transaction » de transfert introduit ainsi est acceptable.

Éveiller l'intérêt du client. Beaucoup de grandes organisations sont habituées à externaliser la gestion du réseau, de la sécurité et de l'accès à Internet. Les services gérés sont également de plus en plus populaires parmi les petites et moyennes entreprises. Les fournisseurs de services gérés (MSP) mettent l'accent sur le partenariat client-fournisseur. Par des foires aux questions ou des programmes de sensibilisation et d'éducation réalisés par webinaires ou baladodiffusion, le MSP explique comment les clients peuvent tirer les meilleurs avantages possibles des services qu'il leur

offre. En plus des mesures décrites ci-dessus, les bureaux d'enregistrement pourraient former et encourager les titulaires de noms de domaine à :

- identifier de multiples points de contact de compte de noms de domaine
- inclure l'administration des informations relatives aux points de contact dans le processus de gestion des ressources humaines pour s'assurer que lorsque les qualifications d'un employé sortant sont retirées, toutes les informations de point de contact d'enregistrement de noms de domaine associées à cet employé sont également modifiées
- imposer une politique de changement de mot de passe
- vérifier les contacts périodiquement
- surveiller l'enregistrement du nom de domaine de manière proactive
- attribuer des adresses de courrier électronique à tous les points de contact d'enregistrement dans un nom de domaine différent du nom de domaine enregistré. (certains titulaires de noms de domaine peuvent vouloir créer de multiples comptes d'enregistrement de noms de domaine comme mesure de protection supplémentaire)
- traiter les tentatives de transfert comme étant des évènements liés à la sécurité (vérifier et revérifier)
- utiliser un nom de domaine pour les comptes de messagerie électronique des contacts d'enregistrement différent de ceux utilisés à d'autres fins commerciales. Par exemple, attribuer des adresses de courrier électronique example.net aux points de contact du nom de domaine example.info
- créer des comptes de rôle (non associés à une personne en particulier mais à une position) : par ex. domainadmincontact@example.com, domainregistrantcontact@example.biz, domaintechnicalcontact@example.net. (Notez que lorsque des comptes de rôle sont utilisés, les vérifications périodiques desdits comptes sont fortement recommandées pour confirmer que le compte de rôle est suivi par un membre du personnel du titulaire du nom de domaine sans interruption due à des changements de personnel, administratifs ou opérationnels au sein de l'organisation)
- alias de destinataires multiples des notifications adressées à un compte de rôle. Utiliser cette forme de liste de diffusion pour fournir une couverture (*blanket delivery*) de la correspondance importante du bureau d'enregistrement et augmenter la probabilité de réception et de traitement opportun de cette correspondance.

Informer le client. Les bureaux d'enregistrement devraient faire l'effort d'être aussi clairs que possible concernant les types de mesures de sécurité qu'ils fournissent comme ils le sont concernant les autres prestations compétitives. Par exemple, un bureau d'enregistrement qui soumet régulièrement ses activités à un audit de sécurité indépendant et passe l'audit, pourrait attirer

l'attention du public sur cette discipline qu'il s'est auto-imposée. Sinon, l'ICANN et les bureaux d'enregistrement pourraient conjointement désigner un vérificateur de sécurité indépendant et établir un contrat avec ce vérificateur pour définir une série de mesures de sécurité obligatoire. Les bureaux d'enregistrement pourraient *de plein gré* demander à ce vérificateur de réaliser un audit de leurs opérations. Pour avoir satisfait à l'exercice de performances de sécurité, les bureaux d'enregistrement qui réussissent l'audit pourraient recevoir une sorte de marque ou de cachet de confiance. Des programmes similaires sont disponibles auprès des autorités de certification SSL.[32,33] Le SSAC note que le traitement de cartes de crédit est commun parmi les bureaux d'enregistrement et que les procédures d'audit sécurité de l'industrie des cartes de paiement (PCI) relatives aux exigences de conformité du marchand et du fournisseur de services aux normes de sécurité des données (DSS) seraient peut-être utiles dans ce cadre.[34]

Mesures mentionnées dans les rapports précédents du SSAC. Beaucoup de bureaux d'enregistrement ont mis en œuvre certaines ou l'ensemble des mesures recommandées dans la section 5.2 du SAC007, « Rapport sur le piratage des noms de domaine, *démarches que les bureaux d'enregistrement peuvent entreprendre pour protéger les noms de domaine* ». Elles sont résumées par la suite afin de fournir un compendium des mesures recommandées nouvelles et précédentes :

1. Utiliser une seule valeur de code EPP authInfo pour chaque nom de domaine enregistré (et non pas pour chaque compte de titulaire de nom de domaine). Certains bureaux d'enregistrement utilisent une seule valeur de code EPP authInfo pour tous les noms de domaine détenus par le même titulaire. Cette pratique expose tous les noms qu'un client a enregistrés à un piratage basé sur un code unique.

2. Établir une définition par défaut uniforme de verrouillages de noms de domaine par tous les bureaux d'enregistrement. Beaucoup de bureaux d'enregistrement verrouillent déjà automatiquement les noms de domaine. Les bureaux d'enregistrement doivent fournir des moyens suffisamment directs pour le déverrouillage afin de ne pas interdire, mal à propos, une requête de transfert légitime de la part d'un titulaire de nom de domaine vérifié.

3. Explorer des méthodes supplémentaires d'amélioration de l'exactitude des registres du titulaire du nom de domaine. Considérer une correspondance plus fréquente ou de forme variée (par ex. par téléphone alternativement au courrier électronique) pour encourager les titulaires de noms de domaine à maintenir leurs coordonnées à jour et pour détecter les abus d'enregistrement.

4. Rassembler les coordonnées de points de contact d'urgence des titulaires de noms de domaine, des bureaux d'enregistrement et des revendeurs correspondant à des personnes pouvant assister et réagir pour un rétablissement urgent en cas d'incident lié à un nom de

---

32 Certificat numérique Thawte, https://www.thawte.com/ssl-digital-certificates/trusted-site-seal/index.html?click=site-seal-tile

33 Certificat numérique VeriSign Secured Seal®, http://www.verisign.com/ssl/secured-seal/

34 Conseil des normes de sécurité PCI, https://www.pcisecuritystandards.org/

domaine. [35] Définir des processus progressifs (procédures d'urgence) que toutes les parties conviennent pouvoir mettre en marche au cas où les contacts d'urgence ne seraient pas disponibles.

5. Considérer des mesures visant à améliorer l'authentification et l'autorisation utilisées dans tous les processus commerciaux des bureaux d'enregistrement.

6. Protéger les coordonnées du titulaire du nom de domaine qui peuvent être utilisées pour faciliter la fraude, l'usurpation d'identité et le vol d'un nom de domaine. Par défaut, traiter toutes les informations utilisées dans les processus d'authentification du titulaire du nom de domaine comme confidentielles. Pour le traitement de ces informations, considérer l'utilisation des mêmes mesures ou de mesures similaires à celles utilisées pour protéger les informations liées aux cartes de crédit ou autres instruments financiers.

7. Améliorer l'audit de conformité des revendeurs aux exigences de tenue des registres.

8. Veiller à ce que les revendeurs comprennent les exigences de tenue des registres des bureaux d'enregistrement (et de l'ICANN) et améliorent la conformité à ces exigences.

9. Fournir des informations claires et facilement accessibles aux titulaires des noms de domaine concernant le verrouillage des noms de domaine et les mesures de protection des noms de domaine offertes par les bureaux d'enregistrement.

Protéger les paramètres de configuration DNS contre les abus

Un des buts de l'obtention d'un accès non autorisé à un compte d'enregistrement de noms de domaine est de prendre le contrôle du service de résolution de nom de l'organisation. Un attaquant modifie le nom ou l'adresse IP des serveurs de noms de sa cible pour les pointer vers un système qu'il opère, d'habitude un ordinateur qu'il a auparavant compromis. L'attaquant héberge sur l'ordinateur compromis un serveur DNS et fichier de zone pour le nom de domaine attaqué. Le serveur DNS de l'attaquant résout les noms du domaine attaqué et les redirige vers des sites Web malveillants ou défacés (comme c'était le cas dans les incidents ayant affecté Comcast, l'ICANN, Panix, et Hush communications décrits dans ce document et dans le SAC007). Certains attaquants n'altèrent pas les paramètres de configuration DNS ; ils utilisent plutôt des comptes d'enregistrement de noms de domaine compromis pour ajouter leurs propres serveurs de noms à une liste de serveurs de noms autrement légitimement gérée. Ceci sert à dissimuler les serveurs de noms qu'ils utilisent dans les variantes '*double flux*' des attaques en 'fast flux'[36] et peut également entraver les démontages. Les deux prolongent la durée de l'hameçonnage, du pollupostage, de la fraude ou des attaques criminelles.

Les mesures décrites dans la section précédente sont applicables dans le cadre des services visant à protéger contre l'utilisation non autorisée d'un compte de noms de domaine d'un client pour

---

35 Voir également SAC 038, Points de contact des bureaux d'enregistrement en cas d'abus, http://www.icann.org/committees/security/sac038.pdf

36 SAC 025 Hébergement 'fast flux' et DNS, http://www.icann.org/committees/security/sac025.pdf

modifier de manière malveillante ou ajouter furtivement des informations de configuration DNS. En particulier, les mesures suivantes, offertes en option par un bureau d'enregistrement ou appliquées par un titulaire de noms de domaine, pourraient fournir une protection importante contre les attaques de configuration DNS :

- Exiger une authentification multifactorielle pour des changements de configuration DNS.
- Exiger des confirmations de changement de la part de contacts multiples par courrier électronique et, éventuellement, par d'autres moyens de transmission. (Note : les mêmes types de méthodes de vérification à étapes multiples décrites plus haut pourraient être appliqués dans ce cas).
- Envoyer des notifications à des contacts multiples lorsque des changements sont réalisés.
- Surveiller les changements de DNS pour détecter les anomalies ou l'abus.

Encore une fois, par le biais de foires aux questions, de formation, et d'éducation, les bureaux d'enregistrement devraient encourager les clients à surveiller systématiquement l'activité de configuration DNS (changements et ajouts). Les bureaux d'enregistrement devraient également encourager les clients à vérifier que les noms de leur domaine résolvent vers les adresses IP prévues. De plus, les bureaux d'enregistrement devraient exhorter leurs clients à maintenir un historique des configurations DNS pour tous les noms de domaine et devraient les aider à comprendre la valeur de l'application d'une estampille temporelle et d'une signature numérique sur ces informations.

Conclusions

Des incidents et de l'étude y liée contenus dans ce rapport, le SSAC tire les conclusions supplémentaires suivantes :

Conclusion (1) Il existe des différences entre les bureaux d'enregistrement en matière de vulnérabilité à l'attaque et de degré de protection offert contre les attaques de comptes de noms de domaine. Beaucoup de titulaires de noms de domaine ne semblent pas avoir les informations suffisantes pour évaluer la mesure dans laquelle un bureau d'enregistrement est capable de protéger leurs comptes de noms de domaine contre l'attaque et leurs configurations DNS contre une modification malveillante.

Conclusion (2) Alors qu'un grand nombre de bureaux d'enregistrement offre des services d'enregistrement de noms de domaine orientés vers le consommateur, et un groupe plus réduit de bureaux d'enregistrement et d'entreprises de « gestion de marque » offre des services de sécurité à des détenteurs de noms de domaine très en vue et hautement ciblés (d'habitude dans le cadre d'un service de protection global de valeur de la marque), le SSAC note que les *fournisseurs de services d'enregistrement « purs et sûrs »* sont rares, en partie compte tenu du fait que l'évaluation des mesures de sécurité n'occupe pas le rôle de premier plan qu'elle devrait occuper dans les décisions des clients relatives au choix d'un bureau d'enregistrement.

Conclusion (3) Les bureaux d'enregistrement pourraient mettre plus d'informations relatives à leurs services de sécurité, à la disposition des clients afin que ces derniers puissent prendre des décisions averties. La soumission volontaire de leurs opérations à un audit de sécurité indépendant et l'annonce à grand renfort de publicité des résultats positifs de tels audits permettraient aux clients de choisir un bureau d'enregistrement sur la base des exigences de sécurité, du coût et des services annexes (tels que l'hébergement Web et DNS).

Conclusion (4) Les services des bureaux d'enregistrement (et les titulaires des noms de domaine) accordent plus de confiance à l'authentification unifactorielle de la connexion aux comptes que la méthode ne le mérite. Cette méthode d'authentification a été à maintes reprises déjouée par diverses formes de piratage psychologique, d'attaques en force, et d'autres techniques.

Conclusion (5) Les attaquants visent la configuration DNS lorsqu'ils réussissent à compromettre un compte d'enregistrement de noms de domaine. Compte tenu de la nature distribuée du DNS, les effets d'une altération des paramètres de configuration DNS persistent au-delà des efforts de reprise et d'atténuation déployés par les bureaux d'enregistrement. Des informations de DNS malveillantes ou incorrectes peuvent persister dans des emplacements à travers l'Internet pendant toute la durée de la valeur TTL associée au(x) registre(s) de ressources DNS altéré(s). Les attaquants peuvent altérer le TTL spécifiquement dans ce but.

Conclusion (6) D'habitude, lorsqu'un utilisateur est authentifié par le portail d'un compte d'enregistrement ou à la connexion, l'utilisateur (ou l'imposteur) détient *tous* les privilèges et peut

modifier les informations de contact ainsi que les informations de configuration DNS. Mettre des contrôles d'accès granulaires à disposition des clients en tant qu'option – notamment, la capacité de limiter le type d'actions que chaque point de contact peut exécuter au regard de changements d'informations de contact et de configuration DNS et d'autorisation de transferts – pourrait réduire ou limiter le risque d'exploitation ou de mauvais usage de noms de domaine et de services de résolution de noms associés à ces noms de domaine.

Conclusion (7) Les fournisseurs de services d'enregistrement se fient plus fortement au courrier électronique non confirmé pour la correspondance liée à la sécurité (par ex. des notifications de changement) que la garantie de transmission du courrier et les caractéristiques de sécurité ne le méritent. Les attaquants mettent souvent en échec cette méthode de correspondance et empêchent la livraison de courrier électronique lorsqu'ils modifient la configuration DNS de noms de domaine par le biais de comptes d'enregistrement compromis. Offrir aux clients le choix de moyens de contact de remplacement ou élargir les services de notification pour inclure une certaine forme d'accusé de réception pourrait réduire ou limiter le risque d'exploitation ou de mauvais usage de noms de domaine et de services de résolution de noms associés à ces noms de domaine.

Recommandations

Le SAC007 faisait des recommandations spécifiques à l'adresse des bureaux d'enregistrement, notamment

Recommandation SAC007-(8) : *Les bureaux d'enregistrement devraient améliorer la prise de conscience du titulaire du nom de domaine quant aux menaces de piratage du nom de domaine, d'usurpation d'identité du titulaire et de fraude, et mettre l'accent sur le besoin qu'ont les titulaires de noms de domaine de maintenir des informations d'enregistrement précises. Les bureaux d'enregistrement devraient également informer les titulaires de noms de domaine de la disponibilité et du but du verrouillage Registrar-Lock, et les encourager à l'utiliser. Les bureaux d'enregistrement devraient également informer les titulaires de noms de domaine du but des mécanismes d'autorisation (EPP authInfo), et devraient élaborer des pratiques à recommander aux titulaires de noms de domaine pour la protection de leurs noms de domaine. Lesdites pratiques devraient comprendre la surveillance du statut du nom de domaine et la maintenance opportune et précise des informations de contact et d'authentification.*

Sur la base de nos analyses des incidents récents, de notre étude pertinente et de nos conclusions, le SSAC fait les recommandations suivantes :

Recommandation (1) Les bureaux d'enregistrement sont encouragés à offrir aux clients qui les demandent ou qui en ont besoin, des niveaux de protection plus renforcés contre l'exploitation ou le mauvais usage de services d'enregistrement de noms de domaine. Les mesures énumérées dans ce rapport peuvent être offertes en option aux clients, en tant que services séparés ou groupés.

Recommandation (2) Les bureaux d'enregistrement devraient élargir les foires aux questions et les programmes d'éducation qu'ils offrent aux titulaires de noms de domaine pour inclure la sensibilisation à la sécurité. Les bureaux d'enregistrement devraient rendre les informations relatives aux services qu'ils offrent en matière de protection des comptes d'enregistrement des noms de domaine plus accessibles aux clients. Ces derniers pourraient ainsi prendre des décisions averties concernant les mesures de protection lorsqu'ils choisissent un bureau d'enregistrement.

Recommandation (3) Les bureaux d'enregistrement devraient considérer la valeur de la mise en œuvre d'un audit de sécurité indépendant et volontaire de leurs activités comme composante de leur vigilance en matière de sécurité.

Recommandation (4) L'ICANN et les bureaux d'enregistrement devraient examiner la mesure dans laquelle les services d'enregistrement pourraient généralement s'améliorer et les titulaires de noms de domaine pourraient profiter de l'existence d'une tierce partie indépendante qui, *à la demande d'un bureau d'enregistrement*, réaliserait un audit de sécurité basé sur une série de mesures de sécurité définie au préalable. L'ICANN distinguerait les bureaux d'enregistrement qui ont volontairement satisfait les tests de performance de cet audit de sécurité à travers un programme

de marque de confiance de sécurité mis en œuvre de manière similaire à celle appliquée par les autorités de certification SSL qui accordent des marques ou des cachets de confiance aux opérateurs de sites Web qui satisfont aux critères de sécurité desdites autorités.

Remerciements

Le comité souhaite remercier les membres suivants pour le temps qu'ils ont consacré, l'expertise qu'ils ont mis à contribution et la révision au cours de l'étude réalisée par le SSAC :

Jaap Akkerhuis

KC Claffy

Steve Crocker

Patrik Fältström

Duncan Hart

Jeremy Hitchcock

Rodney Joffe

Warren Kumari

Danny McPherson

Dave Piscitello

Dan Simon

John Schnizlein

Bruce Tonkin

Rick Wesson

Richard Wilhelm

Déclarations d'intérêt

Les informations biographiques et les déclarations d'intérêt des membres du SSAC sont disponibles à l'adresse : http://www.icann.org/en/committees/security/biographies.htm.

Objections

Aucun membre du comité n'a soulevé des objections à la publication de ce rapport.