25 février 2009

SAC 038 : Point de contact des bureaux d’enregistrement en cas d’abus :

Introduction et contexte

Les accords actuels de gTLD de l’ICANN exigent des registres et des bureaux d’enregistrement de mettre en place un service Whois. La clause 3.3.1[1] de l'accord d’accréditation de bureau d’enregistrement identifie les coordonnées de contact que les bureaux d’enregistrement et leurs agents (revendeurs) doivent recueillir de leurs candidats lorsqu’ils enregistrent un nom de domaine. Les coordonnées de contact d'enregistrement servent habituellement comme moyen de communication initial avec le titulaire d’un nom de domaine ou l’opérateur (administrateur) d’un hôte Internet (serveur) auquel un label est assigné dans ce domaine. Les parties identifiées comme contacts pour un nom de domaine peuvent être contactées pour une variété de motifs y compris des enquêtes générales (par ex. commerciales), des tentatives de notification du titulaire d’une configuration DNS erronée et des enquêtes concernant l’implication éventuelle du nom de domaine dans une activité malveillante, illégale ou criminelle.

Les organismes d’application de la loi, les équipes de réponse aux urgences informatiques (CERT), la communauté anti-hameçonnage et anti-crime (intervenants), les entreprises qui fournissent des services de protection de la réputation en ligne, les opérateurs de réseaux, et les internautes peuvent tenter de contact les bureaux d’enregistrement accrédités par l’ICANN lorsqu’ils ne sont pas capable de communiquer avec un titulaire de nom de domaine en utilisant les coordonnées de contact obtenues des services Whois. Dans le cas de domaines de premier niveau génériques, le registre Whois devrait toujours identifier le nom du bureau d'enregistrement accrédité par l'ICANN (le bureau d'enregistrement commanditaire). Ainsi, les utilisateurs devraient toujours être capables d’obtenir le nom du bureau d’enregistrement qui commandite un nom de domaine en demandant les informations d’enregistrement d’un nom de domaine via un service Whois. L’utilisateur doit alors rechercher les coordonnées de contact du personnel de ce bureau d’enregistrement chargé du traitement des abus, à partir d'une des sources éventuelles.

Il existe de multiples listes et sources pour contacter les bureaux d’enregistrement, mais les parties pouvant être jointes grâce à ces sources de coordonnées de contact ne sont pas toutes en mesure de traiter une plainte pour abus ou de s'occuper d'une complainte pour infraction criminelle. Dans les cas où un point de contact explicite pour les cas d’abus est

[1] Voir http://www.icann.org/en/registrars/ra-agreement-17may01.htm#3.3.1.

fourni sur le site Web du bureau d'enregistrement, l'intervenant a souvent accès à un agent responsable du bureau d'enregistrement. Dans les cas où les coordonnées de contact en cas d'abus ne sont pas en évidence ou facilement situées sur le site Web du bureau d'enregistrement, les tentatives de règlement d'un litige ou d'enquête sur une plainte pour abus peuvent être retardées alors que l'utilisateur essaie de localiser les coordonnées de contact appropriées.

Les utilisateurs peuvent également accéder à la liste publique de coordonnées de contact de bureaux d'enregistrement de l'ICANN. Les bureaux d'enregistrement doivent fournir à l'ICANN les coordonnées de contact principales pour la réception des avis contractuels. Les bureaux d'enregistrement ne sont pas contractuellement obligés de maintenir des coordonnées de contact publiques, ni de disposer d'un point de contact séparé pour les cas d'abus. Actuellement, l'ICANN permet aux bureaux d'enregistrement de fournir une alternative publique à leurs coordonnées de contact principales (contractuelles) et l'ICANN publie cette alternative[2]. Si les bureaux d'enregistrement choisissent de ne pas fournir à l'ICANN des coordonnées publiques séparées, l'ICANN publie les coordonnées de contact principales. Le point de contact identifié sur la liste de l'ICANN peut, encore une fois, ne pas être la partie appropriée chargée de poursuivre une plainte pour abus ou une complainte pour infraction criminelle.

Problématiques

Les exigences actuelles portant sur des coordonnées de contact publiquement accessibles peuvent ne pas satisfaire les besoins de la communauté pour les raisons suivantes :

- Des coordonnées de points de contact de diverses natures sont publiées pour les bureaux d'enregistrement. Elles ne correspondent pas toutes à des points de contact appropriés pour le traitement de plaintes pour abus ou de complaintes pour infractions criminelles. Identifier le point de contact approprié peut retarder une enquête.

- Les utilisateurs qui enquêtent sur ou vérifient un abus et des activités illégales impliquant potentiellement un nom de domaine, doivent se fier à la bonne volonté des bureaux d'enregistrement en matière de publication de coordonnées de contact facilement accessibles. Les informations anecdotiques transmises au SSAC indiquent que :

    a) les bureaux d'enregistrement ne publient pas tous de plein gré des coordonnées de contact publiques sur leurs sites Web,
    b) les coordonnées de contact publiées ne sont pas toutes précises ou complètes,
    c) le personnel joint par le biais de certaines coordonnées de contact publiées peut être incapable de traiter des enquêtes sur abus ou ne pas être familiarisé avec les procédures qui mettraient un enquêteur en contact avec la personne adéquate (par ex. technique) et
    d) les bureaux d'enregistrement ne publient pas tous des coordonnées de contact séparé pour les cas d'abus.

[2] Voir http://www.internic.net/regist.html.

- Un contact public peut n'être disponible que durant des heures ouvrables spécifiques, alors qu'un contact en cas d'abus devrait être disponible 24 heures sur 24, 7 jours sur 7. Les enquêtes impliquant un abus ou des activités criminelles présumées nécessitent d’habitude des réponses opportunes voire urgentes. Par exemple, les enquêtes qui conduiront à la suspension d’un nom de domaine utilisé dans une attaque d’hameçonnage, en appui à une activité illégale (hébergement de pornographie infantile ou ventes illégales de médicaments délivrés sur ordonnance) sont idéalement traitées en quelques heures. Dans le cas d’une attaque « double flux »[3], des minutes de retard fournissent à un attaquant assez de temps pour dévier son vecteur d'attaque vers d'autres noms de domaine qu'il a enregistrés ou sur lesquels il a obtenu un contrôle non autorisé.

[3] Voir SAC 025, Hébergement ‘fast flux’ et DNS, http://www.icann.org/committees/security/sac025.pdf

Recommandations

Le SSAC recommande que les bureaux d’enregistrement et les revendeurs assistent l'enquête sur et l’atténuation des abus et activités illégales dans les cas où les attaquants exploitent des services d'enregistrement et de résolution de noms de domaine. Nous recommandons que l’organisation de soutien aux politiques des noms génériques (GNSO) considère ce qui suit et agisse en conséquence :

1. Chaque bureau d’enregistrement devrait fournir des coordonnées de contact en cas d’abus.

    - Le point de contact en cas d’abus devrait être réceptif et performant. La personne de contact en cas d'abus doit répondre au téléphone et aux courriels rapidement, les personnes chargées de traiter les abus doivent être autorisées à agir de manière efficace, et doivent disposer de critères bien définis concernant leurs actions. Le GNSO devrait considérer les critères de disponibilité et d’accès aux points de contact en cas d’abus (par ex. 24 heures sur 24, 7 jours sur 7 ou heures ouvrables normales), et le temps moyen de réponse à une complainte. L’ICANN et les bureaux d’enregistrement devraient considérer comment la conformité à ces critères serait évaluée.

    - Les bureaux d’enregistrement devraient fournir aux demandeurs un moyen bien défini et vérifiable de suivi des complaintes pour abus (par ex. un système de billetterie ou de suivi similaire). Le GNSO devrait examiner comment la performance d’un bureau d’enregistrement peut-elle être mesurée et évaluée en termes de conformité.

2. Les bureaux d’enregistrement devraient publier les coordonnées de contact en cas d’abus.

    - Le bureau d’enregistrement identifié dans le champ de bureaux d'enregistrement commanditaires d’une entrée Whois devrait avoir un contact en cas d’abus affiché en évidence sur sa page Web. Pour aider la communauté à localiser cette page, le SSAC recommande que les bureaux d'enregistrement considèrent une convention de nommage uniforme pour faciliter la découverte (automatisée et rapide) de cette page, c’est-à-dire, http://www.<registar>.<TLD>/abuse.html.

    - Les bureaux d’enregistrement devraient fournir leurs coordonnées de contact en cas d’abus à l’ICANN qui devrait publier ces coordonnées sur http://www.internic.net/regist.html.

3. Les coordonnées qu’un bureau d’enregistrement publie concernant le point de contact en cas d’abus devraient correspondre aux coordonnées de contact proposées en tant que modification de la section 3.16 du RAA. Chaque méthode de contact (téléphone, courriel, adresse postale) devrait joindre une personne ou une organisation capable d’assister en cas de plainte pour abus ; par exemple, aucun contact ne devrait rejeter

délibérément des demandes postales ou par courriel.

- Le GNSO devrait identifier ce qui constitue des coordonnées appropriées de contact en cas d’abus, comment et où ces coordonnées sont publiées. Le SSAC attire l’attention sur le RFC 2142, noms de boîtes aux lettres pour services communs, rôles et fonctions et suggère que les bureaux d’enregistrement utilisent les conventions de nommage y contenues.
- Les coordonnées du point de contact en cas d’abus devraient être disponibles en un format uniforme lisible par les ordinateurs. Le GNSO devrait décider si une ou toutes ces options de publication sont appropriées.

4. L’ICANN et les bureaux d’enregistrement devraient collaborer avec la communauté pour déterminer les mesures appropriées de sauvegarde contre les fausses complaintes. Les détails de ce qui constitue un abus et des protections qui doivent être fournies contre les fausses complaintes doivent être résolus avec la communauté des bureaux d'enregistrement et la communauté d'utilisateurs. De même, les critères portant sur la rapidité de réaction aux complaintes doivent être élaborés avec les communautés de bureaux d’enregistrement et d’utilisateurs. Le GNSO devrait entreprendre cette activité dans le cadre d’une étude détaillée sur les enregistrements frauduleux.

5. L’ICANN devrait régulièrement (au moins annuellement) vérifier que ces coordonnées sont précises.

Le SSAC estime que la communauté est desservie au mieux lorsque les bureaux d’enregistrement et les revendeurs rendent ces coordonnées de contact facilement accessibles et que l’accessibilité via une liste unique ou une base de données interrogeable offre à la communauté les moyens les plus opportuns pour obtenir des coordonnées de contact. Un seul référentiel, maintenu par l'ICANN, fournit à l'ICANN des moyens simples de vérifier que les coordonnées de contact demeurent précises et complètes et représente pour la communauté une preuve visible que l’ICANN et ses bureaux d’enregistrement accrédités sont engagés envers la fourniture de moyens de communication ouverts et efficaces à des fins aussi bien générales que d'enquête en cas d'abus.

Cette recommandation se concentre sur les bureaux d’enregistrement gTLD et accrédités par l’ICANN. Le SSAC note qu’alors que chaque domaine de premier niveau de code pays (ccTLD) peut avoir ses propres cadres, contrats et dispositions avec les bureaux d’enregistrement, il est souhaitable de traiter les cas d’abus de manière uniforme et de rendre les coordonnées de contact en cas d’abus accessibles à travers l'ensemble des domaines de premier niveau (TLD). Le SSAC invite les ccTLD à partager leur expérience dans le traitement de plaintes pour abus et à collaborer avec l'ICANN pour publier des coordonnées de contact en cas d'abus et le faire de manière cohérente. Le SSAC est préparé à collaborer avec le GNSO et le ccNSO pour étudier ces problématiques de manière plus approfondie.