Rapport du GNSO sur les problèmes liés à l'hébergement ‘fast flux’

STATUT DE CE DOCUMENT

Il s'agit du rapport sur les problèmes liés à l'hébergement ‘fast flux’ demandé par le Conseil du GNSO.

NOTE DE TRADUCTION

La version originale de ce document, qui est en anglais, est disponible sur http://gnso.icann.org/issues/fast-flux-hosting/gnso-issues-report-fast-flux-25mar08.pdf. En cas de différence d'interprétation entre le présent document et le texte original, ce dernier prévaut.

RÉSUMÉ

Ce rapport est soumis au Conseil du GNSO en réponse à une demande reçue par le Conseil suite à une motion proposée et menée pendant la téléconférence du Conseil du 6 mars 2008.
Le rapport a été initialement soumis au Conseil du GNSO le 25 mars. Ce rapport corrigé remplace le document précédent.

TABLE DES MATIÈRES

1 Résumé

Contexte

Le SSAC (Security and Stability Advisory Committee - Comité consultatif sur la sécurité et la stabilité) de l'ICANN a récemment effectué une étude sur la manière dont le DNS peut être utilisé par les cybercriminels sur Internet pour ne pas être repérés et poursuivre leurs activités illégales. Les résultats de cette étude ont été publiés en janvier 2008 dans la recommandation du *SSAC Advisory on Fast Flux Hosting and DNS* (SAC 025) [1], qui décrit les techniques référencées comme « hébergement 'fast flux' », et qui explique comment ces techniques permettent aux cybercriminels d'étendre la durée de vie utile des hôtes compromis utilisés dans des activités illégales et « encourage l'ICANN, les registres et les bureaux d'enregistrement...à établir les meilleures pratiques afin de limiter l'hébergement fast flux et à déterminer si ces pratiques doivent être traitées dans les futurs accords d'[accréditation]. »[2]

Pendant la téléconférence du 6 mars 2008[3], le Conseil du GNSO a retenu la motion suivante, qui stipulait :

> « L'équipe ICANN doit préparer un rapport sur les problèmes concernant les changements DNS « fast flux », qui devra faire l'objet de délibérations au sein du Conseil du GNSO. En particulier, l'équipe doit prendre en compte la recommandation SAC [SAC 025] et définir les prochaines étapes potentielles en matière d'élaboration des politiques GNSO visant à limiter la capacité des criminels à exploiter le DNS via les changements de serveurs de noms ou IP « fast flux ».

Afin de répondre à cette demande, l'équipe ICANN a tenu compte de la recommandation SAC (SAC 025) et a consulté les autres sources d'informations appropriées et pertinentes à propos de l'hébergement fast flux.

Définitions

Fast flux

Dans ce contexte, le terme « fast flux » se rapporte aux changements rapides et répétés apportés aux enregistrements de ressources A et/ou NS dans une zone DNS, qui ont pour effet de modifier rapidement l'emplacement (adresse IP) où le nom de domaine d'un hôte Internet (A) ou serveur de noms (NS) se trouve.

---

[1] http://www.icann.org/committees/security/sac025.pdf
[2] Même si le rapport (SAC 025) se réfère uniquement aux « accords », la présentation SSAC sur l'hébergement fast flux lors de la réunion ICANN de février 2008 à Delhi (http://delhi.icann.org/files/presentation-rasmussen-fast-flux-13feb08.pdf) a mis en évidence que la référence prévue porte sur les « accords d'accréditation ».
[3] http://gnso.icann.org/meetings/agenda-06mar08.shtml

Single flux
Variante de fast flux au sein de laquelle les mises à jour rapides des enregistrements A dans le fichier de zone d'un sous-domaine (généralement de deuxième ou troisième niveau) entraînent la modification rapide de l'emplacement (adresse IP) des hôtes Internet (*par ex.*, les sites Web ou autres serveurs de contenu).

Flux de serveurs de noms
Variante de fast flux au sein de laquelle les mises à jour rapides des enregistrements NS dans le fichier de zone d'un domaine de premier niveau entraînent la modification rapide de l'emplacement (adresse IP) du ou des serveurs de noms pour un sous-domaine ou plus.

Double flux
Variante de fast flux au sein de laquelle le single flux et le flux de serveurs de noms sont utilisés pour provoquer la modification rapide de l'emplacement des hôtes et des serveurs de noms.

Hébergement fast flux
Pratique d'utilisation des techniques fast flux visant à dissimuler l'emplacement des sites Web ou autres services Internet qui hébergent des activités illégales.

Réseau de services fast flux
Réseau de systèmes informatiques compromis (« botnet ») ayant des enregistrements DNS publics qui changent constamment.

Recommandation de l'équipe

Les problèmes liés à l'hébergement fast flux ont généré de nombreux débats au sein de plusieurs collèges et participants, et ils mériteraient un examen plus approfondi. L'équipe recommande ainsi que le GNSO parraine des enquêtes et des recherches plus approfondies sur les directives liées aux meilleures pratiques du secteur avant de déterminer s'il faut initier un processus d'élaboration des politiques formel. Du personnel sera mis à disposition pour prendre en charge ces activités et objectifs de recherche. Afin d'assister la communauté dans son processus de prise de décision, l'équipe ICANN acceptera tous les conseils concernant les orientations spécifiques à prendre pour approfondir les recherches.

Quelle que soit la méthode choisie par le GNSO, l'équipe constate que la réalisation d'enquêtes et de recherches concrètes sera capitale pour informer la communauté lors de ses délibérations.

Afin de déterminer si le point concerné se situe dans le cadre du processus de politiques de l'ICANN et s'il relève de la compétence du GNSO, l'équipe et le bureau de l'avocat-conseil ont pris en compte les facteurs suivants :

- Le point concerné relève-t-il du domaine de compétence de l'ICANN ?
- Le point concerné peut-il largement s'appliquer à diverses situations ou entreprises ?
- Le point concerné est-il susceptible de rester longtemps applicable ou d'actualité (étant entendu que des mises à jour occasionnelles seront nécessaires) ?
- Le point concerné pourra-t-il servir de base pour de futures prises de décision ?
- Le point concerné implique-t-il ou affecte-t-il une politique existante de l'ICANN ?

En fonction des éléments susmentionnés, l'avocat-conseil est d'avis que certains aspects se rapportant à l'hébergement fast flux entrent bien dans le cadre du processus de politiques de l'ICANN et relèvent de la compétence du GNSO. Toutefois, l'avocat-conseil remarque également que la question de fond visant à savoir comment limiter l'utilisation de l'hébergement fast flux pour la cybercriminalité est plus vaste que le processus d'élaboration des politiques du GNSO. Certaines mesures pouvant être utilisées pour décourager ou freiner l'hébergement fast flux, telles que celles pouvant être prises par les ccTLD, les fournisseurs d'accès à Internet ou les utilisateurs d'Internet eux-mêmes, ne se situeront pas dans le cadre de l'élaboration des politiques du GNSO. Les domaines des ccTLD sont également ciblés. De plus, la question de savoir si les options restent longtemps applicables ou d'actualité est une donnée particulièrement importante dans le cadre de l'hébergement fast flux, où de nouvelles règles statiques imposées par un processus d'élaboration des politiques peuvent être rapidement mises à mal par des cybercriminels intrépides.

Selon les informations actuelles, l'équipe suggère d'étudier plus attentivement les options d'élaboration des politiques. Des enquêtes plus approfondies fourniront les éléments requis pour informer au mieux le Conseil quant aux options qui seraient les plus efficaces. Les options préférées pourront alors servir de base au lancement d'un processus d'élaboration des politiques spécifique.

2 Objectif

Ce rapport est soumis en réponse à la demande du Conseil du GNSO visant à obtenir un « Rapport sur les problèmes liés à l'hébergement fast flux ».

Dans ce contexte et en application des dispositions des règlements de l'ICANN :

a. Le sujet proposé pour examen est l'hébergement fast flux.
b. L'identité de la partie soumettant le point concerné est le Conseil du GNSO.
c. Mesure dans laquelle cette partie est affectée par le point concerné : le GNSO est chargé d'élaborer des politiques ayant trait aux domaines de premier niveau génériques. L'hébergement fast flux cible généralement les gTLD (même s'il est également observé dans les ccTLD), et le GNSO est concerné par les actions de hameçonnage, de pharming (détournement vers un site pirate) et par les autres activités de cybercriminalité qui peuvent affaiblir la sécurité et la stabilité opérationnelle d'Internet et qui sont facilitées par les techniques pouvant entrer dans le cadre des responsabilités d'élaboration des politiques du GNSO.
d. Prise en charge du point concerné pour lancer le PDP : la prise en charge adéquate pour la préparation de ce rapport de problèmes a été exposée pendant la téléconférence du Conseil du GNSO du 6 mars 2008. Il y a eu 10 votes en faveur du développement d'un rapport de problèmes pour 14 votes contre. Conformément aux règlements de l'ICANN, un point peut être soulevé comme PDP « par le vote d'au moins 25 % des membres présents du Conseil… ».

3 Contexte

Le terme « fast flux » se rapporte aux changements rapides et répétés apportés aux enregistrements de ressources A et/ou NS dans une zone DNS, qui ont pour effet de modifier rapidement l'emplacement (adresse IP) où le nom de domaine d'un hôte Internet (A) ou d'un serveur de noms (NS) se trouve. Même si certaines utilisations légitimes de cette technique sont connues (voir ci-dessous), elle est devenue au cours de l'année passée l'outil préféré des hameçonneurs et autres cybercriminels qui l'emploient pour éviter d'être détectés par les agents de répression.

Mode de fonctionnement de fast flux[4]

L'objectif de fast flux vise à ce que plusieurs adresses IP (des centaines, voire des milliers) puissent être affectées à un nom de domaine entièrement qualifié (tel que *www.example.com*). Ces adresses IP sont modifiées à l'intérieur et à l'extérieur du fichier de zone A (adresse de l'hôte) et/ou des enregistrements NS (serveur de noms) très fréquemment avec une combinaison d'adresses IP cycliques et une durée de vie (TTL) très brève. Les noms d'hôte de site Web peuvent être associés à un nouvel ensemble d'adresses IP susceptible de changer rapidement. Un navigateur qui se connecte à un même site Web de manière répétée sur une courte période peut en fait être connecté à chaque fois à un ordinateur différent qui est infecté. En outre, les pirates veillent à ce que les systèmes compromis qu'ils utilisent pour héberger leurs manœuvres frauduleuses aient une largeur de bande et une disponibilité de service optimales. Ils utilisent fréquemment un plan de distribution de charge qui prend en compte les résultats du contrôle sanitaire des nœuds de compte, de manière à ce que les nœuds non réceptifs soient sortis du flux et à ce que la disponibilité du contenu soit toujours maintenue.

La redirection proxy ajoute une deuxième couche d'obscurcissement à fast flux. Si une personne hébergeant un contenu malveillant (un site d'hameçonnage par exemple) utilise un réseau fast flux, les hôtes « pris dans le flux » (en changeant rapidement l'adresse IP sur laquelle le nom de domaine se situe) sont généralement des proxy qui redirigent les requêtes sur le site contenant le contenu réel du pirate. La tâche est alors facilitée pour le pirate, car au lieu de copier son contenu malveillant sur de nombreux robots différents, il peut le placer sur un seul hôte et déployer un botnet de redirection des proxy s'acheminant tous vers cet hôte. Le flux a lors lieu parmi les redirecteurs. La redirection évite les tentatives de surveillance et de limitation des nœuds du réseau de services fast flux. Les noms de domaine et les URL du contenu publicitaire ne se situent plus sur l'adresse IP d'un serveur spécifique, mais fluctuent parmi de nombreux redirecteurs ou proxy frontaux, qui à leur tour transmettent le contenu à un autre groupe de serveurs dorsaux. Alors que cette technique a été utilisée à un certain moment dans le domaine des opérations légitimes de serveurs Web dans le but de maintenir une disponibilité élevée et une répartition de la charge, elle traduit ici l'évolution technologique des réseaux informatiques criminels.

[4] La documentation de cette section se base sur la description figurant sur http://www.honeynet.org/papers/ff/fast-flux.html, et est parfois reprise textuellement.

Les « bateaux mère » fast flux sont les éléments de contrôle qui se cachent derrière les réseaux de services fast flux et ils sont similaires aux systèmes de commande et de contrôle C&C figurant dans les botnets habituels. Toutefois, par rapport aux serveurs botnet usuels, les bateaux mère fast flux possèdent beaucoup plus de fonctionnalités. C'est le nœud du bateau-mère fast flux amont, masqué par les nœuds de réseau proxy fast flux frontal, qui rapporte le contenu au client victime qui le demande. Certains systèmes de commande et de contrôle fast flux emploient des applications poste à poste (P2P) et fonctionnent bien pendant très longtemps en toute autonomie. Il a souvent été observé que ces nœuds hébergent des services DNS et HTTP, avec des configurations d'hébergement virtuel de serveur Web capables de gérer la disponibilité de contenu pour des milliers de domaines simultanément sur un seul hôte.

Les réseaux fast flux sont responsables de nombreuses pratiques malveillantes, notamment les pharmacies en ligne, les sites de recrutement de mules financières, les sites Web d'hameçonnage, le contenu extrême/illégal réservé aux personnes majeures, les sites Web d'exploitation malveillante de navigateurs et la distribution de téléchargements maliciels. Hormis le DNS et le HTTP, d'autres services, tels que les services SMTP, POP et IMAP, peuvent être véhiculés via les réseaux de services fast flux. Comme les techniques fast flux font appel aux redirections TCP et UDP, il est probable qu'un protocole de service directionnel ayant un seul port cible rencontre peu de problèmes s'il bénéficie d'un réseau de services fast flux—ainsi, ce ne sont pas seulement des sites Web qui sont concernés ; il peut également s'agir de sites d'e-mail frauduleux.

Utilisations légitimes de fast flux

Au vu de ses recherches préliminaires, l'équipe a compris que certains systèmes d'équilibrage de charge haute capacité peuvent s'appuyer sur des valeurs de courte durée de vie dans les enregistrements DNS qui situent leurs principaux noms de domaine (*par ex.* www.google.com) sur les adresses IP pour répercuter les changements rapidement.[5] Un site à fort trafic peut utiliser cette technique—ce qui correspond à la définition de « fast flux »—pour adapter ses adresses de page d'accueil aux conditions réseau interne et externe, telles qu'une charge de serveur, des surnombres, un emplacement utilisateur et une reconfiguration des ressources. Comme presque tous les navigateurs Web mettent en cache les consultations de nom de domaine pendant au moins 15 à 20 minutes, quelle que soit la TTL annoncée, l'effet net d'une brève durée de vie est de définir le temps d'expiration réel à l' « horizon d'attention » du navigateur. Ces prestataires accordent une importance relativement grande à la capacité de reconfiguration rapide au point de compenser le temps de latence des requêtes supplémentaire généré par des consultations DNS plus fréquentes. Des recherches plus poussées sont nécessaires pour mieux comprendre les utilisations légitimes et leur prédominance.

[5] Les informations reçues par l'équipe suggèrent que des TTL de 300 secondes sont typiques de ces configurations. Là encore, des recherches plus poussées sont requises pour procéder à des vérifications.

L'équipe constate également que les prestataires peuvent engager leurs adresses IP dans un fast flux pour gérer des situations où un état ou un autre acteur bloque délibérément (« formation de trou noir ») leurs adresses afin d'empêcher l'accès à leurs services depuis un pays ou une région. Cela a été décrit de manière anecdotique comme une possible « utilisation légitime ». C'est un autre domaine où ces deux problèmes techniques nécessitent une meilleure compréhension pour étayer d'autres débats.

Pourquoi le fast flux est-il un problème ?

L'hameçonnage, le pharming et les autres activités malveillantes (et souvent illégales) représentent une menace connue pour la sécurité des utilisateurs d'Internet. Les personnes s'adonnant à ce type d'activités peuvent entraver les efforts des enquêteurs cherchant à repérer et mettre fin à leurs opérations en utilisant les réseaux de services fast flux pour changer rapidement et continuellement l'adresse IP où leur contenu est hébergé, gardant ainsi une « longueur d'avance » par rapport aux agents de répression.

Les réseaux de services single flux modifient les enregistrements DNS de leur adresse IP de nœud frontal toutes les 3 à 10 minutes ; ainsi, même si un nœud redirecteur d'agent de flux est arrêté, de nombreux autres nœuds redirecteurs infectés subsistent, prêts à prendre sa place. Généralement, les réseaux fast flux se composent principalement d'ordinateurs domestiques compromis, car, à la différence de l'infrastructure informatique d'une entreprise munie d'un service informatique, il est difficile de protéger les ordinateurs domestiques avec des mesures anti-malicielles.

Les réseaux de services fast flux créent des infrastructures de prestation de services solides et obscures, ce qui complique la tâche des administrateurs système et des agents de répression pour arrêter les manœuvres frauduleuses actives et identifier les criminels qui en sont à l'origine.

Pourquoi l'ICANN doit-elle se sentir concernée par fast flux ?

La communauté de chercheurs, d'administrateurs système, d'agents de répression et d'avocats de consommateurs luttant contre les manœuvres frauduleuses sur Internet qui sont activées ou accélérées par l'hébergement fast flux a conclu que les tentatives visant à contrecarrer l'hébergement fast flux par la détection et le démantèlement des botnets (réseaux de services fast flux) ne sont pas efficaces. D'autres mesures nécessitant la coopération des registres et bureaux d'enregistrement DNS pour identifier ou mettre à mal les techniques fast flux sont censées être beaucoup plus efficaces. L'ICANN doit déterminer si elle peut inciter les opérateurs de registre et les bureaux d'enregistrement à prendre des mesures qui permettraient de réduire les dommages causés par les cybercriminels en entravant l'efficacité de ces exploits DNS, ainsi que les méthodes à employer pour ce faire.

4 Débat quant aux orientations possibles

Les recherches de l'équipe ICANN ont confirmé que l'hébergement fast flux :

- est un véritable phénomène—il a été observé, documenté et rapporté par diverses sources fiables, y compris par les membres du groupe de travail anti-hameçonnage ;
- complique l'identification et l'arrêt des activités malveillantes pour les enquêteurs ; et
- pourrait être considérablement réduit en changeant la manière dont les registres et bureaux d'enregistrement DNS fonctionnent actuellement.

Comme l'hébergement fast flux implique de nombreux participants différents (les cybercriminels et leurs victimes, les fournisseurs d'accès à Internet, les entreprises assurant des services d'hébergement Web, ainsi que les registres et bureaux d'enregistrement DNS), il est possible d'envisager des approches variées pour le limiter. La recommandation SSAC identifie trois approches de limitation, nécessitant chacune la coopération d'un groupe d'acteurs différent :

- éliminer les botnets (utilisateurs et fournisseurs d'accès à Internet) ;
- identifier et mettre fin aux hôtes fast flux (fournisseurs d'accès à Internet) ; et
- changer la manière dont les registres et bureaux d'enregistrement gèrent les mises à jour de zones, ce qui peut réduire le fast flux ou le rendre peu attrayant (registres et bureaux d'enregistrement). Comme développé ci-dessous, des recherches et débats plus poussés sont requis pour déterminer l'efficacité des différentes options dans le temps.

Les experts anti-cybercriminalité ont informé l'équipe que les tentatives visant à mettre fin à l'hameçonnage et aux autres fraudes sur Internet en éliminant les botnets sont vaines. La plupart des botnets sont assemblés à partir d'ordinateurs compromis connectés aux réseaux résidentiels de large bande (par exemple, DSL ou câble), et il est très facile de propager des maliciels dans ces réseaux ; et même si les fournisseurs d'accès à Internet de certains pays coopèrent pour identifier et éliminer les botnets, certains fournisseurs peuvent être hors d'atteinte et fournir des « zones sûres » pour les opérateurs botnet malveillants.

Les enquêteurs anti-cybercriminalité et les agents de répression parviennent généralement à obtenir des injonctions des tribunaux pour fermer les sites d'hameçonnage et de pharming lorsqu'ils sont identifiés, mais le fast flux a été spécifiquement conçu pour échapper à ces efforts de « démantèlement » en compliquant la surveillance de l'activité illégale et l'identification de son emplacement réel.

Les registres et bureaux d'enregistrement peuvent freiner ces pratiques de deux manières : (1) en surveillant l'activité DNS (fast flux est facile à détecter) et en rapportant les comportements suspects auprès des agents de répression ou auprès d'un autre mécanisme approprié ; et (2) en adoptant des mesures qui rendent le fast flux plus difficile à effectuer ou peu attrayant. Parmi les mesures possibles qui ont été suggérées, il faut citer :

- l'authentification des contacts avant d'autoriser toute modification sur les enregistrements NS ;
- la suppression des modifications automatisées sur les enregistrements NS ;
- l'application d'une durée de vie (TTL) minimale pour les réponses aux requêtes des serveurs de noms[6] ;
- la limitation du nombre de serveurs de noms pouvant être défini pour un domaine donné ; et
- la limitation du nombre de modifications des enregistrements d'adresses (A) pouvant être effectuées dans un laps de temps donné aux serveurs de noms associés à un domaine enregistré.[7]

Même si ces mesures sont suggérées, toute mesure peut avoir d'autres implications que l'équipe conseille d'examiner. Il faut remarquer que le processus d'élaboration des politiques du GNSO constitue l'une des manières dont l'hébergement fast flux peut être traité au sein de la communauté ICANN. Cette section décrit les divers mécanismes de traitement de ce problème afin d'informer la communauté ICANN des orientations possibles pouvant être prises.

Élaboration des directives liées aux meilleures pratiques du secteur

Des recherches et débats supplémentaires au sein de la communauté peuvent mener à l'élaboration d'un ensemble de directives liées aux meilleures pratiques du secteur. Dans le domaine de compétence de l'ICANN, elles peuvent constituer la base d'actions volontaires menées par les registres et bureaux d'enregistrement ou, conformément à un processus d'élaboration des politiques ultérieur, la base d'exigences intégrées aux contrats de registres ou aux accords d'accréditation de bureaux d'enregistrement. En dehors du domaine de compétence de l'ICANN, elles peuvent être promues auprès des fournisseurs d'accès à Internet et des autres opérateurs d'infrastructure Internet et prestataires en tant qu'actions et mesures souhaitables qu'ils peuvent appliquer à leur gré.

---

[6] Une durée de 30 minutes a été suggérée comme limite inférieure TTL raisonnable, et l'équipe comprend que certains bureaux d'enregistrement aient adopté une TTL de 30 minutes. Les registres et bureaux d'enregistrement peuvent définir des conditions d'exception pour des utilisations légitimes de TTL plus brèves, mais il peut s'avérer difficile dans la pratique de faire la différence entre les utilisations légitimes et les applications malveillantes.

[7] Il est possible que les activités légitimes ne soient pas entravées en limitant le nombre de serveurs de noms pour un domaine donné à 5 et en limitant le nombre de changements à 5 par mois.

Comme cela est stipulé dans les recommandations de l'équipe (voir Section 5 et Résumé de la Section 1), l'équipe ICANN prend en charge le parrainage des enquêtes et recherches supplémentaires afin d'élaborer les directives liées aux meilleures pratiques, la première mesure devant être prise par le GNSO.

Processus d'élaboration des politiques du GNSO

Une recommandation réglementaire sur ce point peut imposer de nouvelles exigences ou instituer de nouvelles interdictions applicables aux parties contractantes, que l'équipe ICANN mettrait ensuite en œuvre au moyen de ses contrats avec les registres et/ou bureaux d'enregistrement. Toutefois, l'ICANN ne peut imposer de nouvelles obligations aux registres et bureaux d'enregistrement que si l'hébergement fast flux est un problème « pour lequel une résolution uniforme ou coordonnée est raisonnablement requise pour faciliter l'interopérabilité, la fiabilité technique et/ou la stabilité opérationnelle des bureaux d'enregistrement, des registres, du DNS ou d'Internet » (RAA Section 4.2.1).

5 Recommandation de l'équipe

Comme détaillé ci-dessous, l'équipe recommande que le GNSO parraine les enquêtes et recherches supplémentaires afin d'élaborer les directives liées aux meilleures pratiques concernant l'hébergement fast flux. Il peut également être judicieux que le ccNSO participe à ce type d'activité.

Étendue

Afin de déterminer si le point concerné se situe dans le cadre du processus de politiques de l'ICANN et s'il relève de la compétence du GNSO, l'équipe et le bureau de l'avocat-conseil ont pris en compte les facteurs suivants :

Le point concerné relève-t-il du domaine de compétence de l'ICANN ?

Les règlements de l'ICANN stipulent que :
« La mission de la Société pour l'attribution des noms de domaines et des numéros sur Internet (Internet Corporation for Assigned Names and Numbers – « ICANN ») est de coordonner, à un niveau général, les systèmes mondiaux d'identificateurs uniques de l'Internet et notamment d'en assurer la stabilité et la sécurité d'exploitation. En particulier, l'ICANN :

1. coordonne l'allocation et l'attribution des trois ensembles d'identificateurs uniques pour l'Internet, à savoir :
    a. les noms de domaine (formant un système appelé « DNS ») ;
    b. les adresses de protocole Internet (« IP ») ainsi que les numéros de systèmes autonomes (« AS ») ; et
    c. les numéros des ports de protocoles et des paramètres.
2. coordonne l'exploitation et l'évolution du système des serveurs de noms racines du DNS.
3. coordonne l'élaboration des politiques associées de façon raisonnable et pertinente à ces fonctions techniques. »

L'hébergement fast flux implique l'association de noms de domaine avec des adresses IP en faisant appel aux serveurs de noms, incluant les informations sur un domaine délégué de second niveau qui sont conservées par les bureaux d'enregistrement et par le registre pour le TLD dans lequel le SLD est enregistré. L'ICANN n'a qu'une responsabilité limitée en matière d'élaboration des politiques liées à ces fonctions techniques. Alors que les éléments 1a et 3 ci-dessus sont des sujets généraux qui relèvent du domaine de compétence de l'ICANN, certaines options ne seront pas du ressort du GNSO en termes d'élaboration de politiques.

Le point concerné peut-il largement s'appliquer à diverses situations ou entreprises ?

La prise en compte des problèmes liés à l'hébergement fast flux est largement applicable à de nombreuses situations ou entreprises, notamment à chaque gTLD existant sous contrat avec l'ICANN, à chacun des 800+ bureaux d'enregistrement accrédités et à divers registrants existants et potentiels. Il faut néanmoins souligner le fait qu'une politique consensuelle issue du processus d'élaboration des politiques du GNSO ne sera applicable qu'aux registres et bureaux d'enregistrement gTLD étant sous contrat avec l'ICANN (et uniquement si l'hébergement fast flux est un problème « pour lequel une résolution uniforme ou coordonnée est raisonnablement requise pour faciliter l'interopérabilité, la fiabilité technique et/ou la stabilité opérationnelle des bureaux d'enregistrement, des registres, du DNS ou d'Internet », voir par ex. RAA Section 4.2.1).

Le point concerné est-il susceptible de rester longtemps applicable ou d'actualité (étant entendu que des mises à jour occasionnelles seront nécessaires) ?

La réalisation des travaux d'élaboration de politiques concernant les problèmes d'hébergement fast flux peut affecter les gTLD ultérieurs, les bureaux d'enregistrement futurs et les entités commerciales ou non commerciales potentielles qui n'ont pas encore pénétré sur le marché. Il faudra s'efforcer d'élaborer des options qui présentent des avantages durables et qui ne seront pas déjouées rapidement par des personnes malveillantes.

Le point concerné pourra-t-il servir de base pour de futures prises de décision ?

Le résultat d'un processus d'élaboration des politiques peut être durable comme précédemment, même si les circonstances données du marché continueront d'évoluer et établiront ainsi un cadre pour de futures prises de décision concernant des problèmes connexes.

Le point concerné implique-t-il ou affecte-t-il une politique existante de l'ICANN ?

Le point n'implique pas et n'affecte pas de politique existante de l'ICANN. Une liste des politiques consensuelles se trouve à l'adresse http://www.icann.org/general/consensus-policies.htm.

En fonction des éléments susmentionnés, l'avocat-conseil est d'avis que certains aspects se rapportant à l'hébergement fast flux entrent bien dans le cadre du processus de politiques de l'ICANN et relèvent de la compétence du GNSO. Comme les activités d'hébergement fast flux concernent les gTLD, le problème relève de la compétence du GNSO. Toutefois, la question de fond visant à savoir comment limiter l'utilisation de l'hébergement fast flux pour la cybercriminalité est plus vaste que le processus d'élaboration des politiques du GNSO. Certaines mesures pouvant être utilisées pour décourager ou freiner l'hébergement fast flux, telles que celles pouvant être prises par les fournisseurs d'accès à Internet ou les utilisateurs d'Internet eux-mêmes, ne se situeront pas dans le cadre de l'élaboration des politiques du GNSO. De plus, même si l'hébergement fast flux cible fréquemment les gTLD, il est également observé dans les ccTLD. De plus, la question de savoir si les options restent longtemps applicables ou d'actualité est une donnée particulièrement importante dans le cadre de l'hébergement fast flux, où de nouvelles règles statiques imposées par un processus d'élaboration des politiques peuvent être rapidement mises à mal par des cybercriminels intrépides. Selon les informations actuelles, l'équipe suggère d'étudier plus attentivement les options d'élaboration des politiques possibles. Des enquêtes plus approfondies fourniront les éléments requis pour informer au mieux le Conseil quant aux options qui seraient les plus efficaces. Les options préférées pourront alors servir de base au lancement d'un processus d'élaboration des politiques spécifique.

Action recommandée

L'équipe recommande que le GNSO parraine les enquêtes et recherches supplémentaires afin d'élaborer les directives liées aux meilleures pratiques concernant l'hébergement fast flux et de fournir des données pour l'élaboration des politiques et la mise en évidence des options potentielles. L'élaboration des meilleures pratiques doit se dérouler en collaboration intensive avec les entreprises et individus informés et faire l'objet d'un vaste partage afin d'encourager un impact optimal et une large adoption. Il est possible que certains bureaux d'enregistrement appliquent déjà certaines des mesures identifiées dans la recommandation SAC 025 ; l'équipe recommande de consulter ces bureaux pour déterminer l'efficacité de ces mesures et leur mode de mise en œuvre optimal. Du personnel peut être mis à disposition pour prendre en charge ces activités et objectifs de recherche.

L'étude du SSAC sur l'hébergement fast flux, ainsi que plusieurs articles spécialisés, se sont concentrés sur des questions essentielles, parmi lesquelles :

- Qui bénéficie du fast flux et qui en pâtit ?
- Qui bénéficierait de la cessation de la pratique et qui en pâtirait ?
- Comment les opérateurs de registre sont-ils impliqués dans les activités d'hébergement fast flux ?
- Comment les bureaux d'enregistrement sont-ils impliqués dans les activités d'hébergement fast flux ?
- Comment les registrants sont-ils affectés par l'hébergement fast flux ?

Parmi les questions qu'il peut être utile de poser dans le cadre des enquêtes, il faut citer les suivantes :

- Comment les utilisateurs d'Internet sont-ils affectés par l'hébergement fast flux ?
- Quelles règles en vigueur pourraient-elles être appliquées pour réduire ou supprimer les effets négatifs de l'hébergement fast flux ?
- Quel serait l'impact (positif ou négatif) de la mise en œuvre de limites, de directives ou de restrictions au sein des registres et/ou bureaux d'enregistrement par rapport aux pratiques permettant ou facilitant l'hébergement fast flux ?
- Quelles mesures doivent-elles être mises en œuvre par les registres et bureaux d'enregistrement pour limiter les effets négatifs du fast flux ? Ces mesures doivent-elles être documentées et promues comme « meilleures pratiques du secteur », intégrées dans les contrats de registres et les accords d'accréditation de bureaux d'enregistrement, ou promulguées d'une autre manière ?

Annexe 1 – Demande du GNSO d'un rapport sur les problèmes liés à l'hébergement fast flux

Cette annexe reproduit intégralement la demande d'un rapport de problèmes émanant du Conseil du GNSO :

Là où les changements DNS « fast flux » sont de plus en plus utilisés pour commettre des délits et mettre à mal les efforts visant à combattre la criminalité, avec des criminels modifiant rapidement les adresses IP et/ou les serveurs de noms afin d'éviter d'être repérés et de voir la fermeture de leur site Web délictueux ;

Là où le SSAC (Security and Stability Advisory Committee) a rapporté cette tendance dans sa recommandation SAC 025, datée de janvier 2008 : http://www.icann.org/committees/security/sac025.pdf/

Là où la recommandation SSAC décrit les aspects techniques de l'hébergement fast flux, explique comment le DNS est exploité pour favoriser les activités criminelles, traite des méthodes actuelles et possibles visant à limiter cette activité, et recommande que les organismes appropriés envisagent des règles qui rendraient ces méthodes pratiques de limitation universellement disponibles pour tous les registrants, les fournisseurs d'accès à Internet, les bureaux d'enregistrement et les registres ;

Là où le GNSO est probablement une partie adéquate pour envisager de telles politiques ;

Le Conseil du GNSO DÉCIDE que :

L'équipe ICANN doit préparer un rapport sur les problèmes liés aux changements DNS « fast flux », qui devra faire l'objet de délibérations au sein du Conseil du GNSO. En particulier, l'équipe doit prendre en compte la recommandation SAC et définir les prochaines étapes potentielles en matière d'élaboration des politiques GNSO visant à limiter la capacité des criminels à exploiter le DNS via les changements de noms de serveur ou IP « fast flux ».