SAC 050
Blocage de DNS : Bénéfices versus dommages — Une consultation du Comité consultatif pour la sécurité et la stabilité sur le blocage des Domaines de niveau supérieur dans le Système des noms de domaine.

Une consultation du Comité consultatif
pour la sécurité et la stabilité de l'ICANN
(SSAC)
14 juin 2011

Introduction

Ceci est une consultation du Comité consultatif pour la sécurité et la stabilité (SSAC). Le SSAC conseille la communauté ICANN et le Conseil sur des sujets liés à la sécurité et à l'intégrité des systèmes d'attribution de nom et d'adresse Internet. Cela comprend des questions opérationnelles (relatives à l'opération correcte et fiable du système de noms racine), des questions administratives (relatives à l'allocation d'adresse et de numéros d'Internet) et des questions d'enregistrement (relatives au système de registre et de registrant). Le SSAC réalise des évaluations constantes de menace et des analyses de risque des services d'attribution de noms et d'adresses Internet pour évaluer où résident les principales menaces à la stabilité et la sécurité, et conseille la communauté ICANN en conséquence. Le SSAC n'a pas d'autorité officielle pour réguler, imposer ou adjuger. Ces fonctions appartiennent à d'autres, et le conseil offert ici devrait être évalué selon ses mérites.

La liste des contributeurs à cette Consultation, la référence aux biographies des membres du comité et leurs déclarations d'intérêt, et les objections des membres du comité aux découvertes ou recommandations qui figurent dans cette Consultation figurent à la fn de ce document.

Table des matières

1. Blocage de DNS : Bénéfices Versus Dommages

Le blocage ou l'altération des réponses aux requêtes du Système de nom de domaine (DNS) est de plus en plus important. Le filtre des adresses du nom de domaine ou du Protocole Internet (IP) (ou éviter d'une autre manière l'accès au contenu du web en tant que politique de sécurité) peut être perçu par certaines organisations comme une extension naturelle des contrôles historiques de la téléphonie qui avaient pour but de bloquer sur usage au sein des organisations pour que les personnes n'engagent pas de dépenses excessives.

Les approches techniques du blocage de DNS sont destinées à affecter les usagers au sein d'un domaine administratif donné, tel qu'un réseau opérationnel public ou privé. Empêcher la résolution du nom de domaine dans une adresse IP empêchera la connexion immédiate à l'hôte nommé, bien que des techniques déterminées puissent permettre de toute façon la connexion au système donné (ce qui inclut le simple accès au site via l'adresse IP plutôt que via un Nom de Domaine Pleinement Valide (FQDN)). Un résolveur de DNS ou un opérateur de réseau pourrait aussi réécrire une réponse DNS qui contienne une adresse IP qui figure les choix de l'opérateur, que ce soit en réécrivant une réponse pour un Domaine Non-Existant (NXDOMAIN) ou en réécrivant la réponse DNS pour un FQDN existant, avec de potentiels effets nuisibles sur l'Extension de Sécurité du DNS (DNSSEC) des serveurs de nom et de leurs utilisateurs. Une approche particulièrement grossière consiste pour l'opérateur à détacher en silence les réponses DNS, même si cela a pour effet un comportement non-déterministe et peut en soi être problématique.

Quel que soit le mécanisme utilisé, les organisations qui implémentent le blocage devraient appliquer ces principes :

1. L'organisation impose une politique à un réseau et ses utilisateurs, sur lesquels il exerce un contrôle administratif (c'est-à-dire qu'il est l'administrateur d'un domaine politique) .

2. L'organisation détermine que la politique est bénéficiaire à ses objectifs et/ou à l'intérêt de ses utilisateurs.

3. L'organisation implémente la politique en utilisant une technique qui soit le moins perturbatrice pour ses opérations de réseau et ses usagers, sauf si des lois ou des régulations spécifient certaines techniques.

4. L'organisation fait un effort concerté pour ne pas nuite aux réseaux et aux utilisateurs hors de son domaine politique comme conséquence de l'implémentation de la politique.

Lorsque ces principes ne sont pas appliqués, le blocage de l'usage du DNS peut provoquer des dommages collatéraux significatifs ou des conséquences involontaires sans remède disponible pour les parties affectées.

L'évolution de la technologie Internet est fondée sur une adaptation du premier principe de la pratique médicale : *primum no nocere* (d'abord de pas faire de mal), qui requiert que les fournisseurs d'assistance médicale évaluent le dommage potentiel que peut causer une intervention. Dans le cas du blocage de DNS, et sans tenir compte du fait que le blocage s'applique à des Domaines de Niveau Supérieur (TLDs) (ainsi par exemple) ou de second (ainsi par exemple.exemple) ou troisième niveau (ainsi par exemple.exemple.exemple), "ne pas faire de mal" signifie ne pas créer de circonstances dans lesquelles les utilisateurs d'Internet hors du domaine de politique de l'organisation soient défavorablement affectés par la politique de l'organisation ou son implémentation.

Toutes les approches techniques du blocage de DNS, et plus encore les tentatives de circonvenir ce blocage, auront un certain impact sur la sécurité et/ou la stabilité des usagers et des applications, et sur la cohérence ou la résolvabilité universelle de l'espace de nom global. Le SSAC ne peut pas tracer de ligne entre de "bons blocages de DNS" et de "mauvais blocages de DNS", à aucun niveau de TLD, même si le Comité peut s'offrir pour enquêter sur les impacts observables de différentes approches du blocage, et s'il peut suggérer des instructions à utiliser pour évaluer quelles approches du blocage peuvent produire le moins de conséquences involontaires et le moins de dommages possible hors du domaine bloqué. Par exemple, les impacts négatifs du blocage de DNS de domaines spécifiques ou de noms de serveurs sur la sécurité des DNS ont été décrits dans un document récent[1].

Le SSAC comprend que le sujet du blocage de DNS vient dans le sillage de l'addition de XXX TLD génériques (gTLD) à la racine. Le SSAC n'a pas suffisamment d'informations pour adopter une position concernant cette action, cependant, le Comité souhaite qu'il soit clair que, au-delà du fait que le blocage s'applique aux TLDs ou à deux sous-niveaux, réduire les dommages nécessite un effort concerté pour ne pas créer les circonstances dans lesquelles les utilisateurs d'Internet en dehors du domaine de la politique de l'organisation soient défavorablement affectés par la politique de l'organisation ou son implémentation. Étendre aux nations souveraines ce cadre éthique fondé sur l'organisation nécessiterait une meilleure compréhension du paysage politique que celui qu'a actuellement le SSAC. Mais nous pouvons aussi dire avec certitude que le blocage des TLDs entiers au niveau d'un pays interfère fondamentalement avec l'objectif consistant à fournir un système de nom unique, unifié, pour les ressources d'Internet. S'il est implémenté sans un cadre éthique formel pour diminuer les dommages aux parties externes, le blocage pourrait induire plus d'effets négatifs que prévu sur des communautés plus larges, en exacerbant le(s) problème(s) qu'un tel blocage est supposé résoudre. En outre, un blocage aux domaines de deuxième et troisième niveaux et au

[1] Voir <http://www.redbarn.org/files_redbarn/PROTECT-IP-Technical-Whitepaper-Final.pdf>.

niveau du TLD peut donner lieu à des systèmes de noms et/ou de racines alternatifs, ce qui serait déstabilisant et perturbateur pour Internet.

2. Remerciements, Déclarations d'intérêt, et Objections et Abstentions

Ces sections fournissent au lecteur des informations sur trois aspects de notre processus. Les Remerciements énumèrent les membres qui ont contribué à ce document en particulier. Les Déclarations d'intérêt contiennent les biographies des membres du Comité et tout conflit d'intérêt, réel, apparent ou potentiel, qui pourrait être lié au matériel de ce document. Les Objections et Abstentions offrent un lieu pour que les membres individuels expriment leur désaccord avec le contenu de ce document ou son processus de préparation.

2.1 Remerciements

Le Comité souhaite remercier les membres du SSAC suivants ainsi que d'autres contributeurs pour le temps passé, les contributions et leurs apports à la production de ce Rapport.

KC Claffy
Steve Crocker
Patrik Fältström
Jim Galvin
Warren Kumari
Jason Livingood
Danny McPherson
Ram Mohan
Dave Piscitello
Bruce Tonkin
Paul Vixie

2.2 Déclarations d'intérêt

Les informations biographiques concernant les membres du SSAC et les Déclarations d'intérêt sont disponibles à l'adresse :
http://www.icann.org/en/committees/security/biographies-25mar11-en.htm.

2.3 Objections et Abstentions

Il n'y a eu ni objections ni abstentions.