FR

SAC 032
Rapport préliminaire sur la modification de réponse DNS

REMARQUE SUR LES DOCUMENTS TRADUITS

La version originale du présent document, en anglais, est disponible à l'adresse suivante : http://www.icann.org/committees/security/sac032.pdf. En cas de différence d'interprétation entre le présent document et le texte original, ce dernier prévaut.

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

Introduction

Le champ du code de réponse (RCODE) du protocole DNS[1] permet à un serveur de noms de signaler et de décrire les problèmes qu'il rencontre alors qu'il tente de répondre à la requête d'un client (solveur). Un serveur de noms faisant autorité retournera un RCODE avec la valeur *Erreur de nom* pour indiquer que le nom de domaine mentionné dans la requête n'existe pas. Les normes Internet utilisent également les expressions de *domaine non existant* et de *réponse NXDomain* pour décrire cette réponse d'erreur[2].

La valeur Erreur de nom est significative uniquement dans les réponses provenant d'un serveur de noms faisant autorité. Certains registrants de domaine confient leur service de nom faisant autorité à une équipe interne, tandis que d'autres choisissent de confier la gestion de leur DNS à une organisation externe. Le SSAC regroupe ces intermédiaires sous le nom d'agents de service de nom de confiance ou, simplement, agents de confiance. Habituellement, les clients DNS n'interrogent pas directement les serveurs de noms faisant autorité. La majorité des requêtes DNS sont en fait résolues par des systèmes intermédiaires, appelés *solveurs itératifs*. Les solveurs itératifs peuvent être exploités de manière privée par une organisation. Ils peuvent également être gérés publiquement par des fournisseurs de services qui hébergent des services de nom pour leurs clients ou offrent des services de résolution de noms de domaine sur abonnement. Les registrants de domaine entretiennent généralement avec les agents de confiance des relations commerciales et de confiance différentes des relations qu'ils ont avec les opérateurs de solveurs itératifs. Aussi utiliserons-nous, dans le présent rapport, le terme de *tiers* pour désigner cette classe de fournisseurs de services de nom.

Le présent rapport préliminaire contient une description de la pratique de modification de réponse DNS employée par les agents de confiance ou les tiers. Dans le premier cas, un agent de confiance reçoit une requête DNS de nom. L'agent de confiance détermine que le nom mentionné dans la requête n'existe pas dans le fichier de zone qu'il héberge pour le registrant du domaine, mais, au lieu de retourner une réponse DNS indiquant un *nom non existant*, l'agent de confiance retourne une réponse indiquant que le nom existe et contenant un mappage d'adresse IP pour le nom demandé, au choix de l'agent. Dans le deuxième cas, un tiers gérant un solveur itératif reçoit des réponses NXDomain générées par un serveur de noms faisant autorité et en modifie discrètement le contenu, transformant la réponse de *nom non existant* en une réponse indiquant que le *nom existe* et contenant un mappage d'adresse IP pour le nom demandé, au choix du tiers.

---

1 Voir le document RFC 1035, Domain Name System Implementation and Specification (mise en œuvre et spécification du système de noms de domaine), http://rfc.net/rfc1035.html et le registre IANA http://www.iana.org/assignments/dns-parameters

2 RFC 2308, NXDomain, http://rfc.net/rfc2308.html

Ce comportement est désigné par différents termes : redirection de sous-domaine, redirection/réécriture/détournement de domaine non existant (NXDomain), détournement de sous-domaine, résolution d'erreur ou encore marketing d'erreur. Ces appellations soulignent la dimension commerciale et controversée de cette pratique.

L'objectif du présent rapport est de décrire les conséquences d'une modification de réponse DNS pour les registrants de nom de domaine, les opérateurs DNS et les utilisateurs d'Internet, tout en explorant le détournement possible de cette pratique par des personnes malveillantes. Ce rapport initial est consacré à l'explication des conséquences prévisibles et imprévisibles sur les utilisateurs et les registrants de domaine, ainsi que sur les personnes qui s'appuient sur les réponses de domaine non existant à des fins de rapport d'erreur ou administratives.

En quoi consiste la modification de réponse DNS ?

La modification de réponse DNS est une pratique selon laquelle un fournisseur de serveur de noms retourne un message de réponse DNS signalant qu'un *nom existe*, plutôt qu'un message indiquant la non-existence du nom lorsque le nom demandé n'est pas publié dans les informations de zone du registrant du domaine. Dans certains cas, l'agent de confiance du registrant du domaine profite de l'opportunité offerte par un nom non existant dans un domaine (p. ex., une erreur typographique telle que ww.example.com au lieu de www.example.com) pour retourner une *réponse synthétisée*, c'est-à-dire un mappage d'adresse IP pour le nom demandé de son choix. L'agent de confiance peut utiliser un mappage d'adresse IP courant ou par défaut pour tous les noms demandés non publiés dans le fichier de zone : on parle alors de *synthèse générique.*

Dans d'autres cas, un solveur itératif exploité par un tiers examinera la réponse DNS à la requête qu'il a tenté de résoudre au nom de son client. Si une réponse DNS s'avère contenir un code de réponse avec la valeur *Erreur de nom*, le tiers configure alors le solveur itératif pour une modification discrète[3] du contenu de la réponse DNS avant sa transmission au client qui a formulé la requête. Plus précisément, le solveur itératif modifie le code de réponse indiquant la non-existence du nom en une réponse mentionnant que le nom existe. Le fournisseur peut également configurer le solveur de sorte à modifier le contenu de la réponse en y insérant un mappage d'adresse IP pour le nom demandé ; ce mappage n'est pas publié dans le fichier de zone du registrant du domaine et son choix dépend entièrement de la volonté du tiers.

Redirection au niveau du registre du DNS

Le SSAC et l'IAB (Internet Architecture Board, comité d'architecture Internet) se sont déjà exprimés sur les questions de redirection et de synthèse DNS au niveau du registre du DNS[4, 5, 6]. Le SSAC n'a aucune remarque ni recommandation supplémentaire à ajouter sur ce sujet dans le présent rapport. Toutefois, pour un aperçu complet, vous trouverez ci-dessous la description du déroulement de base d'une *réponse synthétisée d'un opérateur de TLD* :

1) Un client soumet une requête DNS à un solveur itératif *A* afin d'obtenir l'adresse IP du nom de domaine *example.tld*.
2) Le solveur itératif A lance le processus de résolution en transmettant la requête à un serveur de noms racine.

---

[3] Nous qualifions ce comportement d'*altération discrète ou silencieuse* car le solveur itératif ne fournit aucune information de protocole explicite indiquant au client ou au serveur de noms faisant autorité que le contenu a été modifié.

[4] SAC 006, Redirection in the COM and NET Domains (redirection dans les domaines COM et NET), 9 juillet 2004, http://www.icann.org/committees/security/ssac-report-09jul04.pdf

[5] SAC 015, Why Top Level Domains Should Not Use Wildcard Resource Records (raisons pour lesquelles les domaines de premier niveau ne doivent pas utiliser d'enregistrements de ressource génériques), 10 novembre 2006, http://www.icann.org/committees/security/sac015.htm

[6] SAC 013, SSAC Response to ICANN Letter re: Tralliance Proposed New Registry Service (réponse du SSAC à la lettre de l'ICANN : Nouveau service de registre proposé par Tralliance), http://www.icann.org/committees/security/sac013.htm

3) Le serveur de noms racine retourne une liste de serveurs de noms capables de résoudre les noms *tld*.
4) Le solveur itératif *A* envoie la requête de résolution d'*example.tld* à l'un des serveurs de noms *tld* identifiés par le serveur de noms racine.
5) Le serveur de noms *tld* détermine que le nom *example* ne correspond à aucun nom du fichier de zone *tld*. Au lieu de retourner un message de réponse DNS avec un code de réponse ayant pour valeur *Erreur de nom*, le serveur de noms *tld* crée et retourne un message de réponse DNS qui indique au solveur itératif A une adresse IP de son choix pour *example.tld*.
6) Le solveur itératif A transmet au client à l'origine de la requête (et, éventuellement, met en cache) la réponse positive.

Réponses DNS synthétisées des agents de confiance

L'exemple suivant illustre comment un agent de confiance peut synthétiser une réponse DNS du domaine pour *example.tld* :

1) Un client soumet une requête DNS à un solveur itératif *A* afin d'obtenir l'adresse IP du nom de domaine *service.example.tld*.
2) Le solveur itératif A lance le processus de résolution en transmettant la requête à un serveur de noms racine.
3) Le serveur de noms racine retourne une liste de serveurs de noms capables de résoudre les noms *tld*.
4) Le solveur itératif *A* envoie la requête de résolution de *service.example.tld* à l'un des serveurs de noms *tld* identifiés par le serveur de noms racine.
5) Le serveur de noms *tld* retourne une liste de serveurs de noms capables de résoudre les noms *example.tld*.
6) Le solveur itératif *A* poursuit le processus de résolution en envoyant une requête de résolution de *service.example.tld* à l'un des serveurs de noms *example.tld* identifiés par le serveur de noms *tld*.
7) Le serveur de noms *example.tld* détermine que le nom *service* ne correspond à aucun nom du fichier de zone d'*example.tld*. Le serveur de noms *example.tld* crée et retourne un message de réponse DNS qui indique au solveur itératif A une adresse IP par défaut, définie dans le fichier de zone, pour *service.example.tld*.
8) Le solveur itératif A transmet au client à l'origine de la requête (et, éventuellement, met en cache) la réponse positive.

La figure 1 illustre ce type de modification de réponse DNS :

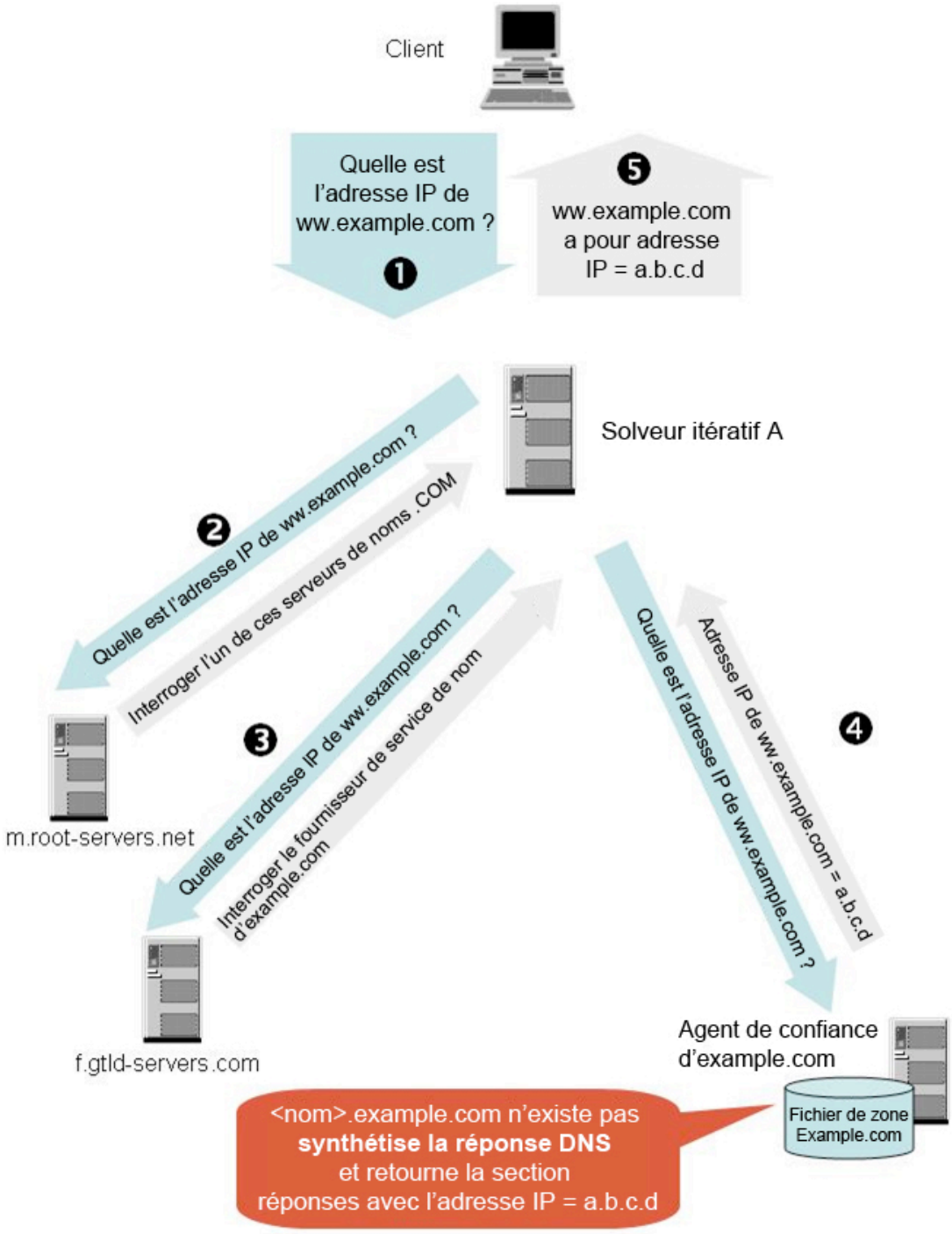

Figure 1. Réponse de domaine non existant (NXDomain) modifiée par un agent de confiance

Modification de réponse de domaine non existant (NXDomain) par des fournisseurs de serveurs de noms tiers

Tout opérateur de serveurs de noms tiers gérant un solveur itératif impliqué dans un processus de résolution de nom peut effectuer une modification de réponse NXDomain (domaine non existant). Par exemple :

1) Un client soumet une requête DNS à un solveur itératif *A* afin d'obtenir l'adresse IP du nom de domaine *service.example.tld*.
2) Le solveur itératif A lance le processus de résolution en transmettant la requête à un serveur de noms racine.
3) Le serveur de noms racine retourne une liste de serveurs de noms capables de résoudre les noms *tld*.
4) Le solveur itératif *A* envoie la requête de résolution de *service.example.tld* à l'un des serveurs de noms *tld* identifiés par le serveur de noms racine.
5) Le serveur de noms *tld* retourne une liste de serveurs de noms capables de résoudre les noms *example.tld*.
6) Le solveur itératif *A* poursuit le processus de résolution en envoyant une requête de résolution de *service.example.tld* à l'un des serveurs de noms *example.tld* identifiés par le serveur de noms *tld*.
7) Le serveur de noms *example.tld* détermine que le nom *service* n'existe pas dans le fichier de zone d'*example.tld* et retourne au solveur itératif *A* un message de réponse DNS avec un code de réponse ayant pour valeur *Erreur de nom*.
8) Le solveur itératif *A* remarque que le serveur de noms *example.tld* a retourné un message de réponse indiquant que le nom n'existe pas. Au lieu de remettre ce message de réponse au client, le solveur itératif *A* modifie discrètement le code RCODE qu'il contient en un RCODE indiquant *nom trouvé* et insère une réponse mappant *service.example.tld* à une adresse IP choisie par l'opérateur du serveur de noms tiers, avant de transmettre cette réponse au client.

Il est important de noter qu'en pratique, toute partie impliquée dans le processus de résolution peut effectuer une redirection NXDOMAIN pour *chaque* nom déterminé ou signalé comme non existant, que le serveur faisant autorité indique ou non que le domaine n'existe pas (NXDOMAIN).

La figure 2 illustre ce type de modification de réponse DNS :

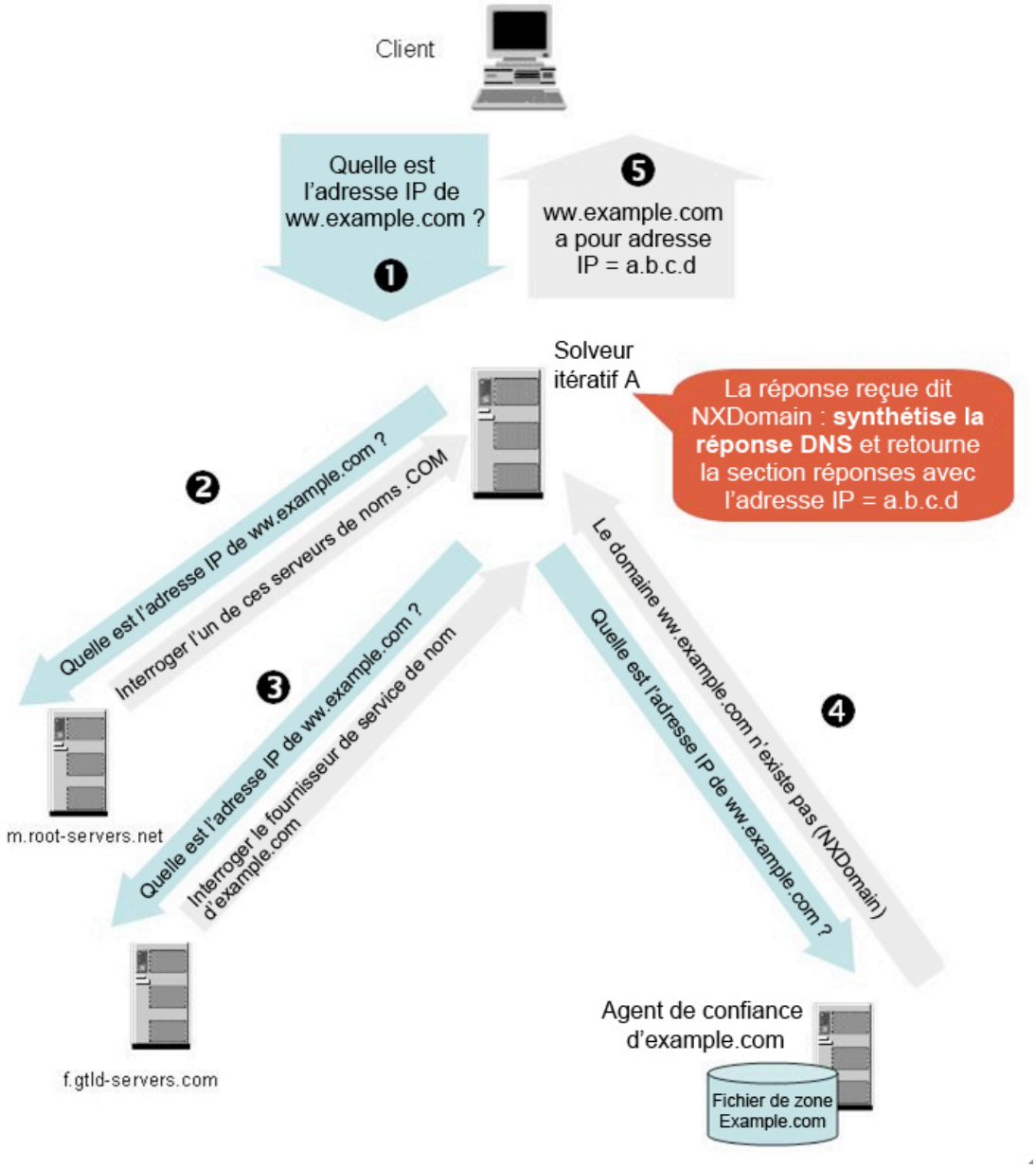

Figure 1. Réponse de domaine non existant (NXDomain) modifiée par un agent de confiance

Qui peut modifier des messages de réponse DNS ?

Les exemples de la section précédente identifient certaines parties capables de rediriger des messages de réponse NXDomain (domaine non existant). Cette liste inclut des agents de confiance et des tiers.

Agents de confiance. L'équipe interne du registrant du domaine peut jouer le rôle de partie de confiance et gérer les informations de zone de ce dernier. Le bureau d'enregistrement qui commandite le nom de domaine, un fournisseur de services Internet ou des fournisseurs de DNS externes (sociétés hébergeant le DNS d'une organisation sous abonnement) peuvent également constituer des parties de confiance et héberger les informations de zone du registrant.

Tiers. Tout opérateur de DNS d'un solveur itératif impliqué dans le processus de résolution d'une requête DNS spécifique est en mesure d'intervenir sur le message de réponse DNS transmis à l'initiateur de la requête par le serveur de noms faisant autorité, notamment :

- Les fournisseurs de services DNS publics, qui génèrent des revenus
    - en rassemblant et en vendant des analyses du trafic DNS, ou
    - en vendant des espaces publicitaires sur les pages hébergées aux adresses qu'ils insèrent dans les réponses DNS modifiées.
- Les FAI ou leurs agents (sociétés qui gèrent le DNS des FAI sous abonnement), qui proposent des résolutions de noms à leurs abonnés ou, d'une manière générale, à toute partie faisant appel à leurs services de nom.
- Les fournisseurs de services, qui proposent des services de résolution de nom ainsi que des services Web proxy.

Des **pirates** peuvent également modifier des réponses DNS dans le cadre de leurs activités malveillantes ou illégales.

Cette liste montre par ailleurs que de nombreuses raisons peuvent être invoquées lors d'une modification de réponse DNS. Ces raisons sont traitées dans la section suivante.

Pourquoi modifier des messages de réponse NXDomain ?

Plusieurs raisons expliquant le choix de certaines parties de modifier des réponses DNS ont été exposées et identifiées par le SSAC. Par exemple, au lieu de remettre une réponse NXDomain (domaine non existant) délivrée par le serveur de noms faisant autorité, un tiers peut intercepter le message et en modifier discrètement le contenu afin d'y insérer l'adresse IP d'une page Web de son choix, à plusieurs fins :

- **générer des revenus** : la page de redirection héberge des publicités ou tout autre contenu générateur de revenus dans un domaine et des sous-domaines de domaines enregistrés.
- **améliorer l'expérience Web de l'utilisateur** : la page de redirection informe l'utilisateur (client potentiel) que le nom de domaine demandé n'est pas disponible et lui propose un moyen de résoudre cette erreur, par exemple à l'aide d'un formulaire de recherche (sponsorisé) accessible à partir de la page de redirection.
- **appliquer une politique** : la page de redirection informe l'utilisateur que le contenu de certaines pages du domaine auquel il tente d'accéder ne sont pas conformes aux conditions d'utilisation stipulées. La page de redirection peut identifier le type de contenu en cause ou fournir à l'utilisateur une copie des conditions d'utilisation afin qu'il en prenne connaissance.
- **fournir des informations préventives** : la page de redirection informe l'utilisateur que le domaine auquel il a tenté d'accéder a été identifié comme un domaine d'hameçonnage et donc suspendu. L'utilisateur a alors l'opportunité de tirer profit de cette expérience d'incident « évité de justesse », grâce à divers supports informatifs dédiés à l'anti-hameçonnage, publiés sur cette page de redirection.
- **soutenir des activités non autorisées ou illégales** : la page de redirection héberge du contenu téléchargeable corrompu sous un nom appartenant au domaine mais non instancié par le registrant, afin de faciliter des activités illégales (hameçonnage, usurpation d'identité, fraude, etc.).

La modification de réponse DNS représente-t-elle une menace de sécurité et de stabilité ?

Plusieurs caractéristiques de la modification de réponse DNS méritent attention. Après avoir examiné les comportements d'agents de confiance et de tiers engagés dans cette pratique de modification de réponse DNS, le SSAC a noté les éléments suivants :

1) Les agents de confiance sont censés agir au nom du registrant du domaine. D'un point de vue opérationnel, les modifications effectuées par ces agents sont autorisées dans le modèle de données du DNS. La question de l'autorisation d'un agent à générer une réponse synthétisée peut être décidée entre l'agent et le registrant. Le registrant peut choisir d'héberger sa zone auprès d'un autre agent si l'agent de confiance est déclaré non digne de confiance.
2) De par la nature même du DNS, tout tiers fournissant un solveur itératif impliqué dans le processus de résolution représente un intermédiaire susceptible

de modifier les messages qu'il reçoit d'un serveur de noms faisant autorité, avant de les transmettre au client. La modification d'une réponse NXDomain par un tiers à un moment donné du processus de résolution peut avoir lieu en dehors de toute relation commerciale impliquant le registrant.

3) Les tiers qui modifient le sens et le contenu d'une réponse DNS peuvent agir dans leur propre intérêt, sans que le registrant du domaine ou l'utilisateur à l'origine de la requête en soit averti ou ait autorisé une telle modification.
4) Les tiers qui modifient des messages de réponse NXDomain fournissent des informations de domaine ne correspondant pas aux informations que le registrant du domaine souhaite diffuser de différentes manières. La réponse affirme que le nom (sous-domaine) a été instancié dans un domaine et est mappé à une adresse IP spécifique. Du point de vue du registrant du domaine, le nom n'existe pas dans sa zone. Une telle réponse n'est pas valide et trahit les intentions du registrant.
5) Le tiers influence la réaction de l'utilisateur qui a formulé la requête en insinuant une association avec le registrant du domaine. Si le but du tiers est de tirer profit d'une relation implicite avec le registrant du domaine, on peut alors parler d'acte frauduleux, d'imposture ou d'utilisation non autorisée d'un nom de marque ou d'une marque commerciale.
6) Les modifications de réponse DNS peuvent avoir des conséquences sur des applications autres que les applications Web et peuvent notamment perturber les services de messagerie électronique et de téléphonie sur IP, entre autres services Internet.
7) Les modifications de réponse DNS peuvent créer des réponses imprévisibles (menaçant la stabilité des noms et pouvant, dans le pire des cas, entraîner une attaque par déni de service).

Nous allons maintenant voir comment ces problèmes de sécurité et de stabilité affectent les registrants de domaines.

Quelles sont les conséquences des modifications de réponse DNS pour les registrants de domaines ?

Lorsque des réponses NXDomain sont modifiées sans l'autorisation expresse du registrant du domaine, le message de réponse ne reflète pas exactement l'état opérationnel du domaine tel que souhaité par le registrant :

1) La non-existence d'un nom dans un fichier de zone doit être signalée au client à l'origine de la requête. Ainsi, une réponse contenant le code de réponse *Erreur de nom* doit être retournée au client par l'agent de confiance ou le tiers qui modifie discrètement le message, ce qui n'est pas le cas.

2) Un enregistrement de ressource de type A est écrit dans la section de réponse du message de réponse. Le mappage nom-adresse décrit dans cet enregistrement de ressource n'existe pas dans le fichier de zone publié du registrant du domaine.

Après un examen attentif, il s'avère que cette pratique est non seulement une méthode alternative de gestion d'erreurs, mais également un moyen de modifier le contenu des messages de réponse. Lorsqu'un agent de confiance d'un registrant de domaine crée un message de réponse DNS, quelle que soit la réponse, l'agent et le registrant s'attendent logiquement à ce que les intermédiaires délivrent le contenu sans le modifier. Si tel n'est pas le cas, il peut y avoir plusieurs conséquences pour le registrant du domaine :

La réponse ne transmet plus les informations souhaitées. Toute application ou activité de gestion dont le bon fonctionnement ou l'intervention repose sur les réponses NXDomain ne fonctionnera plus pour aucun des noms redirigés du domaine.

La réponse corrompt le modèle de confiance de domaine conventionnel. En règle générale, les organisations basent leurs décisions en matière de sécurité sur un modèle de confiance implicite : un domaine parent fera confiance aux sous-domaines du domaine. Cette confiance implicite dérive du principe selon lequel les hôtes nommés dans le domaine d'une organisation sont gérés par l'équipe informatique du domaine ou ses agents de confiance désignés. Une réponse NXDomain modifiée redirige l'utilisateur vers des services fonctionnant sur un hôte non soumis au contrôle administratif du registrant du domaine et n'appartenant pas au domaine de sécurité de ce dernier.

La réponse a des conséquences néfastes sur les tests et audits de conformité. Toute organisation effectuant des audits de sécurité, particulièrement celles qui ont obligation de le faire afin de prouver leur conformité réglementaire, doit prendre en compte le fait qu'un tiers puisse, de manière arbitraire, ajouter un hôte dont le nom apparaîtra dans son domaine mais qui ne sera toutefois ni soumis à son contrôle administratif, ni publié dans sa zone.

La réponse peut perturber la stabilité opérationnelle du DNS. Une résolution de nom réalisée directement par le serveur de noms faisant autorité d'un domaine ou par le biais d'un solveur itératif ne modifiant pas les réponses NXDomain, retournera la réponse attendue par le registrant, mais une même requête pourra retourner des réponses différentes, selon qu'elle sera traitée par un tiers modifiant les réponses de type NXDomain ou par un solveur itératif ou de stubs mettant en cache la réponse modifiée. Cette situation peut se produire lorsqu'un registrant de domaine fait appel à deux agents de confiance pour l'hébergement de son fichier de zone. Il est possible que l'un des agents publie le fichier de zone du registrant avec une entrée générique, tandis que l'autre publie le fichier de zone original (non modifié).

Le risque de conflit de mappage d'adresse est important. Le simple ajout, par un registrant de domaine, d'un enregistrement de ressource de type A pour un nom (ww.example.com) dans son fichier de zone, peut permettre à ce dernier de s'apercevoir qu'un tiers (voire plusieurs) a déjà mappé une adresse IP à ce nom. [Remarque : cela est généralement valable pour tout type d'enregistrement demandé par le client.]

Les hôtes du domaine sont exposés à toute vulnérabilité pouvant être exploitée à partir de l'hôte de redirection ou par son biais. Même lorsque l'hôte identifié dans la réponse NXDomain modifiée est géré par une société légitime (pour la publicité ou des promotions de services, par exemple), cet hôte peut être vulnérable aux attaques de serveurs et d'applications Web, aux attaques de script entre sites ou aux utilisations frauduleuses du système d'exploitation ; les pirates peuvent notamment injecter du contenu dans l'un des systèmes du registrant de domaine via l'hôte identifié dans la réponse NXDomain modifiée. Ces attaques sont bien réelles. Des chercheurs du domaine de la sécurité ont démontré publiquement qu'il était possible d'insérer du script dans le domaine parent par le biais d'hôtes identifiés dans les réponses NXDomain modifiées (serveurs d'annonces publicitaires)[7, 8].

La réponse ajoute au domaine des hôtes dont les sites ne peuvent être contrôlés par l'administrateur du registrant du domaine. Les hôtes identifiés dans les réponses NXDomain modifiées par un tiers profitent de la marque, de la réputation et de la popularité des sites et des liens du registrant du domaine, ainsi que des accords de liens sponsorisés que ce dernier a signé avec des moteurs de recherche. Le registrant ne tire aucun revenu de cette activité et peut même parfois avoir à en subir des conséquences néfastes. Par exemple,

- Un tiers peut publier de la publicité au niveau d'un hôte qu'il a identifié dans une réponse NXDomain modifiée. Ces annonces publicitaires peuvent promouvoir des services ou des produits de concurrents du registrant du nom de domaine.
- Les sociétés dont les annonces publicitaires sont publiées au niveau de l'hôte identifié par un tiers dans une réponse NXDomain modifiée tirent profit des liens sponsorisés associés au nom de domaine et des mots clés associés aux activités commerciales du registrant dans les moteurs de recherche.

---

7 h0h0h0h0, Dan Kaminsky, http://www.doxpara.com/DMK_Neut_toor.ppt

8 Hacking ISP Error Pages (Piratage des pages d'erreur des FAI), Bruce Schneier, http://www.schneier.com/blog/archives/2008/04/hacking_isp_err.html

- Le registrant peut avoir ses propres relations publicitaires ; dans ce cas, les annonces publiées au niveau de l'hôte identifié par un tiers dans une réponse NXDomain modifiée peuvent compromettre les publicités publiées par le registrant du domaine sur ses hôtes Web ou entrer en concurrence avec celles-ci. Les conséquences sont donc réelles pour le registrant du domaine, dont l'affiliation à un service de publicité partenaire se retrouve compromise, comme pour son partenaire publicitaire, dont les opportunités de revenus sont détournées.
- Un hôte identifié par un tiers dans une réponse NXDomain modifiée peut publier des campagnes publicitaires néfastes ou des informations trompeuses ou erronées dont le but est de nuire à la réputation du registrant.

Les réponses NXDomain modifiées ne se limitent pas aux enregistrements de ressource A. Les modifications effectuées par un tiers ne se limitent pas aux réponses NXDomain de résolution de supposés noms d'hôtes à utiliser dans le cadre de connexions HTTP, une réponse NXDomain pouvant se rapporter à une requête de tout type d'enregistrement de ressource de toute application ; le solveur DNS voit uniquement un nom et un type d'enregistrement dans la requête. En théorie, un tiers peut modifier des réponses NXDomain pour la quasi-totalité des types de requête (MX, SRV, NAPTR) ; par exemple, une requête DNS de numéro de téléphone IP (requête retournant un enregistrement de ressource NAPTR) peut, en théorie, être redirigée vers le serveur d'appels indiqué par le tiers.

La réponse engendre des failles de sécurité, portes ouvertes aux abus et attaques. Les attaques réalisées à l'aide de réponses falsifiées incluent notamment les suivantes :

- **Hameçonnage via l'insertion de faux sites au niveau de sous-domaines usurpés**. Les pirates peuvent être en mesure d'exploiter des scripts qu'ils trouvent sur l'hôte identifié dans les réponses NXDomain modifiées afin d'attaquer des systèmes du registrant du domaine. Par exemple, un pirate peut déceler un script qui accepte les entrées sans parvenir à en valider certaines modifications de paramètre. En insérant son propre code exécutable dans le paramètre exploitable, le pirate peut obtenir des visiteurs du site qu'ils exécutent une version falsifiée d'un formulaire de paiement ou de connexion[9]. Les pirates peuvent appliquer des techniques de type annonces publicitaires pour inviter les utilisateurs à télécharger des logiciels malveillants, ou des fenêtres contextuelles invitant les utilisateurs à mettre à jour un logiciel d'application ou de système d'exploitation à l'aide de mises à jour malveillantes illégales.
- **Extraction de données**. L'hôte de redirection peut surveiller le trafic et rassembler des statistiques Web sur les visiteurs redirigés, tout comme le ferait une société chargée du suivi des annonces publicitaires.
- **Récupération arbitraire de cookies**. L'hôte de redirection peut intercepter et copier des cookies adressés par le serveur Web du registrant du domaine au client. Cela peut entraîner la divulgation d'informations personnelles, de coordonnées bancaires ou d'informations d'identification.

[9] *Anatomy of an XSS Attack : Exploit, Impact and Response* (Anatomie d'une attaque XSS : mécanisme, impact et réponse), Russ McRee, ISSA Journal, juin 2008, p. 12-14.

- **Attaques de marque**. De nombreux registrants de nom de domaine protègent leurs marques et marques commerciales en enregistrant leurs noms sous des TLD offensifs, diffamatoires ou pouvant être apparentés, à tort, à un autre nom connu en raison d'une orthographe ou d'une consonance trompeuse. Ces noms peuvent être instanciés comme sous-domaines par un pirate utilisant des caractères génériques pour ses attaques. Au lieu de retourner une réponse de domaine non existant, ces requêtes de nom peuvent être redirigées vers une page Web détournée par défiguration (« defacement ») ou une page de protestation.

Outre ces impacts opérationnels et de sécurité, le SSAC souligne que la redirection de sous-domaines peut soulever des questions de propriété intellectuelle et de droits de marques. Ces questions, bien que n'entrant pas dans le domaine d'expertise du SSAC, mériteront certainement d'être examinées par des parties compétentes lorsque ce sujet sera approfondi.

Duel de réécritures

Les modifications de réponse DNS peuvent elles-mêmes être modifiées. Ce phénomène a été qualifié de *duel de réécritures* et peut être résumé comme suit :

1) Un utilisateur, que nous appellerons Fred, enregistre le domaine *example.tld* via un bureau d'enregistrement *X*.
2) Le registrant d'*example.tld* utilise un service de DNS proposé par le bureau d'enregistrement *X* pour l'hébergement du fichier de zone d'*example.tld*.
3) Le PC de Fred utilise *NS1.mylocalisp.tld* comme serveur de noms par défaut.
4) Fred ouvre une fenêtre de navigateur sur le PC1 et essaie de se connecter à *ww.example.tld*. Il a fait une erreur typographique lors de la saisie de *www.example.tld,* qui correspond au nom d'hôte utilisé par le registrant pour l'adresse de contact de son serveur Web avec le protocole HTTP.
5) *NS1.mylocalisp.tld* lance un processus de résolution afin de résoudre *ww.example.tld*, en interrogeant d'abord un serveur de noms racine sur *tld,* puis le serveur de noms *tld* sur *example.tld*, et enfin le serveur de noms du bureau d'enregistrement X sur *ww.example.tld*.
6) Le serveur de noms du bureau d'enregistrement X retourne une réponse DNS positive au lieu d'une réponse NXDomain pour *ww.example.tld.* Cette réponse contient un enregistrement A dans la section de réponse mappant *ww.example.tld* à *a.b.c.d.*
7) *NS1.mylocalisp.tld* intercepte les réponses DNS du bureau d'enregistrement *X* et s'aperçoit, à partir de précédentes analyses du trafic DNS, que l'adresse de redirection *a.b.c.d* correspond à une page publicitaire.
8) *NS1.mylocalisp.tld* substitue alors à cette adresse ses propres informations de redirection et retourne une réponse DNS positive contenant un enregistrement A dans la section de réponse mappant *ww.example.tld* à *a.x.y.z.*
9) Fred ouvre une fenêtre de navigateur sur le PC1 et essaie de se connecter à ww.example.tld à l'adresse a.x.y.z.

Premiers résultats

Le SSAC propose les premiers résultats et observations suivants concernant la pratique de modification de réponse DNS.

1) Les réponses NXDomain peuvent être modifiées par tout fournisseur tiers qui gère un solveur itératif se trouvant entre le client et le serveur de noms faisant autorité pour le domaine en question. Des agents de confiance peuvent insérer des entrées génériques dans le fichier de zone d'un registrant et retourner le mappage d'adresse correspondant, au lieu de la réponse *Erreur de nom.*
2) Les redirections par modification de réponse NXDomain par un tiers engendrent des dysfonctionnements opérationnels et des problèmes de stabilité pour les registrants de domaine qui ne peuvent bénéficier d'une résolution facile, même en hébergeant leur propre service de nom.
3) La modification de réponse NXDomain et les réponses synthétisées peuvent générer des problèmes de sécurité pour les registrants de domaine. Les relations de confiance entre un domaine parent et ses sous-domaines peuvent notamment en être affectées et ne plus être assurées. La détérioration de ces relations de confiance peut avoir un effet négatif sur les audits de sécurité et les tests de conformité.
4) La modification de réponse NXDomain et les réponses synthétisées peuvent créer des vulnérabilités aux attaques malveillantes à l'encontre du registrant du domaine, permettant ainsi aux pirates d'exploiter les actifs du domaine à des fins malveillantes ou illégales.
5) Les réponses NXDomain modifiées et les réponses synthétisées peuvent être modifiées par les tiers qui les reçoivent.
6) L'existence d'agents de confiance qui synthétisent des réponses et de tiers qui modifient des réponses NXDomain n'est pas que purement spéculative : ces intervenants sont reconnus et identifiables. Certains tiers pratiquent la modification de réponse NXDomain directement ou par le biais de *partenaires de résolution d'erreur*[10].
7) Les agents de confiance et les tiers peuvent ne pas déclarer clairement et explicitement qu'ils exercent cette pratique de modification de réponse DNS et, lorsqu'ils le font, ils ne parlent pas forcément des conséquences néfastes qu'une telle pratique peut avoir sur les intérêts du registrant du domaine. Certains fournisseurs avertissent leur client qu'ils se réservent le droit de procéder à une résolution d'erreur ou à une redirection dans le cadre de l'accord de service conclu, sans offrir au registrant d'autre possibilité d'échapper à cette condition que de s'adresser à un autre fournisseur.
8) Les réponses NXDomain ne signalent pas seulement une condition d'erreur du registrant de domaine, mais fournissent également des informations sur les entrées du fichier de zone de ce dernier. Ces informations doivent être traitées comme toute autre information d'application.

[10] Certains de ces acteurs constatent un marché mondial de l'erreur de plus d'1 milliard de dollars par an (http://barefruit.com/services.htm)

9) Les conséquences d'une modification de réponse s'étendent au-delà des applications Web. La substitution et l'injection de messages électroniques et vocaux dans le cadre de services Internet offrent un terrain idéal pour ce type d'activité.

10) La modification de réponses DNS peut soulever des questions de propriété intellectuelle et de droits de marques.

Recommandations préliminaires

Le SSAC formule les recommandations préliminaires suivantes :

1) Le SSAC s'est déjà opposé à plusieurs reprises à la pratique de synthétisation des réponses DNS au niveau des TLD. Toute action identique au niveau des sous-domaines est également à proscrire.

2) Le registrant doit pouvoir contrôler la manière dont son agent de confiance répond à une requête de nom qui n'existe pas dans son fichier de zone, en instaurant avec ce dernier une relation commerciale de confiance. Le registrant doit notamment décider du type de réponse retournée par son serveur de noms faisant autorité : erreur de nom ou réponse synthétisée.

3) Le registrant doit s'informer de la méthode utilisée par son agent de confiance pour la gestion de ses sous-domaines non enregistrés. Le SSAC rejoint l'IAB sur le fait que les agents de confiance ne doivent pas utiliser de caractères génériques de DNS dans une zone, sans avertir le registrant du domaine des risques identifiés dans le présent rapport et dans d'autres documents, et qu'ils ne doivent pas générer de tels caractères ni de réponses synthétisées sans l'accord préalable et informé du registrant. Le SSAC et l'IAB recommandent par ailleurs la mise à disposition, par ces agents de confiance, de mécanismes offrant aux clients la possibilité de refuser cette pratique et de recevoir les réponses DNS à leurs requêtes telles que formulées à l'origine, sans aucune modification.

4) Les tiers exerçant cette pratique de modification des réponses NXDomain doivent en informer leurs clients et permettre à ces derniers de refuser de s'y soumettre.

5) Les organisations dont la stabilité opérationnelle repose sur un rapport précis des domaines non existants doivent faire appel à un agent de confiance qui s'engage formellement à ne pas modifier les réponses DNS dans ses conditions de service.

6) Les registrants doivent s'efforcer de trouver des moyens de fournir une preuve authentifiée de bout en bout de la non-existence de sous-domaines, c'est-à-dire des extensions de sécurité DNSSEC[11, 12, 13, 14]. Les organisations doivent poursuivre leurs efforts pour réduire le niveau d'exposition des réponses NXDomain à cette pratique de modification, en sélectionnant des parties de confiance pour leurs solveurs itératifs, de sorte à ce que les requêtes de leurs clients ne soient pas traitées par des fournisseurs de services de résolution de nom arbitraires, susceptibles de pratiquer des redirections de sous-domaines.

---

11 RFC 4033, DNS Security Introduction and Requirements (Sécurité des DNS : Introduction et exigences), http://rfc.net/rfc4033.html

12 RFC 4034, Resource Records for DNS Security Extensions (Enregistrements de ressource pour les extensions de sécurité DNS), http://rfc.net/rfc4034.html

13 RFC 4035, Protocol Modifications for DNS Security Extensions (Modifications de protocole pour les extensions de sécurité DNS), http://rfc.net/rfc4035.html

14 RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence (Sécurité DNS - DNSSEC : Déni d'existence authentifié haché), http://rfc.net/rfc5155.html

Perspectives de travail

Les conséquences commerciales, économiques et opérationnelles de la redirection de sous-domaine, ainsi que ses conséquences sur la sécurité, méritent que l'on y consacre une attention particulière. D'après nos connaissances, la modification de réponse DNS reste principalement associée aux applications Web et il nous semble donc important d'examiner plus en détails les conséquences d'une telle pratique sur d'autres services IP. Le SSAC encourage la communauté à considérer les nombreuses implications d'un détournement de réponses négatives en opportunités de revenus qui ne prendrait pas en compte les conséquences opérationnelles ni les souhaits de données DNS du registrant ou du client. En résumé, la résolution d'erreur et les « marchés de l'erreur » générés par de telles pratiques créent des précédents inquiétants en introduisant une certaine ambigüité au sein des modèles traditionnels de gestion d'erreur et de relations de confiance, et en en compromettant la stabilité. L'incertitude règne quant à savoir si ces pratiques pourront être appliquées aux services Internet de messagerie électronique, de communication vocale et de collaboration, voire à l'adressage, au routage ou à d'autres opérations fondamentales d'Internet, tout comme il est encore impossible, à l'heure actuelle, d'évaluer avec précision l'impact que de telles pratiques auront sur les communications via IP.