Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine

Document mis en page à l'aide de LaTeX. Figures réalisées avec les outils TikZ et PGFPlots.

Version 1.2 : 15/02/2015

Vous pouvez adresser vos commentaires et remarques à l'adresse suivante :

guide.dns@ssi.gouv.fr

Table des matières

Chapitre 1

Introduction

Ce document est un guide s'adressant aux responsables de la sécurité des systèmes d'information et aux architectes système et réseau d'organismes de toutes tailles devant diffuser des informations, comme des adresses IP, par l'intermédiaire des noms de domaine dont ils sont titulaires et du protocole DNS [1].

Il détaille les considérations de sécurité relatives à la sélection des prestataires de service intervenant dans le processus de gestion administrative ou technique des noms de domaine.

Parmi ces prestataires peuvent être identifiés :

- **le registre** [2] ;
- **le bureau d'enregistrement** [3] ;
- un éventuel **opérateur technique** (parfois appelé **hébergeur**) ;
- un éventuel **revendeur**.

Ces entités peuvent avoir une incidence forte sur le niveau de sécurité (intégrité et confidentialité) et de résilience (disponibilité) d'un nom de domaine et des services qui en dépendent, comme un site web ou un service de messagerie électronique. Le registre et le bureau d'enregistrement sont, en particulier, deux prestataires incontournables pour l'acquisition et l'exploitation d'un nom de domaine.

Les prestataires de services d'interrogation et de résolution des noms de domaine sont considérés comme hors du champ de ce document.

Il est important de noter que les recommandations émises dans ce document ne sont en aucun cas exhaustives et ne constituent qu'une partie des bases de la sécurité d'une infrastructure d'hébergement DNS. Le lecteur est invité à consulter également les guides et notes techniques suivantes, en particulier s'il assure lui-même le rôle d'opérateur technique :

- Guide d'hygiène informatique [1] ;
- Recommandations de sécurité relatives aux mots de passe [2] ;
- Note d'information du CERT-FR sur les dénis de service [3] ;
- Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques [4].

1. *Domain Name System*.
2. En anglais, *registry*.
3. En anglais, *registrar*.

Chapitre 2

Rappels sur le DNS

Le système de noms de domaine, géré par le protocole DNS, a pour objectif essentiel d'associer à une adresse IP un nom lisible et mémorisable par les utilisateurs. Il permet également de fournir de la stabilité aux identificateurs de ressources informatiques.

Le DNS est aujourd'hui également employé pour le stockage de données diverses : des informations indispensables à la délivrance des emails (enregistrements DNS MX), des politiques de sécurité comme SPF [1] pour la lutte contre le spam [5] ou encore des informations cryptographiques comme la diffusion d'empreintes de clés SSH [6].

Le DNS peut donc être perçu comme une vaste base de données, qui passe à l'échelle grâce à deux propriétés intrinsèques au protocole : son organisation hiérarchique et le caractère distribué des données.

L'organisation hiérarchique signifie que les données sont réparties sous la forme d'une arborescence [2], qui assure l'unicité des noms de domaine. Les domaines plus bas dans l'arbre qu'un certain domaine sont appelés des sous-domaines de ce domaine, et les domaines plus hauts dans l'arbre sont appelés des domaines parents.

Dans le même temps, pour décentraliser les données, chacun des nœuds de cet arbre peut déléguer son autorité sur un sous-domaine à une entité administrative tierce (personne physique ou morale). Ce mécanisme permet ainsi à la racine de l'arbre DNS, symbolisée par un « . », de confier la gestion de sous-domaines, comme `org`, `eu` ou encore `fr`, à des organismes indépendants, généralement appelés registres. Les domaines délégués par la racine sont appelés domaines de premier niveau [3]. Les registres peuvent à leur tour déléguer leur autorité sur des sous-domaines, comme `france.fr` ou `wikipedia.org`, à des titulaires qui en acquièrent un droit d'utilisation, généralement contre paiement d'une redevance.

Les délégations d'autorité forment des frontières administratives. Chaque délégation symbolise la fin de l'autorité de l'entité délégante et le début d'autorité de l'entité recevant la délégation. Les subdivisions de l'arbre ainsi obtenues sont appelées des *zones*.

Ainsi, dans le schéma 2.1, les noms de même couleur et reliés par un trait plein

1. *Sender Policy Framework*.
2. Traditionnellement, la racine de cet arbre inversé est représentée en haut des schémas et les feuilles sont en bas. Un exemple de représentation est fourni avec le schéma 2.1.
3. En anglais, *Top-Level Domains (TLD)*.

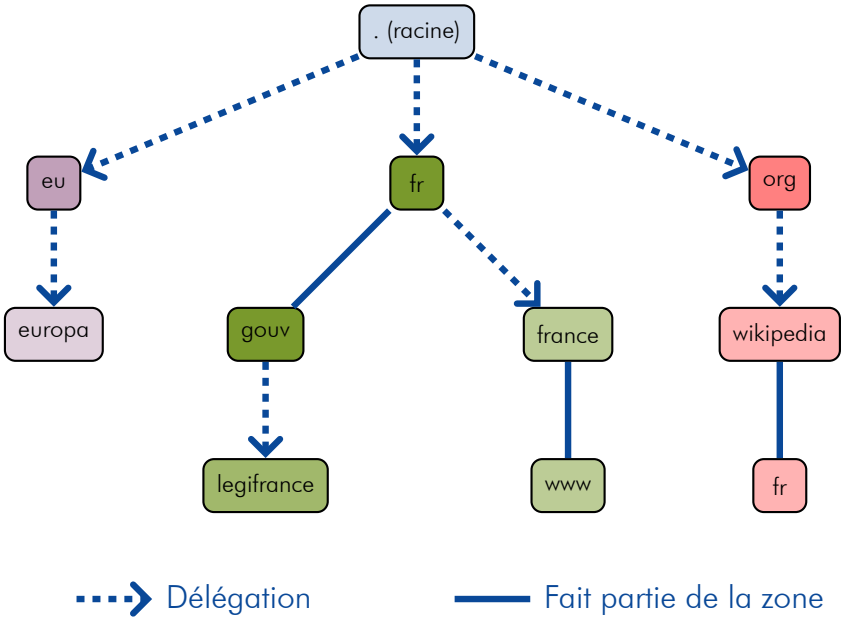

Figure 2.1 – Domaines et zones : le rôle des délégations

sont dans la même zone et sous la responsabilité de la même entité administrative. Par exemple, `europa.eu`, `legifrance.gouv.fr`, `france.fr` et `wikipedia.org` reçoivent une délégation d'autorité de la part de leurs domaines parents respectifs et sont donc dans une zone différente de leur domaine parent. En revanche, `gouv.fr` et `fr.wikipedia.org` sont des sous-domaines, respectivement de `fr` et de `wikipedia.org`, mais ils restent sous la responsabilité de l'entité administratrice du domaine parent. Ils font donc tous deux partie de la même zone que leurs domaines parents respectifs.

Compte tenu du nombre important de titulaires de noms de domaine de deuxième niveau, les registres accréditent généralement des organismes, nommés bureaux d'enregistrement, qui jouent le rôle de mandataires. Ces derniers récoltent les informations relatives aux titulaires et leurs paiements et les font parvenir aux registres par des canaux privilégiés.

Une fois un domaine acquis, le titulaire d'un nom de domaine est en charge du contenu de la zone sous son autorité, et plus particulièrement des enregistrements DNS qu'il y publie. Il peut procéder à l'auto-hébergement des machines servant ce contenu ou désigner des opérateurs techniques prestataires de service d'hébergement.

Enfin, le revendeur est un organisme pouvant intervenir entre le titulaire d'une part et le bureau d'enregistrement et l'opérateur technique d'autre part, afin de masquer la complexité de la gestion administrative et technique du DNS ou d'ajouter une plus-value en offrant des services et prestations supplémentaires, comme la gestion de portefeuilles de noms de domaine ou l'application de politiques de renouvellement des noms de domaine.

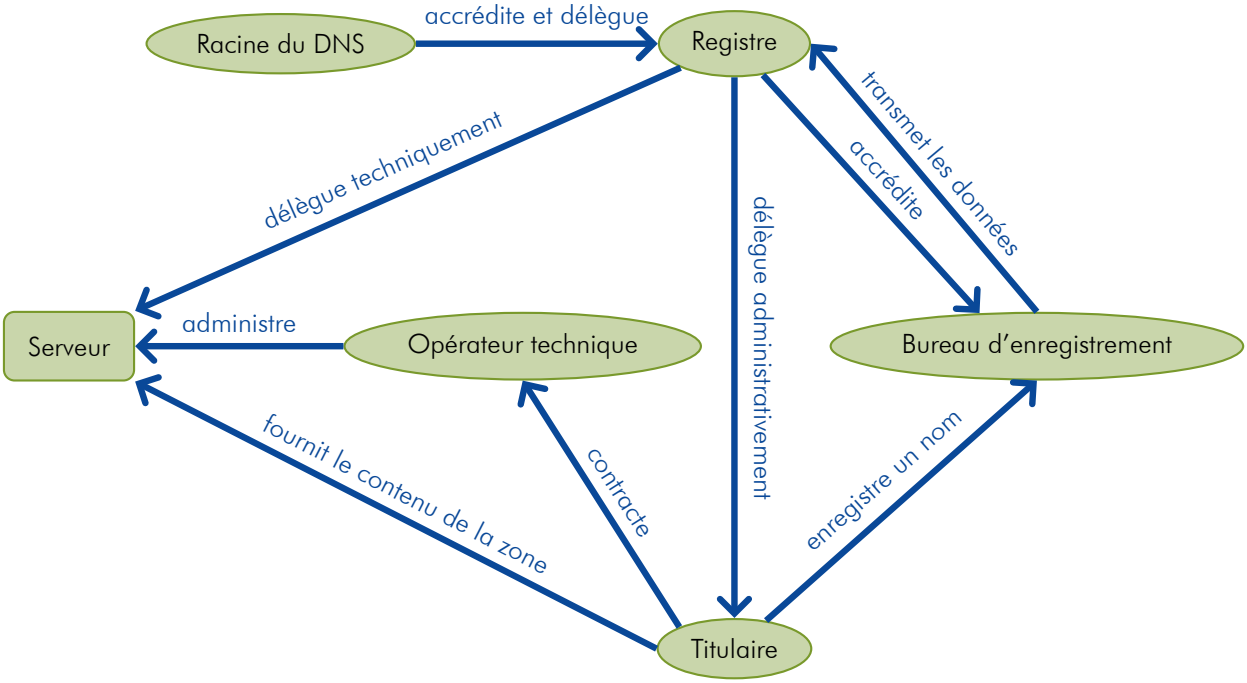

Figure 2.2 – Synthèse des relations entre les acteurs du DNS

Le rôle et les responsabilités des différents intervenants (registres, bureaux d'enregistrement, opérateurs techniques), qui viennent d'être présentés, sont synthétisés par le schéma 2.2. Les rôles sont étudiés en détail dans la section 3.

Il est important de noter dès à présent qu'en raison de la nature arborescente du DNS, le défaut d'un ou plusieurs de ces acteurs peut entraîner un incident sur tous les domaines sur lesquels ils interviennent. Chacun d'entre eux doit donc être sélectionné avec soin par le titulaire afin de diminuer ou d'éviter les risques pesant sur son nom de domaine.

À titre d'exemple, et pour illustrer la responsabilité de chacun des intermédiaires dans le maintien en condition opérationnelle d'un nom de domaine, voici une liste d'incidents récents :

- Le registre IEDR, en charge du nom de premier niveau national irlandais `.ie`, a subi un incident de sécurité en octobre 2012, menant au dévoiement [4] des sites web `google.ie` et `yahoo.ie`. Cet incident n'est pas isolé, puisque ces dernières années, de nombreux autres registres ont déploré des incidents, dont le registre marocain (`.ma`), qatari (`.qa`), malaisien (`.my`) [7, 8]...
- Le bureau d'enregistrement Network Solutions a commis, en juin 2013, une erreur de configuration, en réponse à une attaque en déni de service distribué,

4. En anglais, *pharming*. Ce type d'attaques vise à pratiquer le hameçonnage par la redirection de l'utilisateur, grâce au DNS, sur un serveur contrôlé par l'attaquant.

menant à la modification accidentelle des informations de délégations des noms de domaine de près de cinq mille clients vers des serveurs ne faisant pas autorité pour ces noms. L'ensemble des noms de domaine concernés a donc subi un préjudice lourd en disponibilité [9]. En octobre 2013, ce même bureau d'enregistrement a subi une attaque menant à la modification des informations de délégation et à l'indisponibilité de plusieurs sites Internet à la popularité importante [10].
Le bureau d'enregistrement NameCheap a corrigé, en décembre 2013, une vulnérabilité dans son interface d'administration, qui aurait permis la modification arbitraire par un attaquant d'informations de délégation de noms de domaine [11].
Le bureau d'enregistrement Mark Monitor a subi une attaque, en janvier 2014, menant à la modification des informations de délégation des noms de domaine `ebay.co.uk` et `paypal.co.uk`. Ni le bureau d'enregistrement ni les victimes n'ont commenté publiquement l'incident [12, 13].

- L'opérateur technique Go Daddy, également bureau d'enregistrement, a subi, en 2012, un incident réseau rendant inaccessible pendant une durée de six heures l'ensemble de ses services, y compris l'hébergement des noms de domaine de ses clients. Cette panne a rendu, à leur tour, les services de ses clients inaccessibles, la résolution de leurs noms de domaine ne pouvant plus se faire, et ce même si les-dits services n'étaient pas hébergés par Go Daddy [14].
- Le revendeur en charge du nom de domaine `nytimes.com` s'est fait dérober ses authentifiants d'accès à l'interface d'administration du bureau d'enregistrement MelbourneIT. Cette compromission a mené, en août 2013, au dévoiement des services dépendant de ce nom de domaine pendant près d'une demi-journée [15].

Chapitre 3

Les différents acteurs du DNS

3.1 Les registres

Les registres sont les entités responsables des noms de premier niveau, tels que `.fr`, `.com`, `.org` ou de certains noms de second niveau comme `.co.uk` [16]. Ils sont référencés par l'ICANN [1], association à but non lucratif de droit californien, en charge de la gestion de la zone racine. Les registres en charge des noms de domaine de premier niveau génériques, comme `.com`, sont accrédités par l'ICANN, tandis que ceux en charge des noms de domaine géographiques ou régionaux, comme `.fr` ou `.eu` sont désignés selon des procédures spécifiques à chaque pays ou région.

Certains registres proposent un service appelé « verrou de niveau registre » [2]. Ce service permet à un titulaire de nom de domaine d'indiquer au registre qu'il désire le gel des informations relatives à son nom de domaine, jusqu'à nouvel ordre fortement authentifié émanant du titulaire.

Ce mécanisme de sécurité est mis en œuvre pour protéger les noms de domaine d'éventuelles attaques visant les bureaux d'enregistrement accrédités. L'attaquant peut, en effet, chercher à tirer parti du canal de communication privilégié que les registres mettent à leur disposition. Ainsi, une fois un bureau compromis, l'attaquant pourrait modifier les informations de délégation d'autorité sur des noms de domaine dont ils ont la gestion. Ces attaques portent le nom d'usurpation de noms de domaine [3].

La fonctionnalité de « verrou de niveau registre » est généralement déployée pour les noms de domaine qui sont une cible de choix pour les attaquants, comme les domaines bancaires, étatiques, ou encore les infrastructures critiques. Elle aurait, par exemple, permis de prévenir, en octobre 2013, la modification des informations de délégation de certains noms de domaine populaires, malgré la compromission du bureau d'enregistrement Network Solutions [10].

Sa mise en œuvre est effectuée par le registre. Idéalement, elle repose sur un secret partagé exclusivement par le titulaire et le registre. Ce secret est alors utilisé par le registre pour vérifier que le titulaire est bien à l'origine d'une demande de déverrouillage. Pour que l'authentification soit forte, la vérification ne doit pas faire intervenir le bureau

1. *Internet Corporation for Assigned Names and Numbers*.
2. En anglais, *registry lock*.
3. En anglais, *DNS Hijack*.

d'enregistrement.

L'implantation d'un tel mécanisme peut prendre plusieurs formes, et les exemples suivants ne sont fournis qu'à titre indicatif : un service téléphonique interactif mis en place par le registre, l'envoi d'un code SMS de confirmation au titulaire qui doit alors le saisir dans une interface de confiance, ou encore l'envoi d'un fax de confirmation par le titulaire au registre.

Recommandation 1

Choisir un registre offrant un service de verrou de niveau registre et obtenir des assurances ou des engagements contractuels sur le niveau de service garanti pour cette fonctionnalité.

La disponibilité du service de verrou de niveau registre est à valider auprès de chaque registre, aucune liste officielle de registres qui le prennent en charge n'étant publiée par l'ICANN.

3.2 Les bureaux d'enregistrement

Les bureaux d'enregistrement sont des intermédiaires entre les titulaires et les registres. Ils sont accrédités par les registres, afin de permettre aux personnes physiques ou morales de devenir titulaires de nouveaux noms de domaine situés sous l'autorité d'un registre contre une redevance.

L'opération d'acquisition d'un nom de domaine est appelée enregistrement d'un nom de domaine. Pour l'accomplir, un bureau d'enregistrement est en charge de :

- vérifier les conditions d'enregistrement de nouveaux noms de domaine en accord avec la politique du registre parent des noms enregistrés ;
- réceptionner les éventuels paiements associés à l'enregistrement d'un nom de domaine ;
- envoyer au registre les informations techniques inhérentes au DNS, grâce à des protocoles spécifiques comme RRP [4] [17] ou EPP [5] [18].

Les informations envoyées par les bureaux d'enregistrement aux registres sont d'une importance capitale puisqu'elles permettent au registre de :

- savoir vers quels serveurs DNS la délégation technique d'un nom de domaine doit être faite ;

4. *Registry Registrar Procotol*.
5. *Extensible Provisioning Protocol*.

- collecter les informations sur le titulaire qui pourront être répertoriées dans les annuaires du registre [6].

Le nombre d'attaques par usurpation de noms de domaine a augmenté de manière significative ces dernières années [19, 20]. En conséquence, à défaut de verrou de niveau registre ou en vertu du principe de défense en profondeur, un bureau d'enregistrement offrant une authentification renforcée devrait être sélectionné par le titulaire ou le revendeur éventuel.

Recommandation 2

Choisir un bureau d'enregistrement offrant un mécanisme d'authentification journalisée et renforcée, par exemple grâce à deux facteurs d'authentification et un filtrage des accès à l'interface d'administration.

À l'instar du verrou de niveau registre, les bureaux d'enregistrement peuvent demander au registre le gel des données relatives à un nom de domaine, notamment afin de prévenir le transfert involontaire ou frauduleux d'un nom de domaine d'un bureau d'enregistrement à un autre, ou d'un titulaire à un autre.

Ce mécanisme est parfois appelé verrou de niveau bureau d'enregistrement. Il se distingue du verrou de niveau registre parce que la levée du verrou est contrôlée par le bureau d'enregistrement, sans aucune communication entre le registre et le titulaire. La compromission du bureau d'enregistrement peut donc entraîner la levée du verrou et l'altération des données. Ce verrou, s'il est bien implémenté, contribue donc uniquement à la défense en profondeur mais n'offre qu'un niveau de protection très inférieur au verrou de niveau registre.

Aller plus loin 1

Choisir un bureau d'enregistrement offrant un mécanisme de verrou de niveau bureau d'enregistrement afin de prévenir les transferts frauduleux de gestion de domaines.

Aucune liste officielle des bureaux d'enregistrement mettant en œuvre cette fonctionnalité n'est publiée. Le titulaire d'un nom de domaine doit donc s'enquérir de sa disponibilité auprès des bureaux d'enregistrement.

Les bureaux d'enregistrement jouent également un rôle important dans la sécurisation du DNS, et notamment pour la mise en œuvre de DNSSEC. DNSSEC est une technologie permettant aux titulaires d'assurer l'intégrité des données contenues dans leur

6. Ces annuaires sont ensuite interrogeables grâce au protocole Whois.

zone par l'usage de signatures cryptographiques. Elle permet ainsi de compenser la faible sécurité du protocole DNS [21], notamment face aux attaques réseau visant à remplacer les données d'une réponse DNS lors de leur transit, comme les attaques par pollution de cache ou les attaques de l'homme du milieu.

Les informations relatives aux différentes clés de signature mises en œuvre lors des opérations cryptographiques, comme leurs empreintes, doivent alors être transmises à l'entité faisant autorité sur la zone parente afin de créer une chaîne de confiance. Les bureaux d'enregistrement sont alors le vecteur traditionnel de transmission des informations relatives à DNSSEC entre le titulaire et le registre.

L'absence de prise en charge des informations liées à DNSSEC par le bureau d'enregistrement assurant la gestion d'un domaine interdit la mise en place de cette technologie par le titulaire.

Aller plus loin 2

Sélectionner un bureau d'enregistrement qui permette de publier les informations nécessaires à l'utilisation de DNSSEC.

3.3 Les opérateurs techniques

Les opérateurs techniques (parfois également appelés hébergeurs) sont les entités en charge de la gestion technique des noms de domaine et de leur hébergement sur des serveurs DNS. Bien que ce rôle soit parfois assumé par le titulaire, il est souvent délégué à des opérateurs techniques spécialisés.

Les serveurs de l'opérateur technique sont renseignés dans les informations de délégation fournies au registre. Le chapitre 5 donne plus de détails quant aux architectures recommandées afin d'accroître la résilience du service DNS qu'elles fournissent.

Il est important de noter qu'un même nom de domaine peut être hébergé par plusieurs opérateurs techniques simultanément. Dans ce cas, un des opérateurs est responsable de la version originale de la zone, et les autres opérateurs doivent s'adresser à lui afin d'en obtenir des duplicata. Des exigences contractuelles plus fortes doivent donc être demandées à l'opérateur responsable de la version originale. En effet, un incident affectant cet opérateur pourrait prévenir la distribution des duplicata aux autres opérateurs désignés par le titulaire et causer, à terme, l'indisponibilité de toute la zone. La distribution d'une version originale altérée frauduleusement suite à la compromission de l'opérateur responsable est un autre scénario d'attaque à envisager.

3.4 Les revendeurs

Les revendeurs sont des intermédiaires pouvant fournir une offre de services complète, ou dissimulant, par exemple, la complexité administrative ou technique du DNS. Ils assument alors le rôle de mandataire auprès des bureaux d'enregistrement et des opérateurs techniques.

La sécurité des revendeurs peut influer sur la sécurité des noms de domaine d'un titulaire. En effet, leur compromission peut amener à la perte de maîtrise du nom de domaine. Ce peut être notamment le cas si un attaquant obtient leur mot de passe d'accès aux interfaces du bureaux d'enregistrement, ce qui lui permet ainsi d'altérer des données techniques relatives à la délégation du domaine ou à la chaîne de confiance DNSSEC [15].

Avoir recours aux services d'un revendeur est facultatif pour l'exploitation d'un nom de domaine. Le lecteur est donc invité à mesurer les bénéfices apportés par la souscription à une telle prestation et à les mettre en rapport avec les risques et le transfert de responsabilité qu'elle induit. En particulier, il est nécessaire de s'assurer que les exigences de sécurité sont clairement stipulées dans le contrat, et qu'elles sont conformes avec la qualité de service attendue. Le titulaire peut, par ailleurs, confirmer la mise en œuvre des bonnes pratiques de sécurité du prestataire par le biais d'audits de sécurité.

Pour de plus amples précisions, le lecteur est invité à se référer à la section juridique du présent document, ainsi qu'au guide de l'ANSSI portant sur la maîtrise des risques liés à l'externalisation [4].

Recommandation 3

Lorsqu'un titulaire a recours à un prestataire, comme un revendeur, il doit entamer une démarche d'évaluation et de maîtrise des risques, notamment en suivant les recommandations du guide d'externalisation de l'ANSSI [4].

Chapitre 4

Aspects juridiques

L'attribution d'un nom de domaine est encadrée par un contrat qui organise la relation entre le titulaire et le bureau d'enregistrement. Cet aspect est détaillé dans la section 4.1.

L'enregistrement d'un nom peut être frauduleux ou abusif lorsqu'il correspond à des éléments sur lesquels des tiers détiennent des droits, comme des marques ou des dénominations sociales, ou qu'il fait référence de manière trompeuse à leur nom. On parle alors de « cybersquattage », de « typosquattage », de diffamation, ou encore contrefaçon.

La procédure utilisée pour le règlement des litiges doit faire l'objet d'une attention particulière des titulaires.

Ce chapitre présente les aspects juridiques liés au nom de domaine dans un but informatif et de manière non-exhaustive. En particulier, il n'aborde pas les problématiques liées à l'hébergement des données et au contenu. En cas de doute, le lecteur est invité à se faire assister par un conseiller juridique.

4.1 La relation titulaire - bureau d'enregistrement

Les contrats proposés pour l'enregistrement de noms de domaine sont des contrats d'adhésion dont la négociation est difficile pour le titulaire. Il importe donc d'en vérifier scrupuleusement le contenu et, le cas échéant, d'en accepter la mise en œuvre. Il est important de noter que ces contrats peuvent varier en fonction du registre responsable du nom de domaine parent de celui enregistré.

En dehors du contrôle des aspects techniques et administratifs notamment liés à la sous-traitance, aux modalités financières ou à la qualité de service, il est souhaitable que le titulaire s'assure que les points suivants sont indiqués dans le contrat :

- une convention de service [1], qui permet d'identifier et de définir les besoins du titulaire, de fournir un cadre général de compréhension des deux parties ;
- une procédure de verrou « de niveau registre » ;
- les conditions d'application d'une procédure de retrait d'office du nom de domaine en cas de litige ;

1. En anglais, *Service Level Agreement (SLA)*.

- la procédure de règlement des litiges en référence, le cas échéant, aux recommandations (*best practices*) de l'OMPI [2].

Dans tous les cas, les titulaires sont également invités à vérifier le droit et la langue applicables au registre ou au bureau d'enregistrement. En particulier, les bureaux ne sont pas nécessairement enregistrés juridiquement dans le même pays que le registre qui les accrédite.

De même, chaque registre est soumis aux lois et à l'autorité des tribunaux du lieu où il se trouve. Il est préférable d'adhérer à un registre dont la loi est maîtrisée par le service juridique du titulaire en cas de litige.

Recommandation 4

Choisir un bureau d'enregistrement et un registre soumis à la législation française ou européenne et dont la procédure de règlement des litiges fait référence à une langue et à un système juridique maîtrisés par le titulaire.

4.2 Les procédures de règlement des litiges

L'attribution de noms de domaine peut être source de litiges notamment concernant la contestation de la disponibilité ou de l'exploitabilité du nom de domaine.

Afin de résoudre ces litiges, il est possible de recourir à la fois à des procédures de résolution de litiges extra-judiciaires ainsi qu'au juge.

4.2.1 Solution extra-judiciaire

Chaque registre possède ses propres règles d'attribution des noms de domaine et son propre système de résolution des conflits, notamment en matière de propriété intellectuelle. Il s'agit de procédures alternatives de résolution des litiges qui sont des systèmes extrajudiciaires d'arbitrage mis à la disposition de ceux qui estiment qu'un tiers a porté atteinte à leurs droits en enregistrant un nom de domaine et/ou en l'utilisant d'une manière qui leur porte préjudice. Ainsi :

- l'ICANN met à disposition la procédure UDRP [3] permettant la médiation lorsque le nom de domaine rentre en conflit avec une marque [22]. L'ICANN ne gère pas directement cette dernière. Elle est déléguée à plusieurs centres dont l'OMPI, premier centre d'arbitrage et de médiation à connaître les contestations liées à l'attribution de noms de domaine ;

2. Organisation mondiale de la propriété intellectuelle.
3. *Uniform Dispute Resolution Policy*.

- l'EURID, registre en charge du nom de premier niveau européen `.eu`, met à disposition la procédure ADR [4] qui est la procédure extra-judicaire des litiges liés aux noms de domaine `.eu` et qui est administrée par la Cour d'arbitrage tchèque, organisme indépendant désigné par l'EURID [23] ;
- l'Afnic, registre en charge des noms de domaine de premier niveau français `.fr`, `.pm`, `.re`, `.tf`, `.wf` et `.yt`, met à disposition le Système de résolution des litiges Syreli [24]. Cette procédure voit l'Afnic statuer directement sur les recours qu'elle reçoit. Deux autres procédures sont également disponibles : une médiation par le CMAP [5] afin de permettre un accord amiable et un arbitrage géré par l'OMPI dont la décision s'impose aux parties.

4.2.2 Solution judiciaire

En France, devant les juridictions nationales, les litiges relatifs à la propriété intellectuelle sont fréquemment résolus sur le fondement de la contrefaçon [6] ou sur le fondement de la concurrence déloyale [7] permettant ainsi d'obtenir des dommages-intérêts ou la nullité de l'enregistrement de la marque ou du nom de domaine litigieux.

La loi et la jurisprudence posent notamment :

- un principe de la prédominance de l'antériorité [8], c'est-à-dire que c'est le titulaire du signe distinctif (en l'espèce un nom de domaine ou une marque) enregistré le premier qui est légitime à disposer du droit de demander l'enregistrement des autres signes distinctifs reprenant une dénomination identique ;
- un principe de priorité de l'usage commercial, c'est-à-dire qu'un nom de domaine est attribué de préférence au demandeur qui en fait une exploitation commerciale même si le nom de domaine correspond également à un nom patronymique [9]. La jurisprudence vient ici préciser qu'un nom de domaine ne peut être exploité qu'en l'absence de droits antérieurs. Ainsi un nom de domaine disponible peut ne pas être attribuable à un tiers en raison d'une marque antérieure.

Une attention particulière devra être portée quant aux marques de renommée ou notoires pour lesquelles le principe de l'enregistrement est atténué.

À titre d'exemple, la chambre du commerce de la Cour de cassation a notamment rappelé, le 13 décembre 2005, avec le pourvoi n°04-10.143 et sur la base du fondement de la contrefaçon, qu'« un nom de domaine ne peut contrefaire par reproduction ou

4. *Alternative Dispute Resolution*.
5. Centre de médiation et d'arbitrage de Paris.
6. Article L335-2 du code de la propriété intellectuelle.
7. Articles 1382 et suivants du code civil relatifs à la responsabilité civile.
8. Article 711-4 du code de la propriété intellectuelle et en particulier, TGI Paris, 3e chambre, 2e section, 17 janvier 2014 sur l'opposabilité de l'antériorité d'un nom de domaine à une marque sous la condition d'être exploité.
9. Cour d'appel de Versailles, 12e chambre, section 1, 27 avril 2006, Milka B./ Kraft Foods Schweiz Holding.

par imitation une marque antérieure que si la nature réelle des produits et services offerts sur ce site sont soit identiques soit similaires à ceux visés dans l'enregistrement de la marque et de nature à entraîner un risque de confusion dans l'esprit du public ».

Le tribunal de grande instance de Paris, 3e chambre, 2e section, lors le jugement du 13 juin 2003, a également rappelé que l'exploitation concurrentielle d'un site internet sous le nom de domaine `.fr` alors qu'il existe le même en `.com` est constitutive d'actes de concurrence déloyale et entraîne notamment le paiement de dommages-intérêts.

Recommandation 5

S'assurer de la disponibilité et de la licéité du nom de domaine préalablement à son enregistrement.

Chapitre 5

Résilience du DNS

Les considérations suivantes sont relatives à l'amélioration de la résilience du service DNS, notamment par des mesures techniques et des choix architecturaux. Ces recommandations s'appliquent à l'hébergement de toutes zones DNS, y compris les zones de résolution à rebours (*reverse zones*). Elles sont pour la plupart issues des études menées par l'Observatoire de la résilience de l'Internet français [25].

L'application de ces recommandations doit être effectuée par les opérateurs techniques auxquels le registre délègue techniquement le domaine du titulaire. Si le titulaire ne procède pas à l'auto-hébergement des serveurs faisant autorité sur ses noms de domaine, il lui incombe de vérifier que les opérateurs techniques qu'il désigne s'engagent contractuellement à l'application des bonnes pratiques de sécurité détaillées dans ce chapitre.

5.1 Dispersion topologique des serveurs de noms

Le protocole DNS définit une méthode de réplication standard des données entre les serveurs DNS. Cette méthode permet aux administrateurs système de bénéficier d'un moyen commun pour diffuser les données relatives à un nom de domaine sur de multiples serveurs DNS. L'impact d'une panne sur l'un des serveurs de noms en est alors réduit. Les RFC, normes de fait, développées par l'IETF [1], recommandent l'utilisation d'au moins deux serveurs de noms distincts [26].

Recommandation 6

Servir les noms de domaine depuis au moins deux serveurs faisant autorité distincts.

Idéalement, ces multiples serveurs DNS devraient être organisés et déployés de manière à ne pas être tous dépendants des mêmes installations.

Ainsi, la localisation des différents serveurs devrait être prise en considération afin de limiter l'impact d'incidents environnementaux, comme les coupures électriques, les coupures de fibres optiques, les inondations ou encore les tremblements de terre.

1. *Internet Engineering Task Force*.

De même, la connectivité réseau devrait être étudiée afin de prévenir les points de défaillance unique, que ce soit en termes de routage (incidents BGP) ou de dépendance à des transitaires uniques. Cette problématique est explicitée de façon détaillée dans le rapport de l'observatoire de la résilience de l'Internet français. La technique de l'*anycast* est notamment développée dans le rapport 2012 [25].

Aller plus loin 3

Répartir les serveurs de noms faisant autorité dans plusieurs préfixes (blocs d'adresses IP) ou utiliser la technique de routage *anycast*.

Aller plus loin 4

Éloigner ses serveurs de noms, par exemple, en les plaçant dans différents centres de données, afin de mieux résister aux menaces environnementales et aux incidents techniques.

5.2 Protocoles de transport

Bien que le protocole de transport du DNS soit à ce jour principalement UDP, la RFC 1035 [26] recommande la prise en charge de TCP comme protocole de transport. La RFC 5966 [27] renforce cette recommandation et rend la prise en charge de TCP obligatoire pour toutes les implantations du DNS et pour tous les types de communication DNS, y compris entre les services interrogeant le DNS et les serveurs faisant autorité.

La prise en charge de TCP est à ce jour particulièrement importante pour faire face aux problèmes suivants :

- l'accroissement de la taille des réponses DNS qui ne peuvent parfois pas être transportées de manière standard avec UDP ;
- l'emploi de mécanismes de protection anti-déni de service distribué, déployés notamment par la racine et les principaux opérateurs techniques de noms de premier niveau, qui emploient TCP comme stratégie de repli (voir section 5.9) ;
- l'emploi de mécanismes de protection contre certaines attaques par pollution de cache exploitant la fragmentation IP [28].

Le défaut de prise en charge de TCP expose les infrastructures ainsi configurées à des attaques en déni de service.

Recommandation 7

Configurer les infrastructures dans leur ensemble, notamment les serveurs, les répartiteurs de charge et les équipements de filtrage, pour prendre en charge TCP, en complément d'UDP, comme protocole de transport pour le DNS.

5.3 EDNS0

EDNS0 [29] est une extension au protocole DNS, qui permet notamment d'accroître la taille maximale des réponses DNS de 512 octets à une valeur précisée par l'expéditeur d'une requête [2].

L'accroissement de la taille maximale des réponses permet notamment de limiter l'emploi de TCP, lorsque des réponses trop volumineuses sont générées. En effet, si la prise en charge de TCP est indispensable, il convient de préférer l'usage d'UDP, ce dernier ne nécessitant pas le maintien d'une table d'états en mémoire. EDNS0 contribue donc à l'amélioration de la disponibilité du service.

Cette extension permet également de se préparer au déploiement de DNSSEC. Elle ajoute ainsi de nouveaux champs pour le stockage de drapeaux, et spécifie notamment le drapeau DO [3] permettant à l'expéditeur d'une requête de préciser s'il désire voir adjoindre à la réponse les éventuelles données relatives à DNSSEC, et ainsi que le résultat de la validation DNSSEC effectuée par le serveur interrogé.

Recommandation 8

Configurer ses infrastructures, notamment les serveurs DNS, les répartiteurs de charge, les systèmes de détection d'intrusion et les pare-feu, afin de prendre en charge EDNS0.

5.4 Durée de vie en cache

La durée de vie [4] en cache des enregistrements DNS désigne la durée maximale pendant laquelle une donnée devrait être gardée en cache par les équipements interrogeant les serveurs DNS faisant autorité. Passé ce délai, ces équipements doivent considérer les données mises en cache comme obsolètes et s'enquérir à nouveau des enregistrements DNS auprès des serveurs faisant autorité.

2. Cette valeur peut toutefois être revue à la baisse par le serveur répondant à la requête.
3. *DNSSEC OK*.
4. En anglais, *Time To Live (TTL)*.

La valeur du TTL de chaque enregistrement est du domaine de la politique locale : elle émane d'une réflexion de l'administrateur d'une zone DNS qui est le seul à pouvoir déterminer la périodicité des mises à jour des données qu'il publie dans le DNS. Une valeur de TTL non respectée peut donc avoir une incidence sur la stabilité (impact en disponibilité) voire sur la sécurité (intégrité) en fonction du type de données contenues dans l'enregistrement mis en cache (par exemple, des données cryptographiques).

Il est cependant à noter que le TTL joue un rôle dans la résilience et la disponibilité d'un service. En effet, plus le TTL est long, et plus l'information pourra rester accessible malgré une indisponibilité temporaire des serveurs faisant autorité sur cette dernière.

Des valeurs comprises entre une heure et deux jours devraient être adoptées dans la majorité des cas [30].

Recommandation 9

Configurer des valeurs de TTL relativement élevées, dans le cadre normal des opérations.

5.5 Sauvegardes

Les serveurs DNS sont organisés généralement selon un schéma maître-esclaves, avec le serveur maître hébergeant la version originale des données DNS, et les serveurs esclaves stockant des duplicata de ces mêmes données.

Selon le mécanisme standard de réplication des données, appelé transfert de zone, les serveurs DNS esclaves demandent au serveur maître un duplicata de la zone, et écrasent leur version locale avec la version originale la plus récente.

Ces sollicitations auprès du serveur maître se font, par défaut, à intervalles de temps prédéfinis, mais le maître peut également notifier les esclaves de la présence de données fraiches afin d'accélérer le processus de réplication.

Si une erreur ou un acte malveillant sont commis sur la version originale, la modification pourra donc être répliquée très rapidement par les serveurs esclaves, détruisant leurs versions encore intègres de la zone. Le mécanisme de réplication seul ne peut donc pas être considéré comme un moyen fiable d'effectuer des sauvegardes des zones DNS.

La mise en place d'autres méthodes de sauvegarde des zones DNS est donc nécessaire pour pallier les altérations involontaires ou frauduleuses de données.

La sauvegarde pourrait ainsi prendre la forme d'une simple copie de la base de données contenant les informations de la zone, comme le fichier *master* de Bind, ou bien

être effectuée à l'aide du mécanisme de transfert de zone depuis un serveur de sauvegarde, gardant un historique des versions de la zone.

Recommandation 10

Mettre en place une procédure de sauvegardes régulières des données contenues dans les zones DNS.

5.6 Surveillance

L'administration d'un serveur DNS est une tâche complexe impliquant notamment des mécanismes de réplication et d'éventuelles signatures cryptographiques.

L'introduction d'une erreur dans un fichier de zone ou le dysfonctionnement du mécanisme de réplication peut ainsi entraîner la diffusion d'informations invalides (corrompues ou obsolètes). Le DNS reposant sur des stratégies de mise en cache des informations, une donnée invalide peut, de plus, être longue à purger.

La détection rapide et automatisée des incidents est donc nécessaire, afin de limiter la durée de publication des données incorrectes et de limiter le nombre de serveurs DNS mettant en cache ces dernières.

Étant donné la nature hiérarchique du DNS, les incidents portant sur les intermédiaires situés en amont peuvent également avoir un impact sur les services hébergés sous un nom de domaine. La détection automatisée des incidents en amont peut ainsi être un atout afin de réagir efficacement et de rétablir dans les meilleurs délais la disponibilité des services affectés.

De tels outils de surveillance devraient être déployés depuis des réseaux différents de celui hébergeant le service DNS, afin de pouvoir détecter les pertes de connectivité et permettre l'émission des alertes en tout cas. La détection en elle-même peut être effectuée avec de simples scripts d'interrogation du service DNS, grâce à des outils sophistiqués comme ZoneCheck [31], ou encore à l'aide de plateformes spécialisées comme Nagios [32].

Recommandation 11

Mettre en place un système automatisé de surveillance des données fournies par ses serveurs faisant autorité et par ceux des zones parentes.

5.7 Diversité logicielle

Chaque vulnérabilité logicielle nécessite que l'attaquant écrive un code d'exploitation spécifique à l'implantation visée. Un code effectuant un déni de service sur une implantation n'aura donc pas nécessairement d'effet sur une autre implantation.

La diversité logicielle désigne le fait d'employer plusieurs implantations pour fournir un même service. Elle permet donc de limiter l'impact sur l'ensemble du service d'une unique défaillance logicielle.

En pratique, cela signifie employer différents logiciels de serveurs DNS sur les différents serveurs faisant autorité sur une zone. Différentes implantations des serveurs faisant autorité sont disponibles, parmi lesquelles Bind [33], Knot [34], Microsoft DNS [35], NSD [36], PowerDNS [37], ou bien encore Yadifa [38].

Il est à noter que cette bonne pratique accroît la charge de travail et nécessite des compétences supplémentaires.

Aller plus loin 5

Employer au minimum deux logiciels de serveurs DNS différents sur l'ensemble des serveurs faisant autorité sur un nom de domaine.

5.8 Séparation des rôles

Certaines implantations de serveurs DNS sont en mesure de fournir des services de nature différente aux utilisateurs locaux d'un organisme et aux utilisateurs provenant d'Internet.

Par exemple, des implantations comme Bind, Yadifa et Microsoft DNS offrent à la fois le service d'interrogation du DNS et peuvent également répondre à des requêtes sur des domaines pour lesquels elles font autorité.

Le service d'interrogation est assuré par des relais [5] ou des serveurs DNS récursifs parfois nommés, par abus de langage, serveurs cache. Ces serveurs sont chargés, suite à des requêtes d'utilisateurs, d'effectuer les résolutions de noms de domaine. Le schéma 5.1 illustre une requête DNS de l'utilisateur et la résolution du nom `www.france.fr` en l'adresse IP 8.12.195.126. Pour cela, le serveur récursif interroge la racine, puis suit les délégations d'autorité jusqu'à obtenir l'adresse recherchée du serveur DNS responsable de la zone `france.fr`. Cette dernière est alors retournée à l'utilisateur, après mise en cache par le serveur DNS récursif.

5. En anglais, *forwarders*.

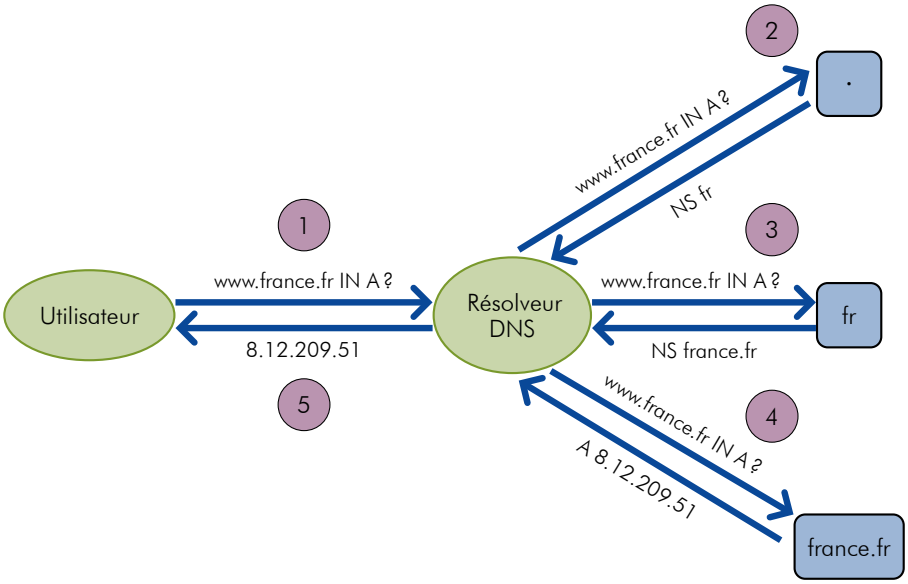

Figure 5.1 – Exemple de résolution DNS récursive

Ces implantations assurant à la fois les rôles de serveurs DNS faisant autorité et de serveurs récursifs, présentent une surface d'attaque accrue du fait des multiples services rendus. L'exploitation d'une vulnérabilité dans l'un des composants (serveur faisant autorité ou serveur récursif) pourrait donc avoir un impact en disponibilité sur l'autre service. Il est à noter cependant que ce risque est affaibli si les serveurs DNS ainsi configurés ne sont accessibles que depuis que des réseaux de confiance et qu'ils n'interrogent que des serveurs au travers de réseaux de confiance.

Il est préférable de séparer les rôles d'interrogation du DNS et de serveur faisant autorité en deux instances logicielles, par exemple en employant des processus ou serveurs séparés et isolés, afin de limiter les interactions.

Aller plus loin 6

Le service d'interrogation DNS devrait être rendu par un serveur ou un processus cloisonné distinct de celui rendant le service DNS faisant autorité sur des noms de domaine.

Le serveur DNS Bind offre un mécanisme de vues, qui lui donne la possibilité de répondre des données différentes en fonction d'informations présentes dans la requête. Ces paramètres peuvent être notamment l'adresse IP source de la requête ou une signature

crytographique spécifique [6].

Ce mécanisme offre une souplesse de configuration pouvant alléger la tâche d'administration du serveur DNS. Elle peut cependant présenter un risque dans le cas où les différentes données présentent des niveaux de sensibilité différents ou si les entités susceptibles d'interroger le serveur DNS bénéficient d'un niveau de confiance différent. C'est notamment le cas lorsqu'une vue présente des données relatives au réseau interne de l'organisme, tandis qu'une autre vue fournit des données relatives aux services exposés sur Internet.

Dans ce genre d'infrastructures, le cloisonnement des informations est uniquement logique. Ainsi, l'exploitation d'une vulnérabilité permettant d'accéder à la mémoire du serveur permettra à un attaquant situé sur un réseau de moindre confiance d'accéder indifféremment à toutes les données présentes dans toutes les vues de ce serveur.

De la même manière, si la vulnérabilité exploitée entraine un déni de service, le service DNS sera interrompu pour tous les réseaux auxquels le serveur DNS offrait son service.

Il est possible de s'affranchir du cumul des risques portés par chacun des réseaux auxquels le serveur est connecté en utilisant des processus distincts et cloisonnés. Les données contenues dans chaque vue seront alors ségréguées en fonction de leur sensibilité et du niveau de confiance des réseaux sur lesquels elles seront servies.

Recommandation 12

Répartir les données internes d'une part, et les données externes d'autre part sur des machines ou des processus distincts et cloisonnés.

5.9 Solutions anti-déni de service distribué

Les serveurs faisant autorité peuvent être exploités comme serveurs de rebond pour des attaques en déni de service distribué par amplification de trafic [39].

Les attaquants utilisent ces techniques afin d'accroître leur débit contre les victimes. Pour ce faire, ils tirent parti de l'asymétrie offerte par le protocole DNS entre la taille des questions et des réponses et des possibilités d'usurpations d'adresses IP.

N'ayant d'autre choix que de répondre aux questions concernant les domaines dont ils sont responsables, les serveurs faisant autorité doivent employer des solutions de limitation de débit afin de réduire l'impact de leur exploitation.

6. Cette signature cryptographique est basée sur un secret partagé et met en œuvre le mécanisme nommé *Transaction SIGnature (TSIG)*. Elle n'est pas liée aux signatures cryptographiques de DNSSEC, et est plus généralement utilisée pour sécuriser les transferts de zone entre serveurs DNS maîtres et esclaves.

Parmi les solutions disponibles, *Response Rate Limiting* (RRL) propose une approche modérée et ciblée, basée sur la détection de réponses DNS identiques envoyées en quantité à des groupes d'adresses IP. Ce mécanisme offre de plus une stratégie de repli en cas de faux-positif (mécanisme déclenché à tort). RRL est disponible pour Bind, NSD et Knot [40, 41, 42].

Le principe de la stratégie de repli (nommée *slipping*) est d'envoyer des réponses DNS tronquées, provoquant un ré-essai de la requête en TCP. L'adresse IP source d'une requête envoyée par TCP étant beaucoup plus difficile à usurper qu'avec UDP, ce mécanisme de repli lutte efficacement contre les attaques par amplification.

Recommandation 13

Employer le mécanisme anti-déni de service distribué RRL sur les implantations le proposant.

Les implantations de RRL de Bind et NSD, y compris les versions les plus récentes à la date de rédaction de ce guide, sont par défaut configurées pour ne répondre qu'à une fraction des requêtes reçues, une fois un seuil de tolérance dépassé.

Une étude menée par l'ANSSI a cependant démontré que l'absence de réponse aux requêtes DNS pouvait accroître l'efficacité de certaines attaques par pollution de cache [43].

La configuration du mécanisme RRL, lorsque les serveurs Bind et NSD sont utilisés, devrait donc être modifiée manuellement. Cela s'effectue en configurant la fréquence d'envoi de réponses (nommée « slip » pour Bind ou « rrlslip » pour NSD) à la valeur « 1 ».

Le serveur DNS Knot a pris en compte les recommandations de l'ANSSI et a adapté sa configuration par défaut.

Recommandation 14

Si RRL est mis en œuvre, utiliser une valeur de « *slipping* » de 1, afin de toujours répondre aux requêtes DNS.

Il est à noter que le risque découvert par l'étude de l'ANSSI ne se limite pas aux implantations employant RRL, mais à toutes les infrastructures disposant d'un mécanisme provoquant la perte de messages DNS. Cela inclut notamment l'usage de pare-feu limitant le nombre de paquets entrants.

```
example.com. IN NS dns1.example.com. ; délégation avec colle
dns1.example.com. IN A 192.0.2.1     ; colle
```

Figure 5.2 – Exemple de délégation d'un nom de domaine avec colle

```
example.com. IN NS ns1.example.net.
example.com. IN NS ns2.example.net.
```

Figure 5.3 – Exemple de délégation sans colle

5.10 Délégations et dépendance tierce

L'ajout d'enregistrements NS dans une zone permet de déléguer un sous-domaine. Ces enregistrements désignent les serveurs DNS devant être interrogés par les serveurs DNS récursif pour rechercher un nom faisant partie du sous-domaine délégué. Ainsi, en pratique, dans la zone `com`, des enregistrements NS indiquent les serveurs DNS de l'opérateur technique désigné par le titulaire et auxquels sont délégués la gestion du sous-domaine `example.com`.

Si le nom indiqué à droite dans l'enregistrement NS fait partie du domaine délégué, des enregistrements A ou AAAA additionnels, appelés « colle »[7] sont nécessaires. Un exemple de tels enregistrements est fourni en figure 5.2. Le serveur d'interrogation récupère ces colles en même temps que la délégation et peut immédiatement continuer la résolution de nom.

Si le nom indiqué dans l'enregistrement NS est hors du domaine délégué, alors ce nom doit être résolu avant de pouvoir reprendre la recherche originale. Ce mode de délégation, appelée « délégation sans colle »[8] peut apporter des risques additionnels par la création d'une dépendance à la disponibilité et à l'intégrité de ce domaine tiers.

Afin d'illustrer ce risque, prenons le cas d'étude d'un utilisateur demandant à résoudre l'adresse IP associée au nom de domaine `example.com`. Ce domaine est délégué comme indiqué dans la figure 5.3.

Lorsqu'un serveur récursif récupère ces délégations, il doit mettre en pause sa recherche de `www.example.com` pour obtenir l'adresse de l'un des deux serveurs DNS situés dans le domaine `example.net`. Si le domaine `example.net` est indisponible ou compromis, le domaine `example.com` le devient également, en conséquence.

Il convient de noter que ce risque est cependant négligeable si l'ensemble des acteurs organisationnels et techniques, c'est-à-dire registre, bureau d'enregistrement, reven-

7. En anglais, *glue records*.
8. En anglais, *glueless delegation*.

deur et serveurs hébergeant les domaines, sont identiques pour le nom de domaine délégué et les noms de domaine utilisés dans la délégation sans colle.

Recommandation 15

Privilégier les délégations avec colle lorsque l'usage de délégation sans colle introduit de nouvelles dépendances tierces.

5.11 Durcissement du socle technique

En plus d'une configuration renforcée des services DNS, le système d'exploitation sur lesquels ils sont installés doit être durci de manière adéquate.

L'ANSSI publie plusieurs guides relatifs à la sécurité des systèmes d'exploitation et des infrastructures réseaux. Le lecteur est notamment invité à se référer aux guides et notes techniques suivantes :

- Guide d'hygiène informatique [1] ;
- Mises à jour de sécurité [44] ;
- Recommandations de sécurité relatives à un système GNU/Linux [45] ;
- Problématiques de sécurité associées à la virtualisation des systèmes d'information [46] ;
- Recommandations de sécurité pour la mise en oeuvre d'un système de journalisation [47] ;
- Recommandations pour un usage sécurisé d'(Open)SSH [48].

Recommandation 16

Durcir le système d'exploitation hébergeant les logiciels DNS.

Chapitre 6

Rappel des recommandations

Recommandation 1

Choisir un registre offrant un service de verrou de niveau registre et obtenir des assurances ou des engagements contractuels sur le niveau de service garanti pour cette fonctionnalité.

Recommandation 2

Choisir un bureau d'enregistrement offrant un mécanisme d'authentification journalisée et renforcée, par exemple grâce à deux facteurs d'authentification et un filtrage des accès à l'interface d'administration.

Recommandation 3

Lorsqu'un titulaire a recours à un prestataire, comme un revendeur, il doit entamer une démarche d'évaluation et de maîtrise des risques, notamment en suivant les recommandations du guide d'externalisation de l'ANSSI [4].

Recommandation 4

Choisir un bureau d'enregistrement et un registre soumis à la législation française ou européenne et dont la procédure de règlement des litiges fait référence à une langue et à un système juridique maîtrisés par le titulaire.

Recommandation 5

S'assurer de la disponibilité et de la licéité du nom de domaine préalablement à son enregistrement.

Recommandation 6

Servir les noms de domaine depuis au moins deux serveurs faisant autorité distincts.

Recommandation 7

Configurer les infrastructures dans leur ensemble, notamment les serveurs, les répartiteurs de charge et les équipements de filtrage, pour prendre en charge TCP, en complément d'UDP, comme protocole de transport pour le DNS.

Recommandation 8

Configurer ses infrastructures, notamment les serveurs DNS, les répartiteurs de charge, les systèmes de détection d'intrusion et les pare-feu, afin de prendre en charge EDNS0.

Recommandation 9

Configurer des valeurs de TTL relativement élevées, dans le cadre normal des opérations.

Recommandation 10

Mettre en place une procédure de sauvegardes régulières des données contenues dans les zones DNS.

Recommandation 11

Mettre en place un système automatisé de surveillance des données fournies par ses serveurs faisant autorité et par ceux des zones parentes.

Recommandation 12

Répartir les données internes d'une part, et les données externes d'autre part sur des machines ou des processus distincts et cloisonnés.

Recommandation 13

Employer le mécanisme anti-déni de service distribué RRL sur les implantations le proposant.

Recommandation 14

Si RRL est mis en œuvre, utiliser une valeur de « *slipping* » de 1, afin de toujours répondre aux requêtes DNS.

Recommandation 15

Privilégier les délégations avec colle lorsque l'usage de délégation sans colle introduit de nouvelles dépendances tierces.

Recommandation 16

Durcir le système d'exploitation hébergeant les logiciels DNS.

Bibliographie

[1] ANSSI, « Guide d'hygiène informatique ». <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/l-anssi-publie-la-version-finalisee-du-guide-d-hygiene-informatique.html>, jan. 2013.

[2] ANSSI, « Recommandations de sécurité relatives aux mots de passe ». <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/mot-de-passe.html>, mai 2012.

[3] ANSSI, « Note d'information du CERT-FR sur les dénis de service ». <http://www.certa.ssi.gouv.fr/site/CERTA-2012-INF-001.pdf>, jan. 2013.

[4] ANSSI, « Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques ». <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html>, déc. 2010.

[5] S. Kitterman, « Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1 ». RFC 7208 (Proposed Standard), avril 2014.

[6] J. Schlyter et W. Griffin, « Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints ». RFC 4255 (Proposed Standard), jan. 2006.

[7] MyNic, « .my domain name incident resolved ». <http://www.mynic.my/upload_media/51d2a8d4edd6a.pdf>, juil. 2013.

[8] M. V. Horenbeeck, « Update on DNS hijackings ». <http://durban47.icann.org/meetings/durban2013/presentation-dns-hijacking-horenbeeck-15jul13-en.pdf>, juil. 2013.

[9] J. Schultz, « 'Hijacking' of DNS Records from Network Solutions ». <http://blogs.cisco.com/security/hijacking-of-dns-records-from-network-solutions/>, juin 2013.

[10] Avira, « Major DNS hijacking affecting major websites, including avira.com ». <http://techblog.avira.com/2013/10/08/major-dns-hijacking-affecting-major-websites-including-avira-com/en/>, oct. 2013.

[11] Henry Hoggard, « Hijacking DNS on NameCheap Domains ». <https://henryhoggard.co.uk/?p=77>, déc. 2013.

[12] Waqas, « Ebay and Paypal hacked by Syrian Electronic Army for not providing services in Syria ». <http://hackread.com/ebay-paypal-hacked-by-syrian-electronic-army/>, fév. 2014.

[13] Fran Berkman, « Syrian Electronic Army : We Hacked eBay and PayPal ». <http://mashable.com/2014/02/01/syrian-electronic-army-ebay/>, fév. 2014.

[14] S. Wagner, « Go Daddy Site Outage Investigation Completed ». <http://www.godaddy.com/news/article/go-daddy-site-outage-investigation-completed.aspx>, sept. 2012.

[15] CNET, « Melbourne IT tells how hacker launched NY Times cyberattack ». <http://news.cnet.com/8301-1023_3-57600368-93/melbourne-it-tells-how-hacker-launched-ny-times-cyberattack/>, août 2013.

[16] ICANN, « List of Top-Level Domains ». <http://www.icann.org/en/resources/registries/tlds>.

[17] S. Hollenbeck et M. Srivastava, « NSI Registry Registrar Protocol (RRP) Version 1.1.0 ». RFC 2832 (Informational), mai 2000. Updated by RFC 3632.

[18] S. Hollenbeck, « Extensible Provisioning Protocol (EPP) ». RFC 3730 (Proposed Standard), mars 2004. Obsoleted by RFC 4930.

[19] Morgan Marquis-Boire, « A Brief History of DNS Hijackings ». <http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf>, mars 2012.

[20] Maarten Van Horenbeeck, « Update on DNS hijackings ». <http://durban47.icann.org/meetings/durban2013/presentation-dns-hijacking-horenbeeck-15jul13-en.pdf>, juil. 2013.

[21] D. Atkins et R. Austein, « Threat Analysis of the Domain Name System (DNS) ». RFC 3833 (Informational), août 2004.

[22] ICANN, « Site web du Uniform Dispute Resolution Policy de l'ICANN ». <http://www.icann.org/fr/help/dndr/udrp/rules>.

[23] EURID, « Site web du Alternative Dispute Resolution de l'EURID ». <http://eu.adr.eu>.

[24] Afnic, « Site web du Système de résolution des litiges de l'Afnic ». <https://www.syreli.fr>.

[25] ANSSI, « L'observatoire de la résilience de l'Internet français ». <http://www.ssi.gouv.fr/fr/anssi/presentation/l-observatoire-de-la-resilience-de-l-internet-francais.html>, juil. 2013.

[26] P. Mockapetris, « Domain names - implementation and specification ». RFC 1035 (INTERNET STANDARD), nov. 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604.

[27] R. Bellis, « DNS Transport over TCP - Implementation Requirements ». RFC 5966 (Proposed Standard), août 2010.

[28] A. Herzberg et H. Shulman, « Fragmentation Considered Poisonous : or one-domain-to-rule-them-all.org », *in IEEE CNS 2013. The Conference on Communications and Network Security.*, 2013.

[29] P. Vixie, « Extension Mechanisms for DNS (EDNS0) ». RFC 2671 (Proposed Standard), août 1999. Obsoleted by RFC 6891.

[30] Peter Koch, « Recommendations for DNS SOA Values ». <http://www.ripe.net/ripe/docs/ripe-203>, juin 1999.

[31] Afnic, « ZoneCheck ». <http://www.zonecheck.fr>.

[32] Nagios Enterprise, « Nagios - The Industry Standard In IT Infrastructure Monitoring ». <http://www.nagios.org/>.

[33] ISC, « Bind Website ». <https://www.isc.org/downloads/bind/>.

[34] CZNIC, « Knot Website ». <https://www.knot-dns.cz/>.

[35] J. Groves, « Guide des opérations du serveur DNS ». <http://technet.microsoft.com/fr-fr/library/cc816603%28v=ws.10%29.aspx>, mai 2008.

[36] NLNet Labs, « NSD Website ». <http://www.nlnetlabs.nl/>.

[37] PowerDNS, « PowerDNS Website ». <https://www.powerdns.com/>.

[38] Eurid, « Yadifa Website ». <http://www.yadifa.eu/>.

[39] Prolexic, « Global DoS and DDoS Attack Reports, Trends and Statistics ». <http://www.prolexic.com/knowledge-center-dos-and-ddos-attack-reports.html>.

[40] ISC Support, « A Quick Introduction to Response Rate Limiting ». <https://kb.isc.org/article/AA-01000>, juin 2013.

[41] Wouter (W.C.A. Wijngaards), « DNS Response Rate Limiting as implemented in NSD ». <http://www.nlnetlabs.nl/blog/2012/10/11/nsd-ratelimit/>, oct. 2012.

[42] Knot Team, « Using Response Rate Limiting (Knot Documentation) ». <https://www.knot-dns.cz/static/documentation/knot.html/Using-Response-Rate-Limiting.html>.

[43] F. Maury et M. Feuillet, « Démonstration d'un détournement possible de technologies anti-déni de service distribué (DDoS) ». <http://www.ssi.gouv.fr/fr/anssi/publications/publications-scientifiques/articles-de-conferences/demonstration-d-un-detournement-possible-de-technologies-anti-deni-de-service.html>, oct. 2013.

[44] ANSSI, « Mises à jour de sécurité ». <http://www.securite-informatique.gouv.fr/gp_article96.html>, mai 2007.

[45] ANSSI, « Recommandations de sécurité relatives à un système GNU/Linux ». <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-a-un-systeme-gnu-linux.html>, juil. 2012.

[46] ANSSI, « Problématiques de sécurité associées à la virtualisation des systèmes d'information ». <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/problematiques-de-securite-associees-a-la-virtualisation-des-systemes-d.html>, juil. 2012.

[47] ANSSI, « Recommandations de sécurité pour la mise en oeuvre d'un système de journalisation ». <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-pour-la-mise-en-oeuvre-d-un-systeme-de.html>, déc. 2013.

[48] ANSSI, « Recommandations pour un usage sécurisé d'(Open)SSH ». <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-reseaux/recommandations-pour-un-usage-securise-d-open-ssh.html>, jan. 2014.

Acronymes

BGP	Border Gateway Protocol
CMAP	Centre de médiation et d'arbitrage de Paris
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EPP	Extensible Provisioning Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
OMPI	Organisation mondiale de la propriété intellectuelle
RFC	Request For Comments
RRL	Response Rate Limiting
RRP	Registry Registrar Procotol
SLA	Service Level Agreement
SPF	Sender Policy Framework
TLD	Top-Level Domains
TSIG	Transaction SIGnature
TTL	Time To Live

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.
En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.
Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Mai 2014

Agence nationale de la sécurité des systèmes d'information
ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : `www.ssi.gouv.fr` et `www.securite-informatique.gouv.fr`
Messagerie : communication [at] ssi.gouv.fr