DNS : types d'attaques et techniques de sécurisation

Le DNS (*Domain Name System*), un élément essentiel de l'infrastructure Internet

L'Internet est aujourd'hui critique pour l'économie comme pour la vie de notre société. Il repose sur une infrastructure très répartie et opérée par des acteurs divers : fournisseurs d'accès, points d'échange et d'interconnexion, opérateurs de télécommunications, hébergeurs, bureaux d'enregistrement… Ces acteurs apportent chacun une contribution essentielle au fonctionnement de l'Internet, et chacun est sujet à des menaces spécifiques.

Parmi ces éléments essentiels de l'Internet ; le « DNS » ou « *Domain Name System* ». Derrière cet acronyme se cache en effet un ensemble d'infrastructures techniques, logiciels et équipements, nécessaires au bon fonctionnement des noms de domaine permettant notamment d'accéder à un site web ou d'échanger des messages électroniques.

Ce dispositif particulièrement robuste fonctionne sans problèmes majeurs depuis les années 80. Il reste néanmoins vulnérable par certains aspects liés à sa conception, au développement de formes nouvelles d'attaques et à l'existence de vulnérabilités connues.

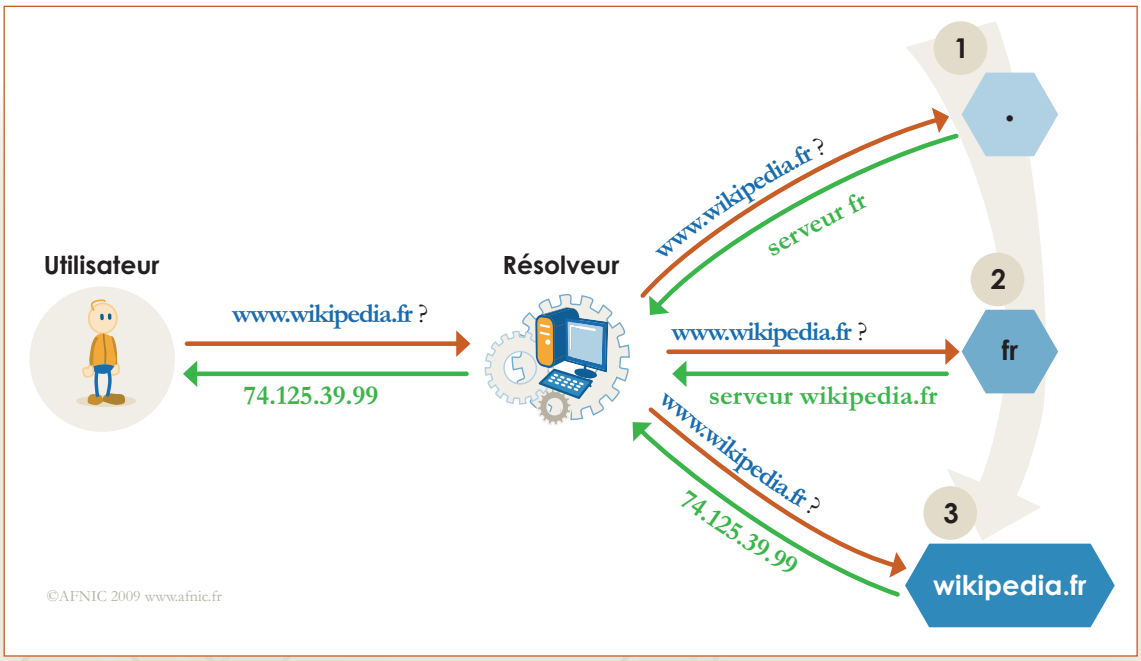
Ce dossier thématique présente de manière synthétique les enjeux liés au bon fonctionnement du DNS, les types d'attaques les plus fréquents et les principales techniques employées pour y faire face.

I Présentation du DNS (*Domain Name System*)

I.1 – Une structure arborescente

Le DNS est organisé sous la forme d'une arborescence inversée, avec une « racine » dont dépendent les différentes « branches ». Au premier niveau de l'arborescence se trouvent les « *Top-Level Domains* » ou domaines de premier niveau, comme les *.fr*, *.com* etc. Au second niveau, nous avons les noms de domaine « classiques » comme « afnic.fr ».

Fonctionnant comme une base de données distribuée sur des millions de machines, le DNS repose sur des interactions entre ces machines permettant d'identifier celle qui est la plus susceptible de pouvoir répondre à la requête d'un internaute.



Dans l'exemple ci-dessus, l'utilisateur veut se connecter au site http://www.wikipedia.fr. Il envoie sa requête via son navigateur. Celle-ci est reçue par un serveur dit « résolveur » qui a pour première mission d'identifier la machine sur laquelle est installé le nom de domaine wikipedia.fr. Le résolveur s'adresse d'abord à la « racine » du DNS (matérialisée par un point seul), qui lui indique quels sont les serveurs « faisant autorité » (c'est-à-dire compétents) pour *.fr* puisque le nom de domaine est en *.fr*. Dans un second temps, les serveurs du *.fr* indiquent à leur tour au résolveur que le nom de domaine wikipedia.fr est hébergé sur tel serveur. Celui-ci est alors en mesure d'indiquer au navigateur l'adresse IP du serveur web hébergeant les contenus du site web www.wikipedia.fr.

Ce schéma est vrai quel que soit le site web auquel on souhaite accéder, et quelle que soit l'adresse électronique à laquelle on souhaite écrire. Aussi la sécurité du DNS et la connaissance des attaques pouvant nuire à son fonctionnement sont-elles des enjeux pour tous les utilisateurs de l'Internet.

I.2 – Les logiciels

Le DNS fonctionne avec des logiciels spécifiques, dont certains sont commercialisés et d'autres disponibles en licence libre. Le plus utilisé de tous est BIND, développé et maintenu par l'Internet Systems Consortium (ISC). L'AFNIC et d'autres registres se sont engagés à soutenir le projet de développement de la future version de ce logiciel libre, BIND 10.

Dans certains cas, les attaques visent les infrastructures proprement dites, donc les serveurs sur lesquels sont installés les noms de domaine. Dans d'autres cas, les agresseurs cherchent à exploiter les possibilités offertes par les logiciels pour créer des situations anormales dont ils espèrent tirer profit. Les stratégies peuvent être subtiles, mais reposent souvent sur des schémas relativement bien identifiés.

II Les grands types d'attaques visant le DNS et les noms de domaine

Les attaques visant les noms de domaine et le DNS sont de plusieurs natures.

II.1 – Attaques ne visant pas directement le DNS

Les noms de domaine peuvent faire l'objet d'actions reposant plutôt sur l'exploitation des procédures administratives que dirigées contre les infrastructures ou les serveurs DNS :

- **le cybersquatting**, consistant à déposer un nom de domaine en portant volontairement atteinte aux droits d'un tiers pour en retirer profit ou pour lui nuire. Il existe beaucoup de techniques de cybersquatting, l'objectif étant généralement d'usurper l'identité de la victime et/ou de capter du trafic à ses dépends ;

- **le « détournement » ou le vol**, par l'appropriation du nom de domaine (mise à jour du champ titulaire et/ou des contacts) ou sa prise de contrôle au plan technique afin de détourner le trafic, en modifiant par exemple les serveurs de noms sur lesquels il est installé. Certaines méthodes sont dites « sociales », par exemple duper la victime pour la convaincre de transmettre un mot de passe à l'attaquant. D'autres sont plus techniques comme les injections SQL consistant à exploiter une faille de sécurité d'une application interagissant avec une base de données. De telles techniques se focalisent sur la prise de contrôle du nom de domaine via les interfaces de gestion proposées par les bureaux d'enregistrement à leurs clients titulaires de noms de domaine ou par les registres à leurs bureaux d'enregistrement.

web

Pour en savoir plus :
www.infoworld.com/t/authentication-and-authorization/google-blames-dns-insecurity-web-site-defacements-722

II.2 – Attaques visant directement le DNS

Les atteintes aux infrastructures DNS sont essentiellement d'ordre technique, faisant appel à des stratégies d'attaques massives ou de corruption des informations échangées entre les résolveurs et les serveurs DNS :

- **l'empoisonnement** vise à intoxiquer le résolveur pour qu'il considère que le serveur « pirate » est légitime, en lieu et place du serveur originel. Cette opération permet notamment de capter et de détourner les requêtes vers un autre site web sans que les utilisateurs puissent s'en rendre compte, avec à la clé, le risque de les voir confier des données personnelles en se croyant sur le site légitime de la victime de l'attaque. La « faille Kaminsky » dévoilée durant l'été 2008 fait partie de ce type d'attaques par empoisonnement des résolveurs DNS ;

- **le déni de service** (*Denial of Service* ou DoS) a pour objectif de rendre l'accès à un service impossible ou très pénible. Cette attaque peut se faire de manière brutale (saturation des serveurs par envoi massif de requêtes simultanées) ou plus subtile si l'attaquant essaie d'épuiser une ressource rare sur le serveur. Les attaques dirigées contre le système racine du DNS en février 2007 étaient typiquement des attaques par DoS ;

- **le déni de service distribué** (*distributed Denial of Service* ou dDoS), forme élaborée du DoS impliquant plusieurs milliers d'ordinateurs, en général dans le contexte d'un BOTNET ou roBOT NETwork : réseau d'ordinateurs « zombies » dont l'attaquant se sert à l'insu de leurs propriétaires grâce à des programmes malveillants diffusés via des vers se propageant d'une machine à l'autre ;

- **la réflexion** : des milliers de requêtes sont envoyées par l'attaquant au nom de la victime. Lorsque les destinataires répondent, toutes les réponses convergent vers l'émetteur officiel, dont les infrastructures se trouvent affectées ;

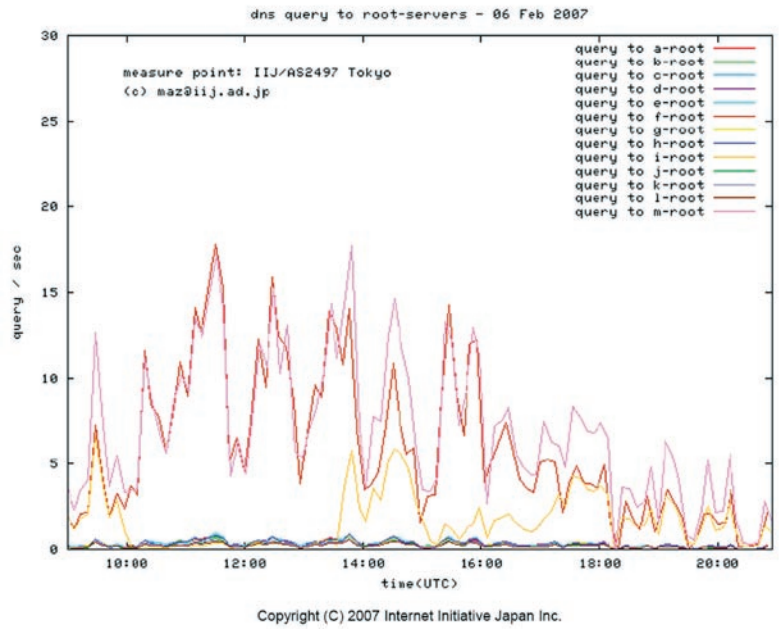
- **la réflexion combinée à l'amplification** : si la taille de la réponse est plus grosse que celle de la question, on dit qu'il y a amplification. La technique est la même que pour la réflexion, mais la différence de poids entre question et réponses crée un effet amplificateur. Une variante peut exploiter les mécanismes de protection mis en place, qui ont besoin de temps pour décoder les réponses longues avec pour effet éventuel un ralentissement dans la résolution des requêtes ;

- **le Fast flux** : afin de ne pas être identifié, l'attaquant peut, en plus de la falsification de son adresse IP, utiliser cette technique reposant sur la rapidité de la diffusion des informations de localisation pour masquer l'origine de l'attaque. Diverses variantes existent, comme le Simple flux (changer en permanence l'adresse du serveur web), ou le Double Flux (changer en permanence l'adresse du serveur web mais aussi les noms des serveurs DNS).

II.3 – Un exemple réel : l'attaque de février 2007 contre le système racine

Le graphique ci-contre met en exergue l'impact de l'attaque du 6 février 2007 contre les 13 serveurs sur lesquels repose le système racine du DNS.

Requêtes sur les serveurs racine



Source: Root Attack – end-user view – Matsuzaki Yoshinobu, 2007
http://www.nanog.org/mtg-0706/Presentations/lightning-maz.pdf

On voit clairement dans ce graphique que certains serveurs sont beaucoup plus touchés que d'autres : « M », « L » et « G » notamment. Ceux-ci ne forment cependant qu'une minorité, fortement impactés entre 10 heures et 16 heures avant de revenir progressivement à des temps de résolution plus habituels. Malgré les ressources engagées dans cette attaque, celle-ci ne s'est finalement pas révélée critique, la plupart des internautes dans le monde n'ayant expérimenté aucune dégradation du service.

S'il est relativement aisé d'impacter le DNS ou la performance d'un serveur, il est beaucoup plus difficile de le faire sur une longue durée et surtout si l'on ne veut pas être repéré. Les infrastructures sont donc conçues pour pouvoir supporter des pics d'activité considérables pendant de brèves périodes.

Bien qu'exposé à des attaques, le DNS reste un système particulièrement robuste dans son ensemble, capable non seulement de supporter des usages de plus en plus intensifs et diversifiés de l'Internet, mais aussi de résister à des attaques massives. Cela n'exclut pas pour autant le recours à des mesures destinées à le protéger encore mieux, les dispositifs adoptés par chaque acteur pris isolément pouvant d'ailleurs s'avérer beaucoup plus faciles à briser que le système dans sa globalité. Toute structure présente sur Internet doit donc s'assurer que cette présence ne repose pas, sans qu'elle s'en doute, sur des bases trop fragiles.

web **Autre exemple réel :**

- Attaque contre une banque brésilienne en avril 2009
  (le seul cas bien documenté d'une attaque Kaminsky)
  www.theregister.co.uk/2009/04/22/bandesco_cache_poisoning_attack/

III Les principales techniques de sécurisation

Chaque acteur présent sur Internet est un maillon d'une chaîne de valeur où tous sont interdépendants. Les conseils suivants ne sont donc pas destinés à une catégorie d'acteurs en particulier mais à tous ceux qui participent du fonctionnement du DNS : gestionnaires de domaines de premier niveau (registre), bureaux d'enregistrement, entreprises, fournisseurs d'accès…

L'objet de ce dossier n'est pas d'entrer dans le détail des actions pouvant ou devant être envisagées pour garantir un niveau de sécurité correct du dispositif DNS d'une structure. Quelques lignes directrices peuvent cependant être citées :

- **assurer la meilleure redondance possible,** de manière à ce qu'un serveur affecté par une attaque puisse être remplacé en toute transparence par d'autres serveurs disposant des mêmes informations mais situés sur d'autres réseaux. C'est la raison pour laquelle les registres de noms de domaine, tel l'AFNIC, exigent toujours que chaque nom de domaine soit installé sur au moins deux serveurs de noms. D'autres techniques plus élaborées, comme le recours à des nuages anycast, permettent d'augmenter encore plus la redondance avec à la clé des gains notables en termes de sécurisation et de performances ;

- **veiller à utiliser des versions à jour des logiciels DNS**, notamment de BIND, corrigées par les « patchs » appropriés, afin de ne pas être vulnérable à des attaques portant sur des failles de sécurité déjà bien identifiées ;

- **assurer une surveillance régulière de ses serveurs et de leur configuration**, de préférence depuis plusieurs points de l'Internet. Il est souvent arrivé, en raison de la robustesse du DNS, que la panne de serveurs ne soit détectée que lorsque le dernier d'entre eux tombe en panne. Pour vérifier la configuration, il existe des logiciels libres comme ZoneCheck. Pour assurer la surveillance depuis l'extérieur, l'organisation qui ne souhaite pas déployer une infrastructure spécifique peut faire appel à des services commerciaux ou communautaires existants ;

- **envisager de déployer DNSSEC**, protocole de sécurisation du DNS par l'authentification des serveurs, ce système limitant notamment les attaques par empoisonnement. La perception de l'intérêt de DNSSEC a été fortement accrue par la révélation de la faille Kaminsky qui a montré comment exploiter efficacement des vulnérabilités déjà connues au plan théorique ;

- **définir un « Plan de continuité d'activité »** permettant à la victime d'une attaque de poursuivre, ou de reprendre en cas d'incident grave, ses activités avec un minimum d'indisponibilité de ses services. Cette précaution est particulièrement essentielle pour tous ceux qui dépendent d'Internet – et donc du DNS – pour leur chiffre d'affaires, notamment ceux qui proposent des services en ligne à leurs clients.

En conclusion

La sécurité de l'infrastructure de l'Internet repose sur une répartition adéquate des rôles entre les différents acteurs (opérateurs de service, FAI, registres, bureaux d'enregistrement, hébergeurs, points d'échange, autorités publiques, CERT…). La diversité des structures, des technologies et des approches est l'un des principaux gages de la résilience de l'Internet.

Chacun des acteurs de cet écosystème doit ensuite appliquer les principes de base d'une sécurité efficace : **coordination**, **communication** et **coopération**, qui constituent les « **3 C** ». Dans le cas de l'Internet, la variété et le nombre des acteurs impliqués soulèvent un défi important, tant au plan national qu'international.

Face à des menaces évolutives et susceptibles de monter en puissance, des réponses isolées ou non coordonnées risquent de s'avérer de moins en moins pertinentes. De la même manière, la sensibilisation continue des différents acteurs aux enjeux de la sécurité fait partie des actions de fond à mener.

Les registres Internet se sont fortement mobilisés depuis plusieurs années sur ces questions, et nombre d'entre eux ont déjà mis au point des systèmes leur permettant d'assurer la continuité de leur activité même en cas d'incident imprévu et échappant à leur contrôle. Cette démarche est aussi adoptée par des prestataires et des clients finaux gérant leurs propres infrastructures. Il subsiste néanmoins une marge de progression significative pour atteindre une situation où tous les maillons de la « chaîne sécurité se seraient parfaitement approprié la règle des « 3 C ».

Pour aller plus loin

- DNS Resources Directory, bon annuaire de ressources web concernant le DNS : www.dns.net/dnsrd/
- Les supports de cours de formation de l'AFNIC, disponibles sous une licence libre : www.afnic.fr/doc/formations/supports
- Une bonne note de synthèse du CERTA : www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002/
- Summary Report du « Global DNS Security, Stability, and Resiliency Symposium, February 3-4, 2009 » : www.gtisc.gatech.edu/pdf/DNS_SSR_Symposium_Summary_Report.pdf

Retrouvez tous les dossiers thématiques de l'AFNIC :
www.afnic.fr/actu/presse/liens-utiles