Rapport du Conseil scientifique de l'Afnic

Conséquences du filtrage Internet par le DNS

afnic

Conséquences du filtrage Internet par le DNS[1]

En France et dans le monde, le filtrage dans l'Internet a été au cœur de récents événements[2] et abordé dans des décrets ou projets de lois (ARJEL[3], LOPPSI2[4], SOPA[5], PIPA[6]...). Les initiatives législatives ou réglementaires concernent différents domaines, comme la protection contre les virus ou malwares, la protection de l'enfance contre la pédopornographie, l'interdiction d'accès à des sites de jeux en lignes non autorisés ou la lutte contre le piratage.

Le filtrage, ou blocage, peut s'effectuer aussi bien au niveau des adresses IP que des noms de domaines. Dans ce document, le conseil scientifique de l'Afnic fait le point sur les techniques pouvant être employées lorsque le filtrage intervient au niveau du nommage dans le DNS (*Domain Name S*ystem, et les conséquences prévisibles de ce type de mesures.

1. Filtrage des noms de domaines

Le filtrage consiste à modifier le processus normal de résolution d'un nom d'un serveur vers une adresse IP soit en bloquant la réponse, soit en répondant un message d'erreur, soit en retournant l'adresse d'un autre serveur indiquant généralement que l'accès à ce site est interdit.

Contrairement aux réseaux téléphoniques qui reposent sur une infrastructure dédiée, le service DNS s'appuie, comme les autres services Internet qui l'utilisent (Web, Mail...), sur le réseau Internet lui-même, pour échanger des données. Il est à noter que le DNS est arrivé relativement tardivement dans l'histoire de l'Internet quand les noms des équipements connectés ne pouvaient plus être stockés dans un simple fichier[7].

---

1 Ce texte reprend notamment des extraits d'un document de référence produit par CENTR, l'organisation européenne des registres de premier niveau de l'Internet, http://centr.org/system/files/agenda/attachment/centr-paper-blocking-20120302.pdf

2 À titre indicatif, affaires "The Pirate Bay" (http://money.cnn.com/2012/01/20/technology/pirate_bay/index.htm), wikileaks (http://fr.wikipedia.org/wiki/WikiLeaks), copwatch (http://abonnes.lemonde.fr/societe/article/2011/10/14/la-justice-interdit-le-site-web-copwatch_1588162_3224.html)...

3 http://www.arjel.fr/

4 http://fr.wikipedia.org/wiki/Loi_d'orientation_et_de_programmation_pour_la_performance_de_la_s%C3%A9curit%C3%A9_int%C3%A9rieure

5 http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act

6 http://en.wikipedia.org/wiki/PROTECT_IP_Act

7 Historiquement, ces informations étaient stockées dans un fichier hosts.txt que l'on peut toujours utiliser prioritairement au DNS, même dans les systèmes d'exploitation les plus modernes.

Le DNS fonctionne de manière distribuée, selon une architecture où l'information de référence est très largement déléguée à de nombreux acteurs. Des registres comme l'Afnic aiguillent vers les serveurs effectuant la correspondance entre les adresses IP et les noms. Pour rendre le système à la fois plus robuste et plus efficace, trois mécanismes sont mis en œuvre : la hiérarchisation de l'information, l'utilisation de plusieurs répliques des serveurs et la mise en cache des réponses obtenues.
La hiérarchisation est basée sur la structuration du nom. Ainsi, lors de la résolution du nom `www.wikipedia.fr`, un serveur, dit racine, est interrogé pour aiguiller sur les serveurs de noms de la zone .fr, zone dite « de premier niveau ». L'un des serveurs de .fr est à son tour interrogé pour aiguiller sur les serveurs de noms de la zone `wikipedia.fr` (zone déléguée sous .fr). Enfin, l'un des serveurs de noms de `wikipedia.fr` est interrogé à son tour. Ce dernier retourne alors l'adresse IP recherchée (celle de `www.wikipedia.fr`).

Les résolveurs permettent de traiter de manière itérative les requêtes précédemment décrites. Ils ont besoin d'une configuration minimale, notamment une connaissance des adresses des serveurs de la racine, et permettent de mettre en cache les réponses obtenues pour éviter de trop solliciter l'architecture du DNS. Les FAI grand public mettent en place pour leurs clients des résolveurs dont les adresses sont fournies avec les autres paramètres de configuration. Mais le client peut très bien configurer une autre adresse de résolveur soit sur sa « box », soit sur son ordinateur. Le nombre de résolveurs dans le monde est très important (de l'ordre de la dizaine de millions) et croît régulièrement[8]. Google[9] et OpenDNS offrent ce service. Un utilisateur peut même installer son propre résolveur sur son ordinateur.

Le blocage d'information de correspondance peut donc se faire à deux endroits, soit au niveau du registre qui ne publie plus les informations qui disparaîtront progressivement des caches, soit au niveau des résolveurs. Sur ceux-ci, le filtrage peut s'effectuer par liste noire (Black List) fournie par les instances gouvernementales ou judiciaires. Ce système dépend de la coopération des FAI ou d'autres opérateurs de résolveurs pour tenir à jour la liste dans la configuration des résolveurs. Techniquement le blocage d'une résolution est disponible dans certaines distributions logicielles telles que BIND (une des plus employées), mais cette fonctionnalité n'est pas standardisée[10]. Notons qu'il y a peu de recul sur l'impact du filtrage à l'échelle d'un pays.

[8] L'ICANN estime leur nombre à environ à 10 millions dans le monde (http://blog.icann.org/2012/03/ten-million-dns-resolvers-on-the-internet/)

[9] https://en.wikipedia.org/wiki/Google_Public_DNS

[10] Ce logiciel possède depuis 2011 l'option RPZ (*Response Policy Zone*) permettant à un serveur de mentir lors d'une résolution soit en retournant une erreur soit en renvoyant une autre valeur.

2. Le filtrage est peu efficace

Tant que le contenu demeure en ligne[11], le filtrage d'un nom de domaine n'atteint pas totalement son objectif. L'utilisateur peut toujours accéder au contenu visé, soit en tapant directement l'adresse IP du serveur, soit en mettant la correspondance nom-adresse dans un fichier sur sa machine. Le site peut également créer des noms alternatifs ne faisant pas partie de la liste des sites bloqués[12].

Si une résolution de nom est filtrée dans un pays, l'utilisation de proxy http anonymes permet d'accéder (généralement gratuitement) au contenu à partir d'un autre pays. Les moteurs de recherche offrent des listes de proxys.

L'utilisation des VPN (réseaux privés virtuels) s'avère plus complexe, mais offre plus de stabilité et moins de risques que le mécanisme de proxy http anonyme. En effet, les VPN permettent à l'utilisateur d'apparaître comme connecté d'un autre lieu. Ils nécessitent souvent un compte payant, mais il est facilement imaginable qu'un site commercial, comme un casino en ligne, l'offre à ses clients en contrepartie de l'abonnement.

L'utilisateur peut également configurer sa machine ou sa box pour utiliser un résolveur DNS alternatif comme ceux de Google ou de OpenDNS. Dans ce cas, le filtrage effectué par l'opérateur devient inefficace, à moins de bloquer les requêtes DNS[13]. Par ailleurs, pour les établissements utilisant leurs propres résolveurs, le blocage au niveau des résolveurs des FAIs n'a pas d'effet.

3. Le filtrage accroît l'exposition de l'utilisateur aux menaces

Le principe de base soutenant le DNS implique que l'utilisateur doit obtenir l'information qu'il recherche et qui lui permette d'atteindre le site désiré. C'est la raison pour laquelle de nombreux messages de sécurité conseillent à l'utilisateur de vérifier le nom du site dans sa barre d'URL avant d'entrer des données confidentielles. Le filtrage et les redirections affaiblissent cette règle. L'utilisateur perd un des repères de confiance lorsqu'il consulte un site web ou reçoit du courrier électronique.

Les utilisateurs peuvent découvrir que le contenu auquel ils souhaitent accéder est toujours en ligne, mais que les règles d'accès ont changé. En modifiant le comportement de leur navigateur ou de leur machine (comme indiqué précédemment), ils pourront de nouveau y avoir accès. Ces modifications risquent de se développer à grande échelle.

11 Il peut être même répliqué comme l'ont montré les cas de wikileaks ou de copwatch.

12 La liste de ces contournements est longue, par exemple les serveurs de piratebay peuvent être accessibles par exemple via l'URL http://www.baiedespirates.be/

13 Plusieurs protocoles sont en cours de définition permettant de chiffrer les requêtes vers un autre résolveur en utilisant TLS, soit en utilisant pour le protocole de résolution un format actuellement plus standard comme XML au dessus de HTTP.

Le proxy ainsi configuré peut, à l'insu de l'utilisateur, détourner le trafic vers un autre site, capturer le trafic de l'utilisateur et obtenir des données confidentielles. L'usage qui est fait de ces données, souvent personnelles, par les fournisseurs de ces services, n'est dans la plupart des cas pas contrôlé par l'utilisateur.

La mise en place de résolveurs alternatifs peut également augmenter les risques d'hameçonnage. Un utilisateur peut configurer son système pour accéder à un site de jeux en ligne. Quelques jours plus tard, voulant se connecter à sa banque, il peut être dirigé vers un faux site, sans faire la relation entre les deux événements.

De manière indirecte, le blocage expose donc l'utilisateur à de nouvelles menaces.

Le filtrage peut également avoir des effets de bord non négligeables. Le blocage par nom de domaine ne permet pas de bloquer au moyen du DNS un sous-ensemble des pages ou URL d'un site[14]. Au contraire, le blocage d'un nom de domaine bloque l'ensemble des URL utilisant ce nom, autrement dit un site web complet. On parle alors de surblocage. Par exemple, on imaginera aisément les perturbations que provoquerait un blocage complet de Wikipedia, Facebook ou Dailymotion suite à un contenu illégal précis (comme cela avait été le cas en Grande-Bretagne pour un article sur l'album musical "Virgin Killer"[15]). De telles possibilités de déni de service par blocage complet pourraient donner lieu à des abus.

De nombreux exemples montrent que des erreurs de configuration ou un mauvais filtrage peuvent avoir des effets néfastes. Par exemple, en 2006, bizar.dk, un site danois, se retrouve bloqué par erreur[16], ce qui amènera le titulaire à menacer la police danoise de procès pour diffamation, avant que celle-ci ne s'excuse et ne supprime le site de la liste de blocage.

4. Les résultats de l'enquête Afnic

L'Afnic a publié l'édition 2012 de son enquête de « toile de fond technologique »[17] sur les tendances et évolutions technologiques prévisibles au cours des dix prochaines années, auprès d'experts et professionnels de l'Internet.

Deux questions de cette enquête sont particulièrement pertinentes pour le présent document. Les questions sont énoncées sous forme d'assertions de prévisions et appellent une réponse exprimant un niveau d'accord sur les assertions.

La première question/assertion (Q70 de l'enquête) est énoncée comme suit : « Les résolveurs DNS locaux (caches installés sur des machines utilisateurs) vont prendre une part significative (25% ou plus) par rapport aux résolveurs des FAI ou résolveurs "ouverts" type

14 Pour une granularité plus fine, il faut bloquer les requêtes HTTP conduisant à un surcoût important.

15 http://www.ecrans.fr/Wikipedia-victime-collaterale-de,5883.html

16 http://translate.google.com/translate?sl=da&tl=fr&js=n&prev=_t&hl=en&ie=UTF-8&layout=2&eotf=1&u=http%3A%2F%2Fm.cw.dk%2Fart%2F33184%2Fpolitiet-erkender-censurbroeler-paa-nettet

17 http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/6392/show/l-internet-dans-10-ans-des-professionnels-repondent-a-l-enquete-afnic.html

Google DNS ». Les résultats de l'enquête montrent une divergence sur les prévisions entre deux « écoles » (40% d'accord, 42% pas d'accord et 18% qui ne se prononcent pas). Il est ainsi possible de retenir qu'il y a tout de même 40% des répondants qui prévoient un recours aux résolveurs individuels en remplacement des résolveurs communs (qu'ils soient ceux du FAI ou d'un fournisseur alternatif tel que Google DNS).

La seconde question/assertion (Q71 de l'enquête) est quant à elle formulée comme suit : « Pour les cas de requêtes DNS confiées à un tiers (FAI ou offreurs de résolveurs alternatifs), le recours aux résolveurs alternatifs dépassera l'utilisation du résolveur de son propre FAI ». Là aussi, il y a divergence entre « deux écoles » (41% d'accord, 39% pas d'accord et 20% nsp). À nouveau, on peut noter que presque la moitié de ceux qui se prononcent prédisent une érosion progressive de l'usage du résolveur du FAI au profit de fournisseurs alternatifs, aboutissant à une inversion du rapport des forces.

Par ailleurs, les répondants qui sont d'accord avec l'une ou l'autre des deux assertions ci-dessous sont interrogés sur la motivation de leur réponse. Ils pensent en majorité que d'une part, « cela permet une meilleure garantie de l'intégrité des réponses », et de l'autre, « cela permet une meilleure performance ». Cela montre le crédit qu'ils accordent à ces méthodes alternatives au résolveur de leur propre FAI.

5. Conclusion

Le DNS est un maillon essentiel dans l'architecture de l'Internet. Beaucoup d'efforts sont mis en œuvre pour le sécuriser, comme l'introduction de la cryptographie pour valider les réponses avec DNSSEC. La sécurité technique apportée par DNSSEC pour protéger de bout en bout l'intégrité du DNS contre les attaques d'intermédiaires malveillants risque d'être perturbée par la mise en place de filtrage par altération des réponses, et de compromettre l'adoption de ces extensions de sécurité.

Par ailleurs, pendant des années, les FAI et les sites de commerce électronique ont éduqué les internautes aux risques courants. En compromettant le mécanisme de résolution de noms, et de ce fait en encourageant un comportement risqué, le filtrage du DNS risque de réduire la confiance dans le commerce électronique.

Le DNS n'a pas été conçu pour filtrer les contenus. Si une décision relative à l'utilisation du blocage reposant sur le DNS ou d'autres techniques était envisagée, elle devrait être évaluée au regard de la proportionnalité entre l'objectif visé, l'efficacité relative de la mesure, et en tenant compte des conséquences ci-dessus[18].

[18] http://www.securityweek.com/dns-blocking-where-technical-considerations-meet-political-considerations