RFC 7686 : The .onion Special-Use Domain Name

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 octobre 2015

Date de publication du RFC : Octobre 2015

https://www.bortzmeyer.org/7686.html

Le TLD .onion est utilisé par Tor pour nommer des serveurs Internet dont la localisation exacte est cachée. Tor est surtout connu pour permettre aux **clients** de demeurer relativement intraçables pendant leurs activités sur l'Internet, et .onion étend cette possibilité aux **serveurs**. Ce TLD n'avait aucune forme d'existence officielle avant, il avait juste été choisi comme cela et était reconnu par les logiciels Tor. Désormais, il est stocké dans le registre des noms de domaine spéciaux <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml> créé par le RFC 6761 [1].

C'est politiquement une certaine forme de reconnaissance de la part de l'IETF pour ces services cachés de Tor (que TF1 et les ministres nomment le "*Dark Web*"). Mais cela ne changera pas grand'chose en pratique, .onion était utilisé depuis des années, illustrant d'ailleurs la déconnexion entre la réalité et certains professionnels de la gouvernance Internet, qui croient que l'ICANN est le « régulateur de l'Internet ».

Techniquement, cet enregistrement de .onion dans le registre des noms de domaine spéciaux mènera peut-être certains logiciels à intégrer une connaissance de ce TLD, pour ne **pas** faire de requêtes .onion dans le DNS (requêtes involontaires et qui peuvent « trahir » un utilisateur de Tor).

La section 1 de notre RFC rappelle le principe de Tor et des .onion. Tor est spécifié dans « "*Tor : the second-generation onion router*" <https://spec.torproject.org/tor-spec> ». Ses services cachés (dont la localisation du serveur est caché : le service lui-même est parfaitement visible, c'est le but) sont identifiés par un nom de domaine en .onion. Par exemple, celui de Facebook, société dont un employé est co-auteur du RFC, est facebookcorewwwi.onion. Comme c'est un nom de domaine, il peut s'utiliser partout où on utilise un nom de domaine, par exemple dans les URI. Ainsi, le blog

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6761.txt

d'Amaelle Guiton est accessible en . Comme ce nom est spécial, on n'utilise **pas** le DNS pour trouver des données comme l'adresse IP. Un nom en `.onion` est un identificateur cryptographique (c'est le condensat de la clé publique du serveur). Il est « auto-authentifiant » ce qui veut dire que le client peut s'assurer qu'il parle au bon serveur, via la signature de la communication par la clé du serveur, sans avoir besoin, par exemple, d'un certificat, et ceci que le réseau sous-jacent soit de confiance ou pas. Comme l'identificateur est un condensat cryptographique, il n'est normalement pas compréhensible par un humain (voir la section 4 pour une nuance à cette affirmation, comme dans le cas du nom de Facebook ci-dessus).

Les noms en `.onion` sont générés localement, sans utiliser une autorité distincte (voir les explications pour mon blog <`https://www.bortzmeyer.org/blog-tor-onion.html`>). Aucun registre n'est utilisé (lors de la chaude discussion à l'IETF sur ce RFC, une minorité avait protesté contre le fait que cet enregistrement du TLD privait l'ICANN d'une source de revenus). On n'enregistre pas un nom en `.onion`, on ne le vend pas, on n'en est « propriétaire » que parce qu'on connait la clé privée correspondante (au passage, comme avec tous les identificateurs cryptographiques, de Namecoin <`https://www.bortzmeyer.org/namecoin.html`> à BitMessage <`https://www.bortzmeyer.org/bitmessage.html`>, **attention à vos clés privées !** Si elles sont perdues, vous n'avez aucun recours).

On a vu que `.onion` n'utilise pas le DNS. Pour éviter les collisions entre un nom extérieur au monde du DNS et un nom identique qui serait dans le DNS, le RFC 6761 avait introduit le concept de « noms de domaine spéciaux ». Ces noms ont la syntaxe et une partie de la sémantique des noms utilisés dans le DNS mais ne sont jamais supposés apparaitre dans le DNS. Dans le registre des noms spéciaux, on précise ce que doivent faire les différents composants du DNS (bibliothèques, résolveurs, registres, etc) s'ils rencontrent ces noms. À part les noms du RFC 2606, devenus « spéciaux » par la suite, le premier nom spécial enregistré était le `.local` d'Apple, via le RFC 6762. Comme pour `.local`, notre nouveau RFC demande que `.onion` soit traité spécialement par les logiciels DNS. En pratique, évidemment, cette demande ne sera pas honorée par tous et il y aura donc pendant encore longtemps des « fuites », des requêtes DNS pour `.onion` qui arrivent aux serveurs racine. Au moment de la publication de notre RFC, `.local` était le troisième TLD le plus demandé à la racine (derrière les indéboulonnables `.com` et `.net`, cf. les statistiques du serveur racine L <`http://hedgehog.dns.icann.org/`>) et le premier, de très loin, des TLD inexistants. Par comparaison, les fuites pour `.onion` sont négligeables.

La section 2 du RFC décrit quelles sont ces règles que devraient suivre les logiciels DNS (cette section est obligatoire pour mettre un nom dans le registre des noms spéciaux, cf. RFC 6761, section 5). Donc, voici les différents composants du DNS qui devraient (idéalement) traiter les `.onion` à part :

— Les utilisateurs humains doivent savoir que les `.onion` ont des propriétés de sécurité particulières, et qu'ils ne sont accessibles qu'avec un logiciel spécial (comme le Tor Browser).
— Les applications comme les navigateurs Web qui mettent en œuvre Tor doivent reconnaitre les noms en `.onion` et les passer à Tor. Les autres devraient générer une erreur tout de suite et ne pas tenter ces noms dans le DNS.
— Les bibliothèques qui font de la résolution de noms (comme la glibc) doivent passer ces noms à Tor ou bien générer une erreur « ce nom n'existe pas », sans utiliser le DNS.
— Les résolveurs DNS doivent renvoyer l'erreur NXDOMAIN ("*No Such Domain*"), idéalement sans utiliser le DNS, comme dans les deux catégories précédentes.
— Les serveurs faisant autorité (a priori, cela ne concerne que ceux de la racine, les autres n'ayant aucune raison d'être interrogés pour ce nom) doivent également répondre NXDOMAIN.
— D'ailleurs, les opérateurs de serveurs DNS ne doivent pas configurer un serveur pour répondre pour ces noms, qui ne doivent être traités que par Tor.
— Les registres et BE ne doivent évidemment pas accepter d'enregistrer des noms en `.onion`...

Le RFC précise explicitement que l'IANA est autorisée à mettre dans la zone racine un mécanisme pour réserver le nom (comme, je suppose, celui du RFC 7535). Et que les opérateurs non-DNS (par exemple les AC, voir la déclaration du CAB sur les .onion <`https://cabforum.org/2015/02/18/ballot-144-validation-rules-dot-onion-names/`>) peuvent évidemment stocker des noms en `.onion`.

Pourquoi ces demandes répétées de ne pas tenter de résoudre les noms dans le DNS ? Car cela ferait connaitre à l'extérieur, en clair, les services Tor cachés auquel vous tentez d'accéder, ce qui annulerait l'effet anonymisant de Tor. Par exemple, ici j'utilise par erreur un logiciel non-Tor pour accéder au blog d'Aeris :

```
% curl http://blog.aeriszyr4wbpvuo2.onion/
curl: (6) Could not resolve host: blog.aeriszyr4wbpvuo2.onion
```

Et si quelqu'un d'indiscret, sur un serveur racine, regardait le trafic, il a vu (ici, avec tcpdump) :

```
18:36:10.252749 IP6 2001:db8:8bd9:8bb0:21e:8cff:fe76:29b6.33562 > 2001:1608:10:167:32e::53.53: \
                65162% [1au] A? blog.aeriszyr4wbpvuo2.onion. (56)
18:36:10.284260 IP6 2001:1608:10:167:32e::53.53 > 2001:db8:8bd9:8bb0:21e:8cff:fe76:29b6.33562: \
                65162 NXDomain*- 0/9/1 (1129)
```

que non seulement je suis un mauvais citoyen qui utilise Tor malgré les injonctions d'un gouvernement bienveillant qui explique qu'il ne faut utiliser que la « cryptographie légale », mais en plus l'indiscret a le nom du site qui m'intéressait (RFC 7626).

En parlant du risque de fuite, la section 4 de notre RFC est consacrée à la sécurité. Outre ce problème de logiciels trop bavards qui en révèlent trop à l'extérieur via les requêtes DNS <https://www.torproject.org/docs/faq.html.en#WarningsAboutSOCKSandDNSInformationLeaks>, elle mentionne le risque de se tromper de nom `.onion`.

En effet, les noms en `.onion` sont certes auto-vérifiables, via la cryptographie, mais cela suppose d'utiliser le bon nom. Si un utilisateur se trompe, ou bien fait trop confiance à un nom indiqué sur un canal IRC de numéristes radicalisés, il peut atterrir sur le mauvais site `.onion`. Le risque est d'autant plus élevé que les noms en `.onion` sont typiquement illisibles par un humain (des techniques, coûteuses en temps de calcul, permettent de générer des noms plus jolis, comme celui de Facebook cité plus haut).

Les utilisateurs pourraient aussi se faire avoir par ignorance de la syntaxe des noms de domaine. Par exemple, un utilisateur ordinaire pourrait être trompé en croyant que `www.onion.example` est protégé par Tor ce qui n'est pas du tout le cas.

Il y a aussi des attaques plus techniques. Un nom en `.onion` est le condensat d'une clé cryptographique. Casser cette clé (trouver la partie privée en n'ayant que la partie publique) nécessite des ressources de calcul colossales mais trouver une clé ayant le même condensat (et donc le même nom `.onion`) est moins coûteux (tout est relatif : il faudra quand même de la puissance de calcul et du temps), et cela pourrait permettre de créer un faux service caché indistinguable du vrai.

Si vous voulez en savoir plus sur comment fonctionnent ces noms en `.onion` (je trouve personnellement que la documentation disponible est insuffisante), voyez les guides officiels « *"Special Hostnames in Tor"* <https://spec.torproject.org/address-spec> » et « *"Tor Rendezvous Specification"* <https://spec.torproject.org/rend-spec> ».

L'enregistrement de `.onion` dans les noms de domain spéciaux a été l'occasion d'un long et houleux débat à l'IETF, tournant parfois au psychodrame, comme toujours quand on parle des TLD. En gros, il opposait les « conservateurs », méfiants vis-à-vis de ces nouveaux services pair à pair et soucieux de rester « respectable » aux yeux de l'ICANN, aux « pairàpairistes » qui ne se soucient pas de l'ICANN et ne sont pas satisfaits du système de nommage actuel. Le RFC 6761, qui fournit la base de cet enregistrement, a été très contesté (bien plus que lorsqu'il a servi à enregistrer le TLD d'Apple `.local`...). L'IETF a finalement pris la décision d'enregistrer `.onion` mais de fermer la porte juste après aux autres demandes en attente (comme `.gnu` ou `.bit`) en attendant une éventuelle révision du RFC 6761. Voici l'article qui annonce cette décision <http://www.ietf.org/blog/2015/09/onion/>. Ce sera un des points chauds de la prochaine réunion de l'IETF à Yokohama.