Mon blog dans les oignons

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 janvier 2015. Dernière mise à jour le 1 septembre 2021

`https://www.bortzmeyer.org/blog-tor-onion.html`

Cela faisait longtemps que je voulais m'amuser avec cela, donc, désormais, ce blog est également accessible en "*Tor hidden service*", c'est-à-dire avec un nom de domaine en `.onion`.

Quel est l'intérêt de faire cela ? Le réseau Tor est connu pour permettre une connexion aux services de l'Internet qui soit anonyme (attention à votre sécurité toutefois : aucune technique n'est parfaite et rien n'est jamais complètement anonyme) et qui résiste à la censure. Tor assure ce service en **relayant** chaque requête par plusieurs nœuds Tor. Seul le premier connait le client initial (il ne connait pas la destination) et seul le dernier connait le serveur visé (il ne connait pas le client initial). Bon, ça, c'est Tor qui protège le client <http://www.slate.fr/story/89673/tor>. Mais si on a envie de protéger le serveur ? Lorsqu'on publie traditionnellement sur l'Internet, on annonce un nom de domaine et n'importe qui peut investiguer, trouver (par exemple avec dig) l'adresse IP associée, se servir de whois pour trouver où et par qui est connectée cette machine, bref, même si on n'a pas mis son nom et son adresse dans les informations distribuées par le serveur, on peut être retrouvé facilement, ce qui est un problème si on veut bloguer alors qu'on vit sous une dictature intégriste et moyenâgeuse <http://fr.globalvoicesonline.org/2015/01/12/180328/>.

C'est là qu'interviennent les "*Tor hidden services*". L'idée de base est que le serveur fabrique une identité sous forme d'une clé cryptographique, l'envoie à quelques relais Tor, qui inscrivent cette identité dans, par exemple, une DHT, et les clients qui se connecteront à Tor trouveront ainsi les points de rendez-vous, permettant de se connecter à votre serveur, sans que les clients ne trouvent son adresse. Comme toutes les techniques de sécurité, cela n'est pas invulnérable à tout attaquant, donc, attention, si les enjeux sont élevés, il faut prévoir également d'autres précautions.

Pour savoir si le serveur à contacter est un serveur « normal » sur l'Internet ou bien si c'est un de ces services discrets (ce que les médias à sensation nomment le « Dark Web »), les services discrets ont un nom dans le TLD (domaine qui a depuis été officiellement reconnu par le RFC 7686 [1]) `.onion`. C'est ainsi que ce blog est (le lien ne marchera que si vous avez un client Tor) .

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7686.txt`

Pour configurer ce service, la documentation en ligne <https://www.torproject.org/docs/tor-hidden-service.html.en> est suffisante. J'ai juste installé Tor sur une machine Debian (`aptitude install tor`), ajouté et configuré Apache (attention à n'écouter qu'en local, avec `Listen 127.0.0.1:80`), puis configuré Tor

```
HiddenServiceDir /var/lib/tor/blog/
HiddenServicePort 80 127.0.0.1:80
```

Et c'est tout (en supposant que l'Apache ne serve qu'un site, sinon il faudra mettre le nom en `.onion` dans `ServerName`). Tor crée la clé et la publie auprès des relais. On peut la lire dans `/var/lib/tor/blog/hostnam` (où `blog` est le nom du service caché, utilisé dans la directive `HiddenServiceDir`). Attention toutefois à certains pièges : le but étant d'être autant que possible anonyme, Tor ne servira à rien si vous laissez des choses comme `ServerAdmin jeankevin@chezmoi.example`, choses qu'Apache publiera dans certains cas. Vérifiez donc bien que vous ne laissez pas d'indications dans vos textes ou votre configuration !

Bien sûr, dans le cas de ce blog, le service discret Tor n'a aucun intérêt pour l'auteur puisque le même contenu est publié par ailleurs par une technologie classique. Mais, dans un monde où on peut être assassiné pour des dessins qui déplaisent aux censeurs, beaucoup de gens ont intérêt à publier discrètement.

De nombreux sites sont ainsi accessibles via `.onion` même si, pour certains, cela peut sembler surprenant <https://www.techn0polis.net/2014/11/04/facebook-cache-dans-tor-pourquoi-cest-u
>.

Si vous voulez des informations techniques en français, il y a l'article de Benjamin Sonntag <https://benjamin.sonntag.fr/Tor-les-onion-le-darknet-a-votre-portee>. Vous y noterez (à la fin de la section « Héberger votre site avec Tor ») un point dont je n'ai pas parlé, la possibilité de choisir un nom plus parlant, au lieu de la clé cryptographique aléatoire que Tor génère par défaut. Cette possibilité me semble une faiblesse de sécurité mais les gens de Tor ne sont pas d'accord <https://blog.torproject.org/blog/facebook-hidden-services-and-https-certs> (la section « *"Part three : their vanity address doesn't mean the world has ended"* »).

Au fait, ce n'est pas tout d'avoir un site en `.onion`, encore faut-il que les gens l'utilisent. Pour aider, le navigateur Tor a, depuis sa version 9.5, la possibilité de découvrir <https://community.torproject.org/onion-services/advanced/onion-location/> une version `.onion` d'un site Web qui l'annonce via l'en-tête HTTP (non standard à ce jour) `Onion-Location:`. C'est ce que j'ai configuré sur ce blog, avec la directive Apache :

```
Header set Onion-Location "http://sjnrk23rmcl4ie5atmz664v7o7k5nkk4jh7mm6lor2n4hxz2tos3eyid.onion%{REQUEST_U
```

Je paie une bière à celui ou celle qui m'indiquera l'adresse IP de la machine qui héberge ce service, je vais peut-être découvrir (c'est mon premier service Tor discret) que j'ai fait plusieurs grosses erreurs de configuration (rappelez-vous l'avertissement plus haut : les erreurs arrivent et, en sécurité, elles peuvent coûter cher). La première faille a été découverte par Xilokar <https://twitter.com/xilokar> et c'était l'oubli du `/server-status` d'Apache, activé par défaut... (Ce problème a fait l'objet d'une alerte de sécurité bien plus tard <http://thehackernews.com/2016/02/apache-tor-service-unmask.html>.)

Avec mes remerciements à Ser Davos, le « chevalier à l'oignon », un des personnages les plus sympathiques de Game of Thrones.

Pour le futur : faudrait quand même que je mette les flux de syndication en `.onion`, eux aussi...
