Comment créer un blog anonyme (à l'heure de la surveillance généralisée)

Blog vraiment anonyme : mode d'emploi !

« Et si vous me trouvez, je serai vraiment très impressionné. »

Comment créer un blog anonyme

How to Start an Anonymous Blog

Anonyme (évidemment) – 26 janvier 2014 – Untraceable
(Traduction : crendipt, aKa, Diab, Penguin, Omegax, amha, nanoPlink, Paul, Scailyna, Scailyna, Asta, Unnamed, goofy, lamessen)

Introduction

Je crois qu'en suivant les étapes que j'expose dans ce billet, personne ne sera capable de dévoiler mon identité. Mon domaine peut être saisi et mon blog peut être fermé, mais je reste persuadé que mon identité restera un mystère.

Si je dis cela, c'est principalement parce que j'ai confiance dans un outil très important appelé Tor. Les développeurs et administrateurs des nœuds de Tor travaillent pour que chacun puisse être anonyme sur Internet. Tor est une sérieuse épine dans le pied pour la NSA et pour les autres organisations et pays qui font de l'espionnage sur Internet.

Vu que le réseau Tor rend très difficile l'identification des adresses IP et que l'enregistrement de domaines est désormais possible via Bitcoin, je n'ai à aucun moment besoin de fournir une quelconque information personnelle pour la mise en place de ce blog.

Outils et ressources

- Clé USB
- Système d'exploitation Tails
- Réseau Tor
- Bitcoins locaux – Acheter des bitcoins en espèces
- Comptes mail gratuits chez outlook.com et anonymousspeech.com
- Nom de domaine acheté chez IT Itch
- Site statique hébergé sur des pages GitHub

Tails / Tor

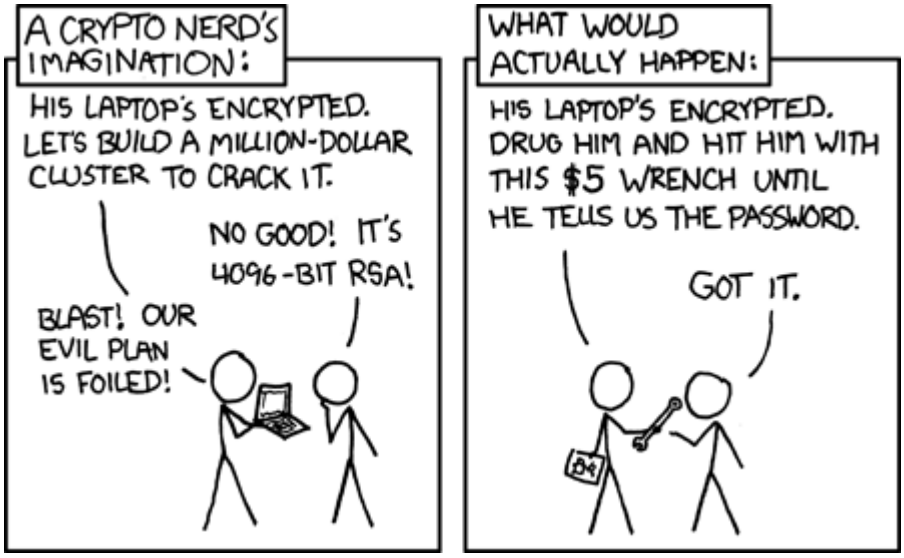
Tails est lancé depuis une clé USB qui inclut une partition chiffrée. Cette partition contient un porte-monnaie Bitcoin, le code source du blog et une base de données Keepass. Mes mots de passe pour des services tiers sont des mots de passe très forts générés aléatoirement. Avec Tails, il est difficile de se tromper, car toutes les connexions doivent obligatoirement passer par Tor. Par exemple, pour développer ce blog en local, je dois ajuster les règles du pare-feu pour autoriser les connexions locales au port 4000, télécharger un navigateur différent (Midori) et régler celui-ci pour qu'il n'utilise pas de serveur proxy. Le pare-feu bloque toutes les requêtes externes de Midori, mais je peux accéder à http://localhost:4000.

Donc, à moins d'agir de manière insensée, par exemple me connecter à StackOverflow au moyen de mon vrai compte Google et utiliser l'identifiant de « untraceableblog », je pense qu'il est quasiment impossible de me pister.

Je fais une sauvegarde de la clé USB sur mon ordinateur principal, sur un volume

caché TrueCrypt. J'aime le concept des volumes cachés, j'ai l'impression d'être un *putain* d'espion. L'idée, c'est d'avoir un mot de passe factice qui déverrouille un faux dossier chiffré et un mot de passe réel pour déverrouiller le vrai dossier chiffré, sans qu'il y ait aucun moyen pour les autres de savoir lequel vous déverrouillez. Dans mon faux dossier chiffré, je garde ma base personnelle de Keypass, de cartes de crédit, et des scans de mon passeport et permis de conduire. Donc si quelqu'un me force à entrer mon mot de passe pour déverrouiller mon ordinateur et découvre que j'ai un volume TrueCrypt, il n'aura aucun moyen de savoir si j'ai entré le mot de passe réel ou bidon.

Cette fonctionnalité autorise une légère protection contre les tentatives d'extorsion de votre mot de passe par la force.



La plupart du temps, je cache la clé dans un endroit secret de la maison. Quand je dois aller quelque part et que je veux pouvoir mettre à jour ce blog, je le sauvegarde sur le volume caché, puis j'efface la clé de manière sécurisée et je peux l'emporter avec moi sans aucune crainte. C'est ce que je devrai faire jusqu'à ce que Tails intègre sa propre fonction pour les « volumes cachés ».

Messagerie électronique

J'ai créé un compte de messagerie gratuit sur Outlook.com et j'utilise anonymousspeech.com pour la vérification et la sauvegarde.

J'ai d'abord essayé Gmail, mais Google rend la création de compte très difficile quand on utilise Tor, à cause de la vérification par téléphone. C'est

compréhensible, à cause des gens qui aiment créer un grand nombre de faux comptes pour envoyer du spam.

Blog

Ce blog est libre sur les pages GitHub, il utilise Octopress pour créer un site statique et j'ai installé le thème Page Turner. J'ai envoyé le contenu sur GitHub avec une clé SSH, bien entendu chiffrée et stockée sur ma clé USB.

Il me vient à l'esprit deux vecteurs susceptibles de vous donner des informations sur mon identité :

L'horodatage des messages

Le système d'exploitation Tails dispose d'une bonne stratégie pour forcer l'heure du système à être systématiquement en UTC. Mais si j'écris une série de billets dans les années à venir, vous pourriez en analyser l'horodatage pour déterminer mon fuseau horaire. Cependant, le site compilé indique uniquement la date. Par ailleurs, je voyage beaucoup (ou pas ?)

Analyse de la fréquence des mots et caractères

Vous pourriez être capables de déterminer mon pays d'origine ou mon identité grâce à mes mots et mes phrases. Vous pourriez même trouver une corrélation avec les autres contenus que j'ai publiés en ligne sous ma véritable identité. Je contre cette possibilité en passant tous mes billets dans Google Translate. Je traduis dans une autre langue, puis en anglais et je corrige ensuite les erreurs. C'est parfait pour diversifier mon vocabulaire, mais j'aurais aimé que ça ne casse pas autant le Markdown et le HTML. Jusqu'ici vous pourriez croire que l'anglais est ma seconde langue. Mais laissez-moi vous assurer d'une chose : je n'ai jamais affirmé ni infirmé ce point.

Un des problèmes, c'est que Google peut voir mes messages originaux et probablement aussi la NSA. Si je voulais l'éviter, je pourrais poster des demandes de traductions anonymes et payer les traducteurs en bitcoins.

Statistiques

Les raisons de l'indisponibilité de Google Analytics vous sont données sous « Messagerie électronique ». À la place, j'ai choisi StatCounter.

Mais même si Google Analytics avait été disponible, je n'aurais pas utilisé une ID de suivi liée à mon identité réelle. Beaucoup de blogueurs anonymes ont été trahis par l'annuaire d'ID inversé proposé par Google.

Acheter des bitcoins avec le maximum d'anonymat

J'ai acheté les bitcoins en utilisant un compte anonyme créé via Tor. J'ai trouvé un vendeur qui souhaitait me rencontrer en personne et nous avons convenu d'un rendez-vous. Nous nous sommes rencontrés, je lui ai donné l'argent et il m'a transféré les bitcoins en utilisant son téléphone.

Acheter un nom de domaine avec des bitcoins

IT Itch est un registrar qui accepte les paiements via BitPay. Leurs noms de domaine sont assez chers,15 USD chacun, mais permettent un enregistrement totalement anonyme. Ce fut une démarche facile, mais il a fallu du temps pour que le domaine devienne actif (plus d'une heure). Une fois activé, j'ai configuré les enregistrements DNS pour GitHub Pages, et ensuite mon blog était accessible sur http://untraceableblog.com.

IT Itch a fait la grosse erreur de m'envoyer mon mot de passe en texte clair après la création du compte. PAS BIEN ! Si quelqu'un parvient à accéder à mon compte Outlook, il peut se connecter et détruire mon site. Donc j'ai effacé le message et changé mon mot de passe, et heureusement ils ne l'ont pas renvoyé par e-mail.

Comment je pourrais être découvert, 1ère partie

Pister les Bitcoins

En théorie, vous pouvez suivre la trace des transactions Bitcoins et découvrir mon identité. Toutefois, dans ce cas, il est très peu probable que même l'organisation la plus sophistiquée et la mieux financée puisse me découvrir.

Voyez-vous, j'ai acheté ces Bitcoins en utilisant un compte anonyme sur localbitcoins.com (créé en utilisant Tor). Nous avons convenu, le vendeur et moi, de nous rencontrer en personne, et j'ai payé en liquide. Pour dévoiler mon identité, il faudrait que vous puissiez casser les défenses de tous les services que j'ai utilisés ou bien travailler chez eux. Il faudrait par exemple :

1. Accéder à la base de données de ititch.com et trouver l'identifieur de la

transaction BitPay pour untraceableblog.com
2. Accéder à la base de données de BitPay et trouver l'adresse Bitcoin qui a envoyé les Bitcoins pour cette transaction
3. Accéder à la base de données de localbitcoins.com. Trouver l'adresse Bitcoin qui a envoyé les Bitcoins à BitPay, retracer la transaction jusqu'à ce que vous trouviez l'adresse localbitcoins du dépôt fiduciaire.
4. À partir de l'adresse du dépôt fiduciaire, vous pourrez trouver le compte localbitcoins, et retrouver les messages que nous avons échangés pour nous rencontrer.
5. Vous devrez vous rendre au point de rendez-vous et espérer qu'il existe des caméras de surveillance qui auraient pu nous enregistrer ce jour-là.
6. Vous aurez enfin besoin d'accéder à la société de sécurité qui possède les enregistrements des caméras de surveillance, obtenir une bonne image de mon visage et faire tourner d'une façon ou d'une autre un logiciel de reconnaissance faciale pour découvrir mon identité. Travailler pour Facebook ou la NSA pourrait aider si vous avez réussi à parvenir à ce point.

Comment je pourrais être découvert, 2ème partie

Tout est hacké. Absolument tout.

Internet est une machine basée sur la confiance et il existe de nombreuses manières de briser cette confiance. Quelqu'un peut générer des certificats SSL de confiance pour n'importe quel domaine, exiger que son FAI route l'intégralité du trafic au travers de ces certificats, ou contrôler un grand nombre de nœuds Tor et réaliser des attaques par analyse de trafic. Je n'entrerai pas dans les détails mais si vous êtes intéressés, vous pouvez en apprendre davantage sur les attaques Tor :

- Comment la NSA attaque les utilisateurs de Tor / Firefox avec quantum et FOXACID
- Articles concernant les attaques sur le blog de Tor

Conclusion

Je n'ai fait ce blog que comme un exercice amusant d'anonymat, même si j'y posterai probablement des choses dans le futur. J'ai simplement utilisé des outils créés par des gens bien plus intelligents que moi et je ne suis sûrement pas le

premier blogueur anonyme, mais j'espère vous avoir appris quelque chose.

Bien évidemment, on peut aller beaucoup plus loin que ça. J'aurais pu héberger ce blog sur un VPS que j'aurais loué avec des Bitcoins et installer le serveur comme un service Tor masqué. L'adresse IP du serveur aurait été totalement protégée mais, de ce fait, vous n'auriez pu consulter ce blog qu'au travers du réseau Tor, et les liens de nœud Tor (TBR) ça ne fait pas très chouette en page d'accueil. J'aurais également pu faire toutes mes actions depuis un cybercafé, juste au cas où Tor serait compromis, mais je n'aurais pas été découvert. Enfin, j'aurais pu choisir un domaine en « .se » si j'avais eu peur de l'intervention du gouvernement américain. C'est ce qui est actuellement utilisé par The Pirate Bay, et les Suédois leur laissent toute liberté d'action.

N'hésitez pas à m'envoyer quelques Satoshis (fractions de Bitcoins) si vous aimez ce billet : 146g3vSB64KxxnjWbb2vnjeaom6WYevcQb.

Et si vous me trouvez, je serai vraiment très impressionné.

Crédit illustrations : AndyRobertsPhotos (Creative Commons By) et XKCD