

Compte-rendu atelier : comment protéger ses sources ?

Contexte :

Protéger ses sources est le premier devoir du journaliste. A l'ère du numérique, comment mettre cette règle en pratique ?

Le comportement est fondamental. Il ne sert à rien de surprotéger son ordinateur, ses communications si en parallèle on se montre trop loquace. Ce serait comme avoir une alarme high-tech et laisser les fenêtres ouvertes.

Il est également nécessaire de s'adapter à sa source et au contexte. Il ne sert à rien d'installer des appli chiffrées si l'enjeu de sa source est de ne pas être vue par son voisin. Dans ce cas précis, la solution est d'organiser une rencontre ailleurs qu'à son domicile.

Nous ne sommes pas confrontés à un risque de surveillance de la NSA pour chacune de nos enquêtes. S'adapter au contexte c'est se référer au « modèle de menaces » (en savoir plus : <https://ssd.eff.org/fr/module/une-introduction-au-mod%C3%A8le-de-menace>) , en l'occurrence cinq questions à se poser avant de mettre en place un protocole pour sécuriser les échanges :

Que souhaitez-vous protéger ?

Contre qui souhaitez-vous le protéger ?

Quelle est la probabilité que vous ayez besoin de le protéger ?

Quelles seraient les conséquences si vous échouiez ?

Quels désagréments êtes-vous disposé à affronter afin de vous en prémunir ?

Dans un échange avec une source il y a 3 étapes :

- le document, l'information à échanger et à anonymiser au préalable
- la communication en elle-même, le moment de l'échange
- le stockage de l'information

Les « solutions » proposées ci-dessous ne sont pas des solutions miracles, chacune a ses inconvénients. En outre, elles peuvent être mise en maintenance. Il est donc nécessaire de se tenir informé de l'évolution des technologies et applications.

Sur téléphone :

- chiffrer son téléphone.

Ainsi en cas de vol, personne ne peut savoir ce qui est enregistré sur l'appareil. La plupart des téléphones proposent le chiffrement (cryptage est un synonyme), généralement dans les paramètres généraux de l'appareil.

Les + :

facile et efficace

Les - :

Ne pas perdre son mot de passe, sinon tout est perdu. Faire des sauvegardes régulières.

- chiffrer les communications. L'application signal.

Elle chiffre de bout en bout les communications, qu'il s'agisse de sms, d'appels, d'envois de son, image ou vidéo.

Les + :

Elle est très simple d'utilisation et est open-source/libre. Il suffit de la télécharger, elle est compatible avec tous les téléphones connectés.

Les - :

L'émetteur et le récepteur doivent être équipés d'un téléphone connecté. Il faut être connecté à internet pour pouvoir utiliser l'application.

Sur ordinateur :

- Sécuriser ses recherches avec Tor.

Tor est un navigateur web qui s'utilise comme firefox ou chrome. Effectuer ses recherches via Tor évite que l'entreprise sur laquelle vous enquêtez sache que vous l'avez dans le viseur, car elle peut le déduire via votre adresse IP. Tor modifie de manière aléatoire votre adresse IP et ainsi vous anonymise.

Les + :

facile à télécharger (torproject.org) et à utiliser.

Les - :

Plus lent qu'un autre navigateur.

Si vous vous connectez à votre boîte email via Tor, vous allez probablement recevoir un message d'alerte vous informant que quelqu'un essaye de vous pirater. Parce que votre adresse IP a été modifiée, votre boîte email soupçonne qu'il y a piratage. En réalité vous vous piratez vous-mêmes. Rien de grave mais c'est pénible.

- Sécuriser des documents : MAT.

Chaque document (pdf, image, son) possède des métadonnées. Certaines sont visibles par un clic droit sur propriétés, d'autres ne sont accessibles que via des logiciels spécialisés.

Pour les effacer et éviter que l'auteur ou la provenance d'un document soit identifié, utilisez MAT qui efface ces métadonnées.

Les + :

Très simple à télécharger et utiliser.

Les - :

Ne prend pas en charge les formats .doc, .wav.

- Échanger, envoyer des documents : Onionshare.

Cette application permet d'échanger de manière sécurisée des documents. Cela ressemble à wetransfer : l'émetteur charge le document, une fois que c'est fait, une URL est générée. Il faut entrer cette URL dans Tor et ensuite, un clic suffit pour lancer le téléchargement.

Cette URL n'est plus valide après un téléchargement effectué.

Les + :

Facile d'utilisation, pas de configuration spécifique à réaliser, ni de création de compte à faire.

Communication directe entre les deux ordinateurs (mais anonymisée via Tor), sans copie du ou des documents sur un service cloud.

Les - :

Il faut télécharger onionshare.

Il faut passer par Tor pour télécharger le fichier.

Il faut qu'émetteur et récepteur soient connectés en même temps pour que le téléchargement puisse avoir lieu.

- Stocker l'information. Chiffrer un disque dur, une clef USB

Via la clef Tails (cf ci-dessous), le chiffrement d'une clef est très simple. Elle ne peut s'ouvrir que via un mot de passe. Sans lui, impossible d'ouvrir la clef.

Les + :

simplicité, possibilité de reproduire le chiffrement sur autant de supports (disques, clefs) que nécessaires.

Les - :

avoir une clef Tails

la clef ou le disque chiffré ne pourra s'ouvrir que sur un ordinateur sous Linux (Ubuntu, Tails...)

Une solution alternative est disponible via le Logiciel VeraCrypt (anciennement Truecrypt).

Celui ci est disponible sous Linux (Ubuntu...), Windows, Mac OS X (un peu plus de travail nécessaire) et permet de chiffrer des disques de données, des disques systèmes (Windows uniquement), ou de dissimuler des données dans un fichier (typiquement un fichier .avi de 700Mo pour le faire passer pour un film).

Les + :

Disponible sur Linux, Windows, MacOS X.

Interface graphique (relativement) facile à utiliser

Outil reconnu.

Les - :

Laisse des traces.

Dépend de la sécurité du système : Si le Windows ou le Mac a des virus, des logiciels téléchargés à droite à gauche ou crackés on ne peut pas avoir pleinement confiance.

- La solution tout en un : la clef Tails.

Il s'agit d'une clef USB sur laquelle le programme Tails est installé. On branche la clef sur l'ordinateur et on allume l'ordinateur. L'ordinateur va démarrer et fonctionner depuis la clef et pas depuis le système de l'ordinateur (Windows, Mac). Ainsi vous ne laissez aucune trace de votre passage sur l'ordinateur concerné.

Sur la clef, vous avez toutes les applications de chiffrement, le pack libre office et les logiciels de base de montage son vidéo, de quoi enlever des métadonnées etc.

Tous les paramètres sont configurés par défaut de manière très sécurisée (par exemple : tout le trafic passe par Tor). La clef est donc prête à l'emploi.

Vous pouvez aussi configurer un espace de stockage (appelé espace de persistance) pour sauvegarder votre travail en cours. Par défaut, la clef ne sauvegarde rien, elle efface tout dès que vous la débranchez de l'ordinateur.

Les + :

C'est totalement sécurisé, pas de configuration à réaliser.

Les - :

Pour que l'ordinateur démarre sur la clef, cela ne se fait pas automatiquement. Il faut rechercher au préalable sur les forums web, sur quelle touche (F1 ou F2 ou F3, etc) il faut appuyer pour dire à l'ordinateur de se lancer depuis la clef tails.

Pour avoir un espace de stockage, il faut d'abord le configurer.

Parce qu'il faut redémarrer l'ordinateur, cela oblige à travailler en « mono-tâche ». Cela est difficilement compatible avec nos habitudes du multitâches.

Contacts pour l'avenir :

Si vous avez besoin d'aide pour une sécurisation poussée, tournez-vous vers RSF (reporters sans frontières) et la FIDH (fédération internationale des droits de l'homme). Ces deux associations ont des services informatique qui développent des outils comme la clef Tails. Elles seront en mesure de vous aider.

Pour comprendre et savoir utiliser la clef Tails, dans de nombreuses villes des cryptoparties sont organisées. Il s'agit d'ateliers pratiques pour vous aider à prendre en main ces outils.

Contacts des intervenants :

Julie Lallouët-Geffroy, journaliste : contact@julielallouetgeffroy.com

Mathieu Goessens, informaticien : gebura@poolp.org ou dnr@mail36.net

Pour les curieux :

- Pour visualiser la manière dont vous êtes tracé sur internet au fil de vos recherches et connexions, télécharger le plug-in Lightbeam.
- Plus d'infos sur Tails : <http://gebura.eu.org/~geb/tails.pdf> et <https://tails.boum.org/support/learn/index.fr.html>
- Une présentation plus générale sur la protection des sources : <http://gebura.eu.org/~geb/formation.pdf>
- le guide d'autodéfense numérique : <https://guide.boum.org>