Autodefense Numérique — Supports de formation Documentation

Release 1.0

Alexis Métaireau & contributeurs

April 28, 2016

Contents

Bonjour ! Si vous vous retrouvez ici c'est que vous êtes potentiellement interessés pour **organiser des ateliers d'autodéfense numérique**.

Cette documentation souhaite regrouper des ressources sur l'organisation d'ateliers sur l'autodéfense numérique (certain.e.s disent Crypto parties). Il existe énormement de ressources autour de l'autodéfense numérique, mais il est parfois dur de s'y retrouver.

L'objectif ici est de fournir quelques contenus assimilables facilement, parce ils ont une visée pédagogique avant tout. Il s'agit d'un endroit ressource pour certains d'entre nous, pour préparer nos formations / ateliers.

Vos modifications et divers retours sont les bienvenus. Il est possible d'éditer cette documentation en cliquant sur le bouton "edit on github" en haut à droite. N'hésitez pas, ceci se veut être un travail collaboratif.

CHAPTER 1

Format des ateliers

L'idée ici est de voir ce qu'il est possible d'aborder dans des ateliers de durées variables.

Les durées ici ne tiennent pas compte des pauses. C'est pour ça qu'il est indiqué 3h30 par exemple.

1.1 Atelier d'une matinée / après-midi (3h30)

- Brise glace (30mn)
- Introduction (30mn)
- Théorie: traces physiques et réseau (1h)
- Atelier Tails - Installation et premiers usages (1h)
- Atelier Tails - Chiffrement des données (30mn)

1.2 Atelier d'une journée

Matin (3h30):

- Brise glace (30mn)
- Introduction (1h)
- Théorie: traces physiques (30mn)
- Atelier traces: metadonnées sur les documents (30mn)
- Atelier Tails - Installation et premiers usages (1h)
- Atelier Tails - Chiffrement des données (30mn)

Après-midi (3h30):

- Brise glace (30mn)
- Théorie: traces réseau (30mn)
- Atelier Tor (1h)
- Théorie: cryptographie (30mn)
- Atelier: PGP (1h)

CHAPTER 2

Brises-glaces

Les brises-glaces permettent aux participant.e.s d'un atelier de se rencontrer et d'intéragir ensemble. Il existe plusieurs types de brise glace.

2.1 Interview mutuelles

En petits groupes de 2 ou 3 personnes (si possible les gens ne se connaissent pas), l'idée est que chacun raconte son vécu sur une situation durant 5mn, puis 5mn de questions et on tourne.

Questions pour faciliter la discussion:

- T'es tu déjà déjà confronté à une situation sensible suite à un manque d'outils / connaissances techniques ?
- Si oui, quel à été l'impact sur ta vie personelle / professionelle ?

Qu'est-ce que vous ressortez des groupes d'interview mututels ? Y a t'il des sujets que vous voulez aborder plus specifiquement ? Constituez des groupes d'envies pour les ateliers.

CHAPTER 3

Introduction

Il est important d'expliquer rapidement pourquoi cet atelier existe, et qu'est-ce qu'on cherche à y faire. Pour ça, il est possible de suivre ce type de fil:

- La technique est omnipresente (qui à un téléphone ? un smartphone ? Qui à ses mails chez google ? Qui n'a pas d'adresse email ?)
- **Les risques existent à plusieurs niveaux:**
  - gouvernemental pour certaines personnes selon les sujets
  - au niveau des entreprises pour certaines personnes qui souhaitent faire fuiter des données (administrateurs réseau)
  - n'importe qui qui serait interessé par votre vie privée (flics, banques, assurances etc.)
- Il est très difficile de se protéger de manière efficace contre tous ces adversaires, il faut que vous identifiez qui peut être interessé par vos activités.
- Il existe plusieurs niveaux de protection / niveaux de bonnes pratiques.
- Il est necessaire d'avoir quelques apports théoriques pour comprendre la pertinence de certains outils.

3.1 Présentation de l'atelier

Rappeller qu'on est pas des pros et qu'il faut donc: - faire attention aux oublis et erreurs - se renseigner par soi même

N'hésitez pas à nous arrêter pour poser des questions ! On va pas parler d'écologie ou de sanitaire

3.2 contexte politique

Il y a actuellement une surveillance globale. On sait qu'en général ces entités aiment espionner, récolter des informations, les vendre, … afin de créer des graphes de relations, cibler des personnes si besoin, cibler leur publicité, contrôler, ...

Cela permet de notemment faire de la prévision des comportements

Vous n'avez rien à cacher ?

- Et si on ouvrait toutes les lettres et colis de tout le monde avant la distribution, et qu'on les scannait/repertoriait ?

- Association : un.e pote a peut-être quelque chose à cacher, ce qui peut te mettre en danger si tu ne te protèges pas
- Ca peut permettre la prévision des comportements futurs
- Permanence de l'information: ce qui n'est pas problématique actuellement le sera peut-être plus tard.
- Agrégation des données de Microsoft, Google, Yahoo !, Facebook, YouTube, Skype, Apple, Dropbox, ...
- Il y a 83% d'erreurs dans les fichiers policiers (fautes de frappe, homonymies, mises à jour, détournements, etc.)
- Acheter une cocotte minute et un sac d'engrais la même semaine est suspect.
- Je ne suis pas d'accord avec les règles d'autrefois, alors QUID d'un gouv. futur ?

En gros, on ne détermine pas soi-même si on est coupable **et** les règles peuvent changer

3.3 Rappel des lois

- voir LQDN
- lois 2014
- loi sur le renseignement
- lois sur l'état urgence

3.4 Modèle de menace

On ne peut pas se protéger de tout le monde en même temps.

5 questions qu'il est utile de se poser:

- Que souhaitez vous protéger?
- Contre qui le protéger?
- À quel point avez-vous besoin de le protéger ?
- Quelles seraient les conséquences si vous échouez ?
- Quelles galères êtes-vous prêt-e-s à affronter pour les éviter?

3.5 Pièges

Il est aussi possible de piéger les personnes présentes, par exemple comme suit:

- Demander si qqn peut donner son mot de passe, à voix haute, devant l'ensemble des personnes présentes ? Probablement que personne ne voudra.
- Demander ensuite si quelqu'un peut venir se connecter à ses emails sur mon ordinateur, en spécifiant bien qu'on ne regardera pas.

Souvent, les personnes se connectent, et c'est alors un bon moyen d'expliquer pourquoi c'est une mauvaise idée.

CHAPTER 4

Matériel

Faire un point d'abord sur l'utilisation du matériel. Quelle utilisation est actuellement faite du matériel en lui même.

Il est important de définir le niveau de confiance que l'on peut avoir envers un matériel donné.

- Utiliser son propre matériel plutôt que celui d'un.e autre.
- Parler de la présence possible de keyloggers.
- et des trojan dans les cybercafés.

CHAPTER 5

Traces physiques

Quelles sont les traces que l'on peut laisser sur un ordinateur ?

- Un ordinateur, même déconnecté, peut laisser des traces suite à son utilisation.
- **Sur un ordinateur, on trouve plusieurs parties importantes:**
  - Le processeur, qui s'occupe de faire les calculs;
  - le disque dur, qui s'occupe de stocker les données de manière pérènne;
  - la mémoire vive, qui s'occupe de stocker les données temporaires.

Ce qu'on va vous dire risque de vous faire peur, c'est normal.

5.1 Le disque dur

- Est-ce que vous avez protégé votre compte via un mot de passe ?
- Vos données sont donc protégées ?

Lorsque votre ordinateur est allumé ou éteint, des données sont stockées sur votre disque dur.

Il est possible pour n'importe qui d'accéder à vos données directement en enlevant le disque dur de l'ordinateur. Je pourrais très bien le faire dès maintenant sur l'un de vos ordinateurs, il suffit d'un tournevis.

Pour éviter que n'importe qui puisse accéder à ces données, la bonne pratique est de crypter (ou chiffrer) ses disques durs.

5.2 La mémoire vive (RAM)

N'importe quel programme qui s'execute sur un ordinateur utilise de la mémoire vive. C'est l'endroit où l'ensemble des données que vous voyez affichées à l'écran sont stockées, par exemple.

C'est aussi l'endroit ou toutes les données (textes etc) que vous rentrez sont stockés.

Quelqu'un qui accède à votre mémoire vive peut donc accéder à toutes ces données (mots de passe compris).

La parade par rapport à ce type d'attaques:

- éteindre son ordinateur lorsqu'on ne l'utilise pas. Il existe des attaques assez poussées qui peuvent même être utilisées sur une mémoire éteinte, jusqu'à quelques minutes après son extinction (cold boot attacks).

5.3 Entrées / Sorties

- Tout ce qui est tapé sur un clavier peut être capté jusqu'à 20 mètres
- Faire attention aux clés USB, la clé peut etre contaminée, et peut même cramer certains pc: il existe des clés avec un gros condensateur qui envoie une charge à l'ordinateur.
  - Les téléphones fonctionnent comme des ordinateurs !
  - Les cartes SIM sont des boites noires, nous ne savons pas ce qui est présent à l'intérieur.
  - Le matériel est souvent fait d'un bloc, ce qui rends parfois difficile l'isolation de certains composants entre eux (difficile à expliquer.)

CHAPTER 6

Traces sur le réseau

Lors d'une connection d'un point A a B, il y a des intermediaires. Voir ça pour du mail et pour du web.

D'une manière générale, la métaphore de la capuche est assez chouette: il existe des routes qui sont observées (les cables par exemple), vous pouvez choisir de mettre une capuche ou non lorsque vous empruntez ces routes.

6.1 Internet physiquement

- Montrer des image de cables sous-marins
- Il y a des gros tuyaux partout dans le monde
- des ordis aux bouts de chaque tuyau ("routeurs")
- des cables qui vont de ces routeurs à la maison
- la quasi-totalité de ces équipements appartient à des entreprises privées, ou des gouvernements.
- Pour aller d'un ordi à un autre, on passe souvent par plein d'ordis (donc nécessité de faire confiance à toute la chaine)
- "Internet" c'est le (ou les) réseau, pas les services (web, mail, torrent)!

6.2 Réseau GSM

- Il y a **90000** antennes-relais en France.
- Il s'agit d'un réseau centralisé (gros points de relais par opérateur)

En pratique: - La localisation est constante, et rétroactive - Les SMS sont stockés, scannés, donnés aux états - Les appels également - le Groupe Orange révélait que 160 personnes sont entièrement mobilisées pour

  l'écoute telephonique

- Écoutes d'ambiance: Ça existe !

6.3 Cartes Wifi

Si la connection n'est pas chiffrée, tout passe en clair entre l'ordinateur et la box.

Le WEP n'est pas un protocole sécurisé, et il est très facile à cracker. Il ne fournit donc pas de sécurité.

Le WPA est succeptible d'attaques par bruteforce (sources ?)

Les cartes wifi ont souvent des pilotes non libres (expliqué ensuite)

D'une manière générale, il est préférable d'utiliser une connexion ethernet (cablée).

6.4 CPL

Les boitiers CPL permettent d'utiliser le reseau electrique comme un réseau ethernet. Il n'est pas vrai que le signal s'arrête avec les disjoncteurs.

Il y a eu des cas ou les voisins pouvaient se connecter au reseau *CPL* sans soucis.

CHAPTER 7

Cryptographie

Voici quelques slides d'une présentation sur la cryptographie, très legers et non commentés, mais qui ont au moins le mérite d'exister.

CHAPTER 8

Tails (The Amnesic and Incognito Live System)

C'est un système d'exploitation (Comme Windows ou Mac OSX) dont l'objectif est de ne laisser aucune trace de son utilisation, ni sur l'ordinateur hote, ni sur le reseau utilisé.

Tails est installable sur une clé USB, ce qui le rends pratique à transporter. Il peut etre utilisable sur n'importe quel ordinateur.

Au niveau de la sécurité, il est important d'utiliser des logiciels auditables, souvent ce sont des logiciels libres qui le sont, puisque si il n'est pas possible d'accéder au code d'un logiciel il est possible qu'il ne soit pas celui qu'il pretende.

Tails embarque un ensemble d'outils qui sont utiles pour vous dans les cas ou vous souhaitez être anonyme sur le web.

CHAPTER 9

Démarrage sur Tails

Pré-requis: Avoir vu la théorie sur les traces physiques laissées par un ordinateur.

Matériel:

- Une clé USB par groupe (si possible par participant). La clé doit pouvoir être effacée.
- Au moins une clé USB avec Tails installé dessus.

Problèmes:

- Il est parfois problématique de réussir à lancer Tails depuis une clé USB, parce que le système d'exploitation d'origine démarre.

  XXX trouver une solution simple / une ressource à suivre !

L'idée est assez simple: donner une clé tails à un groupe / une personne puis les laisser démarrer (en autonomie si possible) et explorer tails.

Il peut être utile de leur faire un tour du propriétaire, par exemple en montrant comment dupliquer une clé ou comment utiliser une messagerie chiffrée.

CHAPTER 10

Téléphonie: comment se protéger ?

Malheureusement, si vous tenez à votre sécurité et vie privée, la meilleure solution est de ne pas utiliser de téléphone !

Si malgré tout vous choisissez d'utiliser un téléphone, il peut être interessant de se poser quelques questions:

10.1 Smartphone ou pas ?

Les vieux téléphones ne sont pas mieux sécurisés que les smartphones, contrairement à une croyance répandue.

Mais les smartphones sont aussi plus facile à véroler, donc il faut faire attention à ce qu'on "installe" dessus. Il est possible de changer le système d'exploitation que l'on installe sur un téléphone (Android par exemple l'alternative nommée "replicant" ou copperhead)

10.2 IMSI Catcher

Il faut savoir qu'il est possible pour des attaquants d'utiliser des malettes nommées "IMSI catcher" qui se font passer pour des antennes relai GSM. Elles:

- Vont demander aux téléphones les plus proches de se connecter à eux plutôt qu'à une autre antenne;
- Demander aux téléphone de virer le chiffrement sur les communications;
- Peuvent ensuite écouter l'ensemble de ce qui est transmis de ou vers votre téléphone.

Il existe des logiciels qui permettent de detecter la présence d'IMSI catchers.

10.3 Geolocalisation

Il est très facile pour les opérateurs téléphoniques de savoir sur quelle antenne relai une carte SIM est connectée (c'est leur boulot !). Selon les types d'antennes les portées sont differentes (de 500m à 2km en ville; de 10 à 30km en campagne). Il est donc possible de savoire très facilement ou vous êtes à cette précision près.

Il est aussi possible de faire de la triangulation: suite à une demande de l'opérateur (installation d'un programme sur la SIM), le téléphone va chercher à se connecter à plusieurs antennes relai et en recoupant les informations il est possible de savoir précisement ou vous vous situez. La localisation s'effectuen en moins de 5 secondes et permet de savoir ou vous vous situez avec une precision de 100m en ville et de 5km dans une zone rurale.

10.4 Changement d'OS

Faire un atelier pour faire un changement d'OS sur le téléphone. Lequel utiliser ? (que quelques téléphones compatibles)

10.5 Échanges de manière chiffrée

Présentation de Signal sur un téléphone Android. Signal permet d'envoyer des messages chiffrés et d'établir des communications vocales chiffrées également.

Quelques limitations:

- Utilisation de services Google par defaut, ce qui peut etre ou non un souci en fonction d'à qui vous cherchez à vous protéger.

10.6 Montrer comment utiliser Tor sur un smartphone

XXX

CHAPTER 11

Mots de passe et phrases de passes

Quelle est le différence entre un mot de passe et une phrase de passe ? Un mot de passe est souvent difficile à retenir **et** difficile à taper. Ce n'est pas pour ça qu'il est bien plus sécurisé.

Une phrase de passe est une phrase que l'on va retenir plus facilement et qui va être plus difficile à deviner par un attaquant.

11.1 Quelles attaques ?

Il existe deux moyens principaux pour trouver des mots de passe: les attaques par "brute force" et les attaques par dictionnaire.

Une attaque par *brute force* vise à essayer l'ensemble des possibilités de manière automatique (d'abord "a", ensuite "b", ensuite "aa", etc.). Ces attaques prennent assez peu de temps pour des mots de passe "simples".

Une attaque par dictionnaire essaye des mots du dictionnaire au fur et à mesure jusqu'à trouver une correspondance.

11.2 Phrase de passe

Exercice, choisissez une phrase de passe. La meilleure manière de retenir le mot de passe est de se le repeter assez souvent, pas de secret !

11.3 Réutilisation des mots de passe

Ne réutilisez pas des mots de passe entre differents services Web. Il est très facile pour quelqu'un de créér un site sur lequel vous enregisteriez un compte avec un mot de passe et donc d'avoir accès à ce mot de passe (et donc tous vos comptes ailleurs si votre mot de passe est le même !)

11.4 Système de gestion des mots de passe

Une bonne manière de ne pas avoir à retenir ses mots de passe et d'utiliser le logiciel "keepassx". Essayons :)

CHAPTER 12

Cryptocat

Cryptocat est un outil qui permet de chatter à plusieurs de manière confidentielle, et de s'echanger des fichiers.

CryptoCat à les propriétés suivantes:

- **forward-secret**: Si une clé de chiffrement est cassée, alors les futurs messages ne sont pas compromis (ni les précédents);
- **deniable**: il est possible juridiquement de nier être à l'origine des messages puisqu'il ne laisse pas de traces qui permet d'identifier les participant.e.s;
- Il permet l'identification des personnes **entre elles** grace à l'utilisation d'une question secrète.

12.1 Utiliser Crypto cat

Pré-requis:

- Avoir TOR d'installé;
- Avoir un navigateur d'installé.

Matériel:

- Idéalement avoir Tails;
- Sinon avoir deux ordinateurs ou un ordinateur avec deux navigateurs web (Chrome ou Firefox).

Problèmes:

- Il est parfois un peu compliqué d'installer CryptoCat sur Firefox.

Rien de sorcier à faire ici: il est possible de tout simplement se connecter à CryptoCat avec deux comptes differents puis:

- Discuter sur le chat;
- Chercher à authentifier les participants (avec une question secrète);
- Chercher à s'envoyer des fichiers.