T2 P3 - Utilisation clé USB bootable

Nous allons maintenant, dans la dernière partie de ce guide, présenter les clés USB bootables. Afin que vous puissiez comprendre ce que vous faites, je pense qu'il est nécessaire de passer par quelques petites explications théoriques.

C'est quoi une clé USB bootable ?

Explication brève : Système d'exploitation

Avant d'expliquer ce qu'est une clé USB bootable, il est d'abord nécessaire d'expliquer brièvement ce qu'est un système d'exploitation.

Généralement, quand nous démarrons notre ordinateur, ce dernier démarre sur ce qu'on appelle un système d'exploitation (Operating System ou OS), cet « OS » peut être Windows, MacOS, Linux, etc. C'est cet OS qui vous permet en gros d'utiliser votre ordinateur

Ce dernier est généralement stocké sur le disque dur interne.
Il stocke sur votre disque dur tout un tas d'informations, comme les logiciels que vous avez installé, les fichiers que vous stockez, etc …
En plus de ça, il peut également retenir des données concernant l'utilisation que vous avez fait de votre ordinateur, que ce soit les logiciels que vous avez ouvert, les fichiers que vous avez utilisé, etc…
Dans le pire des cas, il peut même être « compromis » ou « infecté », pour enregistrer tout un tas d'informations supplémentaires qui seront directement envoyées à « l'attaquant », comme les frappes de votre clavier (keylogger), ou tout autre détail concernant votre activité numérique.

Le but de la clé USB bootable

C'est pour éviter, ou du moins diminuer tout ces risques, que nous recommandons l'utilisation d'une clé USB bootable.
Le principe de cette clé USB bootable est de stocker une sorte de mini système d'exploitation, ainsi, au lieu de démarrer sur le disque dur, votre ordinateur démarrera sur l'OS de votre clé USB.

Nous appelons cela un « Live CD » ou « Live USB ». La particularité de cette méthode, est que le « mini » système d'exploitation hébergé sur votre clé USB ne retiendra aucune information, que ce soit d'éventuels logiciels installés, les fichiers utilisés/créés, les logiciels utilisés, etc …
Il y aura déjà installé de base tout les logiciels dont vous avez besoin, comme VeraCrypt, Libre Office, un gestionnaire de mode passe, Tor, Gimp, etc …

Où stocker vos données militantes ?

Étant donné que le système d'exploitation de la clé USB ne retient en lui même aucune information, vous vous demandez sûrement comment faire pour travailler sur vos données ?

Disque dur ou périphérique externe

Il peut y avoir comme première solution de stocker vos données sur un autre support de stockage que la clé USB, cela peut être une autre clé USB, ou disque dur externe, ou tout simplement le disque dur interne de votre ordinateur, accessible quand vous avez démarré sur votre clé bootable.

Quelque soit le support de stockage sur lequel vous stockez vos données militantes, je vous recommande bien évidemment de les mettre dans un volume VeraCrypt, caché de préférence.

Dans le tutoriel de la partie 2 sur VeraCrypt, vous voyez comment créer un volume VeraCrypt sur votre ordinateur. Ce volume, qui est stocké sur le disque dur interne de votre ordinateur, peut très bien être accessible une fois que vous avez démarré sur votre clé USB bootable

La persistance

La persistance consiste à créer, à part, sur votre clé USB bootable un « espace » sur lequel vous pourrez y stocker vos données.
Ainsi, même si le système d'exploitation en lui même ne stocke rien, vous pourrez stocker sur cet espace toutes vos données militantes.

Cet espace peut être chiffré de base, tout comme il peut ne pas l'être en fonction de la solution utilisée.
Dans les 2 cas, je vous suggère fortement de mettre vos données dans un volume VeraCrypt caché si vous les stockez sur la persistance de la clé USB.

En effet, même si la persistance est chiffrée, les autorités pourront vous obliger à leur donner le mot de passe de déchiffrement, pour accéder aux données.

Si ces données sont elles même dans un volume VeraCrypt caché, vous aurez ensuite juste à leur donner le mot de passe du « faux » volume VeraCrypt, pour qu'ils n'accèdent pas à vos vrais

Maintenant, la pratique !

Maintenant que vous avez survécu à l'explication théorique du pourquoi du comment, il est temps de passer à la pratique.

Tails

Nous recommandons actuellement chez XR, le système Tails.

Tails est un système d'exploitation portable, installable sur clé USB, conçus pour éviter la surveillance, les publicités, la censure, et est particulièrement bien adapté à notre cas de figure.

Tails a également comme particularité de passer par le réseau Tor, tout ce que vous faites quand vous allez sur internet passe par ce réseau Tor.

Si vous voulez savoir ce qu'est le réseau Tor, vous pouvez consulter le tutoriel sur comment naviguer en se protégeant ici

Si vous souhaitez en savoir plus sur le fonctionnement de Tails, vous pouvez vous rendre ICI

Sécurité : Attention à la persistance !

Vous pouvez sur Tails stocker certaines de vos données sur la persistance de la clé USB.
Cette persistance est chiffrée, mais les autorités pourrons légalement vous obliger à donner le mot de passe, pour déchiffrer cette persistance.

Pour éviter qu'ils accèdent aux données de votre persistance, vous pouvez soit :
- Éviter qu'ils n'accèdent à votre clé USB, mais ce n'est pas garanti.
- Rajouter sur votre persistance un volume VeraCrypt caché, pour ça, vous pouvez soit :
    - Copier sur cette persistence un volume Veracrypt que vous avez déjà créé au préalable, depuis le disque dur de votre ordinateur par exemple
    - Créer le volume VeraCrypt directement sur la persistence, depuis Tails, cependant il faut d'abord que vous installiez VeraCrypt qui n'est pas présent de base sur Tails, à partir de ce tutoriel

Accéder à vos volumes VeraCrypt

Bien évidemment, vous pouvez accéder à vos volumes VeraCrypt depuis Tails.

Il faut savoir que le logiciel VeraCrypt tel que présenté dans la deuxième section de ce guide n'est pas installé de base sur Tails, cependant vous n'en n'avez pas besoin pour ouvrir vos volumes, car

il existe sur Tails un gestionnaire permettant de le faire (mais pas d'en créer), dont vous pouvez voir le tutoriel ici.

Si votre volume VeraCrypt se trouve autre part que sur votre persistance, comme sur un disque dur externe, ou sur votre disque dur interne, Tails vous demandera un mot de passe administrateur pour pouvoir y accéder. Pour savoir comment définir ce mot de passe administrateur, cliquez ici

Installer/utiliser Tails

Concernant les étapes de l'installation et de l'utilisation de Tails, il existe sur les site des tutoriels très complets que je vais vous partager ici :

Cliquer pour tutoriel installation/utilisation de Tails

Mettre à jour Tails

Il peut être important de régulièrement mettre à jour la version de Tails présente sur votre clé USB.

Cliquer pour tutoriel de mise à jour de Tails

Révision #8
Créé 31 December 2023 18:04:10 par mollusque
Mis à jour 31 December 2023 20:42:47 par mollusque