T2 P2 - Chiffrer données avec VeraCrypt

Maintenant que nous avons vue dans la partie précédente des techniques pour effacer efficacement les traces de fichiers/logiciels sensibles de votre ordinateur, nous allons maintenant nous attaquer à une autre étape, celle du chiffrement des données !

Au delà des fichiers/logiciels sensibles dont vous voulez potentiellement effacer les traces, vous avez sans doute aussi besoin d'en stocker dans le cadre de vos activités, il est donc primordial de bien les protéger.

Pour cela, nous recommandons chez XR un logiciel assez puissant, et rapide à prendre en main en terme de chiffrement des données, qui s'appelle **Veracrypt**.

Ce logiciel sert à chiffrer à la fois des supports de stockages, que des fichiers.
Vous pouvez par exemple créer un faux fichier, en .png, ou .dll par exemple, et y mettre votre volume chiffré.
Il ne sera ainsi possible de savoir que ce fichier est en réalité un volume chiffré, qu'en essayant de l'ouvrir avec **Veracrypt**.

Mais trêve de balivernes ! Je vous donne ici le lien vers un tutoriel bien plus détaillé sur le fonctionnement et les particularités de ce logiciel, et comment l'utiliser :

Tutoriel VeraCrypt : Cliquez ici

Attention :

Malgrés le fait que vos données soit chiffrées bien au chaud dans un volume VeraCrypt, il reste important d'avoir des copies, car le risque de perdre vos données est toujours présent.
Ces copies peuvent par exemple être d'autres volumes VeraCrypt sur d'autres ordinateurs.
Vous pouvez également les mettre sur un drive, de préférence chiffré, comme Proton Drive, vous permettant de toujours pouvoir accéder à vos données même si tout vos disques dur ont étés perquisitionnés par les FDOs !

Et après?

Une fois votre ou vos volumes chiffrés, il peut être risqué de les déchiffrer et de travailler dessus depuis votre ordinateur « normalement ». En effet, même une fois chiffrés, votre ordinateur risque de mémoriser l'emplacement des fichiers qui ont été manipulés, l'activité que vous avez eu, et

c’est encore pire s’il est infecté !

Vous devez sûrement vous dire, « Mais comment je fais dans ce cas pour faire mon business ? » et c’est une très bonne question !

Cela nous ramène à la 3ème partie de notre tutoriel, qui va concerner les clés USB bootables !

Révision #10
Créé 31 décembre 2023 17:57:26 par mollusque
Mis à jour 7 mai 2024 18:09:08 par mollusque