

Étude des **Virus**





Qu'est-ce qu'un **VIRUS** ?

- ◉ « Logiciel Malveillant »
- ◉ À l'origine : programme **autoréplicatif** qui se propage de système en système
- ◉ Virus informatique != Ver informatique
- ◉ Plusieurs types : polymorphiques, batch, macrovirus...etc



Exemple de **Virus Batch**

- ◉ Fichier **Batch** : commandes interprétables par le *DOS (Windows)*
- ◉ Facile à contrer
- ◉ Exemple



Les **Stealers**

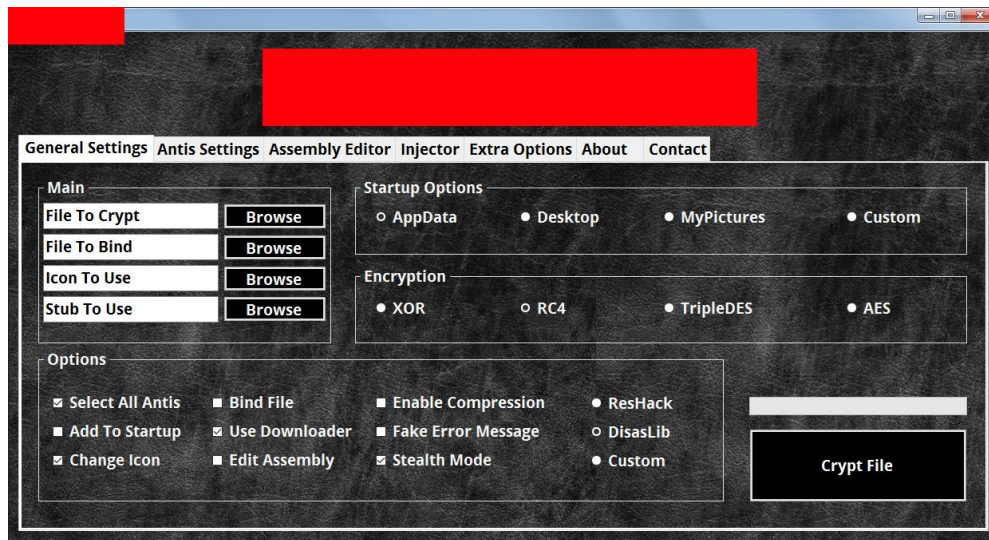
- Outils spécialisés pour voler des informations locales précises





Les Crypters

- Outils spécialisés pour **chiffrer** d'autres programmes malveillants





Comment s'en prémunir

- ⦿ Éviter de sauvegarder des mots de passe localement (ou mdp maître)
- ⦿ Vérifier **l'intégrité** des fichiers (hashs)
- ⦿ Faire des scans (*Virustotal*)
- ⦿ Exécuter dans des environnements d'exécution sécurisés (*Malwr*)
- ⦿ Rester vigilant(e)