Dans un sous-repertoire nommé **viro** à la racine du dépôt du projet.

Notions évaluées	Xp à gagner
virologie et malware	20

Fichier à rendre:

```
.
├── inj_asm_code_begin.asm
├── inj_asm_code_end.asm
├── inj_code.c
├── inj_code.h
├── injector.c
├── makefile
└── test.c

0 directories, 7 files
```

Sujet:

Virologie & Malware - Projet Yharnam

Projet Yharnam

Ce projet reprends en substance les mêmes objectifs que les cours/TP, à savoir:

- Injecteur PE: c'est à dire contaminant un fichier exécutable d'un répertoire.
- Modifie le point d'entrée du fichier cible de sorte à s'exécuter avant toute chose, puis à redonner la main aux instructions originelles.
- Le code injecté affiche une MessageBox afin de constater de l'infection.

Il est recommandé de respecter la démarche des TPs:

- création d'une section à part pour stocker tout le code injectable dans l'injecteur originel.
- makefile pour le compilation.
- compilation conditionnel pour les tests.

Les fonctionnalités sont potentiellements étendues par les bonus suivants:

- Injection dynamique: à chaque exécution contamine tous les fichiers PE/64 bit du répertoire courant.
- Injection process: contamine un type de process connue s'il est actif dans la session (i.e: calc.exe).

- Packing / chiffrement: si votre code n’est pas en clair dans le fichier PE injecté mais à subit des transformations.

Toutefois quelques largesses sont autorisés:

- Si votre malware mets en place un mécanisme de persistance autre que celui présenté en cours (injection de PE), il devra être complétement décrit dans votre fichier README.txt.

Le rendu sera rendu sous forme d’archive (7z chiffré avec mdp ‘yharnam’) contenant l’ensemble des fichiers requis pour la fabrication de votre projet. Celle-ci devra être téléversée sur l’espace google classroom dédié au projet. Est demandé également un fichier *README.txt* expliquant les modalités de compilation.

Vous expliquerez aussi dans votre README.txt les comportements de votre malware:

- infection de process si bonus présent et quel process est ciblé
- packing/chiffrement
- etc…