Rapport

Projet de sécurité

# Contexte

De nos jours, la sécurité informatique est un domaine qu’il faut prendre très au sérieux. Si le développement des nouvelles technologies de l’informatique, ainsi que son expansion (autrefois destiné aux leaders de ce monde mais désormais presque omniprésente dans les foyers) progresse à une vitesse fulgurante, il en est de même pour les menaces qui se veulent à l’encontre de l’intégrité et de la confidentialité de nos informations. Je parle ici des virus informatique. Voici quelques exemples de virus informatique populaire à travers le temps:

* Le 2 novembre 1988, le virus **Morris** parvient à attaquer 6000 ordinateurs connectés à internet
* Le 25 Janvier 2003, le virus **Slammer** paralyse internet en se servant d’une faille découverte à peine 6 mois plus tôt
* Apparu le 27 Juin 2017, le virus **Petya**, probablement le virus le plus cher de son histoire puisqu’il aurait coûté plus d’1 milliard d’euros aux entreprises touchées. (Ransomware)

Aujourd’hui, un virus correctement programmé pourrait paralyser internet en quelques secondes seulement. Vous l’aurez donc compris le développement dans le domaine de l’attaque informatique ne cesse d’évoluer. Forte heureusement il en est de même pour la défense.

Une fois qu'un virus parvient à se joindre à un programme, un fichier ou un document, il reste inactif jusqu'à ce que des circonstances particulières provoquent l'exécution de son code sur l'ordinateur ou le périphérique. Un virus affectera votre ordinateur lorsque vous lancerez (malencontreusement) le programme infecté. Cela provoque le déclenchement du code du virus. Du moment que l’exécution du programme infecté n’a pas lieu le virus restera latent sur votre ordinateur, qui ne montrera aucun signe ou symptôme d'infection majeur. Or une fois que le virus à infecté votre machine il peut voler des mots de passe ou des données, enregistrer la frappe au clavier, endommager des fichiers, envoyer des spams à vos contacts de messagerie électronique, voire prendre le contrôle de votre machine, ect...

Dans le monde de la virologie informatique, il existe plusieurs types de virus. En voici quelques uns:

* **Les virus polymorphes:** Le polymorphisme ou comment faire varier, de copie en copie du virus, les éléments constitutifs d'une signature potentielle (pour un anti-virus), en produisant un code viral vraiment différent dans la forme, mais identique dans ses fonctions d'infections et de charge finale.
* **Les virus souterrains:** Il s’agit d’un virus qui appellent directement les vecteurs d’interruption du DOS et du BIOS. Ce faisant il contourne tout programme de contrôle qui pourrait être chargé et avoir intercepté ces mêmes vecteurs dans le but de détecter l’activité d’un virus.
* **Le ver informatique:** Contrairement aux autres virus informatique, le ver se propage sans avoir besoin de se lier à d'autres programmes exécutables. Il utilise internet pour se propager.
* **Le virus compagnon:** Il s’agit d’un virus qui au lieu de modifier un fichier existant, va créer un nouveau programme qui sera exécuté sans que l’utilisateur soit au courant à la place du programme qui est censé être exécuté. Le programme original est tout de même exécuté de sorte que cela paraisse normal à l’utilisateur. Ceci peut être accompli en créant un nouveau fichier .old portant le même nom que le fichier .exe. Les anti-virus qui ne cherchent que les modifications apportées aux fichiers existants ne détecteront pas ce type de virus.

Pour ce projet, nous allons mettre en place un virus de type compagnon.

On utilisera un Mediaplayer (visionneur de photos) qui provoquera l'infection de la machine. Lorsque l'utilisateur exécute le MediaPlayer tous les exécutables du répertoires courant (utilitaires) vont être infectés. Cela aura pour effet de créer des copies en .old des exécutables et le MediaPlayer.exe en cours d'exécution se recopie lui-même dans son intégralité en version exécutable. Cette copie intégrale prend ensuite le nom original du programme cible.

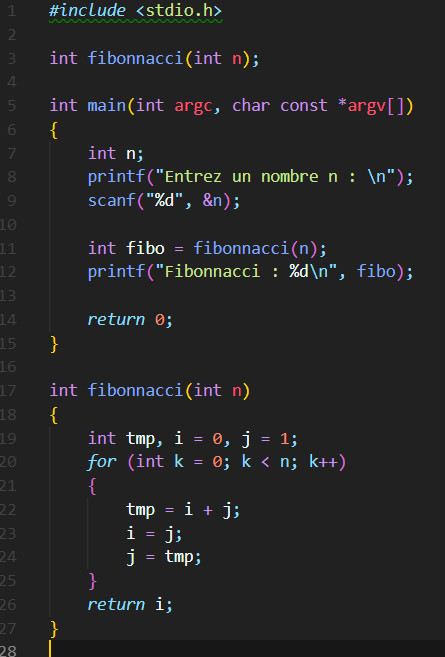
Pour résumer l’infection comporte 3 étapes:

* Renommer le fichier cible courant avec l’extension.old
* Dupliquer le virus, programme en cours d'exécution, copie portant le bon nom
* Cette copie doit être un exécutable

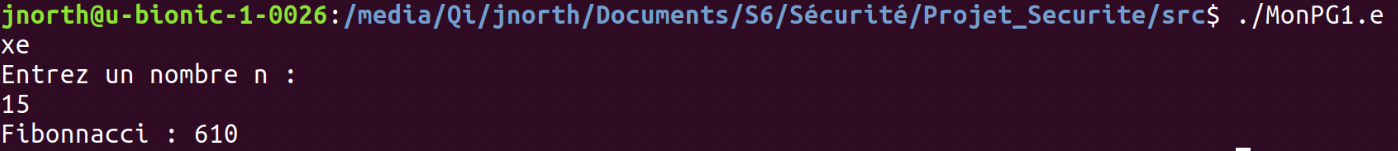
# 

# Présentation rapide des utilitaires qui vont être infectés

## Programme 1

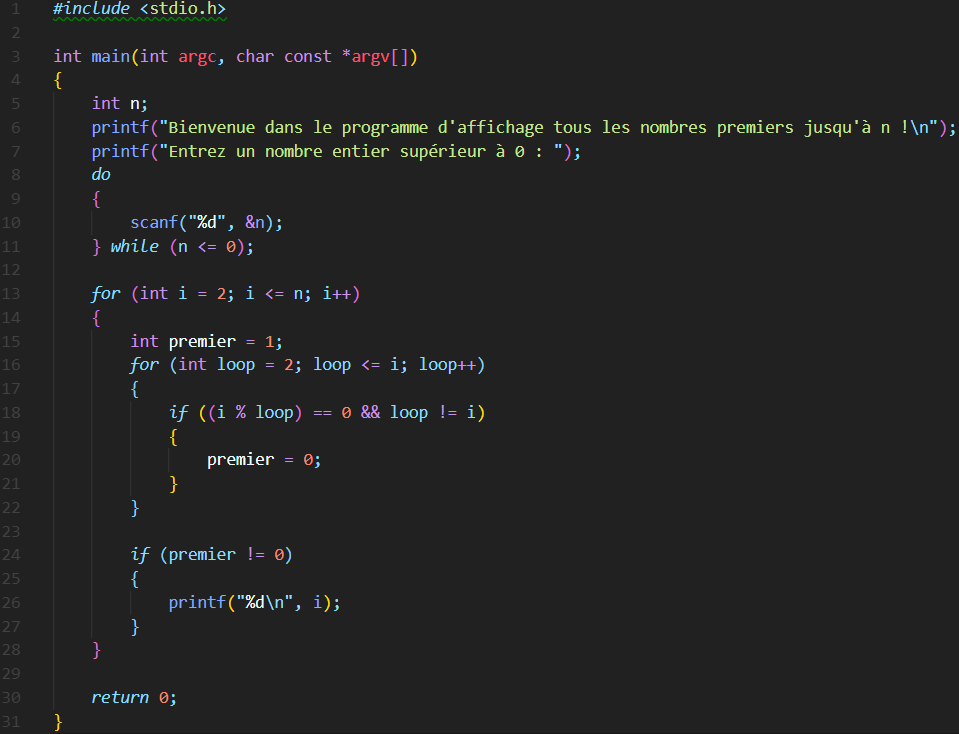
Il s’agit d’une suite de Fibonnacci. 

A son exécution le programme demande à l’utilisateur un nombre N qui correspondra à l’index du nombre de la suite de fibonnacci qu’il renverra.

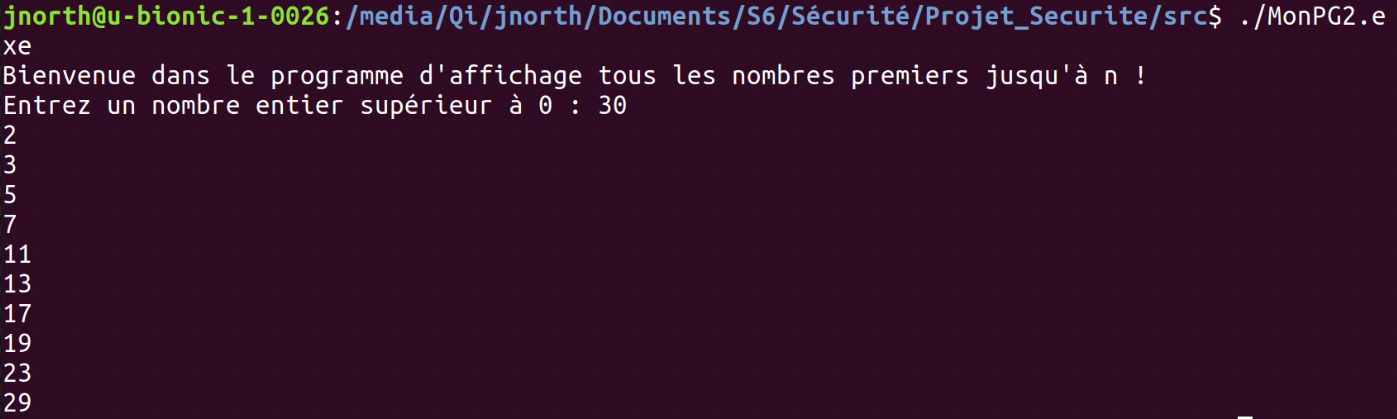


## Programme 2

Ce programme calcul les nombres premiers.

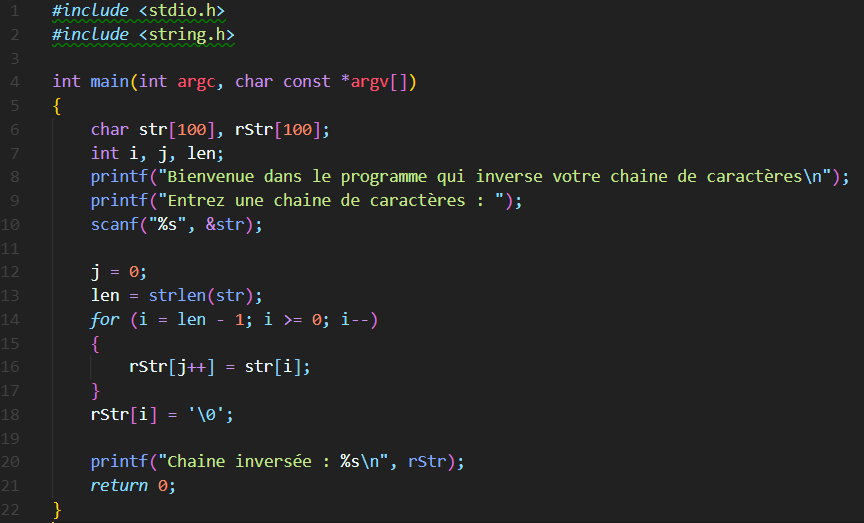


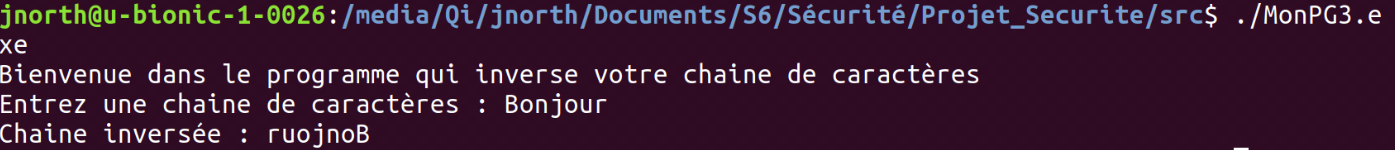
L’utilisateur rentre un nombre dans le terminal, et le programme renvoie les nombres premiers jusqu’à ce nombre.



## Programme 3

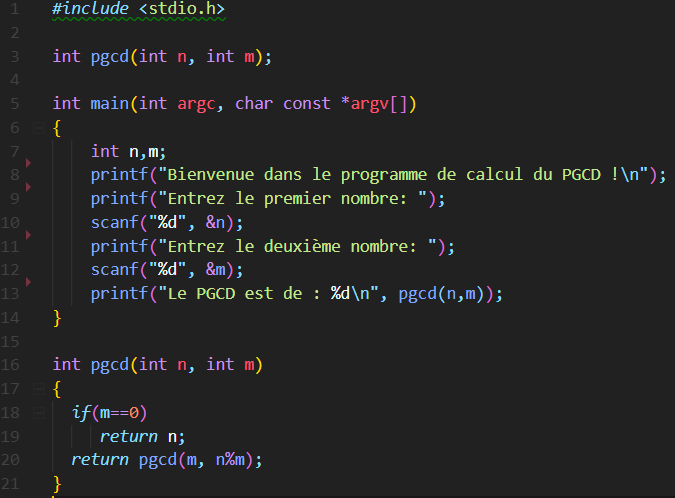
Ce programme inverse la chaîne de caractère que l’utilisateur entre dans le terminal.

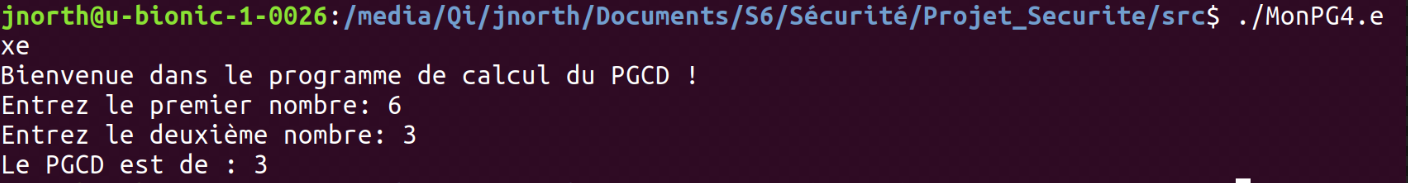
****



## Programme 4

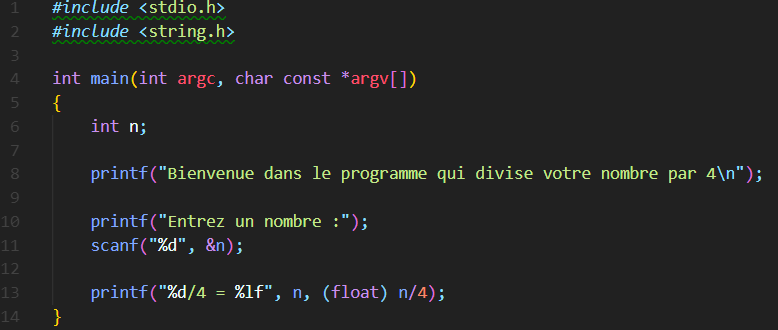
L’utilisateur saisit deux nombres dans le terminal et le programme calcule leur plus grand diviseur commun.

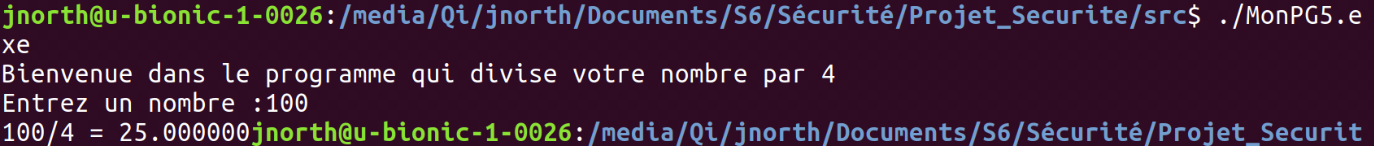
****

****

## Programme 5

Programme simple qui se contente de diviser un nombre par 4.

****

****

Capture d’écran du MediaPlayer se chargeant d’infecter la machine de l’utilisateur

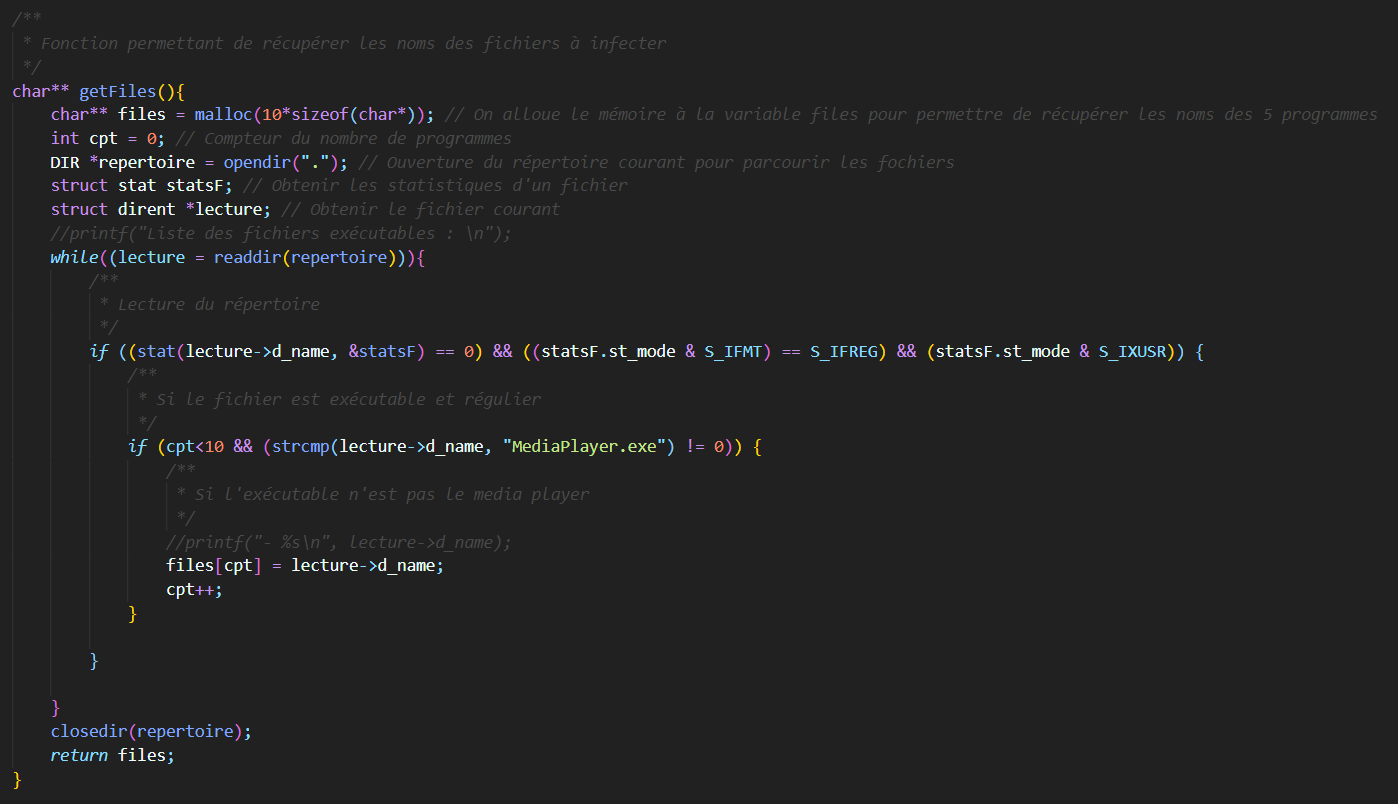


Comme expliqué ci dessus, le lancement du MediaPlayer aura pour effet d’infecter ces programmes. Les .exe initiaux censés lancer le programme deviennent des .old et c’est le MediaPlayer qui prend la place des .exe. De ce fait quand l’utilisateur voudra exécuter l’un des programme, il exécutera le virus à nouveau.

# Présentation des fonctions pour le développement du virus

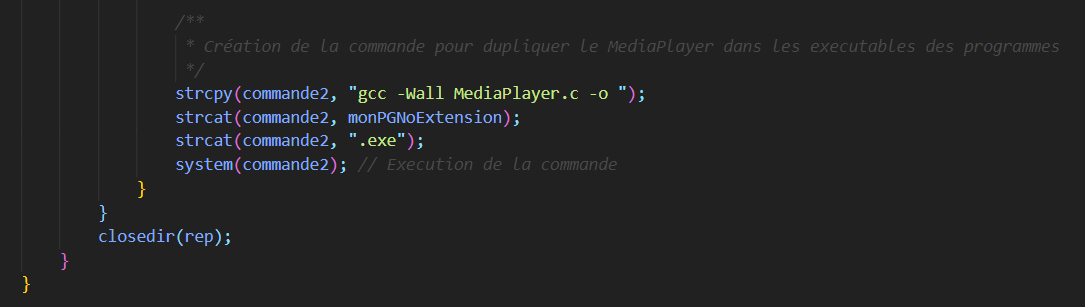
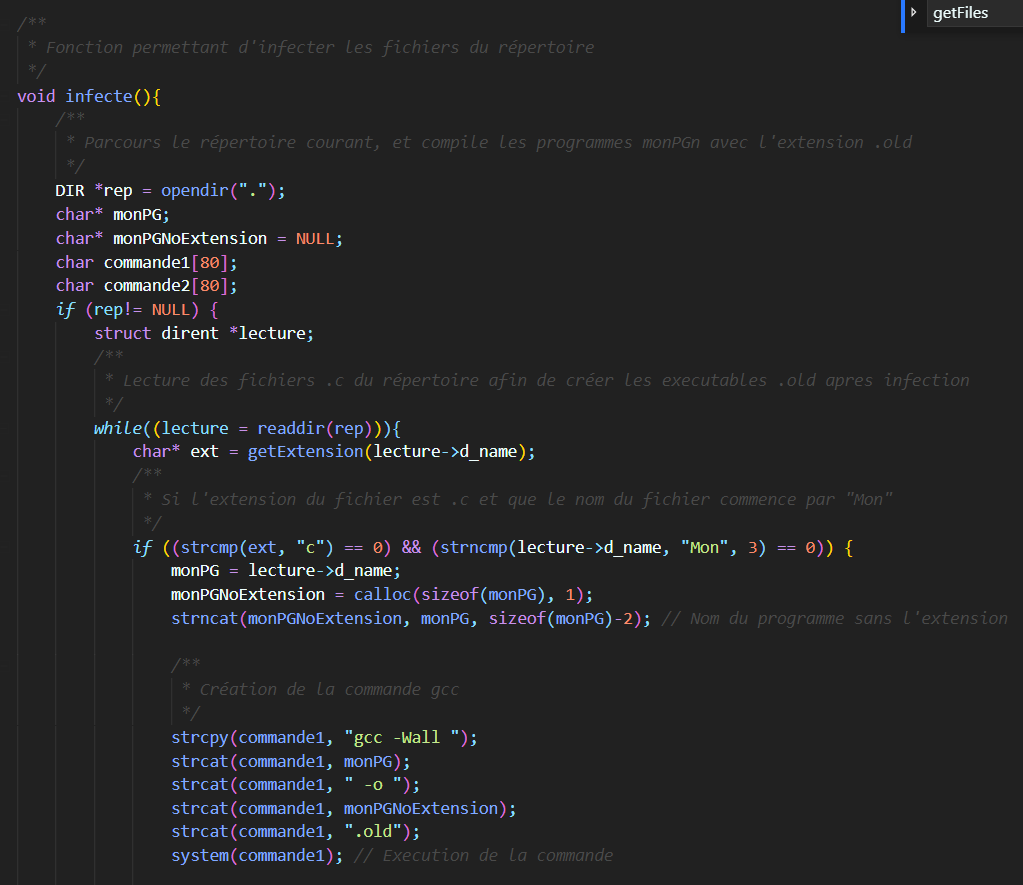
## MediaPlayer.c

### La Fonction getFiles()



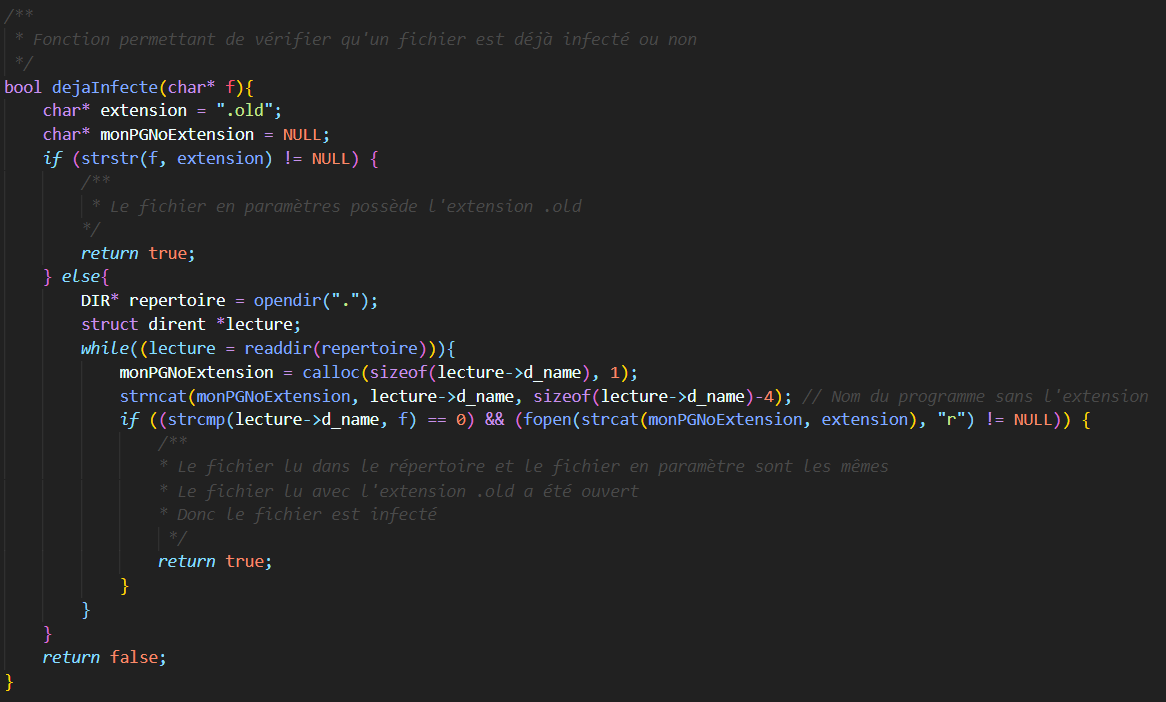
On commence par allouer la mémoire à la variable files, cela nous permettra de récupérer les noms des 5 programmes ou 10 si les .old ont été créés. On utilise stat pour obtenir les statistiques d’un fichier. Ensuite on récupère le nom des exécutables du répertoire courant. Si le fichier est exécutable et régulier et qu’il ne s’agit pas du MediaPlayer on l’ajoute dans files[]. On retourne le tableau contenant le nom des exécutables.

### La Fonction infecte()



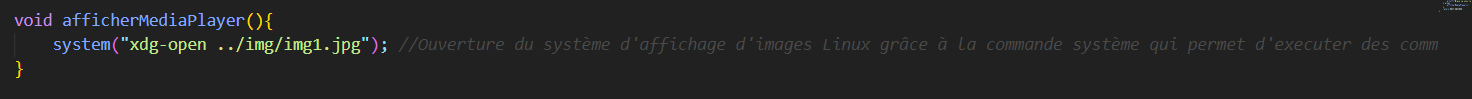
C’est avec cette fonction qu’on infecte les exécutables du répertoire. On commence par trouver les .c, ensuite on récupère leur nom sans l’extension pour créer la copie .old. Une fois cette étape achevé on crée la commande qui aura pour fonction de dupliquer le MediaPlayer dans nos exécutables. Ils sont désormais infecté.

### La Fonction dejaInfecte()



Cette fonction vérifie si le fichier passé en paramètre est déjà infecté ou non. Si le fichier est infecté on retourne true, sinon on retourne false. Pour ce faire on vérifie d’abord si on trouve le fichier f avec l’extension .old. Sinon, on vérifie quand même si on arrive à en ouvrir un (fopen). On utilise strcmp pour comparer les 2 chaînes lexicalement.

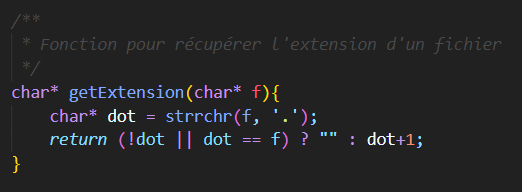
### Fonction afficheMediaPlayer()



On utilise cette ligne de commande pour l’affichage du MediaPlayer.

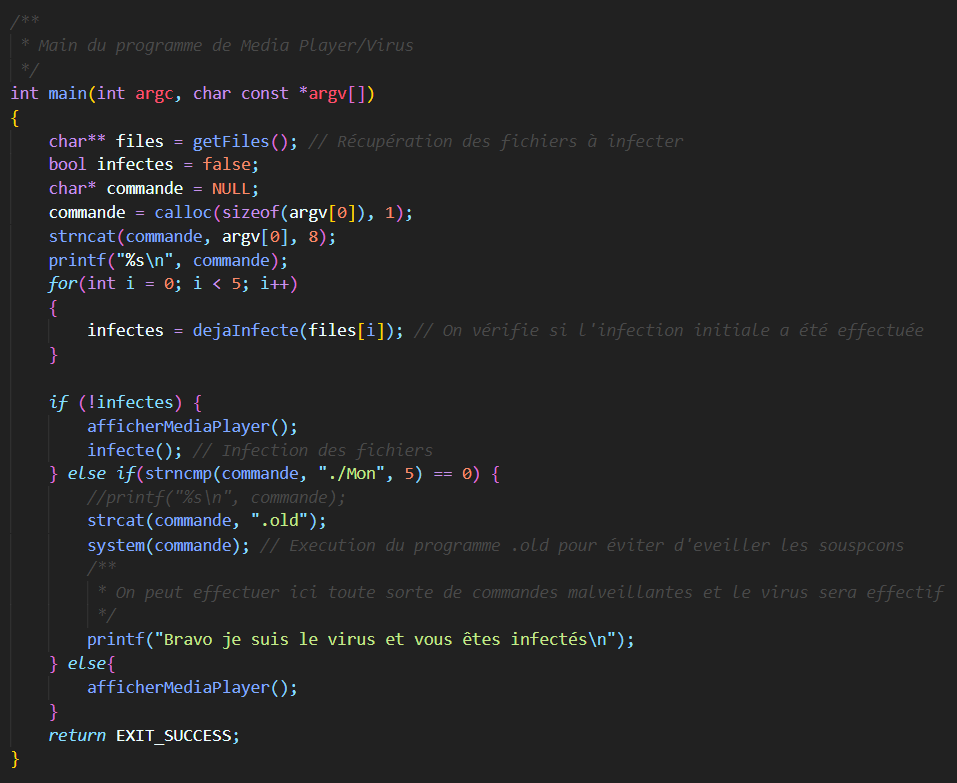
### 

### Fonction getExtension()

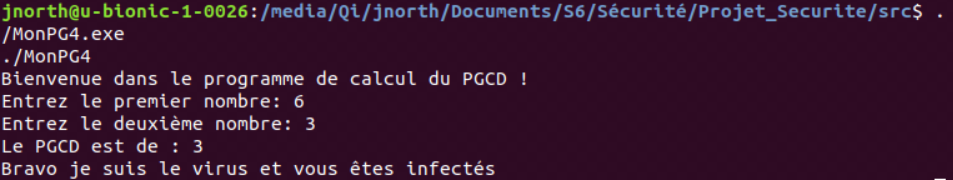


Cette fonction permet de récupérer l’extension d’un fichier, on s’en sert pour vérifier qu’une extension est en .old ou .c ou encore .exe, à l’aide d’un if ternaire et de la fonction strrchr permettant de récupérer la dernière occurrence d’un caractère dans une chaîne.

### Main()



Dans le main, on commence par récupérer les fichiers à infecter. On les parcourt un par un afin de vérifier qu’il ne sont pas déjà infecté. Une fois la vérification effectuée, on entre dans un if.  
S’il ne sont pas infectés alors on affiche le media player à l’aide de la fonction afficherMediaPlayer() tout en infectant les fichiers avec la fonction infecte(). Si les fichiers sont infectés et que la commande qui a été exécutés est un des programmes MonPGn, alors on affiche pas le media player cette fois-ci afin de ne pas éveiller les soupçons et on exécute l’exécutable .old pour que ça ne change pas le fonctionnement pour l’utilisateur. Par la suite on pourrait effectuer n’importe quelles actions malveillantes. Ici, on se contentera d’afficher seulement un message. Sinon on affiche simplement le media player sans infection.



Comme l’atteste la capture d’écran ci dessus, notre virus se contente d’afficher ce message. “Bravo je suis le virus et vous êtes infectés”.

La victime a donc sans s’en rendre compte infecté sa machine. C’est pourquoi il est toujours important de s’assurer de la fiabilité d’un fichier avant de l’exécuter. Cette vérification est d’autant plus importante quand les fichiers proviennent d’une source externe inconnue. Exemple: Téléchargement de jeux vidéos, de films ou de musiques sur le net…

CLIGNY Benjamin

NORTH Justin