Examen Virus & Antivirus

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

Nom / Prénom :

Analyse d'une version simplifiée de 'Valium', dont le code (VBS) est fourni en annexe.
Il n'est pas nécessaire de comprendre le code de manière approfondie et détaillée pour répondre aux questions.

Questions

Question 1 (1pt) : 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, indiquez à quelle(s) section(s) cette fonction est mise en œuvre et expliquez succinctement le principe.

Question 4 (6pt) : 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 (3pt) : 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 en détail le mécanisme de la section 8 sur le plan technique et préciser l'intérêt de cette section pour le concepteur du programme.

Question 8 (2pt) : La version d'origine de ce programme permet d'infecter un grand nombre de types de fichiers, en particulier des fichiers sources de code C++. Quel genre d'instructions peut-on rajouter dans un programme source pour permettre l'exécution de code scripté (à l'exécution du programme compilé) ? Expliquez en quoi ce genre d'instructions peut être considéré comme incriminant pour une analyse heuristique du code source par un anti-virus.

Question 9 (3pt) : La version d'origine de ce programme contient une fonction permettant de le rendre polymorphe. Expliquez ce que cela signifie et proposez 2 idées pour rendre du code VBS polymorphe.