=== How to spread a worm ? ===
=== by PetiK (09/17/2001) ===

```
###################
#FIND SOME ADDRESS#
###################
```

The most difficult to spread a worm is to find some address.
There are in the computer, a lot of file which stock address.

*.WAB file (Windows AddressBook):

We can find this sort of file in the default value of
HKEY_CURRENT_USER\Software\Microsoft\Wab\WAB4\Wab File Name.
Look at the source of Win32.HiV coded by Benny to examine the mechanism.

For this sort of file, I use an other technic. I create in the C:\
a vbs file. This vbs file will search all email in the Oultook Address Book
and save them in a file in the WINDOWS or SYSTEM folder. This file afterwards
is scanned by the worm (look at the source of I-Worm.Passion or I-Worm.Rush).

*.HTM, *.HTML (Internet files):

Windows is full of this sort of file but the problem is that they don't contain
a lot of address. The solution is to scan all *.HTM and *.HTML files in the
MSIE Cache Directory. We can use the api SHGetSpecialFolderPathA in the DLL file
SHELL32.dll (20h). We can use regedit too. The address is the following :
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache.

*.EML file (Outlook Express file):

We can found some address in a email ready to send.

*This is the start of a eml file (Outlook Express)

```
From: "PetiKVX" <petikvx@multimania.com>
To: <victim@multimania.com>                    <= We have our address
Subject: Virus Spread
Date: Sun, 16 Sep 2001 20:54:11 +0200
MIME-Version: 1.0
```

To take this address, we search the string "To: <" in *.eml and we take the address

```
#################
#SPREAD THE WORM#
#################
```

I have imagined something to insert a virus/worm/trojan in a mail which contain already
an attachment. We're going to use *.eml file again

This is the appearance of a EML file :

```
From: "PetiKVX" <petikvx@multimania.com>
To: <victim@multimania.com>
Subject: Virus Spread
Date: Sun, 16 Sep 2001 20:54:11 +0200
MIME-Version: 1.0
Content-Type: multipart/mixed;
       boundary="----=_NextPart_000_0008_01C13EF1.BF420560"   <= The string of the
"boundary"

------=_NextPart_001_0009_01C13EF1.BF420560
Content-Type: text/plain;
       charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

This is a new virus                    <= This is the body of mail
                                       <= We can add something (text, script ??)


------=_NextPart_000_0008_01C13EF1.BF420560
Content-Type: application/x-msdownload;
       name="Winpopup.exe"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
```

```
       filename="Winpopup.exe"                 <= This is a first attachment

HGiAAAAAAAaACgAAAAAA5gUNADAcP4AAAAAA8wUFADAcQIAAAAAA+AUzADAcQoAAAAAAKwZpADAc
Q4AAAAAAlAYLADAcRIAAAAAAnwYJADAcvIAAAAAAqAYLADAcFIEAAAAAswYEADAcFYEAAAAAtwYF
ADAcFoEAAAAAvAYDADAcZYAAAAAACYABAAAAAAC/BgMAMAzcgAAAAAAKgAEAAAAAAMIGAQAwHKoB
AAAAABCAAQAAAAAAwwYfADAMAYAAAAAAA4AGAAAAAACMBC8AEBwBgAAAAAC7BBMAEBwCgAAAADR


------=_NextPart_000_0008_01C13EF1.BF420560     <= Delete "--" at the end of the string
Content-Type: application/x-msdownload;          \
       name="virus.exe"                  |
Content-Transfer-Encoding: base64        |<= This our virus that we want attached.
Content-Disposition: attachment;         |<= The file is of course encode with the
       filename="virus.exe"              |<= Encode64 system.
                                         ----------------------------------
TVpQAAIAAAAEAA8A//8AALgAAAAAAAAAQAAaAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|
AAAAAAAEAALoQAA4ftAnNIbgBTM0hkJBUaGlzIHByb2dyYW0gbXVzdCBiZSBydW4gdW5kZXIgV2lu|
MzINCiQ3AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|
                                         |----------------------------------
                                         |
------=_NextPart_000_0008_01C13EF1.BF420560--   /
```

To attached a file with this way, we must read the "boundary". Here it is the string
"----=_NextPart_000_0008_01C13EF1.BF420560".
We must delete "--" after the last "boundary" before infection.
Like this the mail will contain the second attached
Warning !!
We must add "--" before and AFTER the LAST "boundary" to mark the end of the mail.

There we are !
If you have suggest, please mail me to petikvx@multimania.com.
You can visit my siteweb : http://www.petikvx.fr.fm