EmbedFileInVBScript

Soumis par Gilles LAURENT
01-04-2008
Dernière mise à jour : 02-04-2008

EmbedFileInVBScript est un script encodeur permettant d'embarquer un fichier de type binaire ou exécutable au sein d'un script VBScript. Pourquoi ai-je été amené à developper cet outil ces derniers jours ? Et bien voilà ! J'ai dû intervenir pour un client sur un serveur DNS Windows 2000 dans le but d'analyser les différents paramètres de configuration du service DNS. Je souhaitai utiliser l'outil Microsoft dnscmd.exe pour extraire la configuration complète du service. Malheureusement, les outils du support n'étaient pas installés sur le serveur. Je ne pouvais accéder au serveur que par session TSE et tous les ports étaient fermés mis à part les ports 53 (DNS) et 3389 (TSE). Sans support RPC, l'analyse à distance n'était donc pas possible ! La seule solution consistait donc à copier l'outil dnscmd.exe localement sur le serveur via le presse-papier, seule passerelle entre mon poste de travail et le serveur distant ! J'avais donc besoin d'un outil capable d'une part d'encoder un fichier binaire au format texte pour assurer la compatibilité avec le presse-papier et d'autre part de reconstituer le fichier précédemment encodé.

Historique :
Version 1.0 - première release publique

Plateformes supportées :
Windows 2000+

Pré requis :
Microsoft ActiveX Data Objects 2.5

Listing 1 : EmbedFileInVBScript.vbs

```
- Const adTypeBinary=1
-
- Set oFs=CreateObject("Scripting.FileSystemObject")
- Set oArgs=WScript.Arguments
- Set oStream=CreateObject("ADODB.Stream")
-
- oStream.Type=adTypeBinary: oStream.Open
- oStream.LoadFromFile oArgs(0)
- BinStream=oStream.Read
- oStream.Close
-
- WScript.Echo "Const adTypeBinary=1"
- WScript.Echo "Const adSaveCreateOverWrite=2"
- WScript.Echo "Const adVarBinary=204"
- WScript.Echo "Const adFileName=""" & oFs.GetFileName(oArgs(0)) & """"
- WScript.Echo
- WScript.Echo "Set oFs=CreateObject(""Scripting.FileSystemObject"")"
- WScript.Echo "Set oFile=oFs.OpenTextFile(WScript.ScriptFullName)"
```

```
- WScript.Echo "Set oRs=CreateObject(""ADODB.RecordSet"")"
- WScript.Echo "Set oStream=CreateObject(""ADODB.Stream"")"
- WScript.Echo
- WScript.Echo "oStream.Type=adTypeBinary: oStream.Open"
- WScript.Echo "oRs.Fields.Append ""Data"",adVarBinary,32: oRs.Open: oRs.AddNew"
- WScript.Echo "WScript.Echo ""ReGenerating "" & adFileName & "" ..."""
- WScript.Echo
- WScript.Echo "While Not oFile.AtEndOfStream"
- WScript.Echo "  sLine=oFile.ReadLine"
- WScript.Echo "  If Left(sLine,3)=""# "" Then"
- WScript.Echo "    oRs(""Data"")=Right(sLine,Len(sLine)-3)"
- WScript.Echo "    oRs.Update: oStream.Write oRs(""Data"")"
- WScript.Echo "  End If"
- WScript.Echo "Wend"
- WScript.Echo
- WScript.Echo "oStream.SaveToFile adFileName,adSaveCreateOverWrite"
- WScript.Echo "WScript.Echo ""Done."""
-
- For i=0 To Lenb(BinStream)-1
-   If i Mod 32=0 Then WScript.Stdout.Write VBCrLf & "# "
-   nHexByte=Right("0" & Hex(Ascb(Midb(BinStream,i+1,1))),2)
-   WScript.Stdout.Write nHexByte
- Next
```

L'utilisation de cet outil est très simple. Il suffit de spécifier en ligne de commande le nom du fichier binaire ou exécutable à encoder. A titre d'exemple, nous allons encoder ici un petit binaire nommé Hello.exe. Le script décodeur étant généré automatiquement sur le flux stdout, la sortie de commande sera redirigée vers un fichier VBScript portant, par convention, le même nom que le fichier binaire mais muni de l'extension .vbs :
WSH D:\Test> @cscript //nologo EmbedFileInVBScript.vbs Hello.exe>Hello.vbs

Listing 2 : Hello.vbs

```
- Const adTypeBinary=1
- Const adSaveCreateOverWrite=2
- Const adVarBinary=204
- Const adFileName="Hello.exe"
-
```

```
- Set oFs=CreateObject("Scripting.FileSystemObject")
- Set oFile=oFs.OpenTextFile(WScript.ScriptFullName)
- Set oRs=CreateObject("ADODB.RecordSet")
- Set oStream=CreateObject("ADODB.Stream")
-
- oStream.Type=adTypeBinary: oStream.Open
- oRs.Fields.Append "Data",adVarBinary,32: oRs.Open: oRs.AddNew
- WScript.Echo "ReGenerating " & adFileName & " ..."
-
- While Not oFile.AtEndOfStream
-   sLine=oFile.ReadLine
-   If Left(sLine,3)="'# " Then
-     oRs("Data")=Right(sLine,Len(sLine)-3)
-     oRs.Update: oStream.Write oRs("Data")
-   End If
- Wend
-
- oStream.SaveToFile adFileName,adSaveCreateOverWrite
- WScript.Echo "Done."
-
- '# 4D5A90000300000004000000FFFF0000B8000000000000004000000000000000
- '# 00000000000000000000000000000000000000000000000000000000E0000000
- '# 0E1FBA0E00B409CD21B8014CCD21546869732070726F6772616D2063616E6E6F
- '# 742062652072756E20696E20444F53206D6F64652E0D0D0A2400000000000000
- '# DE5BC68A9A3AA8D99A3AA8D99A3AA8D9F525A2D9913AA8D91926A6D99B3AA8D9
- '# F525ACD9993AA8D99A3AA9D98A3AA8D9AC1CA2D99B3AA8D95D3CAED99B3AA8D9
- '# 526963689A3AA8D900000000000000000000000000000000000000000000000
- '# 504500004C0104008D44E54700000000000000000E0000F010B01060000020000
- '# 00080000000000002040000000400000008000000000400000400000000020000
- '# 04000000000000000400000000000000040010000040000000000003000000
- '# 00001000001000000000100000100000000000001000000000000000000000
- '# 4C8000002800000000000100980300000000000000000000000000000000000
- '# 00000000000000000000000000000000000000000000000000000000000000
```

- '# 0000000000000000000000000000000000000000000000008000003C000000
- '# 0000000000000000000000000000000000000000000002E74657874000000
- '# 6C010000040000000200000004000000000000000000000000020000060
- '# 2E726461746100008601000000800000000200000006000000000000000000
- '# 00000000400000402E646174610000004C00000000C000000002000000080000
- '# 0000000000000000000000000400000C02E72737263000000980300000000100
- '# 00040000000A000000000000000000000000400000400000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 6810C04000FF152080400083C40433C0C3909090909090909090909090909090
- '# 558BEC6AFF6840804000686041400064A1000000005064892500000000083EC20
- '# 5356578965E88365FC006A01FF152C80400059830D40C04000FF830D44C04000
- '# FFFF15288040008B0D3CC040008908FF15248040008B0D38C040008908A10080
- '# 40008B00A348C04000E8C3000000833D20C0400000750C684E414000FF151C80
- '# 400059E894000000680CC040006808C04000E87F000000A134C040008945D88D
- '# 45D850FF3530C040008D45E0508D45D4508D45E450FF15148040006804C04000
- '# 6800C04000E84C000000FF15108040008B4DE08908FF75E0FF75D4FF75E4E8FD
- '# FEFFFF83C4308945DC50FF150C8040008B45EC8B088B09894DD05051E80F0000
- '# 005959C38B65E8FF75D0FF1504804000FF2508804000FF251880400068000003
- '# 006800000100E81B0000005959C333C0C3C3CCCCCCCCCCCCCCCCCCCCCCCCCCCC
- '# FF2530804000FF2534804000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000

- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 24810000C6800000CE800000DC800000E4800000F4800000481000010810000
- '# B0800000348100004481000052810000648100007881000000000000000000
- '# FFFFFFFF1041400024414000748000000000000000000BA80000000800000
- '# 0000000000000000000000000000000000000024810000C6800000CE800000
- '# DC800000E4800000F4800000481000010810000B0800000348100004481000
- '# 52810000648100007881000000000009E027072696E746600004D5356435254
- '# 2E646C6C0000D3005F657869740048005F5863707446696C7465720049026578
- '# 6974000064005F5F705F5F5F696E6974656E760058005F5F6765746D61696E61
- '# 726773000F015F696E69747465726D0083005F5F736574757365726D61746865
- '# 727200009D005F61646A7573745F6664697600006A005F5F705F5F636F6D6D6F
- '# 646500006F005F5F705F5F666D6F6465000081005F5F7365745F6170705F7479
- '# 70650000CA005F6578636570745F68616E646C6572330000B7005F636F6E7472
- '# 6F6C6670000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000048656C6C6F20776F726C64210A000000
- '# 0100000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000

- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000
- '# 0000000000000000000000000001001000000018000080000000000000000000
- '# 0000000000001000100000030000080000000000000000000000000000000100
- '# 0C040000480000006000010038030000000000000000000000000000000000
- '# 380334000000560053005F005600450052005300490004F004E005F0049004E00
- '# 46004F0000000000BD04EFFE000001000000010001000000000010001000000
- '# 3F000000000000004000400010000000000000000000000000098020000
- '# 0100530074007200690060067004600690060C00650049006E0066006F000000
- '# 7402000001003000340030006300300034006200300000001800000001004300
- '# 6F006D006D0065006E00740073000000200000000100430060F006D0070006100
- '# 6E0079004E0061006D006500000000005000140001004600690060C0065004400
- '# 650073006300720069007000740069006F006E000000000480065006C006C00
- '# 6F00200077006F0072006C006400210020007300610060D0070006C0065000000
- '# 36000B000100460069006C006500560065007200730069006F006E0000000000
- '# 31002C00200030002C00200030002C002000310000000000002C00060001004900
- '# 6E007400650072006E0061006C004E0061006D006500000048006500 6C006C00
- '# 6F000000640020000 1004C006500670061006C0043006F007000790072006900
- '# 6700680074000000 43006F007000790072006900670068007400 2000A9002000
- '# 3200300030003800200047006900 6C006C006500730020004C00410055005200
- '# 45004E00540000002800000001004C006500670061006C005400720061006400
- '# 65006D00610072006B007300000000003C000A0001004F007200690067006900
- '# 6E0061006C00460069006C0065006E0061006D006500000048006500 6C006C00
- '# 6F002E006500780065000000200000000100500072006900760061007400 6500
- '# 4200750069006C00640000002C000600010050007200690076006400 7400
- '# 4E0061006D006500000000004800650 06C006C006F0000003A000B0001005000
- '# 72006F006400750063007400560065007200730069006F006E00000031002C00
- '# 200030002C00200030002C00200031000000000020000000010053007000 6500
- '# 6300690061006C004200750069006C006400000044000000010056006100 7200
- '# 460069006C00650049006E0066006F000000000240004000000540072006100
- '# 6E0073006C006100740069006F006E00000000000C04B0040000000000000000
- '# 0000000000000000000000000000000000000000000000000000000000000000

- '# 0000000000000000000000000000000000000000000000000000000000000000

- '# 0000000000000000000000000000000000000000000000000000000000000000

Le script décodeur Hello.vbs au format texte peut maintenant être copié dans le presse-papier puis recréé sur le serveur distant avec par exemple l'éditeur de texte notepad.exe. Il suffira ensuite d'exécuter le script décodeur Hello.vbs sur le serveur distant pour regénérer automatiquement le fichier binaire Hello.exe. Le fichier binaire sera toujours créé dans le répertoire courant :
WSH D:\Test> @cscript //nologo Hello.vbs
ReGenerating Hello.exe ...
Done.

Téléchargement :

Guide PDF : -
Archive : EmbedFileInVBScript.zip

Liens utiles :

Encoding Binary Data into Batch Code
http://www.infionline.net/~wtnewton/batch/conv2bat.htm

Distributing binary files within VBScript
http://www.valls.name/articles/VBScript_binary_files_in_vbs/binary_files_in_vbs_en.html