

# Office如何快速进行宏免杀

---

原创 HACK学习 HACK学习呀

2020-12-02原文

## 前言

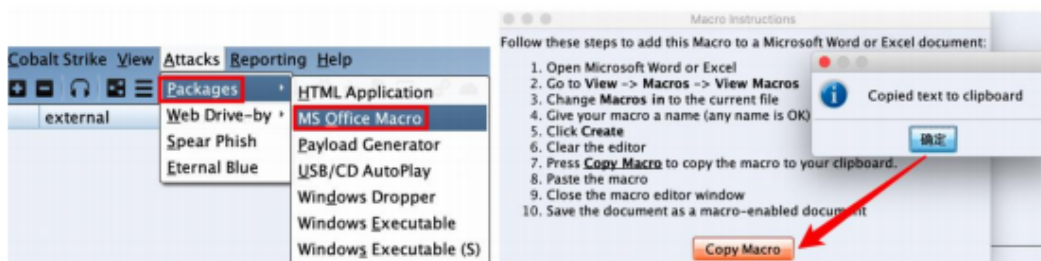
Office 宏，译自英文单词 Macro。宏是 Office 自带的一种高级脚本特性，通过 VBA 代码，可以在 Office 中去完成某项特定的任务，而不必再重复相同的动作，目的是让用户文档中

的一些任务自动化。而宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。

Visual Basic for Applications ( VBA ) 是 Visual Basic 的一种宏语言，是微软开发出来在其桌面应用程序中执行通用的自动化(OLE)任务的编程语言。主要能用来扩展 Windows 的应用程序功能，特别是 Microsoft Office 软件，也可说是一种应用程式视觉化的 Basic 脚本。

## CobaltStrike 生成宏

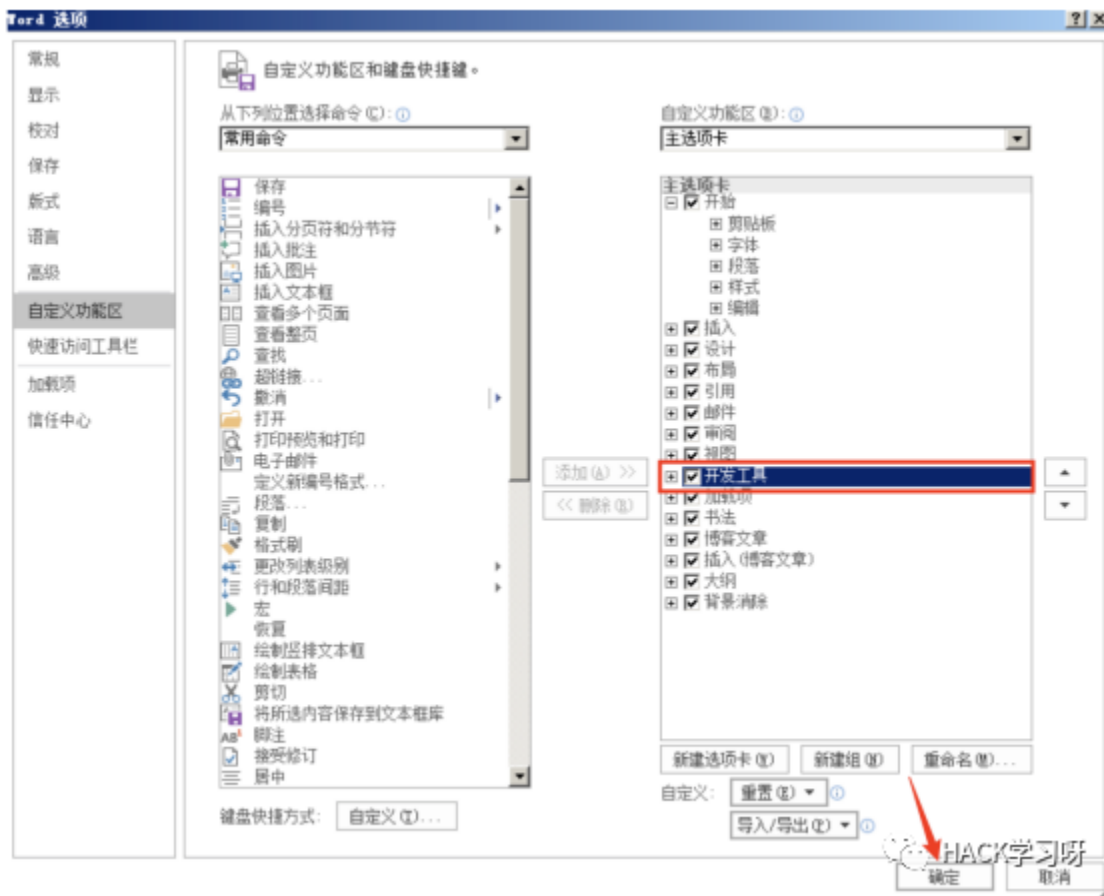
CS 生成 bin 或者直接生成



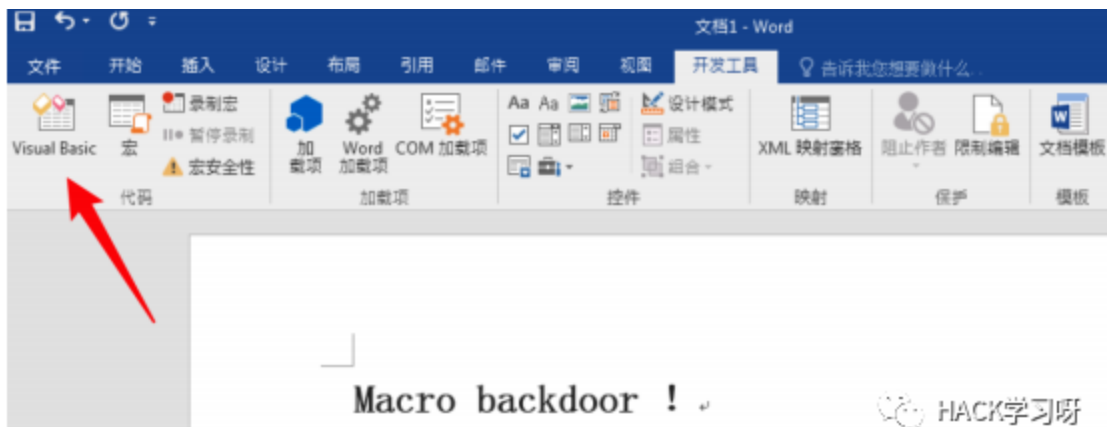
## 创建宏 Word

HACK学习呀

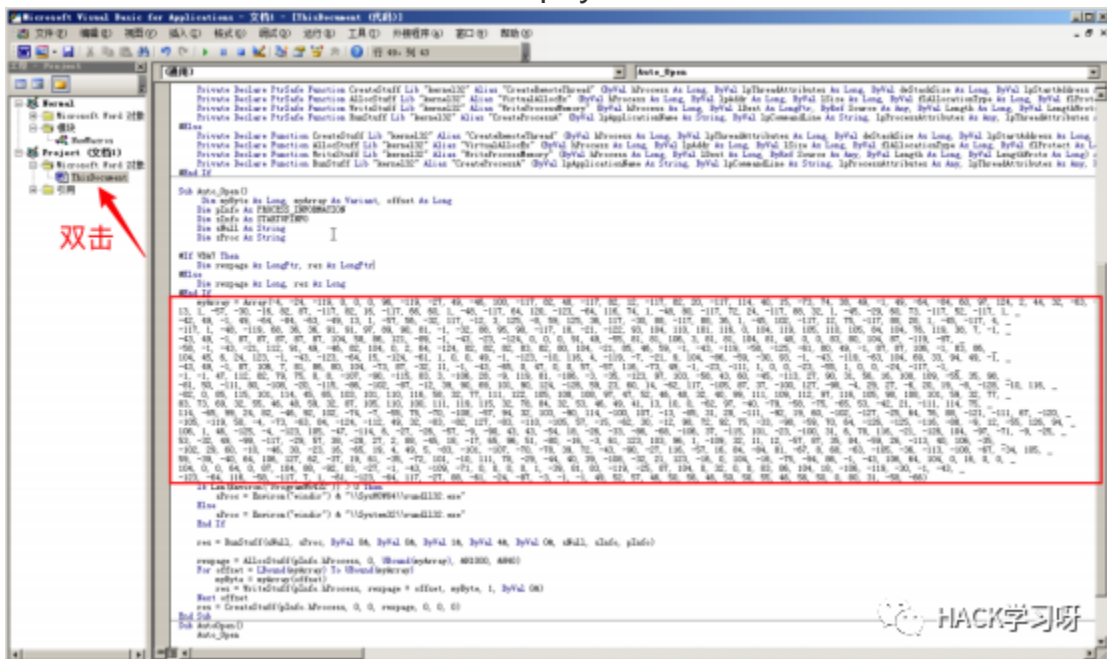
打开 Word 文档，点击“Word 选项 — 自定义功能区 — 开发者工具(勾选) — 确定”。



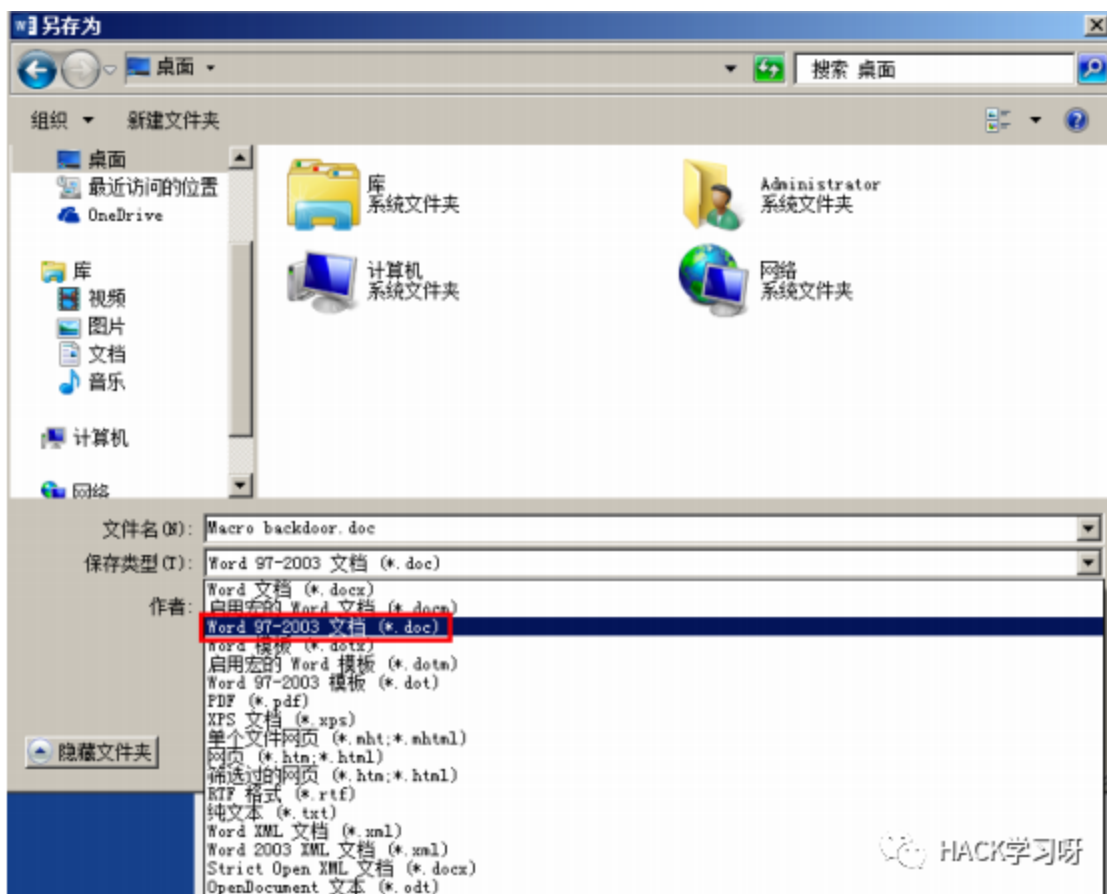
编写主体内容后，点击“开发工具 — Visual Basic”。



双击 “ThisDocument”，将原有内容全部清空，然后将 CobaltStrike 生成宏 payload



全部粘贴进去，保存并关闭该 VBA 编辑器。



另存为的 Word 类型务必要选“Word 97-2003 文档 (\*.doc)”，即 doc 文件，保证低版本可以打开。之后关闭，再打开即可执行宏代码。

## 如何快速处理宏免杀

说到免杀要搞清楚我们的附件在什么环节被杀了，首先科普一下当下杀软的三种查杀方式：1.静态查杀 2.云查杀 3.行为查杀。

邮件服务器为了可用性和隐私性一般只有静态查杀。所以我们只需要规避特征值绕过静态查杀就可以让钓鱼附件进入收件箱了。

如何规避静态查杀？最好的办法当然是自己写恶意代码，但大部分云黑客都是脚本小子，这也没关系，现在 gayhub 上也有很多免杀开源的脚本。这里以 EvilClippy 作为演示 用于创建恶意 MS Office 文档的跨平台助手。

可以隐藏 VBA 宏，踩 VBA 代码（通过 P 代码）并混淆宏分析工具。

在 Linux, OSX 和 Windows 上运行。

github地址：

<https://github.com/outflanknl/EvilClippy>

直接下载编译好的版本： 地址：<https://github.com/outflanknl/EvilClippy/releases>

地址：<https://github.com/outflanknl/EvilClippy/releases>



把这两个下载回来即可 使用方法：

`EvilClippy.exe -s hello.vba diaoyu.doc`

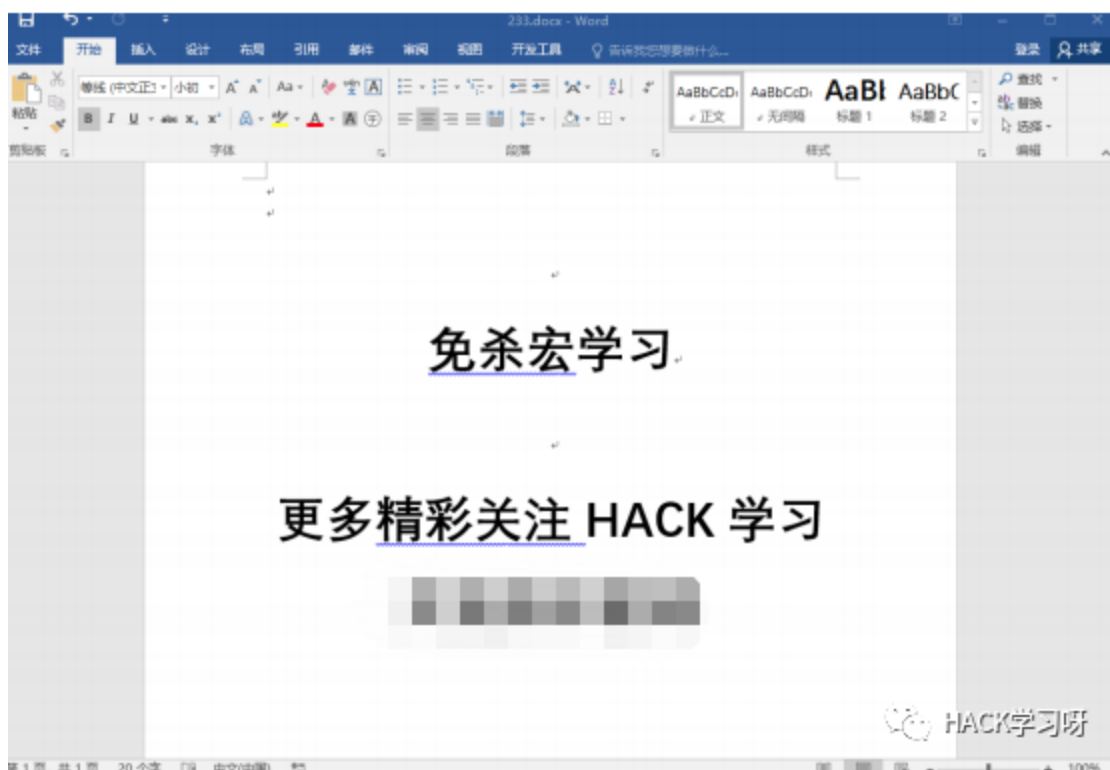
参数说明：-s 参数是通过假的 vba

代码插入到模块中，用以混淆杀毒程序，这里我们需要写一个正常

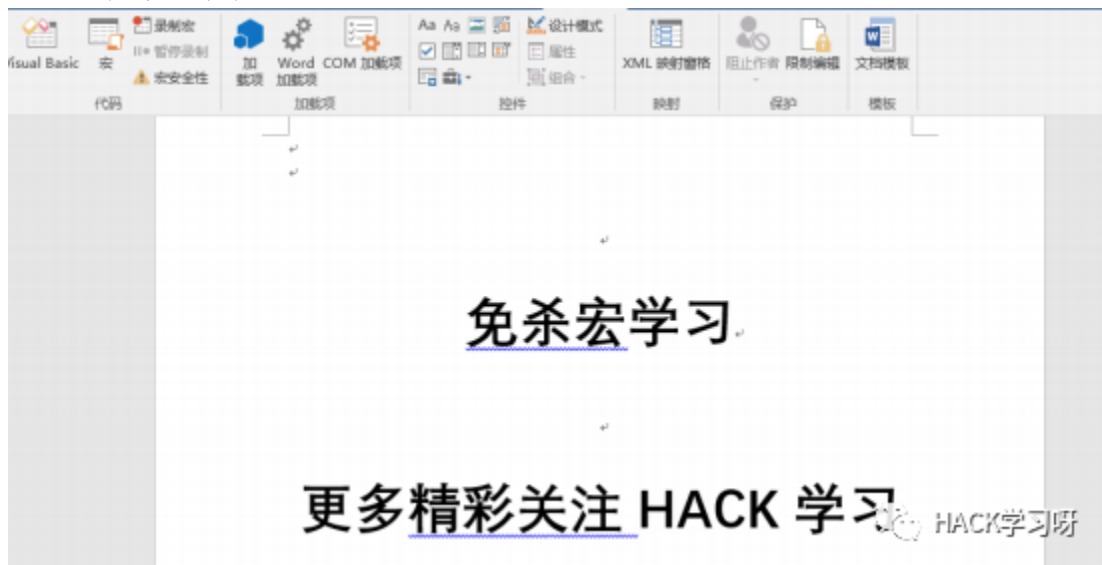
无毒正常的 vba 脚本

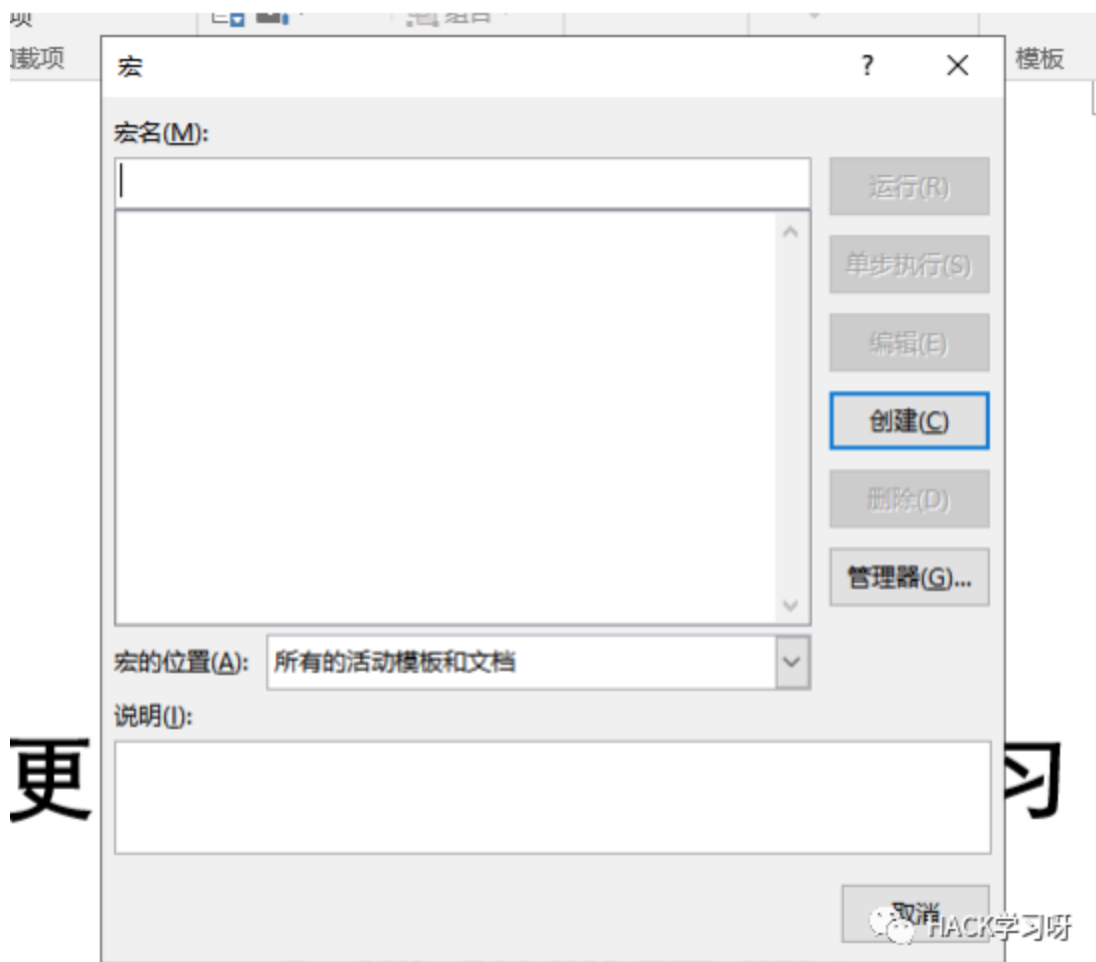
## 免杀测试

新建一个包含宏的 docx 文档

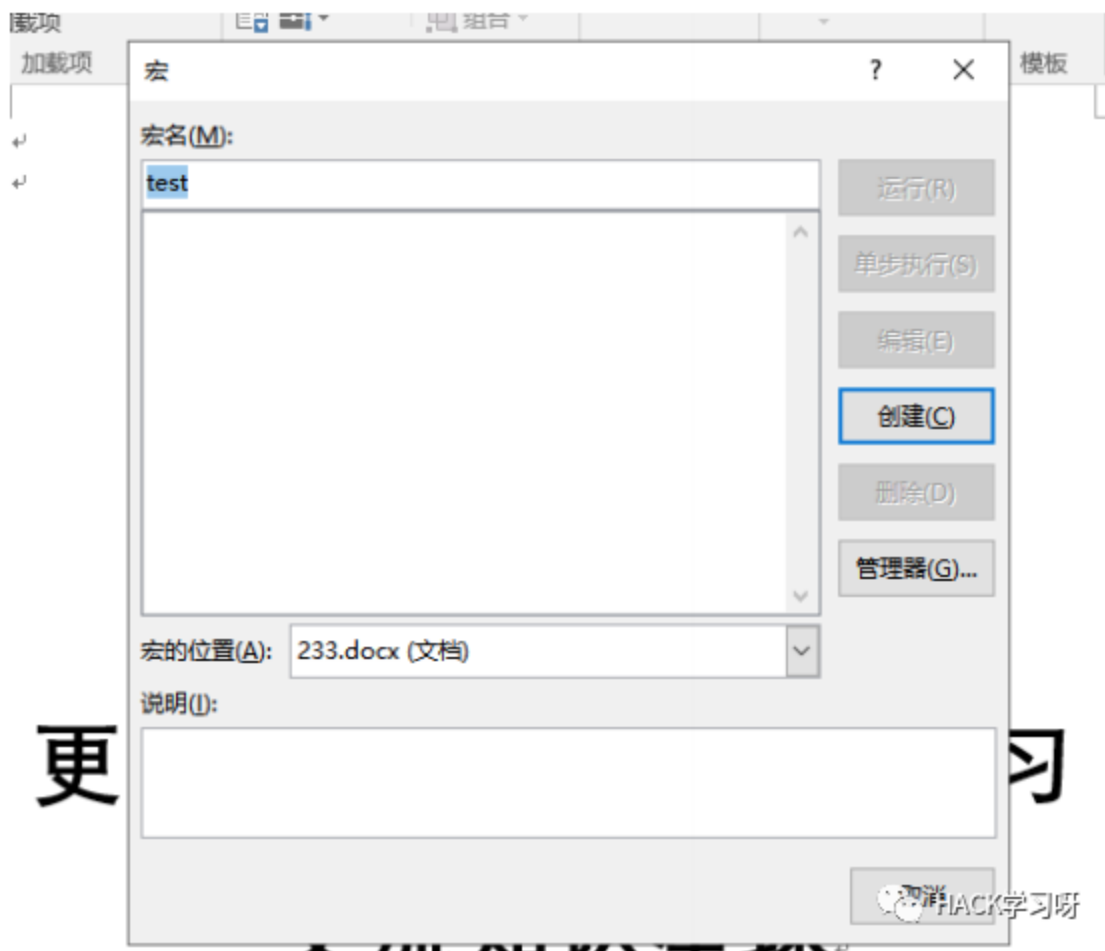


然后点开发工具>>>>点击宏

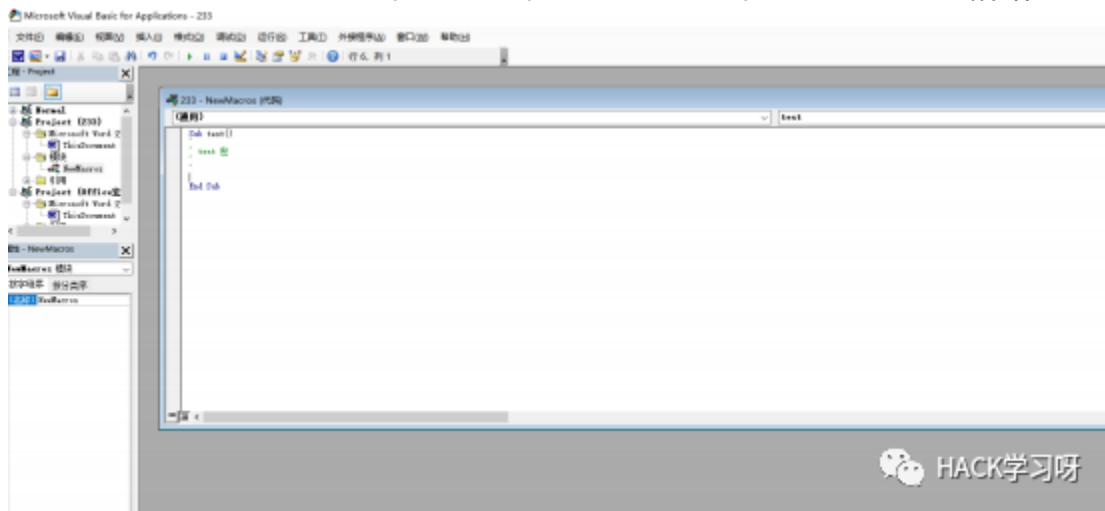




宏的位置选择当前文档，然后点击创建

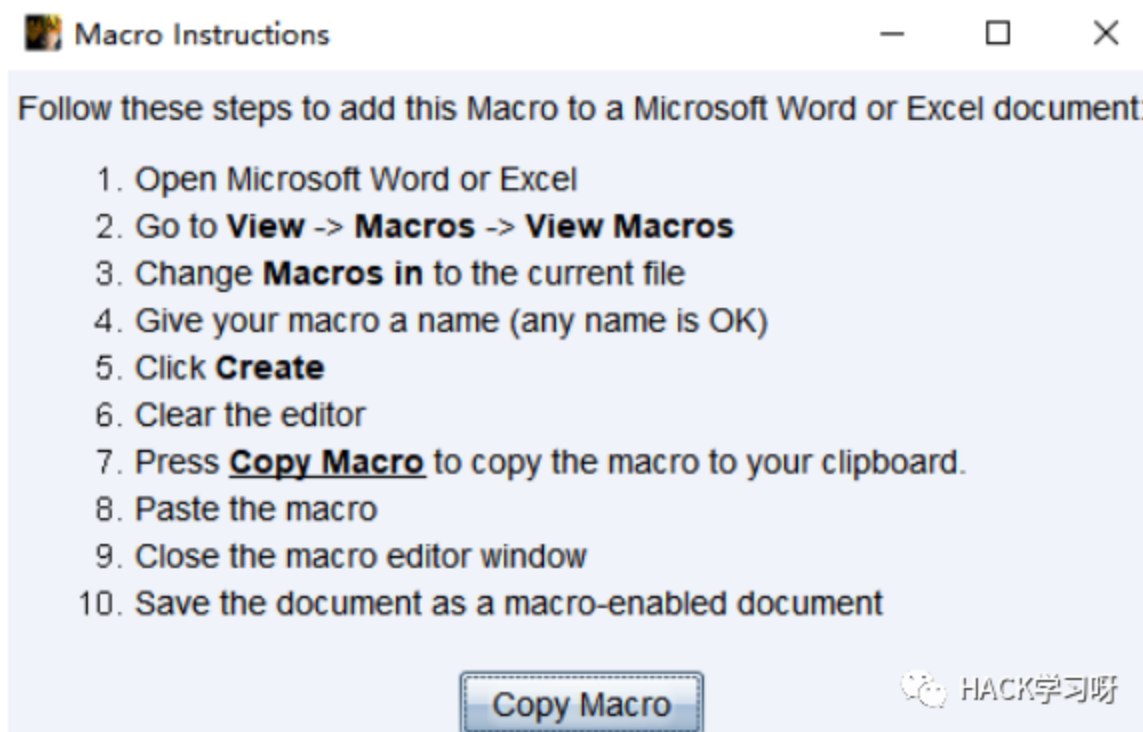
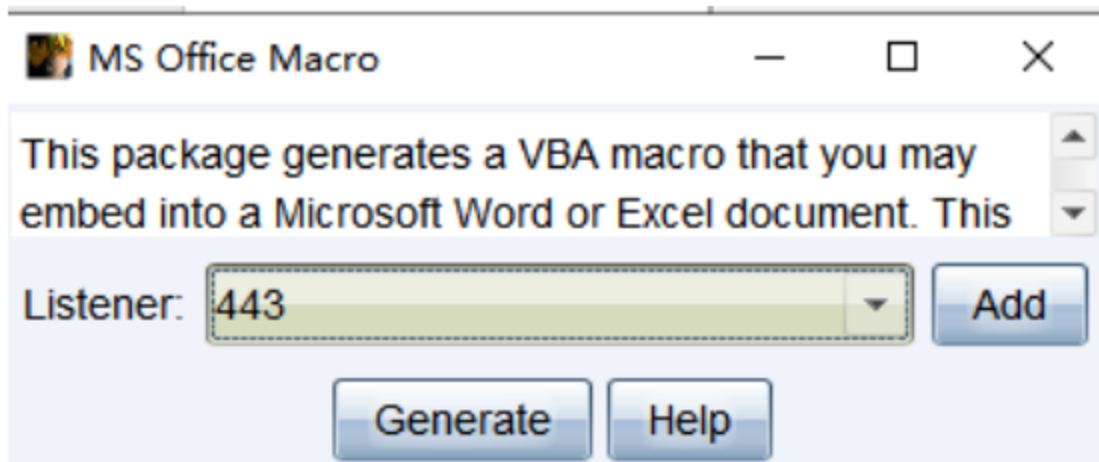
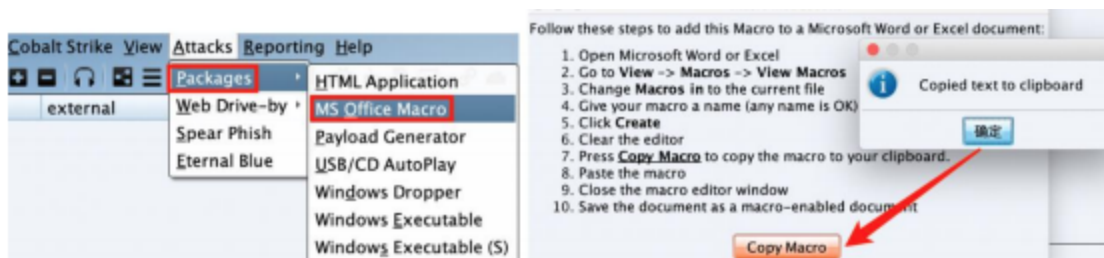


然后再把 CS生成的宏代码复制进去，Ctrl+A 全选，然后 Ctrl+C 粘贴



CS 生成宏代码流程









注意：这里一定要先关闭杀软，不然会保存失败，因为现在还没有做免杀处理

然后文件夹下就有 233.docm 这个文件了 然后再创建一个简单的无毒 vba 脚本

```
Sub Hello()  
  
Dim X  
  
X = MsgBox("Hello VBS")
```

HACK学习呀

保存退出，命名为 2.vba

2.vba	2017/12/2 17:14	VBA 文件	1 KB
233.docm	2017/12/2 17:45	Microsoft Office...	24 KB
233.docx	2017/12/2 17:36	Microsoft Word ...	14 KB
EvilClippy.exe	2017/12/2 17:00	应用程序	56 KB
OpenMcdf.dll	2017/12/2 17:01	应用程序扩展	HACK学习呀

然后按住 shift,点击鼠标右键即可在当前路径下打开 cmd 窗口

```
EvilClippy.exe -s 2.vba 233.docm
```

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\p\宏免杀>EvilClippy.exe -s 2.vba 233.docm
Now stamping VBA code in module: ThisDocument
Now stamping VBA code in module: NewMacros
C:\Users\p\宏免杀>
```

然后就会在当前目录下生成

2.vba	2019/12/12 17:14	VBA 文件	1 KB
233.docm	2019/12/12 17:45	Microsoft Office...	24 KB
233.docx	2019/12/12 17:36	Microsoft Word ...	14 KB
233_EvilClippy.docm	2019/12/12 17:48	Microsoft Office...	18 KB
EvilClippy.exe	2019/12/12 17:00	应用程序	56 KB
OpenMcdf.dll	2019/12/12 17:01	应用程序扩展	HACK学习呀

记得重新命名下，这里我重新命名为帝国时代.docm



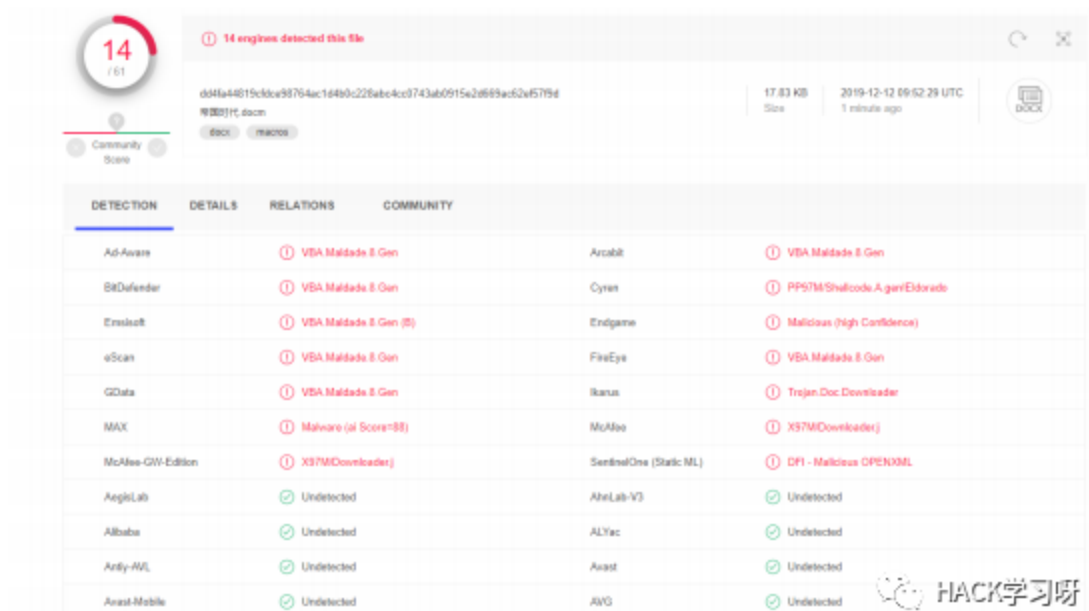
然后咱们去查杀下,火绒查杀



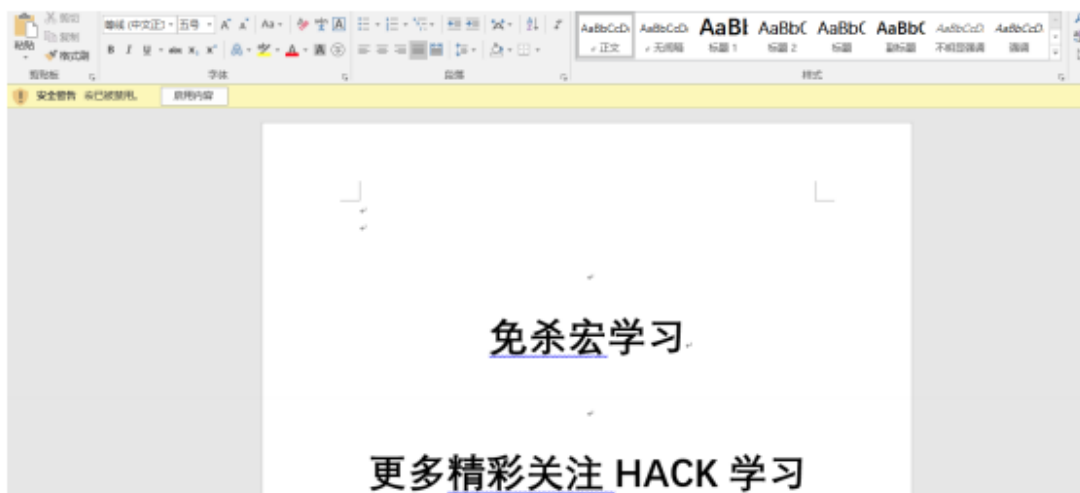
## 360 杀毒



## VirusTotal



效果还不是特别理想，自己可以改下混淆的 vba 脚本，效果会更好  
 包括卡巴斯基以及 windows 自带的杀软均不拦截查杀，效果还很好用  
 试下动态查杀，咱们运行下，火绒和 360 均可以成功上线



点击启用内容，就会上线

成功上线



VirtualAllocEx 指定进程的虚拟空间保留或提交内存区域

WriteProcessMemory 写入某一进程的内存区域

CreateProcess

创建一个新的进程和它的主线程，这个新进程运行指定的可执行文件

其中 Array(-4, -24, -119, 0, 0, 0, 96, -119, -27...就是  
ShellCode，混淆的办法有很多种。

ShellCode 可以自己在 VBA 里解码或者比如每个元素自增  
1，运行的时候-1，达到免

杀 .....



**推荐阅读:**

**office宏**

<https://payloads.online/archivers/2019-05-16/1>

**进击的恶意文档之 VBA 进阶之旅**

<https://forum.90sec.com/t/topic/248>

**7 分钟入门 Excel VBA，从此打开新世界的大门**

<https://www.jianshu.com/p/1a529d5f824a>

**一小时搞定 简单VBA编程 Excel宏编程快速扫盲**

<https://blog.csdn.net/u014339020/article/details/79103059>

**Excel VBA 编程教程**


<https://www.w3cschool.cn/excelvba/>



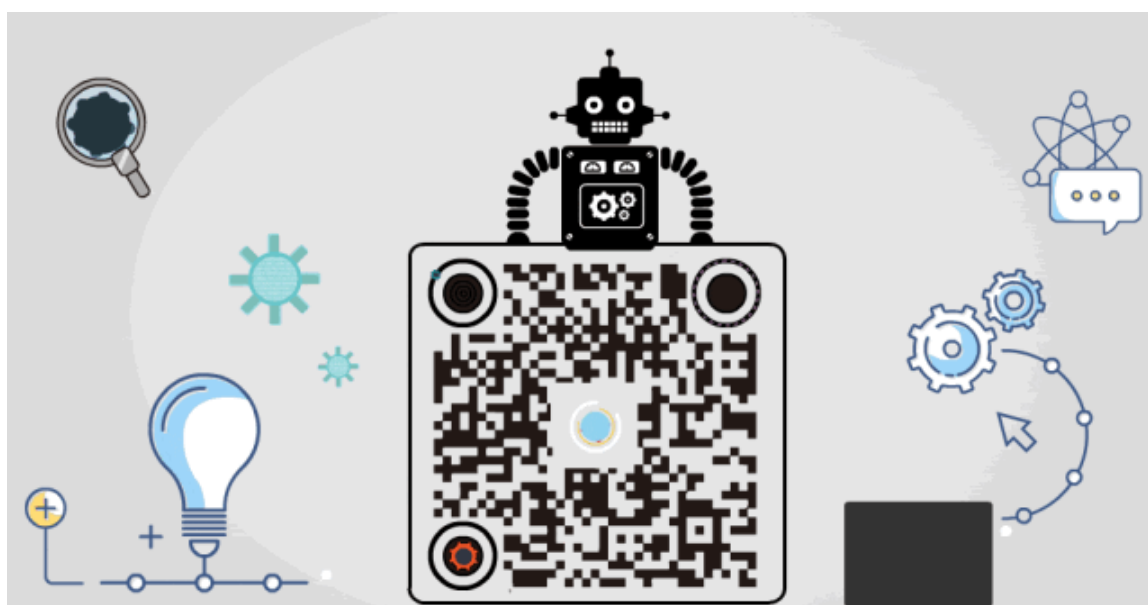
2020年性价比最高安全课程

# 报名线上学习

从零开始学习白帽黑客

 HACK学习呀

点赞，转发，在看



精选留言

---

用户设置不下载评论