**使用远程模板注入DOCX中执行宏命令**

**优势：**

与传统的启用宏文档相比，该方法的好处是显而易见的，首先当已在对目标进行网路钓鱼攻击的时候，你可以直接将docx文件附加到电子邮件或者其他可以诱导用户下载的地方。并且由于此方法的特点，你可以轻松的通过一些网站或者邮箱对于宏扩展文件的安全防护，因为docx文件在正常的情况下是不应该包含有宏文件的。

并且此办法另外的优势是，由于附件本身并不包含恶意代码，所以任何静态的电子邮件扫描程序都不会检测到宏命令，所以被阻止的几率很小。

**主要方法**

本方法需要创建两个不同的文件，第一个是启用宏的模板，即(dotm文件)，他将包含注入的恶意VB宏代码。第二个则是看起来没有任何问题的.docx文件，它的本身并不包含任何的恶意代码，只有指向恶意宏模板的链接。

**工具**

本方法使用的工具问Linux下免费开源的工具Power Shell Empire,此工具的具体使用方法我将会在下面介绍。

**具体过程**

第一步，先介绍下empire的使用，然后再使用它生成我们这次攻击使用的宏代码。Power Shell Empire是一个在域渗透方面十分强大的渗透工具。这里就简单介绍一下它的使用方法。Empire是运行在Linux平台下的，所以这里我们系统使用的是Kali。

1、**安装**

使用命令：git clone <https://github.com/EmpireProject/Empire.git>

下载好之后，我们进入Empire的文件夹进行安装。

命令如下：

cd Empire

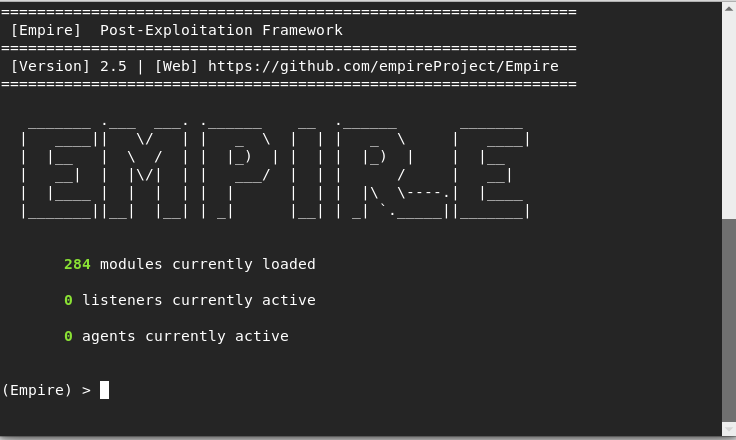
cd Setup

sudo ./install.sh

这里不要忘记给管理员权限，否则后面会安装出错。安装结束后，进入Empire的目录下输入./empire，就能打开Emoire工具。注意如果这里打开出现错误，可能是你本身的python环境配置不完整的原因，建议重新配置python、pip、python3和pip3即可搞定。

**2、设置监听模块**

在打开Empire之后，我们需要新建一个监听，然后再生成需要的木马或者宏，然后在目标主机上运行，我们的监听就会连接上返回的代理。如图：

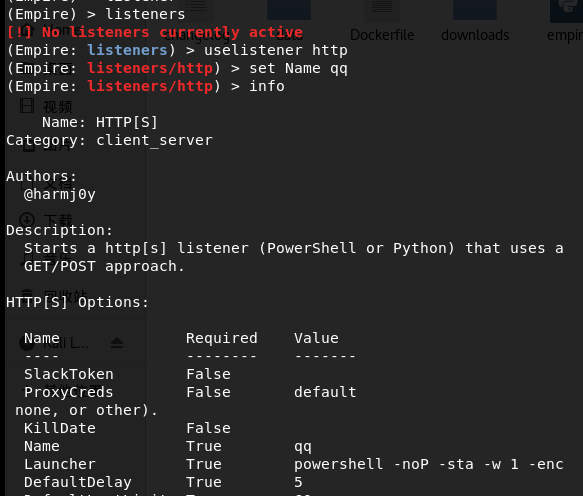


然后我们打开listeners并设置监听模式为http，命令如下:

Listeners

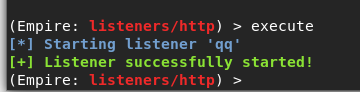
Uselistener http

再设置我们的Name属性，这个Name属性是监听端口的唯一标识，所以必须是独一无二的，在这里我设置为qq，然后使用info命令即可查看端口的相应属性，如图：

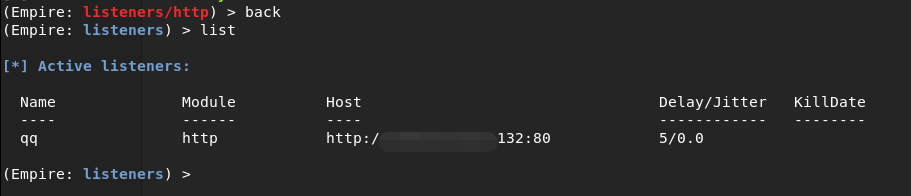


同时也可以使用Host、Post等相关命令来设置监听属性，注意Host里的监听端口必须是独一无二的，当在设置多个监听的时候要注意这一点，否则会出错。

设置完成后我们可以使用execute命令即可开始监听如图：



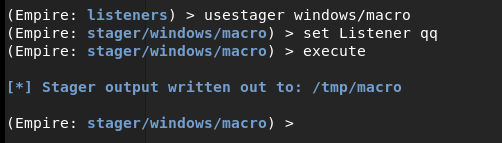
设置完监听端口之后我们可以使用back命令进行返回，在此状态下使用list命令即可查看设置完成的监听，如图：



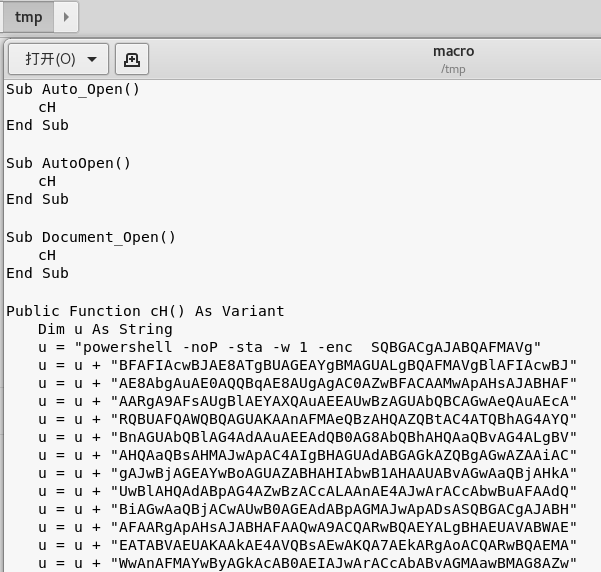
当然，想要删除相关接口只需要执行命令：kill+“监听的名字”即可。

**3、生成宏命令**

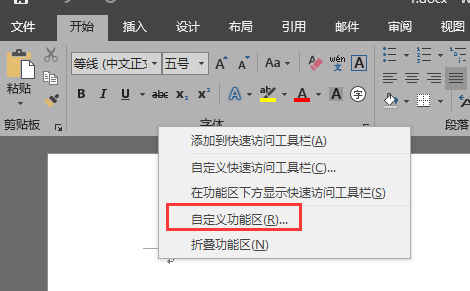
首先，输入命令usestager windows/macro。来设置使用模块为Windows的宏命令类型。此时也可以使用info来查看详细的参数。然后我们设置监听者为qq，命令如下：set Listener qq。最后使用命令：execute即可生成相应代码。如图：



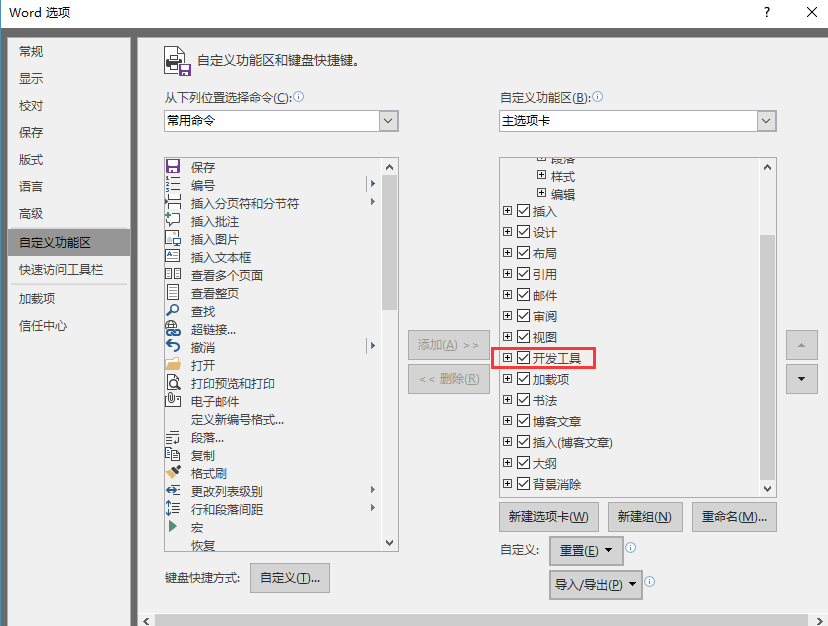
然后在tmp文件夹下即可找到macro文件，打开，里面即时生成的宏代码，如图：



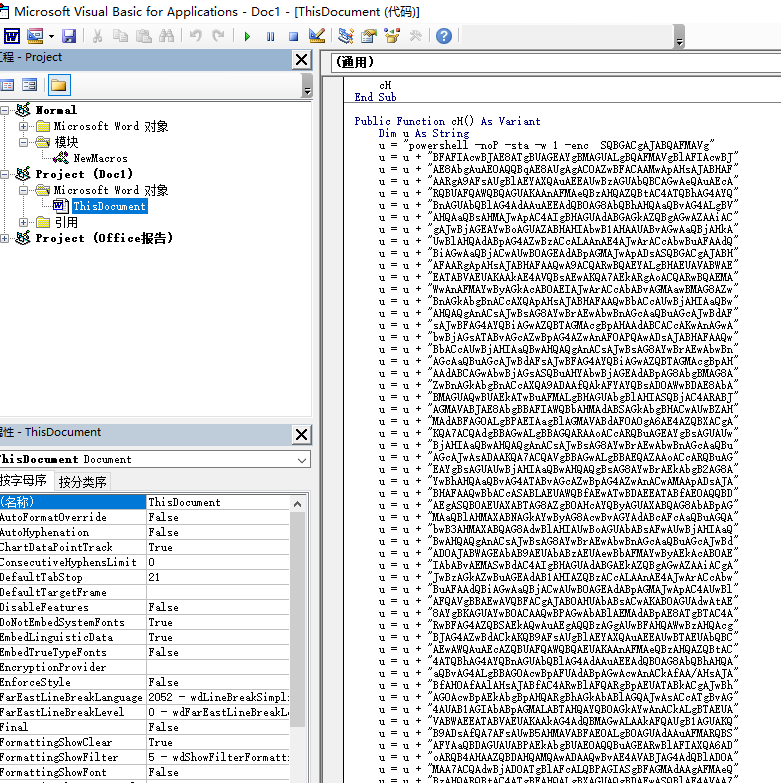
第二步，我们需要新建一个支持宏的Word模板(即.dotm文件)，其中就包含Empire生成的恶意宏文件,我们在word功能区上右键后打开自定义功能区，如图：



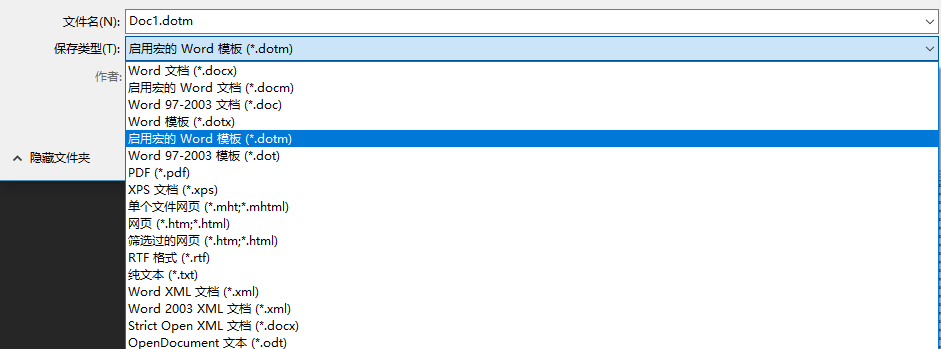
打开后在其中选中开发工具，如图：



这样在功能区中就显示出了开发工具一栏，点击开发工具栏中的Visual Basic编辑器，双击在当前项目下的ThisDocument打开代码窗口，然后我们把刚刚使用Empire生成的宏代码粘贴到里面，如图：

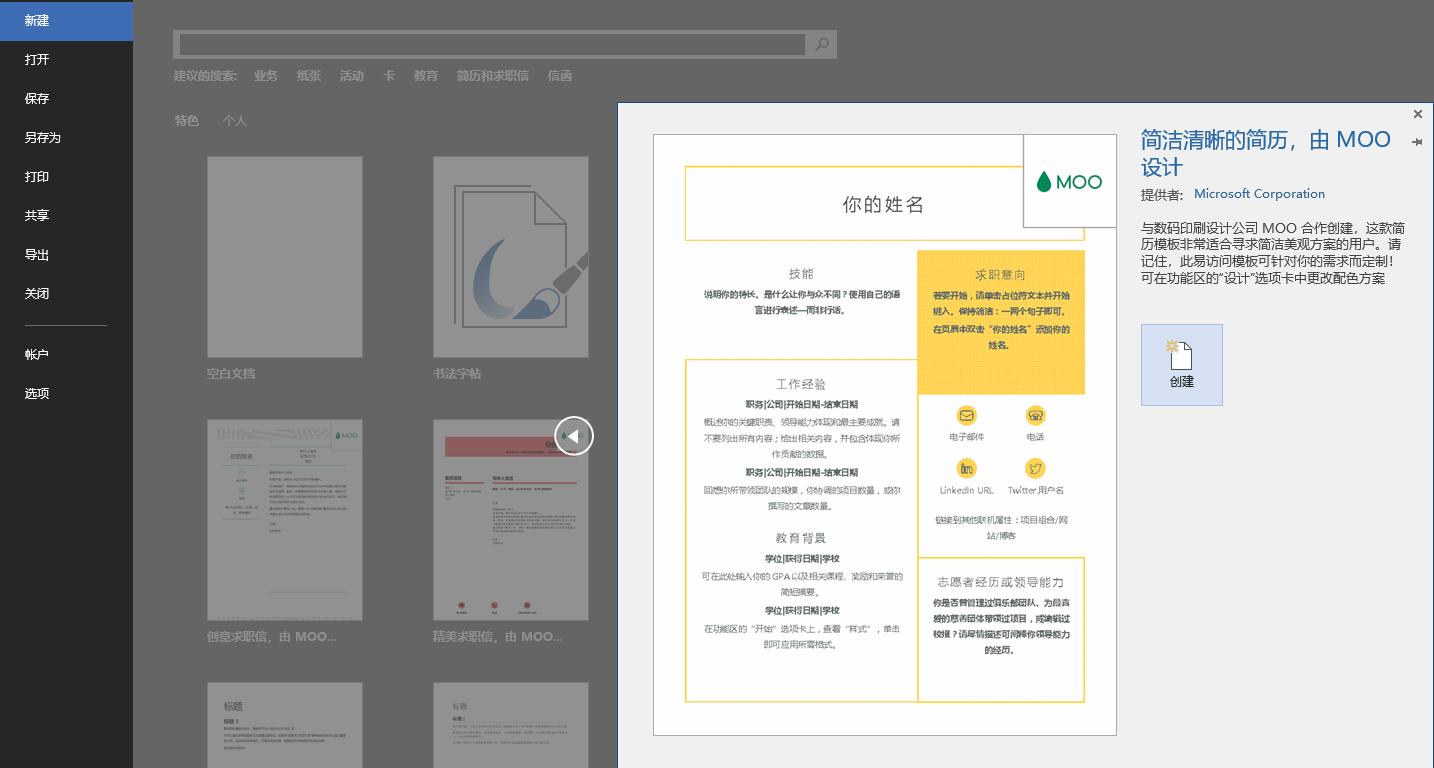


然后注意把其另存为.dotm格式，如图：

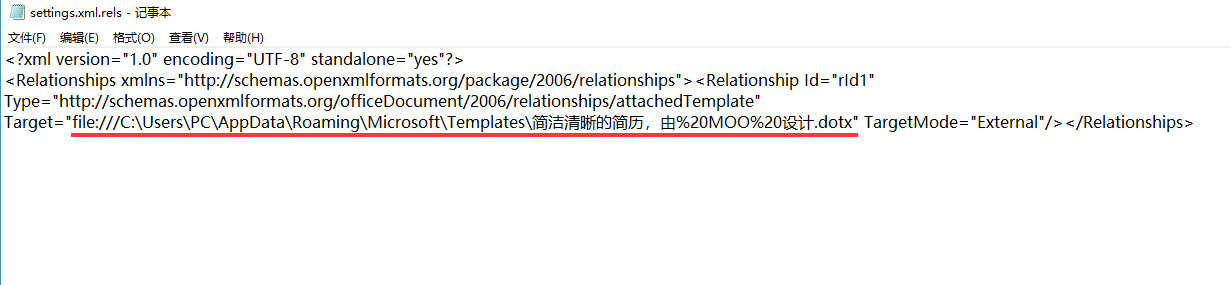


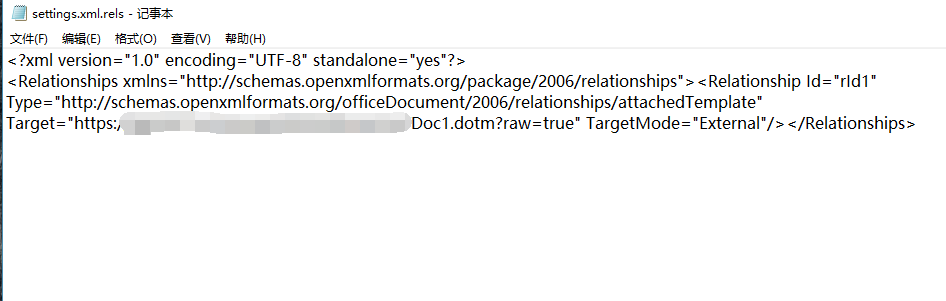
由于该模板在后面使用docx加载的时候会显示出名字，所以建议起名为简历模板、报表设计等名称。到此为止，带有宏命令的模板就完成了，你可以直接打开模板进行实验，运行下宏，看Empire的监听端是否能够捕捉到。

第三步，创建远程模板的加载文档，首先我们需要新建一个.docx文件，并且最好使用word自带的模板，因为这样生成的word会在文件中有一个模板的配置文件，这样我们在后面就可以直接修改模板路径。如图：



然后根据一些需要来改变文档的内容，用其来吸引用户打开即可。然后我们把它保存，我这里保存的名字是“技能”。接着，我们需要修改刚刚保存的文件后缀名为.zip并打开，然后打开“\word\\_rels\settings.xml.rels”文件，如图：

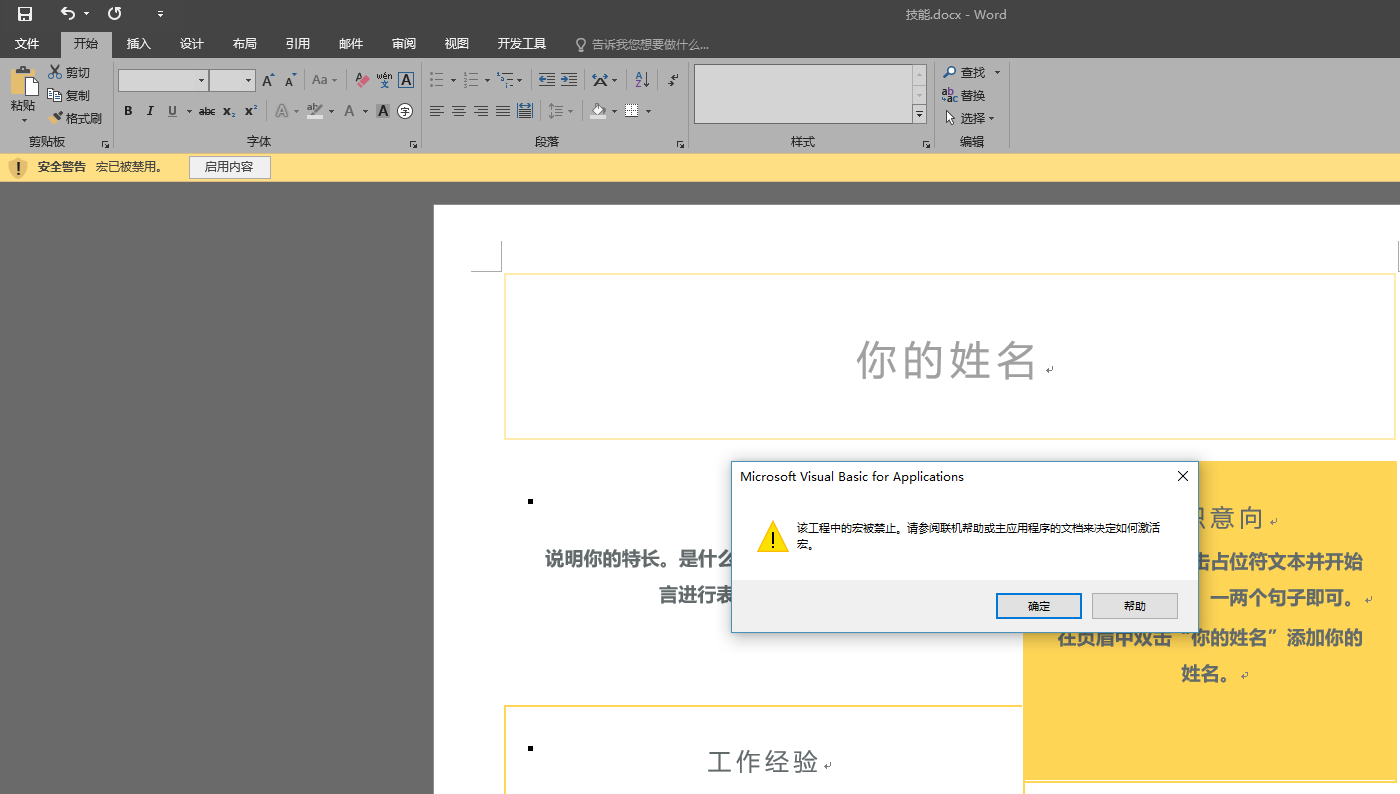
在这里我们可以看见我们word所使用的模板的本地路径，说明在打开word文档时该参数告诉该文件需要加载的模板位置，并且更为重要的是该参数还支持网络地址，这表示如果我能够把该数据改为我的宏模板的网络地址，那么当用户打开我的word时，就会自动在网络上下载我的模板并加载进去。那么我们修改后如图：



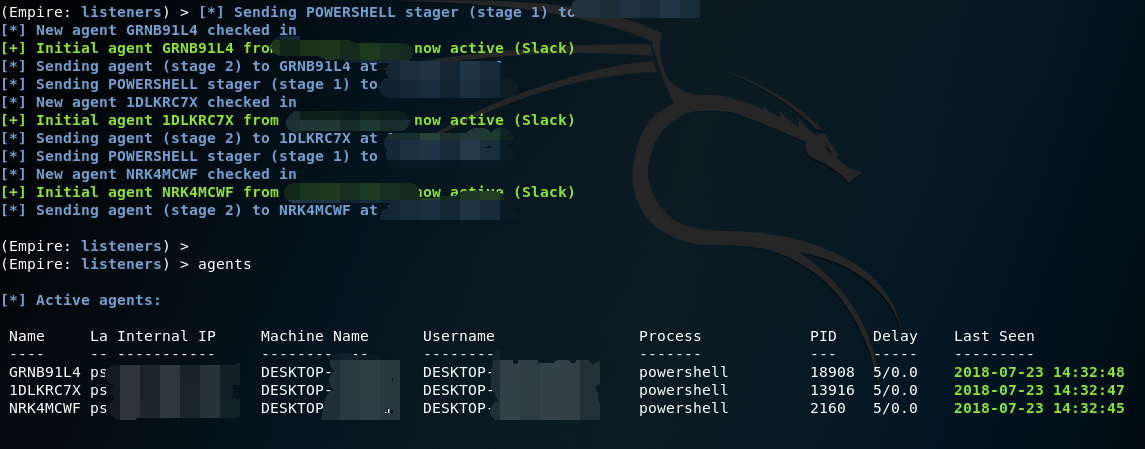
最后再修改后缀名为.docx即可，然后当我们在打开修改后的“技能”文档的时候，如图：



这就表示上传到网络上的带宏命令的.dotm文件被加载到了一个不带任何恶意代码的word之中。打开之后，即可看见Windows会给出警告表示宏已经被禁止运行，如图：



如果通过文档内容的诱骗用户点击允许运行或者用户本身设置为自动运行宏，就会如图：



之后就可以对已经代理的机器进行进一步的操作了。如图：

