赠CD多媒体光盘

赠送作者编写的部分代码和工具

Windows
网络安全技术专家
倾力巨献

张 博 编著

# Windows 黑客技术揭秘与攻防 II

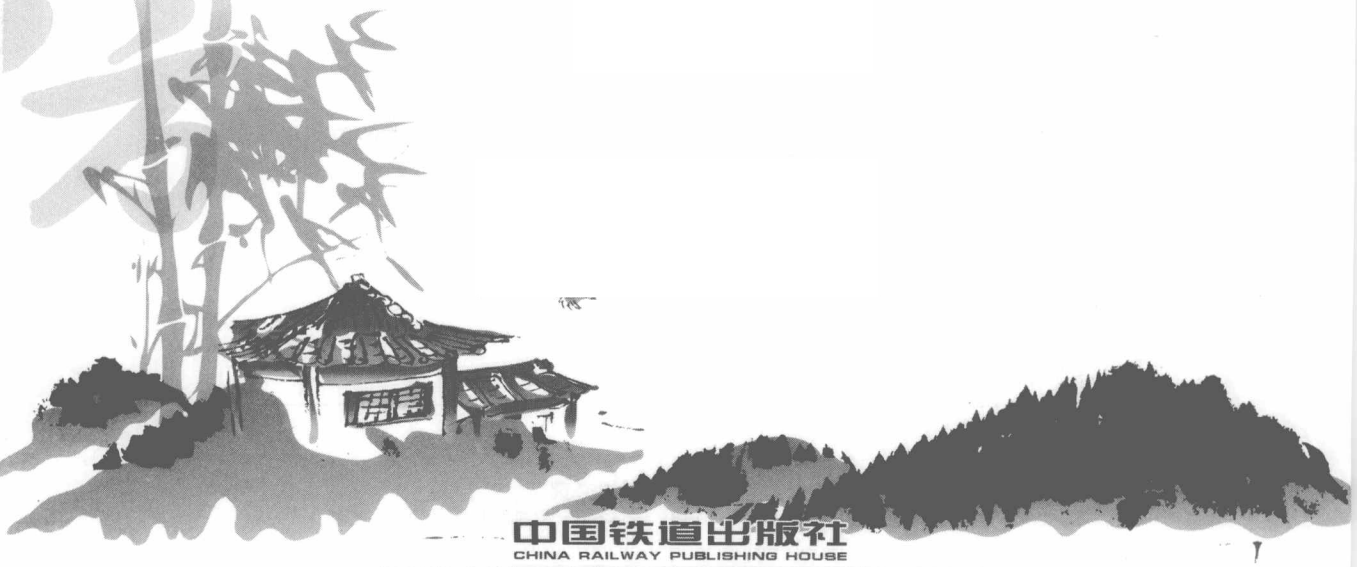
## ——Visual Basic篇

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

张 博 编著

# Windows 黑客技术揭秘与攻防 II

## ——Visual Basic篇



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

## 内 容 简 介

本书由浅入深地讲解黑客攻击和防范的具体方法和技巧，通过具体、形象的案例向读者展示多种攻防方法和攻防工具的使用。本书分为11章，分别介绍VB入门基础、VB基础控件编程、病毒的启动和原理分析、高级控件在黑客编程中的运用、揭秘黑客对系统的操作伎俩与防御、QQ黑客编程、安全工具的编写、反弹木马的实现剖析和防御、“维金/威金”综合蠕虫与木马类病毒的分析与防御、防御软件编写、开发简单的防火墙等内容。

本书力求通过图文并茂的形式和典型常见的案例，引导读者了解并分析黑客攻击技术，从而找到防御手段。

本书适合多个层次的网络编程爱好者阅读，也可以作为网络编程人员和网络管理员的参考书籍，同时还可以作为相关专业师生的用书和参考资料。

**图书在版编目（CIP）数据**

Windows黑客技术揭秘与攻防. 2，Visual Basic篇 /
张博编著. --北京：中国铁道出版社，2010.9
ISBN 978-7-113-11247-9

Ⅰ. ①W… Ⅱ. ①张… Ⅲ. 计算机网络－安全技术
②BASIC语言—程序设计 Ⅳ. ①TP393.08②TP312

中国版本图书馆CIP数据核字（2010）第056892号

书　　名：Windows黑客技术揭秘与攻防Ⅱ——Visual Basic篇
作　　者：张　博　编著

策划编辑：苏　茜
责任编辑：韩中领　　读者热线电话：400-668-0820
特邀编辑：王　惠
封面设计：张　丽　　封面制作：白　雪
责任印制：李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街8号　　邮政编码：100054）
印　　刷：北京鑫正大印刷有限公司
版　　次：2010年9第1版　　2010年9第1次印刷
开　　本：787mm×1092mm　1/16　　印张：22.5　字数：524千
印　　数：3 000册
书　　号：ISBN 978-7-113-11247-9
定　　价：59.00元（附赠光盘）

# 前言

Foreword

本书从实战的角度出发，系统介绍了黑客编程技术。对这些知识的介绍不是要让用户和个别人对他人电脑实施攻击进行破坏和犯罪活动，而是真正学到网络和系统防御方面的相关安全知识，从黑客技术的攻击和防御两个层面的剖析中得到提高，以确保系统和网络的安全。

## 本书的内容安排

本书由浅入深地讲解 VB 黑客编程技术：

- 从 VB 基础控件和函数入手，介绍控件编程和系统的深入控制。
- 对热门的病毒进行解剖性的研究和分析。
- 对大家喜爱的 QQ 工具进行翔实的技术描绘。
- 对网络流行的各种黑客工具的编写进行周详的解析。
- 对网络安全工具进行讲解。
- 编写一个大型黑客软件和防火墙软件。

按照不同的黑客攻防内容，本书共分为 11 章，内容分别如下：

| 章　　节 | 章　节　内　容 |
| --- | --- |
| 第 1 章 VB 入门基础 | 首先介绍了 VB 的前世今生，同时对 VB 编译器进行了详细的讲解，另外还对编译器的改造做了不少的介绍，最后还提供了一些非常不错的 VB 编程站点，读者可以从这些站点中汲取更多知识养分 |
| 第 2 章 VB 基础控件编程 | 在 VB 编程中提供了很多控件，使用控件编程不仅可以让编程更加简单，而且可以提高编程效率，本章介绍了控件的基础内容 |
| 第 3 章 病毒的启动和原理分析 | “久在江湖漂，哪有不挨刀”，自从主机插上网线的那一刹那，用户就一直被木马病毒困扰着，本章就从病毒着手来介绍它们是如何在系统中作怪的 |
| 第 4 章 黑客编程中的高级控件应用原理分析 | 前面介绍基本控件的编程，本章将分析高级控件的使用和其在黑客编程方面的应用 |
| 第 5 章 黑客对系统的操作原理分析与防御 | 前面的章节介绍了很多基本的黑客编程知识，本章将通过使用更加丰富的函数来实现对系统更加深入的控制 |
| 第 6 章 QQ 黑客编程原理分析 | 本章从 QQ 着手，分析一系列与 QQ 相关的工具的编写 |

续表

| 章　　节 | 章　节　内　容 |
| --- | --- |
| 第 7 章　安全类工具的编写 | 在前面的章节中介绍了黑客工具的编写，本书的精神是实现黑客攻击与防御的统一，所以本章通过所掌握的病毒原理来重点学习防御病毒的相关知识 |
| 第 8 章　反弹木马的剖析和防御 | 网络上的木马日益增多，如果对其没有足够的了解，又如何实现对它们的控制和防御呢？本章逐一分析木马的方方面面，包括启动方式、传播方式、连接类型、功能模块等，并对其提出防御 |
| 第 9 章　“维金/威金”综合蠕虫与木马类病毒的分析与防御 | 对于大名鼎鼎的“维金/威金”病毒，大家应该有所耳闻，那么它们是如何作用于计算机的，是如何实现如此强大的生命力的，本章将揭开它们的神秘面纱 |
| 第 10 章　防御软件编写 | 如今的网络上，木马横行，它们如何诞生，又如何肆意传播滋生，如何在计算机中安营扎寨，本章将从编程的角度逐一分析，并编写对其进行防御的软件 |
| 第 11 章　开发简单的防火墙 | 在前面的章节中介绍了木马软件的编写技巧，这里介绍一种有效的防御方法——防火墙。有了防火墙，才能够给木马加上一堵无形的过滤网，从而保证自己计算机的安全 |

## 本书适合读者

本书适合熟悉 Windows 操作系统的计算机安全从业人员、网络管理员、刚刚学会 VB 语言并亲自编写过一些小型程序的读者和网络编程爱好者。同时，本书也可以作为各大院校相关专业的师生用书和参考资料。

## 本书作者

本书由张博编著，作者抱着对读者极其尊重的心情写完此书，在写作的过程中紧紧围绕着本书的主旨思想，力求精益求精，但是由于互联网各项技术的飞速发展，尤其是网络编程类技术日新月异，任何一本书都很难保证所述的内容和实际应用中的操作完全一致，加之作者水平有限，书中难免会有疏漏之处，望广大的读者多提宝贵意见。

## 本书声明

本书中的代码仅供编程学习和测试之用，切勿将其用于非法目的。请注意，编程是一种乐趣，但把编程用于破坏则是违法行为！

编　者

2010 年 4 月

# 目录

Contents

# 第 1 章　VB 入门基础

VB（如果没有特别声明，VB 为 Visual Basic）一直都是微软公司的拳头产品，经过多年的发展，已经拥有了广泛的使用者，并且，目前在网络上有大量的 VB 交流网站和论坛，这些都对学习 VB 有了莫大的帮助。

本章首先介绍 VB 的来龙去脉，然后对 VB 语法和编译器做简单的介绍，让读者朋友能够快速地了解 VB。

## 1.1　VB 的前世今生

很多黑客工具都是使用 VB 编写的，比如著名的 Web 漏洞扫描工具网站猎手就是使用 VB 6.0 进行开发的，如图 1-1 所示。

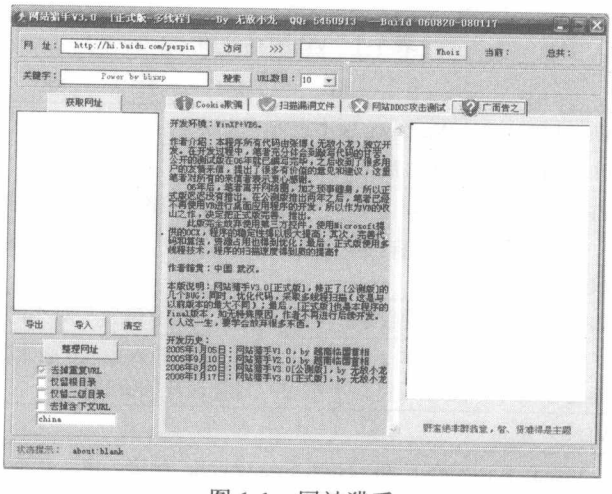



图 1-1　网站猎手

VB 也被用于开发一些网络工具，比如可以开发基于 TCP/IP 协议的远程控制程序等。

### 1. Windows 对于不同对象提供的支持

Microsoft Windows 为程序员和最终用户提供了一个共同的人机界面。

- 对于用户，Windows 提供了一个图形鼠标的操作环境，该环境对所有的应用程序都相同。
- 对于程序员，Windows 提供了一组预定义工具——称之为 Microsoft Windows 的软件开发工具箱（SDK），该工具能使程序员建立一个与 Windows 界面相同的应用程序，而且程序员不必关心最终用户的硬件配置情况。

在 Windows 提供的开发环境中，对程序员而言，唯一的困难是，Microsoft SDK 提供了 600 多个函数和与其一致的事件驱动（event-driven）编程技术。两种新方法的交叉使众多的

程序员重新陷入困境，程序员不仅要掌握程序驱动编程技术和 600 多个函数的功能，而且还要使用 C 语言描述这些问题。

因此一般情况下，程序员首先要掌握 C 程序设计技术，然后再开始学习 SDK。在这样的条件下，就要求在 Microsoft 多任务环境下存在一种操作方便、使用简单的新工具，Visual Basic 由此诞生。

### 2. Visual Basic 含义

英文 Visual 的意思是“视觉的”，“可视的 Basic”这个名称可能有些抽象，但实际上它却是最直观的编程方法，只要看到 VB 的界面就会明白为什么称其为“可视的”，实际上用户无须编程，就可以完成许多步骤。

在 VB 中引入了控件的概念，在 Windows 中控件无处不在，各种各样的按钮、文本框等，都是控件，VB 把这些控件模式化，并且每个控件都有若干属性用来控制控件的外观和工作方法。这样用户就可以像在画板上一样，随意单击几下鼠标，来完成一个按钮的制作，这在以前的编程语言下是要经过相当复杂的工作的。

### 3. Visual Basic 历史

VB 1.0 于 1991 年发布，最初的设计是由阿兰·库珀 （Alan Cooper）完成的。表 1-1 给出了 VB 各个版本的介绍和推出时间。

表 1-1 VB 版本介绍

| 版本时间 | 版　本　介　绍 |
| --- | --- |
| 1991 年 4 月 | Visual Basic 1.0 Windows 版本发布 |
| 1992 年 9 月 | Visual Basic 1.0 DOS 版本发布 |
| 1992 年 11 月 | VB 2.0 发布。它相对于上一个版本的界面和速度都有所改善 |
| 1993 年夏天 | VB 3.0 发布，分为标准版和专业版。其中包含一个数据引擎，可以直接读取 Access 数据库 |
| 1995 年 8 月 | VB 4.0 发布了 32 位版本和 16 位版本，其中包含了对类的支持 |
| 1997 年 2 月 | VB 5.0 发布。程序员可以用 32 位的版本导入由 4.0 版本创建的 16 位程序，并且能进行编译。同时还包含了对用户自建控件的支持 |
| 1998 年夏天 | VB 6.0 发布 |
| 2001 年 | Visual Basic.NET 和 .NET Framework 发布。由于该版本使用了新的核心和特性，所以很多 VB 程序员都要改写程序 |
| 2003 年 | Visual Basic.NET 2003 和.NET Framework 1.1 发布 |
| 2004 年 | 微软开发了 Visual Studio .NET 2005 的测试版本（代号 Whidbey），包含了.NET Framework 2.0 的测试版本 |
| 2005 年 | 微软宣布不会再对非.NET 版本的 VB 进行支持。VB 社群立即做出反应，表示关注这个消息，一些老用户还递交了希望微软能够继续对 VB 进行技术支持的请愿书。微软目前还不愿意改变其决定。Visual Studio.NET 2005 在 2005 年 11 月 7 日发布 |
| 2008 年 | 微软又推出了新的、更加强大的 VB 2008，可以非常容易地实现很多底层操作 |

上面介绍了 VB 的相关历史，读者朋友可以访问微软的官方网站——http://www.microsoft.com/en/us/default.aspx 去了解 VB 的更多知识。

## 1.2　VB 编译器的安装和介绍

本节着重介绍 VB 编译器的安装方法和 VB 编译器界面的各个组成部分，这样才能让编译器更加容易使用。同时，对 VB 编译器的熟悉程度会直接影响编程人员的编程技能。

### 1.2.1　编译器的安装

VB 是一款神奇的编程环境和语言，使用它能编写出几乎所有的 Windows 应用程序，不管是业余人员还是专业人员，几乎都可以使用 VB 编写出自己需要的软件。

首先介绍如何安装 VB。把 VB 的安装光盘放入光驱中，等待一段时间后，弹出安装向导对话框，在弹出的对话框中单击“下一步”按钮即可，如图 1-2 所示。

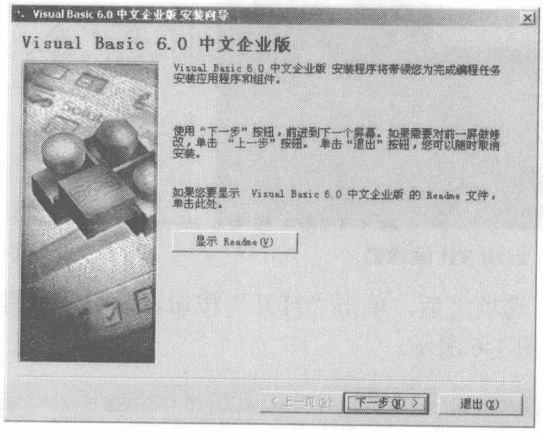



图 1-2　启动安装向导

这里需要注意的是，不要选中中间步骤的“服务器应用程序”单选按钮。如果没有出现安装问题，很快就能进入一个底色为墨绿色的安装界面，此时单击“继续”按钮即可，如图 1-3 所示。

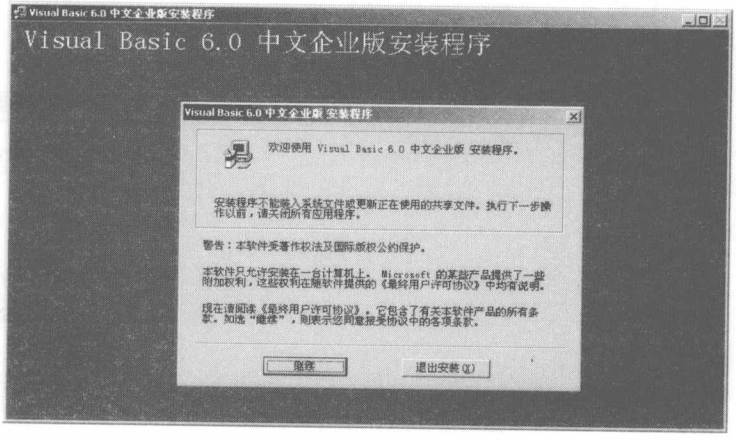



图 1-3　安装 VB 编译器

最后，一路单击“下一步”按钮即可顺利完成安装。

## 1.2.2 编译器界面介绍

安装完毕后，就可以从“开始”|“程序”子菜单中找到 VB 的启动命令，单击“Microsoft Visual Basic 6.0 中文版”命令即可启动 VB，如图 1-4 所示。

现在，在 VB 编译器中，单击“文件”|“新建工程”命令，此时会弹出一个“新建工程”对话框，选择“标准 EXE”选项即可，如图 1-5 所示。

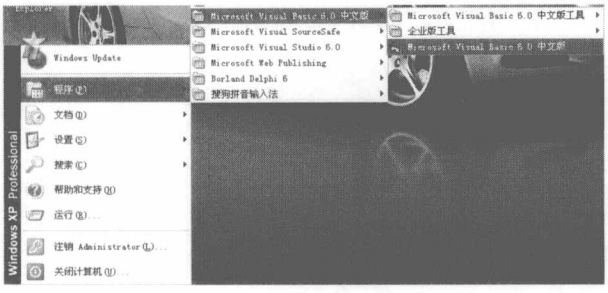



图 1-4 启动 VB 编译器

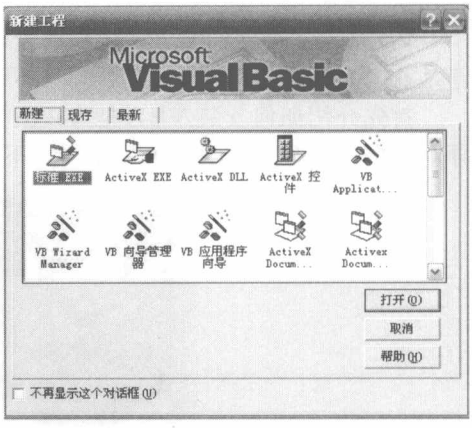



图 1-5 新建“标准 EXE”项目

选中“标准 EXE”选项之后，单击“打开”按钮，此时就会将编译器中支持的全部组件和界面显示出来，如图 1-6 所示。

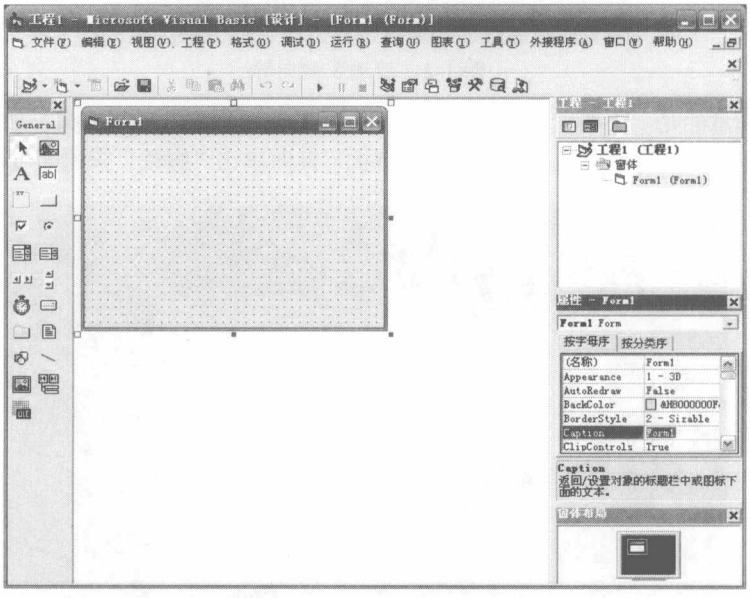



图 1-6 VB 编译器界面

下面为大家逐一介绍 VB 编译器的各个组成部分，界面顶部包括标题栏、菜单栏和工具栏，因为比较简单，这里不再赘述。

其次介绍右上方的工程视图，如图 1-7 所示，这里会显示 VB 工程使用了什么模块，默认只有一个窗体模块。同时，在工程视图上右击，在弹出的快捷菜单中可以选择新建一个标准模块或者一个类模块，这些模块的主要作用就是封装一些重复性的代码，大家在编程深入以后会接触到这些概念。

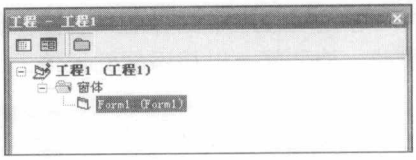



图 1-7　工程视图

工程视图下面是非常重要的属性窗口，在这里可以设置 VB 窗口的属性和 VB 控件的各个属性，通过这些属性的设置，可以让 VB 的控件符合用户的编程要求。

比如，可以修改窗口的 Caption 属性为“演示程序”，如图 1-8 所示，那么程序窗口的标题栏就变成了“演示程序”，如图 1-9 所示。

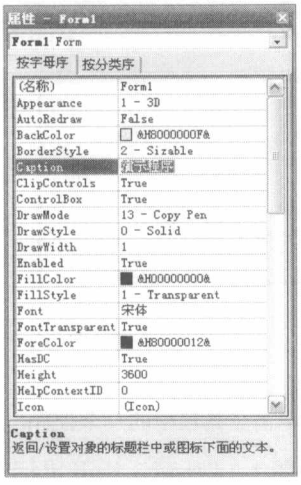



图 1-8　修改 Caption 属性

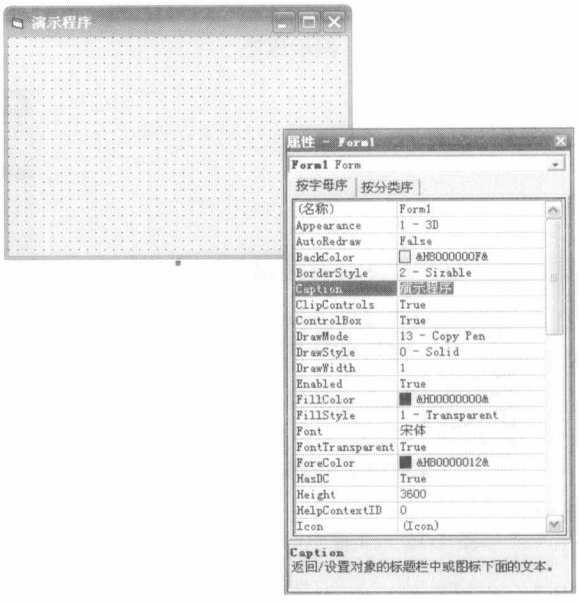



图 1-9　修改 Caption 属性后的效果

此时，可以看到在 VB 编译器的设计过程中，程序的标题栏已经变成了“演示程序”，那么，如何得到程序运行之后的效果呢？可以按【F5】键，此时，程序就会被执行，运行效果如图 1-10 所示。

属性窗口下面是“窗体布局”窗口，在这里可以设置 VB 程序启动时的位置，后面的浅蓝色背景是一个虚拟的计算机显示器界面，前面的 Form1 窗口就是用户的 VB 程序，可以拖动这个 Form1 窗口到虚拟的显示器界面的任意位置，这样 VB 程序启动时的位置就会相同，如图 1-11 所示。

同时，用户可以在这个 Form1 上右击，在弹出的快捷菜单中选择“屏幕中心”命令，这样就可以去掉手工调整位置的烦琐操作，经过这样的设置，程序在启动之后就会显示在屏幕的正中央，如图 1-12 所示。

最后就是画界面，工具箱中有一组控件，这些控件就是编写程序的基石。控件就是控制元件，用户可以通过控件来反馈值、信息或者控制当前程序运行状态及触发事件。如果不知道工具箱在哪里，可以看到 VB 编译器的最左侧一栏即是，如图 1-13 所示。