用VB实现“ 木马 ”式隐形运行程序 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/138/2021_2022__E7_94_A8VB_E5_AE_9E_E7_8E_c97_138195.htm 在一些系统，为了特定目的，经常要求程序隐藏起来运行，例如DCS（集散控制系统）中的后台监控系统、木马控制程序、源码防拷贝等，以减少被发现、截杀和反汇编的风险。这种功能模块要求程序在运行期间不仅不会在桌面出现，也不允许被操作者从任务管理器列表中发现。 程序隐形的原理 对于一个隐形程序而言，最基本的要求是： 1. 不在桌面出现界面； 2. 不在任务栏出现图标； 3. 程序名从任务管理器名单中消失。 对于上述第一点，可以将Form的Visible属性设为False。 要将图标从任务栏中屏蔽掉，可以把Form的ShowInTaskBar改为False。 在Windows环境下，可以调用WIN API函数中的RegisterviceProcess来实现第三个要求。 上述功能，不论用VC、Delphi、VB，还是PB等任何一种高级编程语言都是比较容易实现的。 隐形功能多用于木马程序，但木马程序在许多国家和地区是不合法的，为便于理解，本文用VB结合一个程序防拷贝的实例来讲解。通过获取软件安装路径所在磁盘序列号(磁盘ID)，用做对合法用户的判断。以下程序的目的是用于讲解隐形程序的编制和应用，对程序防拷贝内容作了一定程度的简化。 程序隐形的示例 程序的具体编制操作如下： 1. 在VB6.0编程环境中，新建一个工程Project1。 2. 在Project1中添加模块Modulel，在工程属性中将工程名称改为HiddenMen，应用程序标题也改为HiddenMen（以下程序都经过实际运行测试，可以原样复制使用）。 在模块Module1中加入如下声明： Public Declare

Function GetCurrentProcessId Lib“ kernel32 ”() As Long 获得当前进程ID函数的声明 Public Declare Function RegisterServiceProcess Lib“ kernel32 ”(ByVal ProcessId As Long, ByVal ServiceFlags As Long) As Long 在系统中注册当前进程ID函数的声明 3. 在Project1中新建一个窗体Form1，设置Form1的属性： form1.Visible=False form1.ShowInTaskBar=False 在代码窗口添加如下代码： Private Declare Function GetDriveType Lib“ kernel32 ”Alias“ GetDriveTypeA ”(ByVal nDrive As String) As Long 获得当前驱动器类型函数的声明 Private Declare Function GetVolumeInformation Lib“ kernel32 ”Alias“ GetVolumeInformationA ”(ByVal lpRootPathName As String, ByVal lpVolumeNameBuffer As String, ByVal nVolumeNameSize As Long, lpVolumeSerialNumber As Long, lpMaximumComponentLength As Long, lpFileSystemFlags As Long, ByVal lpFileSystemNameBuffer As String, ByVal nFileSystemNameSize As Long) As Long 获得当前驱动器信息函数的声明 Private Sub Form_Load() Dim drive_no As Long, drive_flag As Long Dim drive_chr As String, drive_disk As String Dim serial_no As Long, kkk As Long Dim stemp3 As String, dflag As Boolean Dim strlabel As String, strtype As String，strc As Long