基于VB6.0的局域网病毒预警软件的设计及实现

周利荣
（浙江工业大学 浙西分校图书馆，浙 江 衢 州 324000）

摘 要：利用VB语言设计的病毒预警软件，对局域网所有计算机内存进程进行监视,发现病毒进程并及时发出预警。

关键词：VB 6.0；局域网；病毒；预警
中图分类号:TP3111.1 **文献标识码**：B

Design and realization of virus forewarning software in lan base on VB 6.0

ZHOU Li Rong
(Zhejiang University of Technology, West Branch Library, Quzhou 324000, China)

Abstract: The paper introduces how to use VB language to design and realize monitoring of all lan computers. If program discovers virus ,then sends out forewarning in time.

Key words: VB 6.0; LAN; virus; forewanring

任何病毒和木马存在于系统中,都无法彻底与进程脱离关系,即使采用了隐藏技术,也还是能够从进程中找到蛛丝马迹。因此,查看系统中活动的进程成为检测病毒木马最直接的方法。但是系统中同时运行的进程很多,哪些是正常的进程、哪些是病毒的进程，这需要用户详细了解并识记进程的名称、出版公司、路径、大小等内容,即使对计算机专业人员这也不是简单的事情。为此,可用ACCESS建立数据库,将正常进程、新进程和病毒进程分别存放于数据库不同的表中,用VB编写类似WINDOWS任务管理的进程监视器,每隔一定时间自动扫描内存进程,并将内存进程分别与数据库中的病毒进程表逐一比较,若是病毒进程提示发现病毒,再将内存进程分别与数据库中的正常进程表逐一比较,若是新进程则加入新进程表中。

1 软件功能

本文中所设计的预警软件有如下功能：

(1)预警功能。进程监视器定时将内存进程与数据库中的病毒进程和正常进程逐一比较,若名称、出版公司、路径、大小等内容与病毒进程相同则提示发现病毒,若与正常进程表中的进程都不相同,则是新进程,加入新进程表中；

(2)下载功能。首先将局域网中的每台计算机安装ftp服务并将该软件的预警模块及进程数据库文件安装在ftp服务所指向的目录中。局域网中的每台计算机都运行预警模块,随着内存中进程的变化,数据库中新进程表是不断变化的,因此软件必须有下载局域网中的每台计算机进程数据库文件的功能,以供管理员分析处理；

(3)进程处理功能。程序能将每一个数据库的新进程表中的进程信息显示在窗口文本框中,管理员根据显示的信息判断是病毒进程还是正常进程,程序根据管理员判断将进程加入相应的表中,这要求管理员有相关的进程方面的知识；

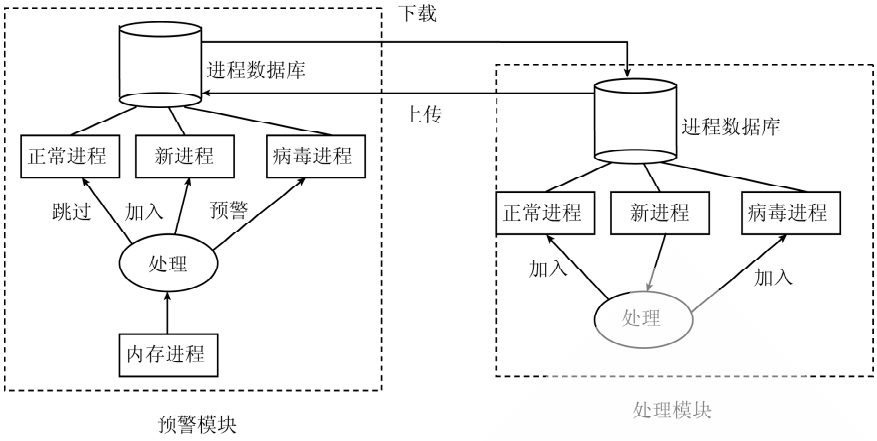

图 1 软件系统功能设计

(4)上传功能。对于已处理的数据库文件，软件应将其传回至相应的计算机 ftp 服务所指向的目录中。

各模块的功能设计及相互关系如图 1 所示。

2 软件设计

2.1 数据库设计

(1)进程数据库中包含 3 个表:正常进程表、病毒进程表、新进程表。3 个表的表结构是相同的，如表 1 所示。

表1 正常进程表、病毒进程表、新进程表结构

字段名	数据类型	字段大小
进程名	文本	50
出版公司	文本	100
版本号	文本	100
创建日期时间	文本	50
大小	文本	50
加入日期时间	文本	50
进程说明	备注	

(2)局域网 ftp 服务数据库包含 1 个表,提供上传及下载时所需的 IP 地址、用户名、密码信息,其表结构如表 2 所示。

表2 ftp服务表结构

字段名	数据类型	字段大小/bit
IP地址	文本	15
用户名	文本	10
密码	文本	10

2.2 预警模块设计

进程监视器定时检测内存中的进程,将其添加到 listview1 中,并与数据库中的进程作比较。若是正常进程则跳过,若是病毒进程提示发现病毒,若既不是正常进程也不是病毒进程,则加入新进程表。进程数据库文件名的基本名为 IP 地址，使用 Winsock1.LocalIP 获取计算机的 IP 地址。由于使用 ACCESS 2003 数据库,扩展名为.mdb。其控件及属性、功能如表 3 所示。

表3 预警模块控件属性及功能表

控件	属性	功能
command1	Caption=“刷新”	单击此命令按钮刷新 listview1 中记录
Command2	Caption=“终止进程”	单击此命令按钮终止某进程
Command3	Caption=“隐藏”	单击此命令按钮隐藏窗口
Listview1	View = lvwReport,FullRowSelect = True,LabelEdit = lvwManual	显示内存中的进程信息
adodc1	ConnectionString、UserName 、Password、CommandType、RecordSource 的值在自定义函数 connect()中用代码设定	连接局域网中某计算机的进程数据库中指定的表，可编写自定义函数 connect()实现连接
Timer1	Interval=65 535	定时刷新 listview1中记录
Winsock1	默认	获取计算机的 IP 地址

2.2.1 刷新过程 command1_click( )设计

(1)清空 ListView1,用 CreateObject( )函数创建文件系统对象;

(2)用 CreateToolhelpSnapshot( )函数获得进程“快照”的句柄;

(3)用 ProcessFirst( ) 函数获取第一个进程的结构信息数据;

(4)从进程的结构信息中获取进程名、进程 ID。通过枚举进程模块函数 Module32First、Module32Next 函数获取进程执行路径。用 GetFileVersionInfoSize( )函数获取进程的出版公司、版本号。通过文件系统对象的 GetFile 方法返回与指定路径中某文件相应的文件对象,根据文件对象的 Size 属性获取进程大小,根据文件对象的 DateCreated 属性获取进程创建日期。用 GetProcessTimes 函数获取进程占用 CPU 时间;

(5)将进程名、进程 ID、出版公司、版本号、路径、进程创建日期、进程大小、进程占用 CPU 时间添加到 ListView1 中;

(6)用 ProcessNext( ) 获取下一个进程的结构信息数据;

(7)重复第(4)~(6)步直到最后一个进程;

(8)关闭进程“快照”句柄。

2.2.2 Timer1_timer( )设计

(1)调用 command1_click( )刷新 listview1 记录;

(2)将 ListView1 中记录逐一与病毒进程表中记录比较,发现是病毒进程给出提示并显示窗口,用户可单击“终止进程”、“刷新”、“隐藏”按钮进行处理;

(3)将 ListView1 中记录逐一与正常进程表中记录比较,若是正常进程则跳过,若是新进程且新进程表无此记录,则加入新进程表中。

2.2.3 form_load( )设计

(1)初始化 ListView1 表头,提升进程的权限;

(2)调整 command1、command2、command3 在窗口中的位置为右下角;

(3)调用 command1_click( )刷新 ListView1 记录。

2.2.4 command2_click( )设计

(1)提示是否要终止所选择的进程;

(2)如果是则提升进程权限、获取进程句柄、终止进程,并给出进程已终止的提示;

(3) 调用 command1_click( )刷新 ListView1 记录。

2.3 下载模块设计

下载模块共有 3 个控件:命令按钮 command1、文本框 text1、ADO DATA 控件 adodc1。其属性及功能如表 4 所示。

表4 下载模块控件属性及功能表

控件	属性	功能
command1	Caption=“开始下载”	单击此命令按钮从局域网下载数据库文件
text1	Multiline=true	显示下载情况
adodc1	同表3	连接局域网数据库中的 FTP 服务表

下载模块的功能详细设计如下:

(1) 利用 FileSystemObject 的 FileExists 方法来判断局域网数据库文件是否存在,如果不存在给出提示,如果存在则连接局域网数据库中的 FTP 服务表;

(2) 如果表中无记录,则提示:“局域网数据库中无记录”,否则执行下一步;

(3) 定位于第一个记录;

(4) 取出 IP 地址、用户名、密码保存于变量中,并根据 IP 地址生成进程数据库文件名;

(5) 用 API 函数 InternetOpen( )打开 FTP 会话;

(6) 用 API 函数 InternetConnect( )连接 FTP 服务器;

(7) 用 API 函数 FtpGetFile( )下载文件;

(8) 在文本框 text1 中显示 FTP 会话、连接 FTP 服务器、下载文件的情况;

(9) 定位于下一条记录,重复(4)~(8)步直到记录末尾;

(10) 断开数据库连接。

2.4 处理模块设计

对所有数据库中新进程表的记录逐一进行人工处理,若是正常进程则加入正常进程表,若是病毒进程则加入病毒进程表。

该模块共有 4 个控件:命令按钮 command1、文本框 text1、ADO DATA 控件 adodc1、label1。其属性及功能如表 5 所示。

表5 处理模块控件属性及功能表

控件	属性	功能
command1	Caption=“开始处理”	单击此命令按钮处理数据库文件
text1	Multiline=true	显示新进程表中记录
adodc1	同表 3	连接局域网数据库中的TP 服务表
label1	Height=490, width= 3 200	显示正在处理的进程数据库文件名

Command1_click( )过程设计如下:

(1)利用 FileSystemObject 的 FileExists 方法来判断局域网数据库文件是否存在,如果不存在给出提示,否则连接局域网数据库中的 FTP 服务表;

(2)如果表中无记录,则提示:“局域网数据库中无记录”,否则将表中所有记录保存在数组 ***A***( )中, 断开与局域网数据库文件的连接;

(3)定位数组 ***A***( )第一个元素;

(4)根据 field(0)的值,判断进程数据库文件是否存在,如果不存在, 给出提示并执行第(13)步,否则连接相应数据库中新进程表;

(5)判断新进程表是否存在记录,如果不存在给出提示并执行第(12)步,否则执行下一步;

(6)取出新进程表中记录,显示在文本框中;

(7)提示:“是否加入正常进程?”;

(8)如果选择是，则将此记录加入正常进程表中；如果选择否，则提示:“是否加入病毒进程?”；

(9)如果选择是，则将此记录加入病毒进程表中；

(10)将此记录删除；

(11)如果新进程中还有记录,定位下一条记录,重复(6)～(10)步,直到取出所有记录；

(12)断开数据库连接；

(13)定位数组下一个元素,重复(4)～(12)步,直到处理完所有数据库。

2.5 上传模块设计

共有3个控件:命令按钮command1、文本框text1、ADO DATA控件adodc1。各控件属性及功能如表6所示。

表6 上传模块控件属性及功能表

控件	属性	功能
command1	Caption=“开始上传”	单击此命令按钮将进程数据库文件上传
text1	Multiline=true	显示上传情况
adodc1	同表3	连接局域网数据库中的FTP服务表

Command1_click( )过程设计如下:

(1) 利用FileSystemObject的FileExists方法来判断局域网数据库文件是否存在,如果不存在给出提示,否则连接局域网数据库中的FTP服务表；

(2)如果表中无记录,则提示:“局域网数据库中无记录”,否则执行下一步；

(3)定位于第一个记录；

(4)取出IP地址、用户名、密码保存于变量中,并根据IP地址生成进程数据库文件名；

(5)用API函数InternetOpen( )打开FTP会话；

(6)用API函数InternetConnect( )连接FTP服务器；

(7)用API函数FtpPutFile( )上传文件；

(8)在文本框text1中显示FTP会话、连接FTP服务器、上传文件的情况；

(9)定位于下一条记录,重复(4)～(8)步直到记录末尾；

(10)断开数据库连接。

3 实现

3.1 创建数据库

按照表1创建进程数据库中3个表:正常进程表、病毒进程表、新进程表的表结构。按照表2创建局域网数据库中ftp服务表结构,并将局域网中每台计算机的IP地址、用户名、密码作为记录添加到表中。

3.2 预警模块实现

新建工程,将表3中7个控件添加到窗口,并设置其属性。要使用Winsock1、ListView1、adodc1控件,需执行菜单命令[工程][部件],选择“Microsoft Winsock Control 6.0”、“Microsoft Windows Command Control 6.0”、“Microsoft ADO Data Control 6.0”,单击“确定”。对预警模块使用的API函数、结构、常量加以声明,编写form_load( )、command1_click( )、command2_click( )、timer1_timer( )过程代码。程序测试完成后将工程生成.exe文件,将MSADODC.OCX、MSCOMCTL.OCX、MSWINSCK.OCX、进程数据库文件复制到.exe文件相同的文件夹。

3.3 为局域网中每台计算机配置FTP服务

可使用IIS提供的FTP服务功能,设置主目录、安全账号、目录安全性等内容。将预警模块安装在FTP服务设置的主目录,修改进程数据库文件名的主名为计算机的IP地址。在任务计划中添加计划任务,使其在系统启动时自动运行预警程序。

3.4 下载模块实现

新建工程,将表4中控件添加到窗口,并设置其属性。编写command1_click( )过程代码,程序测试完成后将工程生成.exe文件。定期运行下载模块,下载局域网中的计算机进程数据库文件。

3.5 处理模块实现

新建工程,将表5中控件添加到窗口,并设置其属性。编写command1_click( )过程代码,程序测试完成后将工程生成.exe文件。运行处理模块,对局域网中的每台计算机进程数据库文件进行处理。管理员应熟悉常见系统进程、服务进程、应用程序进程的名称、路径,了解病毒采用的隐藏措施。通常它们会将系统中正常进程名的o改为0,l改为i,i改为j,然后成为自己的进程名。例如explorer.exe和iexplore.exe本来就容易搞混,再出现个iexplorer.exe就更加混乱了。svchost.exe进程对应的可执行文件位于“C:\WINDOWS\system32”目录下,查看svchost.exe的可执行文件路径,如果在“C:\WINDOWS\system32”目录外,那么就可以判定是病毒了。iexplore.exe进程对应的可执行程序位于C:\ProgramFiles\InternetExplorer目录中,存在于其他目录则为病毒,除非人为将该文件夹进行了转移。rundll32.exe的路径为“C:\Windows\system32”,在别的目录则可以判定是病毒。

3.6 上传模块实现

新建工程,将表6中控件添加到窗口,并设置其属性。编写command1_click( )过程代码,程序测试完成后将工程生成.exe文件。局域网中所有计算机进程数据库文件处理完成后,可运行上传模块将进程数据库文件上传。

杀毒软件的应用有效地遏制了病毒的传染和破坏,但由于使用者的疏忽(如未及时进行系统更新及杀毒软件升级)及病毒的潜伏性、隐蔽性,往往造成病毒已入侵计算机系统中,但用户并不知道的情况,本软件能有效帮

(下转第20页)

（上接第17页）

助用户检测病毒进程并给出预警。本软件设计的关键是将进程保存在数据库中,利用计算机能快速、精确比较字符串的特点,帮助管理员判断是病毒进程还是正常进程,对于新进程的判断还需管理员熟悉常见的系统进程及病毒进程隐藏的方法。本程序在VB6.0+ACCESS 2003,WINDOWS 2003及WINDOWS XP操作系统下运行通过。

参考文献

[1] 张桂勇,陈若瑜.API FOR WINDOWS 2000/XP详解.北京:清华大学出版社,2003.

[2] 刘圣才,李春葆.visual basic 6程序设计导学.北京:清华大学出版社,2002.

[3] 李万人华,尉宏波,李静.Windows API编程范例入门与提高.北京:清华大学出版社,2004.

（收稿日期2009-03-18）