# 【原创】一个俄罗斯木马样本的浅显分析

【作者】：解密小生
【看雪 ID】：YangCoCol
【QQ】：1174968967(解密小生)
【日期】：2010-11-18

前言：

近日，在看雪论坛的一位网友给了我一个木马样本。据该网友描述，这个木马是俄罗斯的一个牛 X 的黑客所编写，目前可以对国外的三十多种杀软免杀，并且国内的几款知名杀软也没有任何危险提示，我通过实际测试除了 360 会提示有可疑程序生成外，其它杀软均无提示。

拿到样本后，决定要一探究竟，我是个菜鸟，深深知道我的行为无非是在以卵击石，关公门前耍大刀。正所谓是出生牛犊不怕虎，更重要的是好奇心和对技术的渴望，于是就有了这篇浅显的木马分析文章，能力有限，还请论坛的大牛们多多指教~~小弟先在这里谢过了！

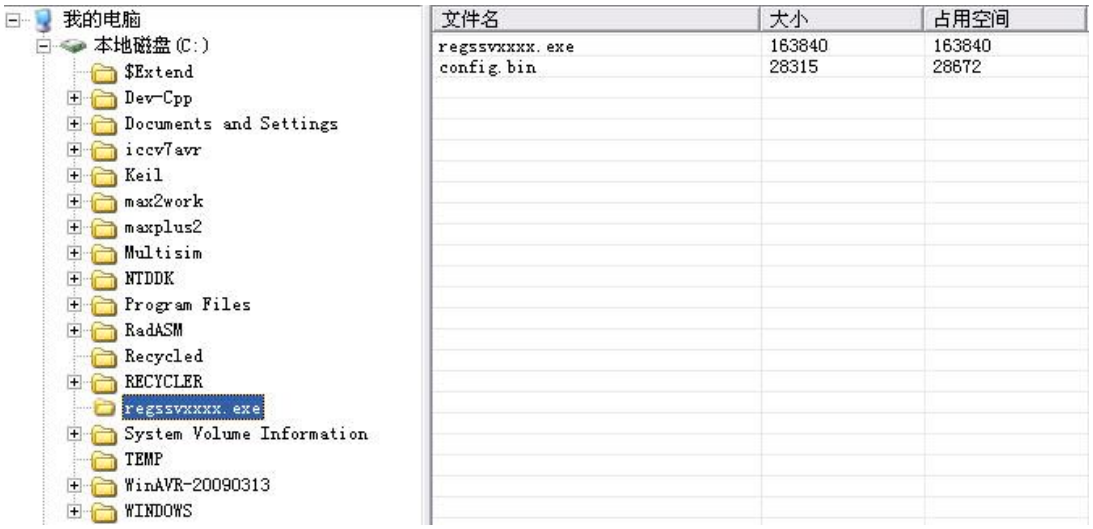
正文：

在正式分析木马样本之前，先要创建一个运行木马的安全环境，在大多数的反病毒公司的反病毒工程师大都是在虚拟机下分析，而我决定就在本机上运行，当然安全措施还是要采取的，之所以做这样的决定，主要是考虑到是个木马，主要任务就是盗取有用敏感信息，保护好自己不被发现，至于其它旁门左道的勾当也许不会做（也许这是在拿自己的爱机来冒险...）。

首先，对系统的安全进行设置，我首先为系统安装了《冰点还原精灵 **6.62**》，并对所有分区进行保护，又写了个内核级驱动，主要是用来监视它是否释放了文件什么的，用驱动目的就是想在更底层监视它的“鬼迹”，装冰点还原软件的目的一方面能保护电脑，另一方面还可以测试这个木马是否能穿还原。

一切准备就绪后运行木马程序，驱动返回的 **log** 信息显示“**C:\regssvxxxx.exe\regssvxxxx.exe**”、“**C:\regssvxxxx.exe\config.bin**”，生成了两个文件。用资源管理器查看，如下图：

在这里根本就没有找到 **regssvxxxx.exe** 文件夹，调整文件夹选项也不能显示，估计是 **hook** 了某些 **API**，接下来用 **Anti-RootKit** 工具查看，显示如下图：




哈哈!!! 终于现身了，把他们拷贝出来，为了方便一会研究，在这里把把文件名改掉后保存，接下来查看注册表项“**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**”。

注册表编辑器中显示如下：


同样用 **XueTr0.37** 查看注册表项如下图：


在 **Anti-RootKit** 工具载入时会有非法线程注入提示，显然是木马程序搞的鬼，通过以上的初步分析，可以分析出木马的大概工作流程：在系统根目录创建 **regssvxxxx.exe** 文件夹**->**复制自身到刚才的目录中，并重新命名未 **regssvxxxx.exe**，同时释放 **config.bin** 到上述目录中**->**添加注册表启动项，向其它进程中注入新的线程来完成 **inline hook API(**隐藏生成的文件夹及文件，隐藏自身注册表启动项，盗取敏感信息**) ->**木马进程退出并删除原木马体。

通过细致分析，该木马不会对应用层的 **svchost.exe**、**lsass.exe**、**services.exe**、**csrss.exe**、**smss.exe** 进程中注入线程，其他进程都会被注入，以下为分析出记事本程序被 **inline hook API** 的情况：

| 挂钩对象 | 挂钩位置 |
| --- | --- |
| **ntdll.dll->LdrLoadDll** | **0x7C9361CA->0x0EAD34B1** |

| | |
|---|---|
| ntdll.dll->NtEnumerateValueKey | 0x7C92D976->0x0EAD91DE |
| ntdll.dll->NtQueryDirectoryFile | 0x7C92DF5E->0x0EAD97DF |
| ntdll.dll->NtResumeThread | 0x7C92E45F->0x0EAD9995 |
| ntdll.dll->NtVdmControl | 0x7C92E975->0x0EAD9897 |
| ntdll.dll->ZwEnumerateValueKey | 0x7C92D976->0x0EAD91DE |
| ntdll.dll->ZwQueryDirectoryFile | 0x7C92DF5E->0x0EAD97DF |
| ntdll.dll->ZwResumeThread | 0x7C92E45F->0x0EAD9995 |
| ntdll.dll->ZwVdmControl | 0x7C92E975->0x0EAD9897 |
| ADVAPI32.dll->CryptEncrypt | 0x77DC1558->0x0EAD6F36 |
| USER32.dll->TranslateMessage | 0x77D18BF6->0x0EAD5879 |
| wininet.dll->HttpAddRequestHeadersA | 0x766940BA->0x0EADF2D0 |
| wininet.dll->HttpOpenRequestA | 0x766936B5->0x0EADEF00 |
| wininet.dll->HttpQueryInfoA | 0x76697812->0x0EAE1E10 |
| wininet.dll->HttpSendRequestA | 0x76696251->0x0EAD7749 |
| wininet.dll->HttpSendRequestW | 0x766E1CDC->0x0EAD7880 |
| wininet.dll->InternetCloseHandle | 0x76694D74->0x0EAE2900 |
| wininet.dll->InternetQueryDataAvailable | 0x766A8A17->0x0EADF540 |
| wininet.dll->InternetReadFile | 0x766980FC->0x0EAE2660 |
| wininet.dll->InternetReadFileExA | 0x766C8148->0x0EAE27B0 |
| wininet.dll->InternetWriteFile | 0x766C7C01->0x0EAD79B7 |
| CRYPT32.dll->PFXImportCertStore | 0x7664F748->0x0EAD23AF |
| ws2_32.dll->send | 0x71A2428A->0x0EADE736 |

附：本人已经将注入的代码复制出，由于篇幅的原因，不再给出，准备将以附件的形式上传到论坛。

为了方便后面的分析，我在这里准备将木马样本反编译，因为木马的躯壳是用 **VB** 写的，用 **VBExplorer** 反编译，得到如下图所示：


每部分伪代码如下所示：

========== Events ==========

```
[UserControl.DragDrop]
:00405398  480C00                ILdPr           ;[SR]=[[STACK_000C]]
:0040539B  575CFF0200            LateMemLdVar    ;vbaVarMove
:004053A0  FC8B                  PopAd           ;check for 32-bit fp exception
:004053A2  360C005CFF4CFF2C      FFreeVar        ;Free 000C/2 variants
:004053B1  13                    ExitProcHresult ;
```

```
[UserControl.DragOver]
:00405530   480C00                ILdPr           ;[SR]=[[STACK_000C]]
:00405533   575CFF0200            LateMemLdVar    ;vbaVarMove
:00405538   FC8B                  PopAd           ;check for 32-bit fp exception
:0040553A   3610005CFF4CFF2C      FFreeVar        ;Free 0010/2 variants
:0040554D   13                    ExitProcHresult ;
:0040554E   41                    Ary1LdPr        ;

[UserControl.Resize]
:004053FC   0478FF                FLdRfVar        ;Push LOCAL_0088
:004053FF   21                    FLdPrThis       ;[SR]=[stack2]
:00405400   0D80000300            VCallHresult    ;Call ptr_00403890
:00405405   046CFF                FLdRfVar        ;Push LOCAL_0094
:00405408   21                    FLdPrThis       ;[SR]=[stack2]
:00405409   0D88000300            VCallHresult    ;Call ptr_00403890
:0040540E   320A0074FF70FF68      FFreeStr        ;Do   SysFreeString   [arg_n];
[arg_n]=0 000A/2 times ~ arg
:0040541B   13                    ExitProcHresult ;

[UserControl.Click]
:00404C98   13                    ExitProcHresult ;
:00404C99   6C7720                ILdRf           ;Push DWORD [STACK_2077]

[UserControl.DblClick]
:00404D34   13                    ExitProcHresult ;
:00404D35   42                    CR4Var          ;vbaR8Var

[UserControl.GotFocus]
:00404B2C   13                    ExitProcHresult ;
:00404B2D   333034                LdFixedStr      ;

[UserControl.KeyDown]
:0040508C   13                    ExitProcHresult ;
:0040508D   37                    PopFPR4         ;

[UserControl.KeyPress]
:00404E4C   13                    ExitProcHresult ;

[UserControl.KeyUp]
:00405044   13                    ExitProcHresult ;
:00405045   203137                CRec2Uni        ;vbaRecAnsiToUni

[UserControl.LostFocus]
:00404D68   13                    ExitProcHresult ;
```

```
[UserControl.MouseDown]
:00405338   13                  ExitProcHresult     ;

[UserControl.MouseMove]
:004051B8   13                  ExitProcHresult     ;

[UserControl.MouseUp]
:00405278   13                  ExitProcHresult     ;
:00405279   27272F              LitVar              ;PushVar STACK_2F27

[UserControl.Paint]
:00404BFC   13                  ExitProcHresult     ;
:00404BFD   0000                LargeBos            ;IDE beginning of line with 00
byte codes

[UserControl.Initialize]
:00404BC8   13                  ExitProcHresult     ;
:00404BC9   384230              CopyBytes           ;

[UserControl.Terminate]
:00404CCC   13                  ExitProcHresult     ;
:00404CCD   0000                LargeBos            ;IDE beginning of line with 00
byte codes

[UserControl.OLEDragOver]
:00405218   13                  ExitProcHresult     ;
:00405219   F0                  CCyI4               ;

[UserControl.OLEDragDrop]
:004052D8   13                  ExitProcHresult     ;

[UserControl.OLEGiveFeedback]
:00405000   13                  ExitProcHresult     ;
:00405001   0000                LargeBos            ;IDE beginning of line with 00
byte codes

[UserControl.OLEStartDrag]
:00404E10   13                  ExitProcHresult     ;
:00404E11   0000                LargeBos            ;IDE beginning of line with 00
byte codes

[UserControl.OLESetData]
:00404DD4   13                  ExitProcHresult     ;
```

```
:00404DD5   0000                LargeBos            ;IDE beginning of line with 00
byte codes

[UserControl.OLECompleteDragWriteProperties]
:00404EC4   13                  ExitProcHresult     ;
:00404EC5   2F272A              FFree1Str           ;SysFreeString [STACK_2A27];
[STACK_2A27]=0

[UserControl.ReadProperties]
:00404D00   13                  ExitProcHresult     ;
:00404D01   0000                LargeBos            ;IDE beginning of line with 00
byte codes

[UserControl.InitProperties]
:00404C30   13                  ExitProcHresult     ;
:00404C31   0000                LargeBos            ;IDE beginning of line with 00
byte codes

[UserControl.AsyncReadComplete]
:00404C64   13                  ExitProcHresult     ;
:00404C65   53                  CBoolCy             ;

[UserControl.EnterFocus]
:004054C8   0478FF              FLdRfVar            ;Push LOCAL_0088
:004054CB   480C00              ILdPr               ;[SR]=[[STACK_000C]]
:004054CE   0D20000100          VCallHresult        ;Call ptr_00403A4C
:004054D3   046CFF              FLdRfVar            ;Push LOCAL_0094
:004054D6   480C00              ILdPr               ;[SR]=[[STACK_000C]]
:004054D9   0D24000100          VCallHresult        ;Call ptr_00403A4C
:004054DE   320A0074FF70FF68    FFreeStr            ;Do  SysFreeString  [arg_n];
[arg_n]=0 000A/2 times ~ arg
:004054EB   13                  ExitProcHresult     ;

[UserControl.ExitFocus]
:00404B94   13                  ExitProcHresult     ;

[UserControl.Show]
:00404B60   13                  ExitProcHresult     ;
:00404B61   45                  Error               ;

[UserControl.AccessKeyPress]
:00405460   800C00              ILdI4               ;Push DWORD [STACK_000C]
:00405463   465CFF              CVarStr             ;
:00405466   5D                  HardType            ;
```

```
:00405467   FC646CFF              LitVar_NULL          ;
:0040546B   FB2F4CFF              EqVar                ;
:0040546F   800C00                ILdI4                ;Push DWORD [STACK_000C]
******Possible String Ref To->""
                                  |
:00405472   1B0000                LitStr               ;Push ptr_004039C8
:00405475   FB30                  EqStr                ;
:00405477   FDF83CFF              CVarBoolI2           ;
:0040547B   FB1F2CFF              OrVar                ;
:0040547F   FF1B                  CBoolVarNull         ;vbaBoolVarNull
:00405481   353CFF                FFree1Var            ;Free LOCAL_00C4
:00405484   1C2A00                BranchF              ;If Pop=0 then ESI=0040548A
:00405487   1E2A00                Branch               ;ESI=0040548A
:0040548A   13                    ExitProcHresult      ;

[UserControl.AsyncReadProgress]
:00404E88   13                    ExitProcHresult      ;
:00404E89   2D2D2D                AryUnlock            ;
```

========== frmTip ==========

```
[Form.Load]
:004060A4   0470FF                FLdRfVar             ;Push LOCAL_0090
:004060A7   0474FF                FLdRfVar             ;Push LOCAL_008C
:004060AA   050A00                ImpAdLdRf            ;Push ptr
:004060AD   240B00                NewIfNullPr          ;[Pop] [SR]
**********Reference To:Global.App
                                  |
:004060B0   0D14000C00            VCallHresult         ;Call ptr_00402E78
:004060B5   0874FF                FLdPr                ;[SR]=[LOCAL_008C]
**********Reference To:[propget]App.EXEName
                                  |
:004060B8   0D58000D00            VCallHresult         ;Call ptr_00403384
:004060BD   2860FF0100            LitVarI2             ;PushVarInteger 0001
:004060C2   25                    PopAdLdVar           ;
******Possible String Ref To->"Mostrar sugerencias al iniciar"
                                  |
:004060C3   1B0F00                LitStr               ;Push ptr_00403EB8
******Possible String Ref To->"Opciones"
                                  |
:004060C6   1B1000                LitStr               ;Push ptr_00403EA0
:004060C9   6C70FF                ILdRf                ;Push DWORD [LOCAL_0090]
**********Reference To->msvbvm60.rtcGetSetting
                                  |
```

```
:004060CC  0B12001C00          ImpAdCallI2       ;Call ptr_004010D6; check
stack 001C; Push EAX
:004060D1  235CFF              FStStrNoPop       ;SysFreeString [LOCAL_00A4];
[LOCAL_00A4]=[stack]
:004060D4  50                  CI4Str            ;vbaI4Str
:004060D5  7178FF              FStR4             ;Pop DWORD [LOCAL_0088]
:004060D8  32040070FF5CFF      FFreeStr          ;Do SysFreeString [arg_n];
[arg_n]=0 0004/2 times ~ arg
:004060DF  1A74FF              FFree1Ad          ;Push [LOCAL_008C]; Call
[[[LOCAL_008C]]+8]; [[LOCAL_008C]]=0
:004060E2  6C78FF              ILdRf             ;Push DWORD [LOCAL_0088]
:004060E5  F500000000          LitI4             ;Push 00000000
:004060EA  C7                  EqI4              ;Push (Pop1 == Pop2)
:004060EB  1C6000              BranchF           ;If Pop=0 then ESI=00406104
:004060EE  6C0800              ILdRf             ;Push DWORD [STACK_0008]
:004060F1  FD9C74FF            FStAdNoPop        ;
:004060F5  050A00              ImpAdLdRf         ;Push ptr
:004060F8  240B00              NewIfNullPr       ;[Pop] [SR]
**********Reference To:Global.UnLoad
                               |
:004060FB  0D10000C00          VCallHresult      ;Call ptr_00402E78
:00406100  1A74FF              FFree1Ad          ;Push [LOCAL_008C]; Call
[[[LOCAL_008C]]+8]; [[LOCAL_008C]]=0
:00406103  13                  ExitProcHresult   ;
:00406104  F501000000          LitI4             ;Push 00000001
:00406109  E4                  CI2I4             ;Verify [stack] high word is
0000, ECX=[ECX]
:0040610A  080800              FLdPr             ;[SR]=[STACK_0008]
:0040610D  0FFC02              VCallAd           ;Return the control index 01
:00406110  1974FF              FStAdFunc         ;
:00406113  0874FF              FLdPr             ;[SR]=[LOCAL_008C]
**********Reference To:[propput]CheckBox.Value
                               |
:00406116  0DE4000E00          VCallHresult      ;Call ptr_00403EF8
:0040611B  1A74FF              FFree1Ad          ;Push [LOCAL_008C]; Call
[[[LOCAL_008C]]+8]; [[LOCAL_008C]]=0
:0040611E  274CFF              LitVar            ;PushVar LOCAL_00B4
**********Reference To->msvbvm60.rtcRandomize
                               |
:00406121  0A13000400          ImpAdCallFPR4     ;Call ptr_004010DC; check
stack 0004; Push EAX
:00406126  354CFF              FFree1Var         ;Free LOCAL_00B4
:00406129  0446FF              FLdRfVar          ;Push LOCAL_00BA
:0040612C  0470FF              FLdRfVar          ;Push LOCAL_0090
```

```
:0040612F   0474FF                  FLdRfVar            ;Push LOCAL_008C
:00406132   050A00                  ImpAdLdRf           ;Push ptr
:00406135   240B00                  NewIfNullPr         ;[Pop] [SR]
***********Reference To:Global.App
                                    |
:00406138   0D14000C00              VCallHresult        ;Call ptr_00402E78
:0040613D   0874FF                  FLdPr               ;[SR]=[LOCAL_008C]
***********Reference To:[propget]App.Path
                                    |
:00406140   0D50000D00              VCallHresult        ;Call ptr_00403384
:00406145   6C70FF                  ILdRf               ;Push DWORD [LOCAL_0090]
******Possible String Ref To->"\"
                                    |
:00406148   1B1400                  LitStr              ;Push ptr_00403F1C
:0040614B   2A                      ConcatStr           ;vbaStrCat
:0040614C   235CFF                  FStStrNoPop         ;SysFreeString [LOCAL_00A4];
[LOCAL_00A4]=[stack]
******Possible String Ref To->"TIPOFDAY.TXT"
                                    |
:0040614F   1B1500                  LitStr              ;Push ptr_00402D98
:00406152   2A                      ConcatStr           ;vbaStrCat
:00406153   FDC748FF                PopTmpLdAdStr       ;
***********Reference To:sub_00405B70
                                    |
:00406157   10F8060500              ThisVCallHresult    ;Call ptr_00402387
:0040615C   6B46FF                  FLdI2               ;Push WORD [LOCAL_00BA]
:0040615F   F400                    LitI2_Byte          ;Push 00
:00406161   C6                      EqI2                ;
:00406162   32060070FF5CFF48        FFreeStr            ;Do SysFreeString [arg_n];
[arg_n]=0 0006/2 times ~ arg
:0040616B   1A74FF                  FFree1Ad            ;Push [LOCAL_008C]; Call
[[[LOCAL_008C]]+8]; [[LOCAL_008C]]=0
:0040616E   1C2401                  BranchF             ;If Pop=0 then ESI=004061C8
******Possible String Ref To->"de que no se ha encontrado el archivo "
                                    |
:00406171   1B1600                  LitStr              ;Push ptr_00403F24
******Possible String Ref To->"TIPOFDAY.TXT"
                                    |
:00406174   1B1500                  LitStr              ;Push ptr_00402D98
:00406177   2A                      ConcatStr           ;vbaStrCat
:00406178   2370FF                  FStStrNoPop         ;SysFreeString [LOCAL_0090];
[LOCAL_0090]=[stack]
******Possible String Ref To->"\r\n"
                                    |
```

```
:0040617B   1B1700              LitStr          ;Push ptr_00403F78
:0040617E   2A                  ConcatStr       ;vbaStrCat
:0040617F   235CFF              FStStrNoPop     ;SysFreeString [LOCAL_00A4];
[LOCAL_00A4]=[stack]
******Possible String Ref To->"\r\n"
                                |
:00406182   1B1700              LitStr          ;Push ptr_00403F78
:00406185   2A                  ConcatStr       ;vbaStrCat
:00406186   2348FF              FStStrNoPop     ;SysFreeString [LOCAL_00B8];
[LOCAL_00B8]=[stack]
******Possible String Ref To->"Cree un archivo de texto llamado "
                                |
:00406189   1B1800              LitStr          ;Push ptr_00403F84
:0040618C   2A                  ConcatStr       ;vbaStrCat
:0040618D   2340FF              FStStrNoPop     ;SysFreeString [LOCAL_00C0];
[LOCAL_00C0]=[stack]
******Possible String Ref To->"TIPOFDAY.TXT"
                                |
:00406190   1B1500              LitStr          ;Push ptr_00402D98
:00406193   2A                  ConcatStr       ;vbaStrCat
:00406194   233CFF              FStStrNoPop     ;SysFreeString [LOCAL_00C4];
[LOCAL_00C4]=[stack]
******Possible String Ref To->" con el Bloc de notas, con una sugerencia por l?nea. "
                                |
:00406197   1B1900              LitStr          ;Push ptr_00403FCC
:0040619A   2A                  ConcatStr       ;vbaStrCat
:0040619B   2338FF              FStStrNoPop     ;SysFreeString [LOCAL_00C8];
[LOCAL_00C8]=[stack]
******Possible String Ref To->"A continuaci?n, col quelo en el mismo directorio que la
aplicaci?n."
                                |
:0040619E   1B1A00              LitStr          ;Push ptr_0040403C
:004061A1   2A                  ConcatStr       ;vbaStrCat
:004061A2   2334FF              FStStrNoPop     ;SysFreeString [LOCAL_00CC];
[LOCAL_00CC]=[stack]
:004061A5   21                  FLdPrThis       ;[SR]=[stack2]
:004061A6   0F0C03              VCallAd         ;Return the control index 05
:004061A9   1974FF              FStAdFunc       ;
:004061AC   0874FF              FLdPr           ;[SR]=[LOCAL_008C]
**********Reference To:[propput]Label.Caption
                                |
:004061AF   0D54001B00          VCallHresult    ;Call ptr_00403F08
:004061B4   320E0070FF5CFF48    FFreeStr        ;Do SysFreeString [arg_n];
[arg_n]=0 000E/2 times ~ arg
```

```
:004061C5  1A74FF              FFree1Ad          ;Push [LOCAL_008C]; Call
[[[LOCAL_008C]]+8]; [[LOCAL_008C]]=0
:004061C8  13                  ExitProcHresult   ;
:004061C9  0000                LargeBos          ;IDE beginning of line with 00
byte codes

[sub_00405B70]
:00405AC0  2750FF              LitVar            ;PushVar LOCAL_00B0
**********Reference To->msvbvm60.rtcFreeFile
                               |
:00405AC3  0B06000400          ImpAdCallI2       ;Call ptr_004010BE; check
stack 0004; Push EAX
:00405AC8  7072FF              FStI2             ;Pop WORD [LOCAL_008E]
:00405ACB  3550FF              FFree1Var         ;Free LOCAL_00B0
:00405ACE  800C00              ILdI4             ;Push DWORD [STACK_000C]
******Possible String Ref To->""
                               |
:00405AD1  1B0700              LitStr            ;Push ptr_004039C8
:00405AD4  FB30                EqStr             ;
:00405AD6  1C2400              BranchF           ;If Pop=0 then ESI=00405AE4
:00405AD9  F400                LitI2_Byte        ;Push 00
:00405ADB  707AFF              FStI2             ;Pop WORD [LOCAL_0086]
:00405ADE  FF2F10000200        ExitProcCbHresult ;
:00405AE4  F500000000          LitI4             ;Push 00000000
:00405AE9  6C0C00              ILdRf             ;Push DWORD [STACK_000C]
:00405AEC  4D60FF0840          CVarRef           ;
**********Reference To->msvbvm60.rtcDir
                               |
:00405AF1  0B08000800          ImpAdCallI2       ;Call ptr_004010C4; check
stack 0008; Push EAX
:00405AF6  234CFF              FStStrNoPop       ;SysFreeString [LOCAL_00B4];
[LOCAL_00B4]=[stack]
******Possible String Ref To->""
                               |
:00405AF9  1B0700              LitStr            ;Push ptr_004039C8
:00405AFC  FB30                EqStr             ;
:00405AFE  2F4CFF              FFree1Str         ;SysFreeString [LOCAL_00B4];
[LOCAL_00B4]=0
:00405B01  1C4F00              BranchF           ;If Pop=0 then ESI=00405B0F
:00405B04  F400                LitI2_Byte        ;Push 00
:00405B06  707AFF              FStI2             ;Pop WORD [LOCAL_0086]
:00405B09  FF2F10000200        ExitProcCbHresult ;
:00405B0F  800C00              ILdI4             ;Push DWORD [STACK_000C]
:00405B12  6B72FF              FLdI2             ;Push WORD [LOCAL_008E]
```

```
:00405B15   F4FF                    LitI2_Byte          ;Push FF
:00405B17   FE5D0100                OpenFile            ;vbaFileOpen
:00405B1B   6B72FF                  FLdI2               ;Push WORD [LOCAL_008E]
**********Reference To->msvbvm60.rtcEndOfFile
                                    |
:00405B1E   0B09000400              ImpAdCallI2         ;Call    ptr_004010CA;    check
stack 0004; Push EAX
:00405B23   C3                      NotI4               ;
:00405B24   1C9A00                  BranchF             ;If Pop=0 then ESI=00405B5A
:00405B27   6B72FF                  FLdI2               ;Push WORD [LOCAL_008E]
:00405B2A   0474FF                  FLdRfVar            ;Push LOCAL_008C
:00405B2D   FCC0                    LineInputStr        ;vbaLineInputStr
:00405B2F   27FCFE                  LitVar              ;PushVar LOCAL_0104
:00405B32   271CFF                  LitVar              ;PushVar LOCAL_00E4
:00405B35   2750FF                  LitVar              ;PushVar LOCAL_00B0
:00405B38   0474FF                  FLdRfVar            ;Push LOCAL_008C
:00405B3B   4D60FF0840              CVarRef             ;
:00405B40   080800                  FLdPr               ;[SR]=[STACK_0008]
:00405B43   063400                  MemLdRfVar          ;Push [SR]+STACK_0034
:00405B46   240100                  NewIfNullPr         ;[Pop] [SR]
:00405B49   0D20000200              VCallHresult        ;Call ptr_00403E7C
:00405B4E   36060050FF1CFFFC        FFreeVar            ;Free 0006/2 variants
:00405B57   1E5B00                  Branch              ;ESI=00405B1B
:00405B5A   6B72FF                  FLdI2               ;Push WORD [LOCAL_008E]
:00405B5D   FD3D                    Close               ;
**********Reference To:sub_004055E0
                                    |
:00405B5F   1000070500              ThisVCallHresult    ;Call ptr_00402373
:00405B64   F4FF                    LitI2_Byte          ;Push FF
:00405B66   707AFF                  FStI2               ;Pop WORD [LOCAL_0086]
:00405B69   FF2F10000200            ExitProcCbHresult   ;

[sub_004055E0]
:004055A0   2758FF                  LitVar              ;PushVar LOCAL_00A8
**********Reference To->msvbvm60.rtcRandomNext
                                    |
:004055A3   0A00000400              ImpAdCallFPR4       ;Call    ptr_004010B8;    check
stack 0004; Push EAX
:004055A8   7354FF                  FStFPR4             ;Fstp#4 [LOCAL_00AC]
:004055AB   0478FF                  FLdRfVar            ;Push LOCAL_0088
:004055AE   080800                  FLdPr               ;[SR]=[STACK_0008]
:004055B1   063400                  MemLdRfVar          ;Push [SR]+STACK_0034
:004055B4   240100                  NewIfNullPr         ;[Pop] [SR]
:004055B7   0D24000200              VCallHresult        ;Call ptr_00403E7C
```

```
:004055BC   6C78FF              ILdRf           ;Push DWORD [LOCAL_0088]
:004055BF   EC                  CR8I4           ;
:004055C0   6E54FF              FLdFPR4         ;fld#4 [LOCAL_00AC]
:004055C3   B3                  MulR8           ;
:004055C4   F401                LitI2_Byte      ;Push 01
:004055C6   EB                  CR8I2           ;
:004055C7   AB                  AddR8           ;
:004055C8   FBE7                FnIntR8         ;
:004055CA   E8                  CI4R8           ;
:004055CB   080800              FLdPr           ;[SR]=[STACK_0008]
:004055CE   8F3800              MemStI4         ;Pop WORD [[SR]+0038]
:004055D1   3558FF              FFree1Var       ;Free LOCAL_00A8
:004055D4   050300              ImpAdLdRf       ;Push ptr
:004055D7   240400              NewIfNullPr     ;[Pop] [SR]
:004055DA   0DFC060500          VCallHresult    ;Call ptr_00403D88
:004055DF   13                  ExitProcHresult ;

[cmdOK.Click]
:004050D4   6C0800              ILdRf           ;Push DWORD [STACK_0008]
:004050D7   FD9C78FF            FStAdNoPop      ;
:004050DB   050A00              ImpAdLdRf       ;Push ptr
:004050DE   240B00              NewIfNullPr     ;[Pop] [SR]
**********Reference To:Global.UnLoad
                                |
:004050E1   0D10000C00          VCallHresult    ;Call ptr_00402E78
:004050E6   1A78FF              FFree1Ad        ;Push [LOCAL_0088]; Call
[[[LOCAL_0088]]+8]; [[LOCAL_0088]]=0
:004050E9   13                  ExitProcHresult ;
:004050EA   0000                LargeBos        ;IDE beginning of line with 00
byte codes

[cmdNextTip.Click]
**********Reference To:sub_004055E0
                                |
:00404D9C   1000070500          ThisVCallHresult ;Call ptr_00402373
:00404DA1   13                  ExitProcHresult ;
:00404DA2   0000                LargeBos        ;IDE beginning of line with 00
byte codes

[sub_004055E0]
:004055A0   2758FF              LitVar          ;PushVar LOCAL_00A8
**********Reference To->msvbvm60.rtcRandomNext
                                 |
:004055A3   0A00000400          ImpAdCallFPR4   ;Call ptr_004010B8; check
```

```
stack 0004; Push EAX
:004055A8   7354FF              FStFPR4             ;Fstp#4 [LOCAL_00AC]
:004055AB   0478FF              FLdRfVar            ;Push LOCAL_0088
:004055AE   080800              FLdPr               ;[SR]=[STACK_0008]
:004055B1   063400              MemLdRfVar          ;Push [SR]+STACK_0034
:004055B4   240100              NewIfNullPr         ;[Pop] [SR]
:004055B7   0D24000200          VCallHresult        ;Call ptr_00403E7C
:004055BC   6C78FF              ILdRf               ;Push DWORD [LOCAL_0088]
:004055BF   EC                  CR8I4               ;
:004055C0   6E54FF              FLdFPR4             ;fld#4 [LOCAL_00AC]
:004055C3   B3                  MulR8               ;
:004055C4   F401                LitI2_Byte          ;Push 01
:004055C6   EB                  CR8I2               ;
:004055C7   AB                  AddR8               ;
:004055C8   FBE7                FnIntR8             ;
:004055CA   E8                  CI4R8               ;
:004055CB   080800              FLdPr               ;[SR]=[STACK_0008]
:004055CE   8F3800              MemStI4             ;Pop WORD [[SR]+0038]
:004055D1   3558FF              FFree1Var           ;Free LOCAL_00A8
:004055D4   050300              ImpAdLdRf           ;Push ptr
:004055D7   240400              NewIfNullPr         ;[Pop] [SR]
:004055DA   0DFC060500          VCallHresult        ;Call ptr_00403D88
:004055DF   13                  ExitProcHresult     ;

[chkLoadTipsAtStartup.Click]
:0040568C   0474FF              FLdRfVar            ;Push LOCAL_008C
:0040568F   0478FF              FLdRfVar            ;Push LOCAL_0088
:00405692   050A00              ImpAdLdRf           ;Push ptr
:00405695   240B00              NewIfNullPr         ;[Pop] [SR]
**********Reference To:Global.App
                                |
:00405698   0D14000C00          VCallHresult        ;Call ptr_00402E78
:0040569D   0878FF              FLdPr               ;[SR]=[LOCAL_0088]
**********Reference To:[propget]App.EXEName
                                |
:004056A0   0D58000D00          VCallHresult        ;Call ptr_00403384
:004056A5   046EFF              FLdRfVar            ;Push LOCAL_0092
:004056A8   21                  FLdPrThis           ;[SR]=[stack2]
:004056A9   0FFC02              VCallAd             ;Return the control index 01
:004056AC   1970FF              FStAdFunc           ;
:004056AF   0870FF              FLdPr               ;[SR]=[LOCAL_0090]
**********Reference To:[propget]CheckBox.Value
                                |
:004056B2   0DE0000E00          VCallHresult        ;Call ptr_00403EF8
```

```
:004056B7   6B6EFF              FLdI2           ;Push WORD [LOCAL_0092]
:004056BA   FBFD                CStrUI1         ;vbaStrI2
:004056BC   2368FF              FStStrNoPop     ;SysFreeString [LOCAL_0098];
[LOCAL_0098]=[stack]
******Possible String Ref To->"Mostrar sugerencias al iniciar"
                                |
:004056BF   1B0F00              LitStr          ;Push ptr_00403EB8
******Possible String Ref To->"Opciones"
                                |
:004056C2   1B1000              LitStr          ;Push ptr_00403EA0
:004056C5   6C74FF              ILdRf           ;Push DWORD [LOCAL_008C]
**********Reference To->msvbvm60.rtcSaveSetting
                                |
:004056C8   0A11001000          ImpAdCallFPR4   ;Call ptr_004010D0; check
stack 0010; Push EAX
:004056CD   32040074FF68FF      FFreeStr        ;Do SysFreeString [arg_n];
[arg_n]=0 0004/2 times ~ arg
:004056D4   29040078FF70FF      FFreeAd         ;
:004056DB   13                  ExitProcHresult ;


[Frame1.Click]
:0040516C   6C0800              ILdRf           ;Push DWORD [STACK_0008]
:0040516F   FD9C78FF            FStAdNoPop      ;
:00405173   050000              ImpAdLdRf       ;Push ptr
:00405176   240100              NewIfNullPr     ;[Pop] [SR]
**********Reference To:Global.UnLoad
                                |
:00405179   0D10000200          VCallHresult    ;Call ptr_00402E78
:0040517E   1A78FF              FFree1Ad        ;Push [LOCAL_0088]; Call
[[[LOCAL_0088]]+8]; [[LOCAL_0088]]=0
:00405181   13                  ExitProcHresult ;
:00405182   0000                LargeBos        ;IDE beginning of line with 00
byte codes
```

========== frmSplash ==========

```
[Form.Load]
******Possible String Ref To->"Versión "
                                |
:00405DF8   1B0300              LitStr          ;Push ptr_004041BC
:00405DFB   0476FF              FLdRfVar        ;Push LOCAL_008A
:00405DFE   0478FF              FLdRfVar        ;Push LOCAL_0088
:00405E01   050000              ImpAdLdRf       ;Push ptr
```

```
:00405E04   240100                NewIfNullPr         ;[Pop] [SR]
**********Reference To:Global.App
                                  |
:00405E07   0D14000200            VCallHresult        ;Call ptr_00402E78
:00405E0C   0878FF                FLdPr               ;[SR]=[LOCAL_0088]
**********Reference To:[propget]App.Major
                                  |
:00405E0F   0DB8000400            VCallHresult        ;Call ptr_00403384
:00405E14   6B76FF                FLdI2               ;Push WORD [LOCAL_008A]
:00405E17   FBFD                  CStrUI1             ;vbaStrI2
:00405E19   2370FF                FStStrNoPop         ;SysFreeString [LOCAL_0090];
[LOCAL_0090]=[stack]
:00405E1C   2A                    ConcatStr           ;vbaStrCat
:00405E1D   236CFF                FStStrNoPop         ;SysFreeString [LOCAL_0094];
[LOCAL_0094]=[stack]
******Possible String Ref To->"."
                                  |
:00405E20   1B0500                LitStr              ;Push ptr_004041D4
:00405E23   2A                    ConcatStr           ;vbaStrCat
:00405E24   2360FF                FStStrNoPop         ;SysFreeString [LOCAL_00A0];
[LOCAL_00A0]=[stack]
:00405E27   0466FF                FLdRfVar            ;Push LOCAL_009A
:00405E2A   0468FF                FLdRfVar            ;Push LOCAL_0098
:00405E2D   050000                ImpAdLdRf           ;Push ptr
:00405E30   240100                NewIfNullPr         ;[Pop] [SR]
**********Reference To:Global.App
                                  |
:00405E33   0D14000200            VCallHresult        ;Call ptr_00402E78
:00405E38   0868FF                FLdPr               ;[SR]=[LOCAL_0098]
**********Reference To:[propget]App.Minor
                                  |
:00405E3B   0DC0000400            VCallHresult        ;Call ptr_00403384
:00405E40   6B66FF                FLdI2               ;Push WORD [LOCAL_009A]
:00405E43   FBFD                  CStrUI1             ;vbaStrI2
:00405E45   235CFF                FStStrNoPop         ;SysFreeString [LOCAL_00A4];
[LOCAL_00A4]=[stack]
:00405E48   2A                    ConcatStr           ;vbaStrCat
:00405E49   2358FF                FStStrNoPop         ;SysFreeString [LOCAL_00A8];
[LOCAL_00A8]=[stack]
******Possible String Ref To->"."
                                  |
:00405E4C   1B0500                LitStr              ;Push ptr_004041D4
:00405E4F   2A                    ConcatStr           ;vbaStrCat
:00405E50   234CFF                FStStrNoPop         ;SysFreeString [LOCAL_00B4];
```

```
[LOCAL_00B4]=[stack]
:00405E53   0452FF              FLdRfVar            ;Push LOCAL_00AE
:00405E56   0454FF              FLdRfVar            ;Push LOCAL_00AC
:00405E59   050000              ImpAdLdRf           ;Push ptr
:00405E5C   240100              NewIfNullPr         ;[Pop] [SR]
**********Reference To:Global.App
                                |
:00405E5F   0D14000200          VCallHresult        ;Call ptr_00402E78
:00405E64   0854FF              FLdPr               ;[SR]=[LOCAL_00AC]
**********Reference To:[propget]App.Revision
                                |
:00405E67   0DC8000400          VCallHresult        ;Call ptr_00403384
:00405E6C   6B52FF              FLdI2               ;Push WORD [LOCAL_00AE]
:00405E6F   FBFD                CStrUI1             ;vbaStrI2
:00405E71   2348FF              FStStrNoPop         ;SysFreeString [LOCAL_00B8];
[LOCAL_00B8]=[stack]
:00405E74   2A                  ConcatStr           ;vbaStrCat
:00405E75   2344FF              FStStrNoPop         ;SysFreeString [LOCAL_00BC];
[LOCAL_00BC]=[stack]
:00405E78   21                  FLdPrThis           ;[SR]=[stack2]
:00405E79   0F1003              VCallAd             ;Return the control index 06
:00405E7C   1940FF              FStAdFunc           ;
:00405E7F   0840FF              FLdPr               ;[SR]=[LOCAL_00C0]
**********Reference To:[propput]Label.Caption
                                |
:00405E82   0D54000600          VCallHresult        ;Call ptr_00403F08
:00405E87   32100070FF6CFF60    FFreeStr            ;Do  SysFreeString  [arg_n];
[arg_n]=0 0010/2 times ~ arg
:00405E9A   29080078FF68FF54    FFreeAd             ;
:00405EA5   0470FF              FLdRfVar            ;Push LOCAL_0090
:00405EA8   0478FF              FLdRfVar            ;Push LOCAL_0088
:00405EAB   050000              ImpAdLdRf           ;Push ptr
:00405EAE   240100              NewIfNullPr         ;[Pop] [SR]
**********Reference To:Global.App
                                |
:00405EB1   0D14000200          VCallHresult        ;Call ptr_00402E78
:00405EB6   0878FF              FLdPr               ;[SR]=[LOCAL_0088]
**********Reference To:[propget]App.Title
                                |
:00405EB9   0D60000400          VCallHresult        ;Call ptr_00403384
:00405EBE   6C70FF              ILdRf               ;Push DWORD [LOCAL_0090]
:00405EC1   21                  FLdPrThis           ;[SR]=[stack2]
:00405EC2   0F1803              VCallAd             ;Return the control index 08
:00405EC5   1968FF              FStAdFunc           ;
```

```
:00405EC8   0868FF                  FLdPr               ;[SR]=[LOCAL_0098]
**********Reference To:[propput]Label.Caption
                                |
:00405ECB   0D54000600          VCallHresult        ;Call ptr_00403F08
:00405ED0   2F70FF              FFree1Str           ;SysFreeString [LOCAL_0090];
[LOCAL_0090]=0
:00405ED3   29040078FF68FF      FFreeAd             ;
:00405EDA   13                  ExitProcHresult     ;

[Form.KeyPress]
:00405120   6C0800              ILdRf               ;Push DWORD [STACK_0008]
:00405123   FD9C78FF            FStAdNoPop          ;
:00405127   050000              ImpAdLdRf           ;Push ptr
:0040512A   240100              NewIfNullPr         ;[Pop] [SR]
**********Reference To:Global.UnLoad
                                |
:0040512D   0D10000200          VCallHresult        ;Call ptr_00402E78
:00405132   1A78FF              FFree1Ad            ;Push   [LOCAL_0088];   Call
[[[LOCAL_0088]]+8]; [[LOCAL_0088]]=0
:00405135   13                  ExitProcHresult     ;
:00405136   0000                LargeBos            ;IDE beginning of line with 00
byte codes
```

通过观察以上反编译的结果可以基本确定，木马的核心部分并不在其中，在结果中也没有发现明显相关的“违规操作”，所有的这些都指向的那个 **config.bin** 文件，分析到这，我不准备继续下去，所以我只能说“大牛只能模拜，无法学习！”。

不过在这里可以做个简单而大胆的猜测，**O(∩_∩)O~**

猜测：那个大牛黑客先准备好了一份用汇编写好的木马核心功能代码，通过加密后存放在一份二进制文件中，作为资源存放在用 **VB** 写好的躯壳里，而躯壳在这里充当个“**VM**”的作用，这纯属本人的想象，还请高人指点~~~~

综合以上的分析，我想也许可以写个免疫软件，或者写个专杀啥的！~~~